Attack Graphs Analysis for Network Anti-Forensics

RAHUL CHANDRAN

A thesis submitted to Auckland University of Technology
in partial fulfillment of the requirements for the degree of
Master of Forensic Information Technology (MFIT)

2013
School of Computing and Mathematical Sciences

Declaration

I hereby declare that this submission is my own work and that, to the best of my knowledge and belief, it contains no material previously published or written by another person (except where explicitly defined in the acknowledgements), nor material which to a substantial extent has been submitted for the award of any other degree or diploma of a university or other institution of higher learning.

Signature: ____________________ Date: 10 June 2013

Acknowledgements

This research was completed as part of Master of Forensic Information Technology course at the School of Computing and Mathematical Sciences in Faculty of Design and Creative Technologies of the AUT University in New Zealand. I would like to thank my parents for their incredible love and support throughout my entire academic life. The entire school of the AUT University has been extraordinary helpful in bringing this work to completion. I would like to thank in particular all teachers, supervisors and administration.

Dr WeiQi Yan had been everything one could hope for in a supervisor. I would also like to thanks to my secondary supervisor Dr. Jairo Gutierrez and our school administrator Ms. Ann Wu for their support and guidance throughout the Master of Forensic Information Technology program. I would like to take this opportunity to thank Dr. Su Zhang of Kansas University for helping me with figuring out the software issues and Ms. Changwei Liu of George Mason University for the valuable suggestions and contributions. Finally I would like to say thanks to my MFIT peers for their great help in the past two years.

Rahul Chandran

Auckland, New Zealand

June 2013

Abstract

The development of technology in computer networks has increased the percentage of cyber-attacks and attackers are able to penetrate even the strongest IDS and firewalls. Anti-forensics in computer networks is an emerging concept in the area of computer forensics and anti-forensics. The traditional anti-forensics which deals with data hiding, disk wiping and data obfuscation has been prevailing for the past few years. The application of these techniques in computer networks which hinders network forensics process (investigation of network crimes) is the main focus of this research. Given that the tools and techniques used by network forensic investigators for examination and by hackers for breaching the security are found the same. The research will focus on an in-depth analysis of the effects of anti-forensic techniques for the betterment of network security.

With the help of anti-forensic techniques, attackers are able to defend themselves from being traced and are able to destroy evidence. The main modus of operation of network forensics is to detect and prevent such kind of attacks. Another goal of this research is the successful implementation and analysis of attack graphs, which are built from gathered evidence. This research study conveys the main concepts of attack graphs, the requirements for the modelling of graphs, how they can be implemented and it also contributes with the incorporation of anti-forensic techniques in attack graphs which will help in the analysis of the diverse possibilities of attack path deviations, thus aiding in the recommendation of various defense strategies to achieve better security. To the best of our knowledge, this is the first time network anti-forensics techniques has been fully discussed and attack graphs have been employed to analyze anti-forensic incorporated network attacks.

The attack graph methodology is utilized in this research to identify the attack path and to deduce ways an attack can propagate. The experimental analyses of anti-forensic techniques using attack graphs conducted in the proposed test-bed helped to evaluate the model proposed and suggested preventive measures for the improvement of security of the networks. Finally, this thesis discusses ways to deploy methodologies for successful generation of attack paths for both normal attacks and for anti-forensic incorporated network attacks. The analysis of attack graphs developed will help in identifying the flaws of the network and how an attack propagates. This methodology helps to take precautionary measures in network security.

Keywords: anti-forensics, network forensics, network security, computer forensics, forensic analysis, attack graphs**.**

Table of Contents

List of Figures

List of Tables

Chapter 1 Introduction

1.1 Background and Motivation

Security of the networks has always been a major concern in the current era of technology. As the internet technology advances, cyber-attacks and threats evolve with new multiple phases such as multi stage and multi host strategies which are able to penetrate the most powerful firewall and IDS systems (Albanese, Jajodia, Pugliese, & Subrahmanian, 2011). Most of the companies spend large amount of their profit share to maintain a robust security system for the computer networks in their company. The possibility of intrusion and the data theft are growing as the companies are moving from their LAN network to the public and global internet. The corporate security mainly deals with the key assets of the company in which the data and valuable information and the knowledge of how the information can be used (Ammann, Wijesekera, & Kaushik, 2002). In order to employ and maintain a robust security of the computer networks, the network security professionals spend hours to implement the monitoring tools, intrusion detection and prevention systems.

The security measures should be one step ahead of the current attack strategies of the hackers. But, today's defensive mechanisms are insufficient to tackle the multi-phase kind of attacks. In order to investigate such kind of attacks and provide preventive and precautionary measures, a wide variety of tools and techniques are developed. Network forensics, the sub-category of digital forensics is trying hard to cope-up with the latest technology attacks. Both offline and live network forensics are needed jointly to trace back the attack path and find the source of the attacks. There are many approaches using various network monitoring tools and network security tools which help in detecting attacks and threats. Through forensic investigation of the network traffic and packet capture, one can find the immediate source of the attack (IP address), thus discovering the location of the attacker. But, the key area which is unnoticed during the investigation is the mode and the strategy of the attacks. The analysis of the attacks in a deeper way is best recommended to harden the network configuration.

The leading forms of attacks by the hackers are by IP spoofing, port scanning, packet sniffing, Denial of Service attacks (DoS). According to Open Web Application Security Project (OWASP), top web security risks are Cross Site Scripting, Cross Site Request Forgery, Injection (Almulhem, 2009), Security Misconfiguration and broken authentication and session management (Fairbanks, Lee, Xia, & Owen, 2007). The investigation of attacks in networks is what we call as network forensics. It can be defined as techniques used to collect or capture, analyse and identify, record the network traffic. In network forensics the network logs and packets are retrieved using the network security software and it is analyzed and investigated to trace back the attack methodology and to certain extend the source of the attack and attacker (Vasiliadis, Antonatos, Polychronakis, Markatos, & Ioannidis, 2008).

Network forensics can be divided into two main streams such as static analysis and dynamic analysis. The static analysis is the process of identifying the conduct of the attacks or crime without executing it. The phases include the analysis of the system file, log files, firewall logs, network logs, checking the presence of malware and virus and reverse engineering. The dynamic analysis on the other hand deals with the live network analysis, analysis of network traffic, network packet capture, file system monitoring for changes and registry file analysis (Endicott-Popovsky & Frincke, 2007). One of the main approaches of dynamic analysis is the use of honeypots (Chandankhede & Nimbhorkar, 2012; Krawetz, 2004). Collection of honeypots known as honey-nets which can be isolated from the rest of the network can be used for network traffic analysis and prevent unwanted traffic onto public networks (Levi & Güder, 2009). The success of network forensics is with identification of the source, approach and techniques of the attack. This can be achieved by reverse engineering of the network attacks. One of the algorithms that help in tracing out the path of the attack is the network attack graph. These network attack graphs are used to analyze the path of attacks from known vulnerabilities of the system.

The internet technology and network infrastructure are blessed with evolution of various IDS/IPS systems, powerful network monitoring and security techniques and systems. New approaches, methodologies and algorithms are developed for forensic investigations of network attacks. One of the main approaches is the reverse engineering methodology in which approximate attack path is found out with the help of attack graph algorithms. This approach dates backs from the year 2002 where methodologies for generation of attacks graphs were first suggested. Attack graphs are designed to acquire the approximate strategy or modus of operation of an attack or threat. This may works for false negatives and true negatives as well. Using attack graphs, evidence can be detected and analyzed which leads to evidence graph generation. Evidence graph and attack graphs can be combined together to compute the attack strategies thereby estimating the preventive measures and enhancing the network security.

The increasing scale of cyber-attacks and computer crime has leaded the investigators to utilize the latest technology to discover new ways of investigative methodologies for forensic process. But on the other side, the attackers and lawbreakers tend to invent new ways of attacks and ways to hide their source of attack and identity and hinder the investigation. This modus of operation is called *Anti-Forensics*. Current forensics deals with two types of evidence analysis such as live analysis and dead analysis. Live analysis mainly monitors and gathers evidence from live networks and systems (Barford, Kline, Plonka, & Ron, 2002; Sy, 2009) and offline analysis deals with evidence processing after physical or logical imaging of the entire system.

Computer forensics can be defined as the investigative and analytical techniques to identify, collect, examine and preserve electronic information and data that can be potentially used as evidence in a court. It always appears to have legal issues with the acceptance of evidence and questions are raised on the integrity of evidence (Rasmi & Jantan, 2011). Frame works, policies and methodologies are implemented for better forensic investigation (Jiang & Shuai, 2011). Computer Forensics is classified into two main categories – Traditional Computer system forensics (Barnes & Harary, 1983) which deals with the investigation regarding the hard disks, personal computers, USB (GS Dardick & Roche, 2007) and Network Forensics which deals with computer networks. Classic computer forensics process can be classified into four main phases such as Collection of evidence, Evidence Processing, Analysis and Reporting. All these phases are accompanied by the Preservation of Evidence and Documentation. The main drawback of the forensic process is to discover whether the evidence has been modified prior to the collection by the investigators. There are many ways to obstruct computer forensic investigation such as destruction of evidence, obfuscation of evidence and hiding the evidence. One of the main problems that hinder the digital investigation is that, the investigators fail to evaluate whether the evidence gathered are adequate to prove events of the crime, detect any anti-forensics attacks and to lighten these effects on the compromised evidence (Rekhis & Boudriga, 2010b).

The anti-forensics can be defined as (Harris, 2006) "*the methods used to prevent (or act against) the application of science to those criminal and civil laws that are enforced by police agencies in a criminal justice system*." The main aim of anti-forensics is to destroy the logical evidence gathered by the investigators so that the evidence proves to be insufficient and incapable of confirming the crime occurred. For example, once the attacker had succeeded in compromising a system, the first step carried out is to delete the traces of occurred events. Anti- forensics techniques are carried out to reduce the qualitative and quantitative substantial evidence (Baier & Breitinger, 2011) on the compromised systems (Hilley, 2007; Kessler, 2007; Rekhis & Boudriga, 2010b). As the technology advances, new anti-forensic tools and techniques has been discovered and implemented.

Anti-Forensics deals with deletion of evidence from network logs and deletion of files from compromised system such as sudden death in mobile phones when a forensic procedure is detected and android ant-forensics which deletes log files from android phones (Azadegan, Yu, Liu, Sistani, & Acharya, 2012; Distefano, Me, & Pace, 2010; Pietro Albano, Aniello Castiglione, Giuseppe Cattaneo, & Alfredo De Santis, 2011). Another way is to avoid detection by spoofing, zombie attacks and misinformation, disabling logs and traditional ways such as encryption and steganography. The main anti-forensic tools is Metasploit Anti-Forensic framework (Bosschert, 2007) which is an open source collaborative investigating about the limitation of the computer forensics tools and helping them to improve digital forensic process and evidence validation. MAFIA (Metasploit Anti-Forensic Investigation Arsenal) (Chris B. Simmons, Danielle L. Jones, & Lakisha L. Simmons, 2011; Schlicher, 2008; Shanmugam, Powell, & Owens, 2011) had provided a suite of programs such as SAM Juicer, Slacker, Transmogrify and Time-stomp (Shanmugam et al., 2011) which are revelation of the ways by which forensic examinations can get confused. The detailed explanation will be given later. The new victim of anti-forensics is the network security field which is one of the crucial components of any network infrastructure.

There are few major concerns about forensics. As most of the tools and techniques for forensics and anti-forensics are available open source and are exploited to a great extent, even by the script kiddies. Numerous tutorials are available on internet which provide handful of information about hacking and data theft (Kotenko & Stepashkin, 2006). Another area is the incorporation of anti-forensics such as data hiding, hiding IP, network steganography, data destruction, obfuscation and log cleaning into attacks to hinder the investigation (W. Wang & Daniels, 2008). One of the key drawbacks of network forensics is that they fail to prove the adequacy and integrity of gathered evidence (W. Wang & Daniels, 2008). The main challenge is in the evidence collection phase. As there are a lot of heterogeneous noisy evidences which need to be filtered. The key research is based on identification of relevant events and evidences of occurred attacks from various piles of evidence. Our research goal is to find out whether the existing evidence is enough for finding the source of attacks using evidence collected from the attack graphs. In the area of digital forensics, some forensic methods could find attackers, some could not. The research focus on the adequacy of evidence collected from attack graphs for identification of source, less than the amount of information, attackers cannot be found.

The other major concerns about the forensics are the rapid advancement of the technology towards wireless technology (Ding & Zou, 2011; Jing, Han, & Mishra, 2004; Pollitt, 2008), peer to peer networks (Ding & Zou, 2011; Eggendorfer, 2008) and the increasing influence of the social networks. Another field which threats the forensic investigation is the anti-forensic tools and techniques which make the forensic process even harder and to taunt its reliability and integrity (K. Dahbur & B. Mohammad, 2011).

The sophisticated multi-staged cyber-attacks are one of the main challenges of network forensics. Since analysis of network attacks are mainly carried out manually which error prone and time consuming (O. Sheyner, Haines, Jha, Lippmann, & Wing, 2002). The analysis has to be made automated and incorporated in current defense mechanisms such as IDS and Firewalls. Intrusion Detection and Intrusion Prevention System (IDS/IPS), firewalls and various network security / monitoring systems are implemented at different nodes of the network. Thus helping in intrusion alerts and blocking attacks. Most of the attacks exploit vulnerabilities of network infrastructure and systems.

The recent studies convey that hackers implement robust measures of anti-forensic techniques to conceal their identity and trace out path along with their normal attack strategies. Incorporation of anti-forensic techniques in network attacks, challenges the investigative process as they postulate ambiguity in attack mode and their paths. The key issue deals with differentiation of normal attacks and anti-forensic attacks. One of the methodologies for identification of such kind of attacks is the attack graph reasoning (Albanese et al., 2011). Analysis of attacks using attack graphs aids in implementing precautionary measures, collecting evidence for investigation in forensically sound manner and helps in identifying network flaws accurately.

1.2 Objectives of the Thesis

Network security has always been the primary concern for all the firms and corporations in the world. Precautionary and preventive measures are implemented to defend the threats and attacks. But incorporation of anti-forensic tools and techniques in network attacks can break the walls of security system. This thesis identifies major anti-forensic tools and techniques and the hazards caused by them. Anti-forensic techniques have always been a challenge to the forensic investigators which hinders the forensic process in identifying the evidence.

A new approach of attack graph methodology is utilized to track the changes in the path of attacks. A comparative study of normal attack paths and anti-forensic incorporated attack paths is performed in this research. An approach for identifying the different flaws in a network and how an attack can propagate through different peripherals of the network is the main focus of the research in this thesis. This helps in detection of vulnerabilities of the network and assists in taking precautionary measures for inside or outside threats and attacks.

1.3 Structure of the Thesis

The structure of the thesis is shown in the Figure 1.1 below. The whole thesis is divided into three main parts. The first part introduces the concept of anti-forensics in which emphasis is given on to the network-anti-forensics. The second part introduces the methodology of attack graphs for analysis of network attacks and the third part deploys the practical implementation, analysis, discussion and conclusion of the thesis.

Chapter 2 introduces the topic of anti-forensic techniques, network attacks and survey of network monitoring tools, network forensic tools and anti-forensic tools and techniques. It also defines and explains network forensic process cycle. The chapter covers an in-depth assessment of various anti-forensic tools and techniques. The main approach methodology of attack graphs and its related studies are also mentioned in this section. Finally, the chapter details latest trends and improvements in network security and forensics as well as in network attacks.

Chapter 3 explains the research methodology of the thesis. The main hypothesis are developed and put forth in this section. The in-depth study in the main problems and possible solutions to the suggested problem is explained. An experimental design, dataset and implementation procedure is also described in the final part of the section.

Chapter 4 details the full-fledged experimental results and main outcomes. The section explains the experimental test-bed and analysis of experiments conducted on the simulation environment. The outcomes of the experiments are detailed with the help of facts and figures.

In Chapter 5, complete analysis and discussion is carried out for the outcomes and results obtained. The main research hypothesis is tested and analyzed with the final experimental results. It also discusses the limitations of the research and practical application. The conclusion and future work are comprehended in Chapter 6.Thesis winds up with the appendices that provide information with regards to findings, results from data testing and configurations of the systems and peripherals of the simulation environment.

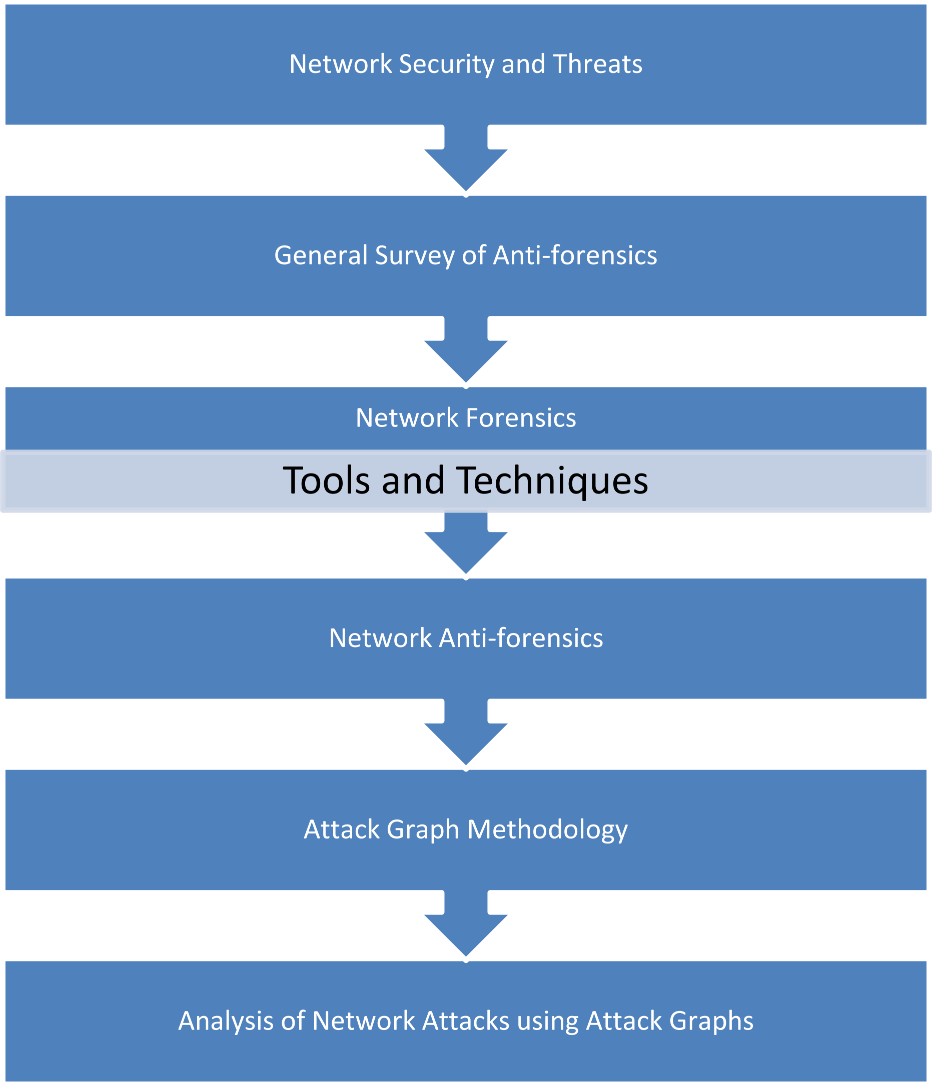

Network Security and Threats
General Survey of Anti-forensics
Network Forensics
Tools and Techniques
Network Anti-forensics
Attack Graph Methodology
Analysis of Network Attacks using Attack Graphs

Figure 1.1 Structure of the thesis

Chapter 2 Literature Review

2.1 Introduction

The main objective of this chapter is to comprehend the related work and research studies with regards to digital forensics standards, network security tools and anti-forensic techniques and tools. By addressing the recent studies and research background, the literature review bestows a foundation for the thesis research. The research problem is identified in the final part of this chapter. The main goal of the thesis is to find possible solutions for the problems identified and practicality of the solution suggested is experimented in the following chapters.

A large number of research and studies have been concentrated on how to "harden" the network security and prevent the network from attacks and threats. A precise prediction of behavior of the attacks is necessary to reduce the risk and implement preventive and precautionary actions (Harbort, Louthan, & Hale, 2011). Passive measure such as firewalls and IDS (Intrusion Detection System) are not sufficient to prevent attacks. Active defensive measures should be implemented to calculate the possible attacks in network structure before being hit by an attack (Bursztein & Mitchell, 2011). Real-time analysis and visualization may provide better perceptive of attack paths and attack strategies especially for multi-staged attacks (Harbort et al., 2011). The key elements of attack analysis are the alert system and system logs, and are implemented using alert correlation and event correlation techniques. Multi-level alert clustering model provides well managed techniques to eliminate false positives from IDS (Shaojun, Lan, Jianhua, Shanshan, & Xiuzhen, 2009). Attackers exploit vulnerabilities of the system and software installed in it. Most of the vulnerabilities are exploited due to issues such as unstable patches and slow patch release time.

As mentioned earlier (Harbort et al., 2011; Hart, 2013), multi-staged attacks exploiting individual vulnerability is difficult to analyze. Researches have been conducted in the field of attack graphs as the stepping stone to analysis of vulnerabilities and attack paths. Attack graphs generate attack path using all vulnerabilities are exploited during an attack. This provides a measure to harden the network security. Fuzzy Cognitive Maps and Genetic algorithms are used for generation of minimal attack sets with the help of attack graphs (Diamah, Mohammadian, & Balachandran, 2012). The worst case scenarios are calculated using this algorithm. Assumption of cost of launching attacks to be equal is one of drawbacks of the system as it varies to a great extend in practical scenarios (L. Wang, Singhal, & Jajodia, 2007b). As network infrastructure becomes large, attack graphs become larger and complex (Ou, Boyer, & McQueen, 2006) . In order to handle and generate larger attack graphs, scalable analysis is required incorporating probabilistic knowledge of behavior of attacker (L. Wang, Singhal, & Jajodia, 2007a; Xie, Wen, Zhang, Hu, & Chen, 2009).

Introduction of security metrics to attack graphs provide extraction of security-relevant information regarding the number of ways an attacker can strike and most frequent and affluent path an attacker covers (Katipally, Yang, & Liu, 2011). Merging of various security metrics (Idika & Bhargava, 2012) with the help of proposed algorithm increases the probability of gathering security relevant information from attack graphs (Fen, Xinchun, & Hao, 2012; Li, Lei, Wang, & Li, 2007). Ranked attack graphs provide a measure of which part of the attack graph is relevant and has to be concentrated by the system administrators to harden the network (Homer, Varikuti, Ou, & McQueen, 2008; L. Wang, Noel, & Jajodia, 2006). The Threat Modeling method for Attack Path Analysis (T-MAP) calculates acuteness of attack paths and security performance of Commercial Off the Shelf (COTS) systems (Khaitan & Raheja, 2011).

The main limitations of attack graphs generated in the previous years are that they are too generalized; the methods have high computational complexity and dependent on empirical formulas. The attack graphs also vary with the false negatives of alert systems installed in the network infrastructure which in turn affect the prediction process of attack (Ou & Singhal, 2011; L. Wang et al., 2007b). Another key limitation for attack graphs is that they don’t provide methods to measure the probability of each attack pattern (Homer et al., 2008; L. Wang et al., 2007b). Studies shows that scalability of alert correlation techniques implemented in IDS and other network monitoring tools are not yet referred. Scalability problem redirects to readability issue so as to calculate precise configuration decisions (Homer et al., 2008).

Most of the real-time approaches for intrusion detection and prevention are carried out in the assumption that vulnerability scan provides precise vulnerabilities and connectivity of network to develop attack graphs (Harbort et al., 2011). However, prediction of intrusion paths for normal attacks is possible to an extent. As technologies advances, network intrusions are carried out with new strategies and techniques. Incorporation of anti-forensic techniques in network intrusions helps the attackers to obfuscate the attack paths. There is no effective model to analyze the network attacks consisting of anti-forensic techniques using attack graphs. The main aim is to analyze and measure the significant changes occurred in the developed attack graphs for normal attacks as well as anti-forensic network attacks. To the best of the knowledge this is the first time network anti-forensics has been fully discussed and the attack graphs are employed to analyze the network attacks.

The literature review will try to achieve a successful background studies to identify the potential issues in the related fields of digital forensics and anti-forensics. The following sections focus on the general survey of anti-forensic techniques in computer networks and the explanation of the same to contribute to the enhancement of the network security. In Section 2.2 a summary of digital forensics, network security and network forensics are presented. It is followed by detailed review of the anti-forensic technique is section 2.3. In Section 2.4, the state of the art is explained. In section 2.5, explains the approaches, methodologies and techniques. Section 2.6 covers various network security and monitoring tools (NMT), network forensic analysis tools (NFAT) and anti-forensic tools and a comparison is provided. In section 2.7, the research problem and the motivation is introduced. The section intends to explore the new possibility of constructive deployment of anti-forensics for the improvement in network security and to find out the research gap in digital forensic field.

2.2 Network Security and Forensics

The internet security is one of the most exponential growing fields and is one of the major concerns for all business corporations and industries as they have to make sure that their assets are completely secured. The possibility of intrusion and the data theft are growing as the companies are moving from their LAN network to the public and global internet. The corporate security mainly deals with key assets of the company in which the data and valuable information and the knowledge of how the information can be used. The approach of risk management is the fundamental step for a company to protect the assets. The risk can be defined as the likelihood of impact of threat in a company. The company should be able to understand and analyze all the threat environments (type of attacks and attackers). Threat assessment is performed to find out the best way to secure a system from compromises and safeguard the security goals Confidentiality, Integrity and Availability. It also helps to implement preventive, detective and corrective counter measures for threats and vulnerabilities (Panko, 2010).

A computer network security in any place is as strong as the weakest vulnerability found inside the network. Vulnerabilities can be defined as weak points in a network that are the most prone to attackers to attain unauthorized access to the system. Vulnerabilities can be of software installation flaws, network configuration flaws and because of human error. The attackers have the ability to exploit the existing vulnerabilities and to create vulnerabilities in less secured systems.

The network attacks can be classified in two types such as passive attacks and active attacks. Passive attacks can be defined as attacks where the original information remains unchanged, but make use of the information obtained. In active attacks, for example man in the middle attacks, the original information is changed and the receiver gets the manipulated message from the attacker instead of the sender.

Once the occurrence of an attack or threat is identified in a particular network system, forensic analysis of the same is launched. The experts make use of the various forensic tools and techniques to analyze the evidence they collected. The section below explains ore about forensic process.

The digital forensics is the application of analysis and investigative techniques to collect and preserve digital evidence from a particular device which helps the court of law to identify and judge a crime. The digital forensic life cycle contains mainly four processes such as Detection, Collection, Analysis and Presentation. In all these phases, the evidence undergoes the process of Preservation and Documentation. Network forensics can be defined as classification of digital forensics which mainly deals investigation of network attacks and threats. There are two types of network forensic analysis; Live or online analysis and Offline analysis. Live analysis is carried out on live networks. The data packets travelling in the networks are analyzed and threats and attacks are identified and analyzed. In Offline analysis, data packets are first captured using different network capturing tools and stored. They are then investigated using network forensic tools. Due to complexity of collection and preservation of evidence in live analysis, most commonly used investigative process is the offline analysis.

The Network Forensic process can be divided into two main phases.

Phase 1: Network data/traffic Capture via Network monitoring

The phase one can be articulated as the collection of evidence from the network for analysis. The evidence acquisition can be carried out either offline or online/live. There are a large number of tools and systems that can be used for monitoring and capturing the packets. *TCP Dump* and *Wire Shark* are two of the most common tools used for monitoring. The table shows various network security and monitoring tools.

The detection of network attacks is the base objective behind network monitoring. It is very challenging task in today’s internet technology. It has been very difficult to make sure that the attack is a true positive one, as lots of attacks are carried out in disguise with the help of anti-forensic tools and techniques. A considerable amount of work has been seen in the network attack detection area. The recent work of autonomous network security for detection of network attacks is an attempt to implement an independent system that identifies intrusions automatically without statistical learning using clustering method for unsupervised anomaly detection. Most of the intrusion detection systems use data-mining algorithms, Neural Network, Support Vector Machine, Genetic Algorithm and Fuzzy Logic for behavioral and anomaly based detection methodologies (Goodall, Lutters, Rheingans, & Komlodi, 2006). These algorithms help in detecting failed attacks and false positives (Oleg Sheyner & Wing, 2004).

In order to secure a network form outside attacks, it is necessary to understand the network traffic flow and the content of the network packets. Content based and Context based monitoring (Kiley, Dankner, & Rogers, 2008) is another effective approach for network monitoring and detection of attacks which incorporates data mining and database auditing techniques (Ingols, Chu, Lippmann, Webster, & Boyer, 2009). The data mining techniques utilized in IDS helps in pattern comparison (Heydari, Martin, Rjaibi, & Lin, 2010) and sequence analysis and identify attacks in an effective manner . The output from various network monitoring tools is the network traffic packets such as .pcap extension files that can be analyzed using network forensic tools.

Phase 2: Network Forensics and Analysis

The evidence consists of network packets, firewall logs, IDS logs, system logs, router logs and audit logs. The gathered information should be documented using techniques such as OpenSVN subversion (Fairbanks et al., 2007; Rekhis & Boudriga, 2012). Once the packets are captured, they can be analyzed using various network forensic tools such as Wire Shark, Encase, Network Miner and Net Detector. The forensic tools also incorporate the Intrusion Detection System (IDS) and Intrusion Prevention Systems (IPS). NIDS (Network Intrusion Detection System) such as SNORT make use of pattern matching algorithms and techniques (Heydari et al., 2010) for network packet analysis and attack detection. TNV (Time Based Network Traffic Visualizer) is another tool used for analysis of network traffic over a time period. Filtering mechanisms and ID analysis helps in identifying anomalous behavior (Kiley et al., 2008). The main evidences scrutinized in network forensics are authentication logs, operating system logs, application logs and network device logs which constitute date and time stamps IP address and error boots. The main network forensic tools are described in the table.

The network forensic processes are hindered nowadays by the counter forensics and anti-forensic techniques. Most of the attacks today incorporate anti-forensic techniques that challenge the forensic investigators in collecting valid evidence. The integrity of the evidence becomes a questionable factor in evidence collection process. Identification of occurrence of anti-forensic techniques in attacks is another major concern for forensic investigators. The section below gives a detailed survey of most common anti-forensic techniques and tools.

2.3 Fundamentals of Anti-Forensic Techniques

The digital evidence can be easily altered, removed, hidden, and prevented from creation of the source without any trace. To cope up with these, the investigators must be familiar with the anti-forensic techniques. The main anti-forensic goals are a) avoiding detection of the attack, b) disruption and prevention of collection of valid evidence, c) To increase the time duration for collection and analysis of evidence, d) to subvert the forensic tools from gathering the right evidence, e) Leaving no trace of the anti-forensic tool or technique deployed (Rekhis & Boudriga, 2012). In order to achieve these goals, there are various tools and techniques are introduced (Caloyannides, 2009; Cao, Zhao, Ni, & Tian, 2010; Forte & Power, 2007; Harris, 2006; Rekhis & Boudriga, 2010b; Sartin, 2006; Shanmugam et al., 2011). The sub-sections below details the techniques used for anti-forensics.

2.3.1 Data Destruction

The basic anti-forensic technique is the data destruction which causes the investigation to a full stop. It can be also being named as secure deletion. It can be either logical or physical destruction of the data. Logical destruction is accomplished through frequent overwriting. Physical destruction can be carried out with the help of magnetic tapes by degaussing the media (Caloyannides, 2009). Data destruction is used to remove the residue of the deleted files, erase the logs, timestamps and registries of the system activities, thus by securing the identity of the crime. CCleaner is software that supports the permanent deletion and removal of all temporary files and unnecessary files from the system. Necrofile (Barford et al., 2002) rewrites the selected partition or portion of the hard disk with mock data destroying the evidence completely. Active Eraser is another data destruction tool which is used for secure erase of data. In networks, Data Packet Destruction using NS2 (Network Simulator) and Random Packet Destruction (RPD) using DDoS Attacks are the main data destruction techniques.

2.3.2 Data Hiding

Data Hiding is one of the most traditional and successful anti-forensic techniques. Inserting the data in different places where it shouldn’t be or in metadata files. The data or the information can be stored in slack spaces, scattered all over the memory and empty spaces in the disk sectors (Berghel, 2007). But it largely relies on the forensic tools used and the lack of the investigator as the ability to find hidden data which is outside the normal visibility is the main factor. Renaming the file is one example of incriminating the data by hiding. Encryption, watermarking, covert cannels (Rekhis & Boudriga, 2010b) and steganography are the main techniques used to obscure the network traffic and data. It should be made sure that while encrypting and using covert channels the data or information should not be lost. This technique can be exploited for both constructive and destructive purpose.

The data is hidden in portions of the medium which is outside the specific format of that medium such as slack space at the end of the partition and fake bad sectors. Data hidden in these areas are hard to discover as it need special tools. But it is very difficult to hide from the normal analysis. Another way is to hide the data inside the specific format of the medium and the data should not be any other format other than the medium. It mainly relies on security through obscurity as it is easy to discover once the method is known. Virus hiding within the exe code section and steganography -hidden texts in documents are other forms of data hiding. It is very hard to detect without specific tools and have complex algorithms especially in steganography. Hiding information in empty headers of network layer and transport layer packets is hard to be traced (Almulhem, 2009).

Slack Space - The areas in the hard disk that have limited access is considered to be the slack space. The unused space of the sector in a RAM that cannot be addressed by an OS is known as RAM slack space (Berghel, 2007). Since the files in a hard disk doesn't end within the last sector of the block which leads to slack space in the consecutive sector. A volume slack space can be defined as the unused space between the end of the file system and the end of the partition where the file resides. Faked bad clusters can also be used for data hiding (Lewthwaite & Smith, 2008). The NTFS file system identifies bad clusters ($BadClus) that have defects in it using the MAT (Master File Table). Once some clusters are marked as bad clusters, they can be used to hide data of unlimited size. The tools such as bmap and Slacker from Metasploit can be used for data hiding in slack spaces.

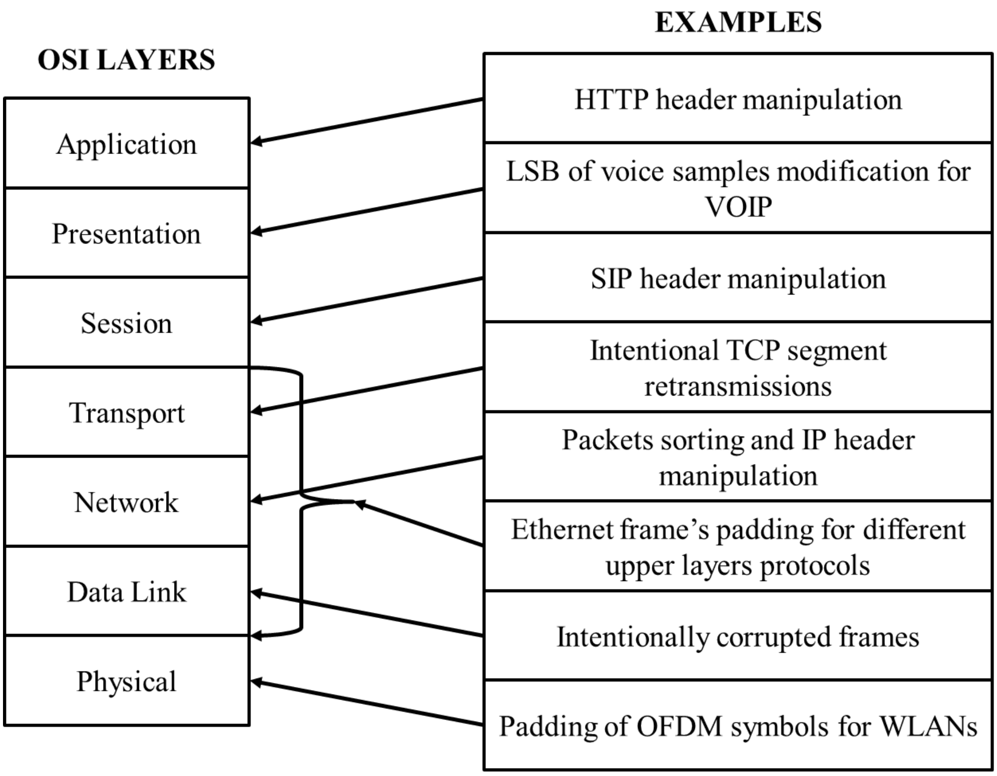
Encryption – The evidence files can be found by search methods. The detected evidence cannot be accessed if it is encrypted (Rekhis & Boudriga, 2010b). Thus encryption becomes another kind of anti-forensic technique. The article (Sang Su, Ku-Young, Deokgyu, & Do won, 2007; Suhyung & Dowon, 2008) proposed anti-forensic tool using encryption methodology. There are lot of encryption algorithms such as XOR, Blowfish, AES and RSA. Strong and good encryption algorithms are easy to be misused and make the forensic analysis hard due to the key management. The encryption can be used in network communications which makes the network analysis harder. For example encrypted packets are difficult to be analyzed by the network forensic tools.

Steganography-It can be defined as hiding information in messages, images and files. The art of steganography dates back from centuries where messages are sent hidden in pictures (Suhyung & Dowon, 2008) . There are several methods and algorithms for hiding data in various files. In steganography, only the sender and the receiver are aware of the information hidden in the files (Rasmi & Jantan, 2011). The detection of steganographic files is a challenge for the investigators.

Steganography in networks communications make use of the covert channels to hide secret data into user's normal data transmission which cannot be seen by the third parties. Steganography not only provides security but also anonymity and privacy. As Internet has provided covert channel communications, network steganography is currently rising and is a threat to network security. Network Steganography utilizes communication protocol control elements which make it harder to detect and destroy. It can use more than protocols in the OSI layer such as HTTP Header manipulation in Application layer, LSB of voice sample modification for VOIP as shown in the figure 2.1.

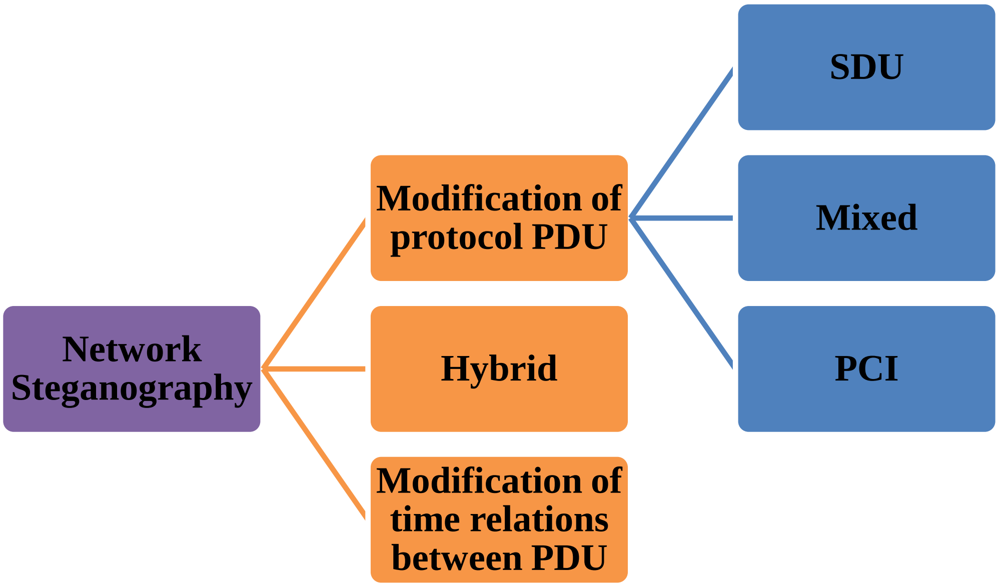
Network steganography can also be classified according to the modification of the Protocol Data Unit such as modification of SDU (Service Data Units), modification of PCI (Protocol Control Information) and time relation between PDUs as shown in figure 2.2.

HICCUPS (Hidden Communication System for corrupted Networks) are another steganography technique for wireless communications especially for voice data.



OSI LAYERS
EXAMPLES
Application
Presentation
Session
Transport
Network
Data Link
Physical
HTTP header manipulation
LSB of voice samples modification for VOIP
SIP header manipulation
Intentional TCP segment retransmissions
Packets sorting and IP header manipulation
Ethernet frame's padding for different upper layers protocols
Intentionally corrupted frames
Padding of OFDM symbols for WLANs

Figure 2.1 Steganography in OSI layers(Lubacz, Mazurczyk, & Szczypiorski, 2012)



Network Steganography
Modification of protocol PDU
Hybrid
Modification of time relations between PDU
SDU
Mixed
PCI

Figure 2.2 Network steganography classifications(Lubacz et al., 2012)

2.3.3 Data/Trail Obfuscation

The main function of this technique is to divert the digital forensic process. It can be successfully achieved by modification of metadata, anonymization techniques such as IP spoofing, MAC Spoofing, VPNs and proxies and covering the trace of evidence. Digital forensic investigators can be misled by the attacker by false email header generation, log alteration and SMTP proxies (Rekhis & Boudriga, 2010a). Timestamp alteration and modification of headers is another form of trail obfuscation. Traffic content obfuscation is successfully implemented using virtual private networks (VPN) and SSH tunneling (Velupillai & Mokhonoana, 2008). The major techniques which implement the data/ trail obfuscation are as follows (Shanmugam et al., 2011).

- Log Cleaners
- Spoofing
- Misinformation
- Zombie accounts
- Trojan commands

2.3.4 Attack against Forensic Tools

The attacker introduces modification on the target machine of the investigator so that they provide the wrong evidence. This includes the root kit attacks, file signature altering, exploiting the vulnerabilities in the hash algorithms to create hash collisions (Rekhis & Boudriga, 2010a; Smith, 2007). The time and cost of analysis and digital investigation is the key feature for an organization. If the attacker is able to control these constraints, then the investigators will be forced to stop the forensic procedures. The use of an intermediate system by the attacker which makes the investigation difficult as it requires corporation of different system administrators, is an example of this anti-forensic attack technique. Development of disk-avoiding tools prevents the forensic tools from detecting the attacker activities by direct access to the memory (Smith, 2007).

2.4 The State of the Art

The network infrastructures in any organization demand 100% security so that their assets are secured from threats. Thus, network security becomes the crucial component in corporate environment. Today's technology provides a wide variety of security features such as Intrusion Detection System and Intrusion Prevention System (IDS/IPS), Firewalls, Anti-Virus Guards, Honeypots (Meghanathan, Allam, & Moore, 2009) and Computer Forensic Tools (Benjamin & Jill, 2007; Smith, 2007). Even if these tools impart a sufficient defensive mechanism, attackers are able to penetrate the networks. It has become difficult to investigate network attacks as the attackers utilize recently developed robust anti-forensic tools and techniques to hide their identity and attack paths (Jian, Chang-peng, & Mo, 2010). IP spoofing, trace obstruction, covert channels(Gorodetski & Kotenko, 2002; Rekhis & Boudriga, 2010b), tunneling, anti-honeypot technology (Krawetz, 2004) and network steganography are some of the techniques used by the attackers for the defense strategy.

In the past few years anti-forensic techniques had been utilized by the attackers for data destruction, data hiding and data obfuscation in traditional computer systems and storage devices. The advanced technology has helped them to extend the application of anti-forensic techniques to computer networks and network infrastructure (Nikkel, 2006). This makes investigative process which includes evidence collection, evidence process and analysis challenging than ever.

In order to prevent the various threats and attacks, various network security and monitoring tools can be implemented on different nodes of a network. Similarly, network forensic tools supports in investigation and analysis of attacks and helps to discover the birthplace of attack, analysis of the evidence and present evidence report. The various network forensic frameworks suggested by Digital Forensic Research Workshop (DFRWS) and other researchers such as framework for distributed forensic, soft computing based frameworks(Hunt & Slay, 2010), honeypot based framework and attack graphs provide ample proof of research in this area (Saad & Traore, 2010; Taylor, Haggerty, Gresty, & Berry, 2011).

The key objective is an inclusive survey of the tools and techniques utilized for anti-forensics, network forensics and network monitoring and security tools. This survey will help to study about the wide range of tools used for forensics in computer networks and anti-forensics. Understanding of techniques and algorithms used by the attackers; assists in better and proper network security framework (Hartley, 2007). For successful implementation of a robust defensive infrastructure, it can be an effective measure.

The survey is the base for practical experimentation of tools and techniques. Most common anti-forensic framework used is Metasploit framework tools such as Time-stomp and Slacker (Shanmugam et al., 2011). Anti-forensic techniques such as data hiding, encryption, destruction, obfuscation and data wiping can be tested in networks. The main platforms used for the implementation of the above techniques are Windows 7 and Linux Back Track 5 R2. Most of the tools can be run on multiple platforms even in the latest Windows 8.The analysis of the techniques is carried out with the aid of forensic tools such as Encase, Access-Data Forensic Tool Kit (FTK) and Internet Evidence Finder. Identification of anti-forensic techniques and its effect in network evidence is the key part of the experimental analysis. Thus by deducing effective ways of counter measures to improve network security.

2.5 Approaches, Methodologies and Techniques

The network attacks have always been a threat to the internet technology. The recent studies convey that most of the anti-forensic tools and techniques were applied with the normal attacks, in order to conceal the identity and source of the attacker. These techniques have been used previously deployed against the traditional forensics (Chan et al., 2011). As the technology advances, new ways of attacks are discovered and with the help of anti-forensics techniques such as data hiding, obfuscation and destruction.

Network attacks have always been a challenge for the security field and digital forensic investigators. The network attack process is divided into 5 stages in Howard taxonomy of computer and network attacks. They are the attackers, tools which are used by attackers, Access using vulnerabilities and unauthorized users, results of the attacks and the objectives (Jantan, Rasmi, Ibrahim, & Rahman, 2012). Another approach mentioned is the Lough’s taxonomy called the VERDICT (Validation Exposure Randomness Deal-location Improper Condition Taxonomy) which is based on the characteristics of the attacks. A dimensional classification with sub-levels of the different attacks gives a good overview of the attacks paths and attack scenarios.

Most of the attacks make use of the vulnerabilities of the network infrastructure, system or the software. Common Vulnerabilities and Exposures (CVE), Vulnerability Database (VDB) from Security Focus, Open Source Vulnerability Database (OSVDB) (W. Wang & Daniels, 2008) and National Vulnerability Database (NVD) (Zheng, Yang, & Yujun, 2011) are vulnerability repositories which provide a good range of vulnerability description can be used for investigative purpose. The Open Source Vulnerability and Assessment Language (OVAL) and CVSS (Common Vulnerability Scoring System) (Szczypiorski, 2009) are two standardized frameworks for rating vulnerabilities in IT industries (W. Wang & Daniels, 2008).

The traditional anti-forensics deals with hiding of data in the disk and slack space, destruction of data and data obfuscation through MACE alteration. Anti-forensic techniques has been extended to network infrastructure such as hiding IP through proxy (Changwei Liu, Anoop Singhal, & Wijesekera, 2012), encrypted packets, deleting the logs, steganography and covert tunneling. Due to integration of anti-forensic techniques in network attacks, the attack path identified from forensic analysis will be different from the original and will be a strenuous effort to acquire the latter. The first step is to differentiate between an anti-forensic attack and a normal attack. Normal attacks can be easily identified as there will not be any ambiguity in the process of analysis of evidence and attack paths. There are many methodologies (Kamal Dahbur & Bassil Mohammad, 2011; Peron & Legary, 1995; Weihan, Peng Chor, & Chai Kiat, 2009) and approaches suggested in various studies to identify an anti-forensic attack.

The figure 2.3 shows a framework for forensic process which includes detection of anti-forensic attacks (K. Dahbur & B. Mohammad, 2011). The main processes involve preparation for collection of evidence from the scene which includes isolation of the crime scene. The next phase is the evidence collection and preservation. Evidence is collected using various forensic tools. The next step involves analysis of evidence to identify anti-forensic attacks. This mainly consists of three main phases. One is search for anti-forensic attacks occurred, next is identification of affected evidences and last is cancelling the effects of anti-forensic attacks. The analysis of evidence integrity is key objective of the framework. Further process of evidence collected is carried out similar to that of regular attack analysis. The final phase represents presentation and reporting.

The frame work provides an effective model for forensic investigation of anti-forensic attacks. The thesis focus on a comprehensive study of anti-forensic techniques and its effects on evidence gathered. Most of the anti-forensic techniques are deployed hide the attack source, strategy and modus of operation of attacks. Inside a particular network infrastructure, attacks are successfully deployed exploiting the vulnerabilities of system configurations and network configurations. The in-depth analysis of attacks can be successfully examined using reverse engineering techniques of network attacks. One of the main reverse engineering techniques is the analysis using network attack graphs.

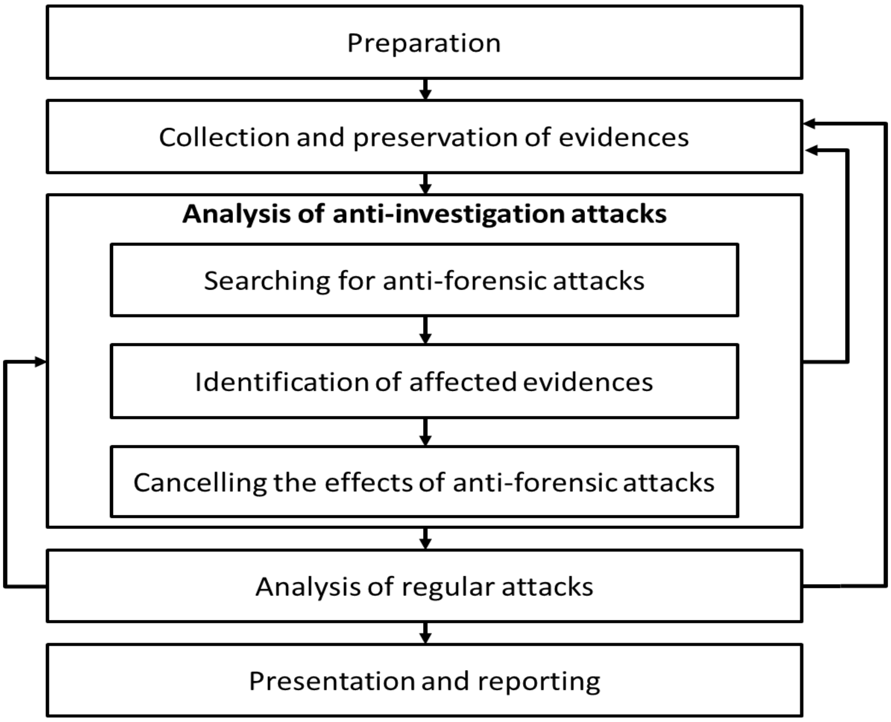

Preparation
Collection and preservation of evidences
Analysis of anti-investigation attacks
Searching for anti-forensic attacks
Identification of affected evidences
Cancelling the effects of anti-forensic attacks
Analysis of regular attacks
Presentation and reporting

Figure 2.3 Digital investigation process with anti-forensic technique detection

2.5.1 Graph Theory

Analysis of network security is one of the main challenges faced by network security professionals. There are a number of studies and research related to analysis of attacks in network security. The key challenge of network security professionals is to find the vulnerabilities in the system, analyze them and to remove or to reduce their effect in the particular network system. Security risks in network infrastructure are hard to quantify. An ideal network vulnerability assessment system would be able to identify the vulnerabilities. Application of graph theory on to the networks contributed a new platform for research and analysis of network security.

A study on a group of objects (vertices) when connected by links (edges) is known as graph theory. There are two types of graphs, namely directed and undirected graphs. A graph in which the edges have specific direction (orientation) is known as a directed graph. Information flow in these graphs can be easily identified. This enables the insertion of test cases or breakpoints, thus enhancing the quality of the output or the desired result. For example, air routes between two or more locations can be considered as a directed graph, where the airports become the vertices and the routes which the airlines choses become the edges. A graph in which the edges have no direction (orientation) can be called as an undirected graph. Flow of information in such graphs is usually unpredictable. The molecular structure of a compound can be considered as an undirected graph, where the vertices are the atoms and the edges become the bond between them, is an example.

Today, graph theory has become one of the major research topics in the world, owing to its varied uses and advantages. One of its main advantages can be quoted for its usability in determining the shortest path between two vertices (source and destination). An algorithm that is used for this purpose is known as the Shortest Path Algorithm, which identifies the best or least cost-effective path between the source and destination nodes. Two commonly used SPA methods are Bellman-Ford Algorithm and Dijkstra’s Algorithm.

For example, a student who identifies a path that helps in reaching the next lecture class at the earliest possible time, soon after the completion of the current lecture class, within the same campus, can be considered as a real-life application of the Shortest Path Algorithm.

2.5.2 Network Attack Graphs

To investigate normal as well as anti-forensic incorporated attacks, challenging and new approaches such as attack graphs should be deployed. Attack graphs can be defined as an instrument to compute hierarchical steps of an attack scenario with the help of known vulnerabilities and configuration. They are used by the system administrators and investigators to analyze the type of attacks, different ways of attacks, precautionary and preventive measures applied to counter those attacks (W. Wang & Daniels, 2008). IP trace back process is not a straight forward process because of IP spoofing and compromised intermediate host (Benjamin & Jill, 2007). The article (Bosheng, Marshall, Wenzhe, & Kun, 2008) describes an automated forensic analysis of network attacks utilizing attack graphs and focus on better analysis of evidence to detect attacks. Incorporation of anti-forensic nodes onto the attack graphs (Ingols et al., 2009) may provide sufficient information regarding the attacker's intention of reducing the generation of evidence and gives two possibilities of trace path, one with normal attack nodes and other with anti-forensic nodes.

The research (Velupillai & Mokhonoana, 2008) proposed three different algorithms. One for attack alert aggregation which utilized Leader Follower similarity based alert correlation (Ou, Govindavajhala, & Appel, 2005), second for building evidence graph (Cohen, 2009) and third for expansion of the attack graph to gather hidden members of the attack group. Automated analysis of evidence graph is employed using Fuzzy Cognitive Map (FCM). Minimization of attack graphs using various algorithms provides identification of precise path of attacks (Changwei, Singhal, & Wijesekera, 2012).

Using the attack evidence graphs, investigators can determine the existence of anti-forensic attacks and identify the tools and techniques used by the attacker. Thus, they can reconstruct the attack scenario with the minimum evidence they have.

Tools for Generating Attack Graphs

TVA (Topological Analysis of Network Attack Vulnerability) - It generates attack graphs using a graph search algorithm. It utilizes dependency graphs to create pre and post conditions (Zheng et al., 2011).

NETSPA (Network Security Planning Architecture) - A framework for generation of network models using known vulnerabilities and firewall rules. This act as a source for generation of attack graphs to identify the potential attacks and trace out the paths (Jha, Sheyner, & Wing, 2002).
MULVAL (Multi-host, Multistage Vulnerability Analysis) (Singhal & Ou, 2012) - A framework for integration of vulnerabilities and network configurations which uses Data log as its language. It consists of a scanner and an analyzer. The reasoning engine which has data-log rules captures system behavior.

The integration of attack graph workflow with the IDS management using vulnerability databases and attack graph generation tool is an effective forensic measure (W. Wang & Daniels, 2008). The attack intention analysis algorithm proposed in (S. Roschke, Feng, & Meinel, 2010) provide a new method for network forensics which helps in identifying similar attacks for evidence analysis using alert correlation and distance based similarity measure to identify the relationship strength between attack evidences. It can be suggested that integration of attack intention analysis (Catania & Garino, 2012; Harshbarger, 2010) with the IDS may provide precise attack alerts and identify accurate attack paths.

In order to investigate network attacks, to find the source of the attack and the attacker, one has to trace back the entire path of the attack. The attack path can be resolved using reverse engineering of the attack from destination with the help of attack graph technique. Using vulnerability and system configuration as input, attack graphs can be created using various tools. An anti-forensic technique such as trace path obstruction technique hinders the development of attack graphs (Velupillai & Mokhonoana, 2008).

2.6 Evaluations and Comparisons of Tools & Techniques

Network forensic system comprises of network monitoring and network analysis tools which captures network traffic packets. Detection of an incident and its validation should be made for proper decision making of false alarm. Tools such as TCPDump, Snort, Bro-IDS are used for proper evidence collection using network traffic packets. Forensic examination of the gathered packets are conducted using network forensic tools such as Wireshark, TCP flow, Nessus, Bro and Snort. The analysis of the network packets provides evidence for threats and attacks in a network. Due to application of anti-forensic techniques such as network steganography and covert channels complete valid evidence collection cannot be achieved.

The below sections provides detailed information with relevance to most common tools and techniques used in network forensic process and anti-forensics. The main aim of the study of anti-forensic tools and techniques is to identify the functioning and effects of these techniques in evidence collected. Thus methods and measures can be undertaken to discover and reduce the effects of anti-forensic techniques on the evidences.

2.6.1 Network Forensic Analysis Tools

Table A in the appendix A shows some of the main Network Forensic Analysis Tools (NFATS) which helps in the analysis phase of the evidence collected as a part of the forensic procedure (Benjamin & Jill, 2007; Samalekas, 2010). The table A shows the different network forensic tools used for network evidence analysis.

2.6.2 Network Security and Monitoring Tools

Table B in the appendix B shows the main network security and monitoring tools used for the evidence collection and analysis (Arnold & Yang, 2011; Benjamin & Jill, 2007).

2.6.3 An Overview of Anti-forensics Tools and Techniques

Table C in the appendix C shows the features and functions of different anti-forensic tools.

2.7 Trends and Research Problems

Network security has always been a crucial issue in the current world of technology as the entire corporate environment relies on internet and their assets have to be secured for successful management of their organizations. Its advancement technology aims to deploy better secured network to prevent threats and attacks. Advanced intrusion detection and prevention system (IDS/IPS) (Nikkel, 2006) with inbuilt data mining, intentional analysis and neural fuzzy logic helps in alerting attacks and threats with least possibility of false positive alerts. Numerous researches have been done in various fields of network security and network forensics to discover better defensive measure against attacks and threats especially in the field of wireless technology. Various researches should be carried out to gather effective evidence form wireless network (Berghel, 2003).

Network forensics is one of the sensitive areas in digital forensics as it contributes evidence to identify the identity and source of the attacker. The forensic investigation process has changed from traditional system forensics to live forensics and incorporated various methodologies to defend anti-forensic techniques and/or to reduce their effect in the collected digital evidence. The difficulty level of investigation of network attacks has risen in the recent years. As technology advances, new tools which are portable and handy (Endicott-Popovsky & Frincke, 2007) and techniques are developed for digital forensic investigation. But on the other side, criminals exploit the technology and finds new ways to thwart the forensic process.

As mentioned earlier, due to advancement in anti-forensic techniques, collection and analysis of evidence from computer networks which have been vulnerable to attacks, have been very challenging. Anti-forensics is not completely about tools which assist to cover up the trace but it is a combination of techniques, tactics and strategy (Cao et al., 2010; Johansson, 2002). The current trend in anti-forensics shows that, the application of techniques has moved from conventional areas of data hiding and deletion of evidence and logs in system to computer network. Techniques such as network steganography, covert tunneling, trace obstruction and hiding IP are now frequently used by the attackers for defense mechanism. Apart from this, law-breakers tries to obfuscate the forensic investigators by providing fake evidence, attacking forensic tools with compromised systems.

The main effect of anti-forensic techniques is on the integrity (Johansson, 2002) and dependence of the evidence collected. The tools and techniques are robust enough to alter (modify, delete and hide) the evidence source and evidence itself. The validation of evidence thus becomes a vital factor during the forensic investigative process. It becomes necessary to validate the evidence in each and every step of process by detecting the presence of anti-forensic techniques or use of anti-forensic tools, especially during live forensics. Robust methodologies and frameworks (Mansfield-Devine, 2010; Shanmugam et al., 2011) will be developed in for this purpose. Integration of intelligent analysis such as fuzzy logic and neural networks (Pilli, Joshi, & Niyogi, 2010), and anti-forensic detection algorithms and frameworks in forensic tools, network security and monitoring systems such as IDS/IPS will prove to be effective countermeasure.

The current security features in computer networks have various flaws and (Peron & Legary, 1995) utilized to gain access to systems and network infrastructure. Another key point is the compatibility of network infrastructure with the current forensic tools. The latest version of forensic tools such as Encase and Access Data Forensic Tool Kit (FTK) tries to cope up with the advancement of technology. These tools incorporate techniques for network forensics and internet forensics such as web analysis (Beverly, Garfinkel, & Cardwell, 2011), blog analysis (Pajek & Pimenidis, 2009) and email forensics (Nilsson & Larson, 2008). In order to trace out the path of the attack, to find the source and identity of the attacker, several methods such as attack graph theory, packet analysis and Metasploit forensic frameworks can be handy. To conclude, key areas where advancement has to be carried out are tools for development for network evidence graphs(Cohen, 2009) and attacks graphs, detection of anti-forensic attack tools and reduce their effect (Harris, 2006) in evidence so that integrity is not lost completely.

2.8 Conclusion

Anti-forensics was confined only to storage devices and computer systems for the past few years. Network forensics is one of the main challenging fields of digital forensics in this current era of latest technology. As new and robust attack techniques are discovered, it has become almost impossible to find the exact source of the attack. When anti-forensics combines with these network attacks, it will be far more robust and intense way of attacking and even more difficult to gather evidence, analyze and find the trace route and source. One of the latest forensic processes to identify the trace route (Goodall et al., 2006) is the reverse engineering of the attacks using network attack graphs.

An in-depth survey on the anti-forensics techniques has been conducted. The survey describes about the main anti-forensic tools which are classified with relevance to the techniques and algorithms they exploit. As the survey deals with how anti-forensics can be combined with network attacks, a review of the common network attacks have also been mentioned. The evidence collection and analysis of the network attacks are carried out using network security and monitoring tools (NSMs and network forensics analysis tools (NFAT). A detailed review of network tools has been carried out in the survey.

The key issue for forensic investigators while during the forensic process is the validation of evidence (Barford et al., 2002). The integrity of the collected evidence has to be questioned at each stage of analysis. Hash analysis and signature analysis are helpful to a certain extend. Sometimes hash collision techniques obfuscate the investigators. Another aspect is that the forensic investigation process itself will be under attack using rootkits (Boran, 1999), compromised hosts and attack on forensic tools (Forte, 2008). Research has to be conducted in these areas for implementation of effective countermeasures.

The challenges and issues in various tools and techniques have to be studied so that the vulnerabilities can be discovered. Anti-forensics techniques will focus on the vulnerabilities of the digital forensic software by obfuscation and misinformation. In order to defend such kind of attacks against the forensic tools, anti-forensics techniques and network anti-forensics have to researched further in depth and provide better security measures.

Chapter 3 Research Methodology

3.1 Introduction

The research methodology explains key research questions developed from literature review in the field of digital forensics. The challenges of anti-forensic techniques in digital forensics are put forth in the section of related studies. Network anti-forensics is found to be the main concern and emerging field in counter digital forensics. As technology advances, more and more cutting edge developments are discovered in forensic field. Similar developments are there in counter-forensic fields as well. The application of anti-forensic techniques and tools are prominent with network attacks. To the best of my knowledge, this is the first time network anti-forensics is explained which can be defined as network attacks combined with anti-forensic techniques.

In this chapter, the research problem and hypothesis is discussed in detail with relevance to the research gap identified from the background review in Chapter 2. The main aim of this chapter is to identify the potential research problem and explain experimental design, data requirements, and initial test bed for the design. Controlled experimental research is applied to find the most precise solution for the hypothesis developed from the literature review.

There are five major sections in this chapter which covers in detail the research hypothesis and associated research design. The section 3.1 covers the related studies of the research which explains the background. The section 3.2 pinpoints the research question and explains its importance with respect to the research gap. In section 3.3 depicts the hypothesis developed from the problem identified. The research design is explained in the section 3.4 and data requirements in section 3.5. The chapter concludes with section 3.6 depicting limitations of the research.

3.2 Related Studies

In this section, the concept of network anti-forensics is introduced. Network anti-forensics implies application of anti-forensic techniques in network attacks and forensics. Anti-forensic techniques such as data obfuscation (Krawetz, 2004), IP table misconfiguration, IP proxy, hiding IP help the network attack source to be unidentifiable. Generally, anti-forensic techniques are used to avoid detection of attacks, disruption and prevention of collecting valid evidence, subverting the forensic tools in collecting the right evidence. The main goals of network anti-forensic tools and techniques are not only to assist the network attacks, but also to make sure that no trace or evidence of the attack is left behind. Using attack graph methodology, we intend to analyze these attacks.

The current methodology of attack graphs helps to create graphs for normal attacks. The research defines normal attacks as those without the incorporation of network anti-forensic techniques and tools. The analysis and comparison of attack graph generated in the two scenarios: one with normal attacks and other with anti-forensic attacks will help in identifying the main changes occurred in attack graphs and thus helps in improving the network flaws and harden the network configuration. The main focus of our research is to identify how much valuable information and evidence can be collected from attack graphs and how it can be used to identify the source of the attacks.

3.2.1 Network Anti-Forensics

As mentioned earlier in chapter 2 literature review, anti-forensics is classified into different categories and it has advanced from traditional anti-forensics such as data hiding in slack space, in metadata files, watermarking, in bad sectors and using encryption; data destruction using tools such as Eraser, CCleaner (Velupillai & Mokhonoana, 2008) and techniques such as frequent overwriting. Anti-forensic techniques associated with network attacks are the one which is focused on and can be defined as network anti-forensics. Basically, network anti-forensics is can be classified under anti-forensic techniques. The figure 3.1 shows the classification of anti-forensic techniques in wide range.

From the figure 3.1 below, some categories of network anti-forensic techniques are hiding IP, Routing table misconfiguration, IP Proxy, network steganography and packet destruction using various techniques. Stegtunnel uses covert channels to hide data in TCP connections. OpenPuff and Socat used to hide data in carrier files. The attackers use these kinds of tools to obfuscate the investigators.

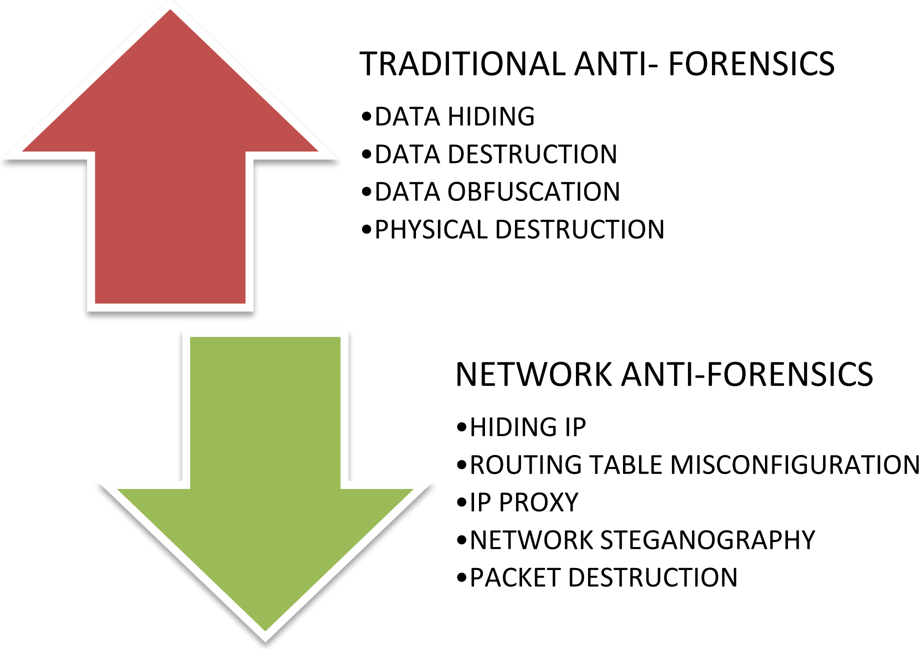


Figure 3.1 Classification of anti-forensic

The key objective of an attacker using anti-forensic techniques is to mislead with inappropriate evidence collection, challenging the integrity and validation of collected evidence, misdirecting the forensic investigators which make forensic investigation more time consuming and tricky and challenging. The incorporation of network anti-forensic techniques strengthens the network attacks to a new level as it helps to modify the attacks to delete the source and trace route and even makes the attacks invisible. Tools and techniques aids to break the trace path and obfuscate the forensic investigators from tracking down the source of attacks.

Forensic investigation of network attacks is classified into two such as live forensics and offline forensics. Live forensics involves analysis of traffic packets as it flows through the network and offline analysis involves analysis of suspicious data packets after capturing from network. The research mainly focuses on identification of different ways to prevent network anti-forensic attacks. In order to achieve this, most suspicious and probable attacks occurring in a network infrastructure is identified and attack graphs are generated to trace the exact path of attacks. Once the path is tracked, preventive measures can be implemented to stop the progress of attacks in each stage.

3.2.2 Network Attack Graphs

Attack graph reasoning utilizes reverse engineering techniques used by the investigators for scrutinizing computer attacks in hierarchical way (Anming, Zhuhua, Cong, Jianbin, & Zhong, 2009). This methodology is the main part of the evidence process phase in network forensics. The major advantage of this approach is that one can easily locate the path, vulnerabilities exploited, main techniques and strategies operated during the entire course and type of attack. Graphs are generated by tools such as TVA (Topological Analysis of Network Attack Vulnerability), MULVAL (Multi-host, Multistage Vulnerability Analysis) and NETSPA (Network Security Planning Architecture) with the help of known vulnerabilities, system configuration, security policies and host connectivity on networks.

The common reported vulnerabilities can be found from the databases and repositories such as National Vulnerability Database (NVD), Common Vulnerabilities and Exposures (CVE), Open Source Vulnerability Database (OSVDB) (Sebastian Roschke, Cheng, Schuppenies, & Meinel, 2009) and Vulnerability Database (VDB) from Security Focus or with the help of vulnerability scanners. Host connectivity can be identified using tools such as netstat and firewall rules. This will help in developing and implementing preventive measures to counter threats and attacks.

Attack graphs were developed to analyze the worst case scenarios of network security with consideration of network connectivity, system and network configuration, firewall rules, privileges, exploits and vulnerabilities. Attack graphs depict the relationship between the main three components such as network configurations, vulnerabilities and intrusion action. They provide a concise representation of attack approaches that compromises network security policies by exploitation of existing vulnerabilities(Oleg Sheyner & Wing, 2004). They also reckon all forms of possible sequences of exploits operated to compromise the resources.

Attack paths are the entire trace of an attack from the source (attacker) to the destination host (victim). This tells us how an attacker gains access to the destination host whether it is by single staged or multi-staged attack. In multi-staged attack, attack path defines the each stage vulnerability exploited and the damage caused. There are various techniques and algorithms developed to find the minimal optimal path of attack using attack graphs. Attack path consists of nodes and edges. Nodes define each step where vulnerability is exploited and edges define the route or transition from states and nodes, the attacker propagates. With the aid of the pre-conditions and the post conditions of attacks, most likely path is generated (Homer et al., 2008). Most of the researches have been carried out to find the optimal path and the shortest path of attack graph. Automation, integration and analysis of attack path generation into existing alert technologies are other areas of research.

Evidence graphs can be explained as extension or derivation of attack graphs which details the evidence analyzed and acquired from the attack graphs. Attack graphs which are generated by the tools such as MULVAL provide nodes which indicate each and every phase of the path with parameters (network vulnerability, network configuration and system configuration) that are exploited. Thus evidence graphs can be defined as the abstraction of attack graphs.

The process of attack graph generation consists of two main factors. One is the input parameter which comprises of the known vulnerabilities of the system and the system configuration. The network vulnerability information is collected from vulnerability scanner such as Nessus. The second one is the graph generation tool and algorithms. Tools such as TVA and MULVAL are mainly used to develop graphs (Li et al., 2007). Attack graphs are processed in visualization and analysis phase at the end. Network scanning and vulnerability scanning is performed which provide sufficient information to develop attack graph. Port scanning, fingerprint scanning and vulnerability scanning are the main scanning techniques utilized to gather attack information. Since different scanning tools provide different outputs, an integrated network scanning platform combines all the results of scanners into single entity in XML format (Katipally et al., 2011).

As the number of nodes and hosts increases, the graph built will become complex and difficult to analyze. In order to reduce the complexity of the attack graphs minimization algorithms are suggested by various studies. There are few numbers of tools that develop attack graphs. TVA (Topological Analysis of Network Attack Vulnerability) which generates attack graphs using a graph search algorithm. It utilizes dependency graphs to create pre and post conditions. Scalability of attack graphs was an issue when it was first developed (Albanese et al., 2011; Homer et al., 2008). NETSPA (Network Security Planning Architecture) is a framework for generation of network models using known vulnerabilities and firewall rules which was developed in C++. This acts as a source for generation of attack graphs to identify the potential attacks and trace out the paths. The tool generates the worst case attack graphs and was created using depth-limited forward chaining depth first search (Homer et al., 2008; Khaitan & Raheja, 2011). MULVAL (Multi-host, Multistage Vulnerability Analysis) is a framework for integration of vulnerabilities and network configurations which uses Data-log as its language. It consists of a scanner and an analyzer. The reasoning engine which has data-log rules captures system behavior. The detailed explanation of MULVAL tool is given below (Homer et al., 2008).

The main attack graph generation tool for the experimentation is the MULVAL tool which is open source as it provides a concrete graph for vulnerability analysis and has the option of generating both minimal and extended graphs. The key inputs are host configurations, network configurations, vulnerability information and policies.

3.3 The Research Questions and Hypothesis

The primary objective of this thesis is the survey of is to understand the prime challenges and effects of anti-forensic techniques in digital forensic field. Evidence collected by digital forensics techniques and tools are considered to be valid in the court of law to prove digital crimes. As technology advances, digital forensic investigators are finding it difficult to cope up with the hackers' new techniques and tools. Even it has become easy for script kiddies and normal people to break through the networks and gather valuable information and assets of any corporations, as there are a wide range of books, open source information, tutorials and tools available in the internet and testing websites as well.

Anti-forensics and counter forensics, by definition they are similar, are emerging techniques to counter the forensics process. Anti-forensic techniques have the capability of destroying, hiding, misconfiguring and obfuscating information and data in their target system which alters the integrity of evidence. Forensic investigators should be well aware of these kinds of these kinds of techniques as the validation and integrity of the gathered evidence matters in the court of law. The thesis also focuses on new emerging techniques of anti-forensics in network attacks and defines it as network anti-forensics. Presence of an anti-forensics technique in a normal attack is difficult to find, as the evidence collected from the victim system must prove to be valid.

As mentioned earlier in the literature review, the analysis part of digital forensic process should be divided into sub-divisions such as searching anti-forensic attacks, identification of anti-forensic techniques and cancelling their effects without changing the integrity of original evidence. Network attacks incorporated with the anti-forensic techniques challenges even the first step of the forensic model as it obfuscates or deletes proof of evidence that anti-forensic techniques were applied.

The investigators will find it hard to trace down the modus of operation, path and strategy of the attack. This becomes more complex and investigators find it time consuming for the forensic process. Thus forensic process fails to identify the source of attack. In order to avoid this situation, this research suggests an effective preventive and precautionary measure to identify and trace down the path of attacks using attack graph techniques. The main research hypothesis developed is:

“Whether the effects of anti-forensic techniques can be reduced using the attack graph methodology?”

This research attempts to identify a successful solution to the following sub-questions developed from the above hypothesis.

1. ***What are anti-forensic techniques and how it affects forensic procedure?***

2. ***What are the key requirements for generation of attack graphs to identify the attack path?***

3. ***How is the attack graph helpful in determining the occurrence of anti-forensic techniques in a particular attack and how it helps to improve the network security?***

The following sections describes the main approach opted for finding the solution to the research questions.

3.4 Research Design and Data Requirements

3.4.1 Research Design

The research design is explicitly same as that of the thesis structure in the figure1.1. The key objective of the thesis is to find the most appropriate solution to the research questions identified from the background literature review. The importance of first research question is that valuable in-depth information regarding anti-forensics is needed to analyze the same and find counter measures to reduce the effects. Challenges and after effects of any system is best known when a comprehensive study is conducted.

In order to obtain a rational solution to the research question, experimental approach is chosen. The expected outcome of the research is to identify the best precautionary and preventive measures to strengthen the network security and to reduce the effects of anti-forensic techniques incorporated with the network attacks. A test bed is created using virtual environments to conduct experiments and analysis of the experiments is performed using attack graphs to locate and identify valuable information.

The experimental test bed is a small scale office environment generated using virtual simulation environment. The research is conducted in two main phases, one for normal attacks and other for network anti-forensic attacks. Each phase has two main kind of attacks generated and applied onto the test bed and valuable information is collected. Attack graphs are generated for each kind of attacks. The first phase is the training phase where the attack graph methodology is utilized for normal attacks (attacks without anti-forensic attacks). Second phase is the testing phase where anti-forensic attacks are analyzed using attack graphs.

3.4.2 Data Requirements

The dataset is collected from the various sources for conducting the experiments. In order to conduct attacks of the simulation environment, vulnerabilities of the system are collected using vulnerability scanner 'Nessus' (Cheng, Roschke, & Meinel, 2011; Xie et al., 2009). Each system designed in the virtual environment has its own vulnerabilities and are identified using scanner. The vulnerabilities are then compared manually with the National Vulnerability Database (NVD). The database servers have got MySQL databases which contains information regarding customers of an particular website uploaded.

The system configurations and network configurations are collected as the simulation environment is set. The main outcomes of the experiments are in the form of attack graphs. As mentioned earlier, the main input parameters are the network configurations and vulnerabilities. The input file for the attack graph generating tools is either the 'Nessus' output file or the input file created manually. A secondary dataset of vulnerability database is downloaded from NVD which is one of the parameters for MULVAL tool (Oleg Sheyner & Wing, 2004). Information needed for analysis of the scenario is the vulnerability exploited and the IP address of the suspicious system from the snort alert file. This is necessary to extend the attack graph analysis to the next level.

3.5 Limitations of the Research

Numerous network attacks are there in the current era of digital technology. The prime limitation of this research is that of analysis of all network attacks to be carried out. The network attacks itself has its own categories and sub-categories. Analysis and attack graph generation of each and every attacks are practically impossible. When it comes to multi-staged attacks, hackers exploit various vulnerabilities and utilize more than one technique to break through. Similar to normal attacks, anti-forensic techniques are increasing in number and the survey details the most prominent and common techniques.

The second limitation of the research is the assumption that anti-forensic attacks are identified in analysis of the attacks. The research mainly focuses on the preventive measures to reduce effects of anti-forensic attacks. The main challenge is to assume the most probable network attack and anti-forensic techniques that can exploit the vulnerability of a network infrastructure. The test bed is created on virtual environment using virtual machines and virtual networks. The actual effects in real networks are to be calculated and analyzed. This is another limitation of the research.

Once the network attacks are detected using IDS systems, attack graphs are generated with the aid of vulnerability information gathered from vulnerability scanner, system configuration and network configuration. They are manually collected from system, routers and firewall rules. The experiment is conducted in controlled environment in which training phase collects all information needed to generate attack graph. The testing phase analyzes attack graphs with anti-forensic techniques. All the virtual machines in the test bed use Linux OS as it is open source and security strength is low. The comparison of attack graphs are on qualitative basis. Thus, it may be seen that the main limitation of the research is the identification of best and most common network attacks and anti-forensic techniques.

3.6 Expected Outcomes and Conclusion

The main expected outcomes are the anticipated results of the research question depicted on section 3.2. From the proposed research experiment, the analysis of anti-forensic techniques and network attacks are intended to be carried out. Thus form the literature review, the expected outcome can be established through attack graph generation of each phase of attacks on the network system configured.

The expected outcome also includes the main effects of anti-forensic techniques on network evidence and attack graph generated. The generated attack graphs on normal attacks and attacks incorporated with anti-forensic techniques can be utilized to compare and analyze the changes occurred and thus identifying the network flaws.

This chapter conveys a comprehensive review of related studies and works of the research area suggested. The section 3.2 introduces the new concept of network anti-forensics which is the main area of analysis. It also establishes a strong methodology for analysis of anti-forensic attacks using attack graphs.

The research project on anti-forensics for network attacks uses experimental research methodology. This methodology helps in analysis of anti-forensic techniques to the core level. Primarily it was identified that the forensic investigation and preventive measures for network anti-forensic attacks are highly complex and difficult to analyze. Due to the high growth rate of technology, counterfeiters make use of the most developed technology to break through the strongest walls of network security.

The research mainly focuses on the effects of anti-forensic techniques in network attacks. The attack graph generation of network attacks and attacks with anti-forensic techniques are compared and preventive measures are suggested. The following chapter provides exhaustive description of the research experimental approach, details of the experimental simulation environment, test bed and different phases of the experiment, thus describing the findings of the research project.

Chapter 4 Research Findings

The key objective of the thesis is the analysis of normal network attacks and anti-forensic incorporated network attacks. From chapter 3 research design, in order to trace down the path, attack strategy and modus of operation of normal network attacks and anti-forensic incorporated network attacks, the best solution suggested is the use of attack graphs. Attack graphs generated for a particular network infrastructure shows how attacks propagates through a network and which all vulnerabilities are exploited by the attacker.

This chapter depicts the entire experimental scenarios and environments in which experiments are conducted and network attacks are analyzed. The main research findings are portrayed in this chapter which helps in investigation of anti-forensic techniques implemented in network attacks and aids in suggesting preventive measures to relegate their effects.

4.1 Approach

In this section, we conduct experimental analysis on how attack graph can be utilized for forensic analysis and improving the network security. The key phases include development of virtual environment of test-bed and generating attack graphs with the help of input parameters such as network configurations, vulnerabilities and system configurations. The last phase includes incorporation of anti-forensic attacks instead of normal attacks and remodeling the attack graphs using MULVAL tool (Ou et al., 2006).

The target system configuration is required for generating attack graphs, which can be acquired by scanning techniques. The later section of the chapter provides details regarding experiments conducted using anti-forensic techniques on a sample network created in a virtual environment. Anti-forensic techniques are sophisticated attack associates and detection using normal forensic technique is complex and problematic. Once the identification of occurrence of anti-forensic techniques is confirmed, it can be incorporated in attack graph generation system.

The challenging part of the experiment was to incorporate anti-forensic techniques and its effects in attack graphs and to trace out the variation from normal attacks. The changes occurred in the attack graphs generated relates to security discovery of security flaws in the proposed system and network configuration. Thus, the hardening of the network security of the infrastructure can be implemented (Bursztein & Mitchell, 2011).

4.2 Experimental Test-Bed

The test-bed is created using virtual machines with the tool VMware Workstation. The simulation test-bed consists of a small network with internal and external firewalls, database server, router, IDS system workstations and webserver. All the VMs are using different versions of Ubuntu. The main advantage of VMs is the options of getting snapshots of the main installation phases can be generated.

The virtual network editor provides all options for generating static IPS and network configurations for each and every VM. All the virtual networks were provided with a bridged connection with the host system so as to access internet.

The virtual network configured consists of two main parts. The first part is mainly an intranet and is simplified into a small office based environment which consists of a workstation, webserver, database server, router with firewall and IDs system. All the peripherals in the first part of the system have different versions of Ubuntu OS as it is more vulnerable than any other OS and the experimental attacker can exploit all the vulnerabilities. Figure4.1 shows the attack simulation environment for experimental analysis.

The key parts of the intranet network are the router, IDS and webserver. The router (RouterR) is configured to direct the traffic to specific destination and for giving to and fro access to the workstation PC and webserver / database server. The webserver (Rwebserver2) consists of two main websites which has inbuilt vulnerabilities. The IDS incorporated in the system is Snort which runs on Ubuntu 12.0.4 and functions as an alarm system for detecting attacks. The workstation acts as normal PC having access to both the webservers and database servers. All the servers are given static IP address and configured in the router. The IDS in the network notifies threats and attacks and is used mainly for the testing phase.

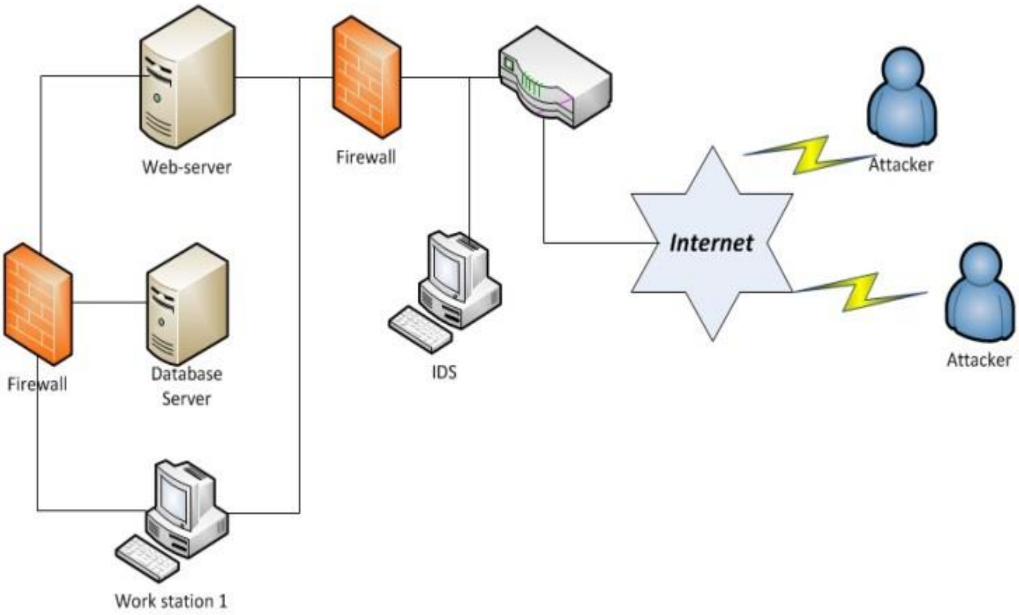


Figure 4.1 Simulation environment

The second part consists of internet access and attacker systems. The attacker system runs on Backtarck5 R3 which contains all the attacking tools such as metasploit for remote exploitation of target and burp-suite for SQL injection. The attacker system is simulated ones with incriminated static IP address.

The forensic machine is an independent integral part of the experiment which is operated for analysis of the target victim, network packets and traffics. Network monitoring tools such as Wireshark, Network Miner and Net-Detector are installed. The forensic machine is used for analytics of the network traffic packets and monitoring attacks. The table 4.1 below shows the network peripherals with characteristics and function of each.

Table 3.1 Network peripherals and its configurations

Network peripherals	Operating Systems	Components	Functions
Workstation	Ubuntu 12.0	Normal PC having cable internet and intranet connection	Have access to webserver and database server
Webserver	Ubuntu 11.2	Apache and Tomcat 7 installed and contains websites such as DVWA and Mutillidae	Serves as Webserver which is the victim1
Database Server	Ubuntu 11.2	MySQL server	Victim 2
Router	Vyatta 1.0	Router and firewalls configured	Main function is to control and direct traffic, routing configuration
IDS system	Ubuntu 12.0	Snort IDS	For attack and threat indication
Attacker1	Backtrack 5R3	SQL injection tools and Website vulnerability tools installed	To Attack database server and webserver
Attacker2	Backtrack 5 R2	Metasploit and Armitage installed	To attack work station and gain control, then access webserver/db server
Forensic Machine	Ubuntu 12.4.0	Wireshark, Network Miner installed	Forensic analysis of packets traced.

4.3 Experiments

Innumerable attacks can be generated and utilized for the purpose of simulation. The most common network attack on webservers and database servers is the SQL injection and remote exploitation tools such as metasploit (L. Wang, Liu, & Jajodia, 2006). The attack scenarios are divided into two main phases. The first phase generates normal attacks and is implemented for both webserver and database server. In second phase, each attack is incorporated with network anti-forensic techniques. Due to high complexity of implementation, this attack is carried out for remote exploitation in the work station. The analysis of attack scenarios is carried out with the attack graph reasoning (Albanese et al., 2011). For both cases, the generated attack graphs are analyzed and attack path and network flaws are identified.

Before the start of the experiments, snapshot of default configurations of target servers and PC machines are taken and backed up as the system configuration changes at each stage of attacks. Attack graph changes with the system configurations and network configurations, router configurations are also backed up.

4.3.1 Phase 1

This phase generates normal attacks and exploitation of vulnerabilities in both the webserver and database server. The main types of attacks are remote exploitation and SQL injection. A backdoor is created in the workstation of the office network using social engineering techniques. The backdoor is utilized to exploit the work station, gather credentials, gains access to webserver and database server. The vulnerabilities of both the servers are exploited and sensitive information is retrieved. The key advantage of this type of attack is that the attacker has full access of the work station root system.

The webserver system log file indicates the chronicles of the workstation IP address. Similarly, the websites in the webserver have vulnerabilities that can be exploited. Using attack techniques such as SQL injection, blind SQL injection and burp suite, these vulnerabilities are exploited. This is a direct attack to the webserver. Figure 4.2 shows directed graph of different stages of experiment. The simulated network environment includes network monitoring IDS system. Once the attack is discovered, using the network configurations and vulnerability database, attack graphs are generated.

The block diagram below shows the experimental model using normal attacks. First, the network is attacked using different attack techniques such as SQL injection and remote exploit using back door. The attacks are detected using the IDS systems installed in the network infrastructure. The analyses of attacks were carried out using the attack graph methodology. The generated attack graphs for each phase of experiments are analyzed. The attack graphs are generated using the tool MULVAL. The main inputs to the tools are the vulnerabilities of each peripheral, system configuration and the network configuration which is gathered from the firewall rules and router configurations. The vulnerabilities of the system are gathered from the Nessus scanner.

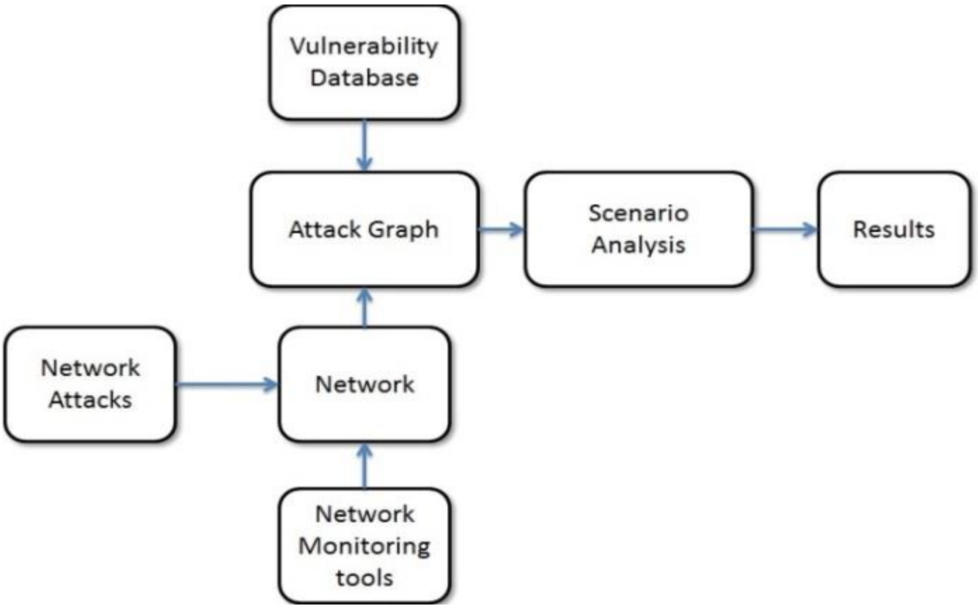
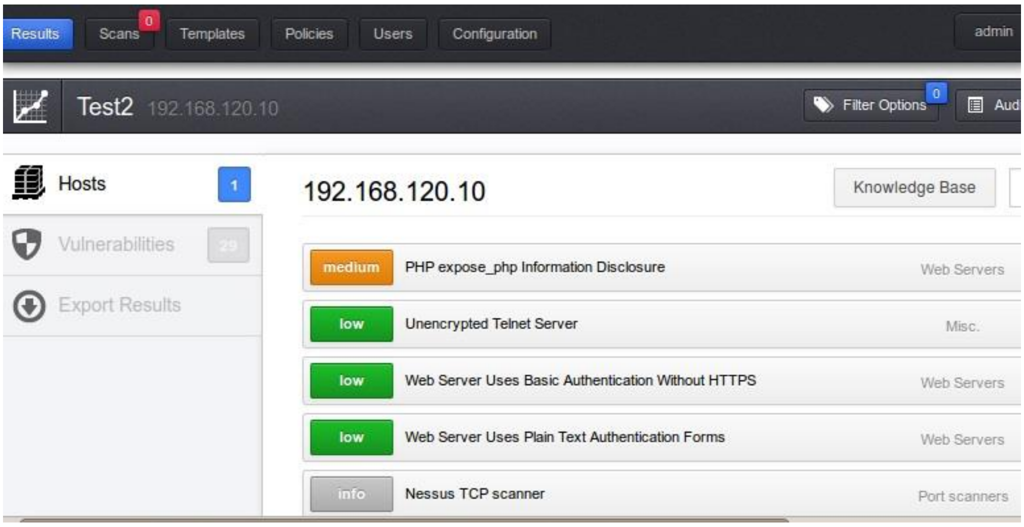


Figure 4.2 Block diagram of experimental model without incorporating anti-forensic attacks

The figure 4.3 below shows the Nessus scanner result for the webserver which identifies some vulnerability in the pilot test conducted.



192.168.120.10

medium	PHP expose_php Information Disclosure	Web Servers
low	Unencrypted Telnet Server	Misc.
low	Web Server Uses Basic Authentication Without HTTPS	Web Servers
low	Web Server Uses Plain Text Authentication Forms	Web Servers
info	Nessus TCP scanner	Port scanners

Figure 4.3 Nessus scanner result during pilot test.

4.3.2 Phase 2

In this phase of attack generation, normal attacks combined with network anti-forensic techniques are utilized. As normal attacks can be identified by IDS, network monitoring and forensic systems, incorporation of anti-forensic techniques will change the modus of attack operation completely. The main aim of this kind of attack is to hide the evidence, obfuscation of evidence and system logs. Each and every attack can be assisted with network anti-forensic technique which will strengthen normal attacks. In multi-stage attacks, each stage can be assisted with network anti-forensic techniques. Some of the common techniques includes hide IP, changing log file, A4 proxy and root file exploitation. Direct attack to the webserver and remote exploitation of workstation are backed by the above techniques. The figure 4.3 shows the flowchart of different stages of the experiment.

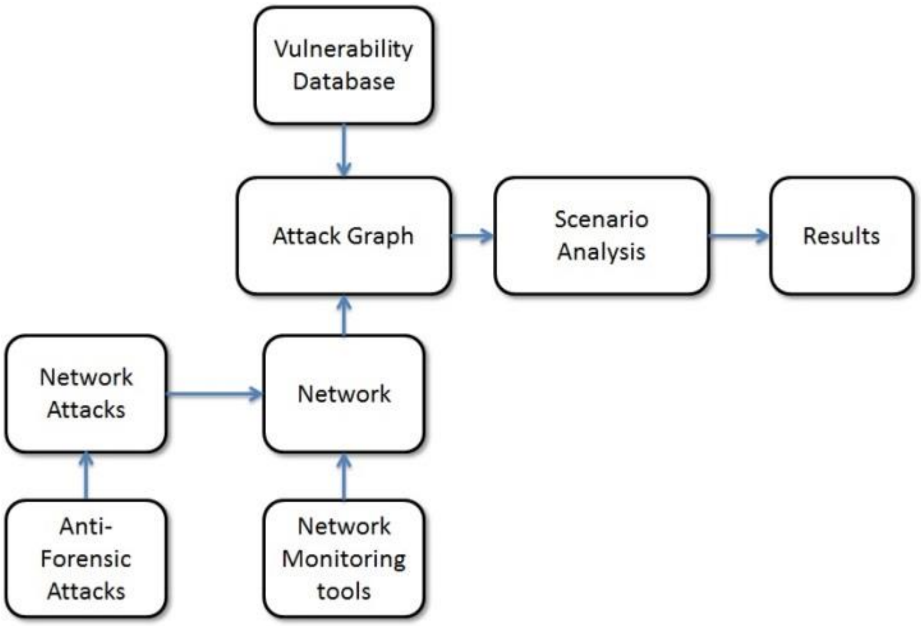


Figure 4.4 Block diagram of experimental model incorporating anti-forensic attacks.

4.4 Experiment Results

The experiments are conducted in two different phases as mentioned earlier. The first phase of the experiment is again sub-categorized into two main experiments. In the first experiment, attacks are carried out in the workstation through webserver using the input validation attack then to the database server exploiting the SQL injection vulnerability and by exploitation of remote exploit vulnerability in the work station. The attack graph generated from MULVAL clearly depicts the two attack paths from which attacks can occur. The main vulnerabilities exploited in the system are clearly shown in the figure 5.1

The second experiment is conducted by attacking the database server using sql injection. First, attacker gains control over the work station exploiting the remote client vulnerability such as Mozilla Firefox (using malicious input). From there, via webserver (exploited using web input check vulnerability), database server is attacked with the help of blind SQL injection exploiting the vulnerability of the database server.

The phase two experiment is conducted with the aid of anti-forensic techniques such as Hide IP, file content deletion, event logging disabling and log file deletion in each stage of the attacks. The main analysis of the attack graphs generated is explained in detail in the Chapter 5.

From the experimental results gathered, it can be concluded that attack graphs provide crucial information in relevance to the propagation of an attack inside a network. The in-depth analysis of these attack graphs can help implementing preventive measures and identify the weakness and location of weakness of a network infrastructure. Thus, attack graphs offer significant contribution to the network security.

Chapter 5 Discussions

5.1 Introduction

The previous chapter 4 details the experimental scenario and research findings were also reported. There are no variations in the data requirements apart from the vulnerabilities collected by scanning the network peripherals. The experiment is divided into two main phases as explained in chapter 4. Both the phases was conducted and analyzed in detail to find the most appropriate solution to the research questions developed in chapter 3. The significant findings from the research experiment performed are parameters required for generation of attack graphs and effects of anti-forensics on attack graphs which will be explained in detail in the below sections.

Chapter 5 will discuss the main research findings to evaluate the importance of the outcomes. The developed research question in section 3.3 is analyzed and discussed with justifications. The discussion summaries explained in the below sections helps to evaluate the research outcome comprehensively. The recommendations and practical implications are finally drawn in the last section of this chapter.

5.2 Attack Graph Analysis

The attacks created and launched on to the simulated network are utilized to study the strength of network security configurations. Since the attacks are successful in penetrating into the network, it can be deducted that network has flaws. In this section, in order to evaluate how efficient attack graphs are in terms of identifying and deducting the source of attacks, when network anti-forensic techniques are detected as attack associates. We throw lights on quantitative analysis of the attack graphs, and try to comprehend the effectiveness of attack graphs in countering anti-forensic techniques in networks.

For analysis of attacks identified, attack graph methodology is used. Attack graphs generated for both phase 1 and phase 2. For generating attack graphs MULVAL tool is used. For various attacks, different attack graphs are generated. The directed graphs generated are compared against each other. Each phase, two attacks are implemented such as SQL injection and remote exploitation using metasploit and graphs are created. The network configurations and simulation environment are set to default configuration after each attack is implemented. The main outcome of the graphs expected are where the attacks are from, paths showing which all vulnerabilities are exploited, modus of operation and strategies of the attack. The sections below explain the detailed analysis of each phase of experiments.

5.2.1 Phase 1

This phase of the experiment mainly focuses on normal attacks which intend to gather information regarding the network flaws and vulnerabilities of the workstation, webserver and the database server and to determine the preconditions and post conditions for generation of attack graphs. The normal attacks are deployed using general SQL injection techniques, metasploit remote exploitation and local exploitation of workstation vulnerabilities. The attack is implemented in virtual simulation environment mentioned above. The forensic analysis of the attacks is carried out using attack graphs.

Attacks are deployed onto the database server via webserver using SQL injection techniques. Once it is found that web-sever is under attack, the attack graphs are generated using the forensic machine with the help of MULVAL tool. The figure 5.1 shows the attack graph generated with the above simulation environment with SQL injection attack on to the database server via webserver and finally to the workstation exploiting the server application vulnerability of the system.

The main inputs for the attack graphs are system configurations, network configurations and the vulnerabilities of the entire network peripherals. The main vulnerabilities exploited are the webserver vulnerability of input validation which exploits the privilege escalation on to the database server. The paths defined by the attack graph suggest that the most probable attack is through webserver and database server to the work station as the final attack target was provided to be the workstation. Each time the trace path differs according to the target specified by the attack graph. With the same network configurations, if the attack target is the database server, exploiting the local application vulnerability of work station we get an entire different graph.

Using the local exploit, the attacker can access the root of the workstation gaining privileges and penetrate the database server. The figure 5.2 shows the possible ways of attacks from the attacker to the destination (database). From the attack graph generated, it can be understood that there are two main possible ways of attack from the internet to the database server. One is through the webserver, workstation and to the database server. The second is through the direct access from the webserver to the database server. After gaining access to either to the webserver or the workstation, database server can be exploited using bind SQL injection attacks utilizing the vulnerability of MySQL database. The in-depth analysis of attack graph shows that the main flaw of the network configuration is the multi-directional access of the database server from the webserver and workstation.

It can be deducted that for specific network configurations, vulnerabilities and system configurations as inputs, attack graph shows all different possible paths. It is prominent that the attack graphs provide the exact trace for collecting evidence and indicates the exact location from where valid evidence can be collected. But the probabilities of the paths are undefined and it is unsure that through which path actual attack took place.

The main limitation of the attack graph generated is that the information that main source of attack is the internet. The main inputs to the MULVAL tool are OVAL and Nessus output files which can be converted to DATALOG output. Another option is manual generation of input file. All these alternatives provide source of the attacker as the “internet”. The Snort IDS, if configured on to the network infrastructure, it will generate alerts which explain the vulnerability and immediate source IP address of the attacker. The output of the Snort log files and alert files can be suggested as the evidence that attack had occurred. It can be recommended that extraction of the vulnerabilities and IP address from the Snort log file and alert file to integrate to MULVAL input makes the process more precise and automated.

The attack graph shows the source of attack as internet. As the next development, we recommend two new input parameters such as the IP address node and the main vulnerability node. The IP address node indicates the immediate IP address from where the attack packet came from. As mentioned earlier, if the network system has IDS installed such as Snort, from the alert files, the IP address and the main vulnerability or protocol exploited by the suspicious system can be gathered. Addition of these nodes to the main attack graph will increase the precision of the path. As the number of vulnerabilities increase, the trace path also increases, but if the main vulnerability is known, attack path can easily be identified.

The figure 5.3 shows the attack graph with new nodes inserted and the bold red arrows defines the actual attack path identified. The nodes 33, 34, 35 in figure 5.3 are the new ones inserted which shows the main vulnerability and the immediate source IP address. In order to automate the process of entering the vulnerability and source of the suspicious system from the Snort IDS, generation of a script which will collect all the details from the alert file of IDS system, match with the CVE details of the IDS rules is recommended.

5.2.2 Phase 2

In this phase, attacks assisted with anti-forensic techniques are introduced to the network. The main network anti-forensic techniques that can be incorporated for the attacks are hiding the IP address, deleting the log files and deleting the file content. There exists an ambiguity in the attack graph generation as the input parameters for the graph generation do not change when network anti-forensic techniques are applied. The current tool does not incorporate any rules regarding these techniques and the pre-conditions and post conditions for these kinds of attacks are not defined.

To identify potential network anti-forensic techniques associated with the network attacks on the attack graphs, new rules in the MULVAL tool are recommended. We incorporate additional nodes and their outcomes and effects to the attack graph are analyzed. The figure 5.4 shows the detailed attack graphs with nodes incorporating anti-forensic techniques. The attack graph is also integrated with main vulnerability node and source IP address node. The main advantage of the IP address node is that the forensic analyst can easily notice any hitches affected by the same on the target machine. But, the main challenge faced in this experiment is that the value of IP node is “null” as the attacker uses techniques to hide IP address. Thus the immediate IP address of the attacker cannot be gathered. The IP address collected from the IDS is the fake IP as the integrity of the IP address is questionable in this scenario.

The changes occurred in attacks generated in different scenarios will reflect the reliability of graphs for each attacks. The analyses of network anti-forensic techniques are complex and time consuming. In order to effectively analyze the effect of anti-forensic techniques before any attack occurs, simulation of an attack scenario and generation of attack graphs indicates all possible trace paths vulnerability nodes of a network configuration. This helps to implement precautionary measures on the network infrastructure and strengthen the network security.

The scenario used to generate the attack graph figure 5.3 and figure 5.4 are the same in order to carry out a comparison of what all changes that can occur. As mentioned above, incorporation of network anti-forensics on to the network attacks make it hard to trace down the path. The figure 5.4 shows a detailed path of the attack path as the main vulnerability is known. Integration of anti-forensic nodes A, B, C, D which are delete file content, delete log file, disable event logging and hide IP respectively in attack graphs challenges the forensic analysts in gathering valid evidences. This notification of network anti-forensic nodes in attack graphs helps the investigators to identify the valid evidence. Thus by in-depth examination, proper evidence can be collected.

The integrity of the attack graphs matters when anti-forensic techniques are associated with the attacks. To the best of the knowledge, there are no methods that checks the integrity of the attack graphs produced. The attack graphs generated become complex as the number of host in network increases. Apart from those said above, attack graph proves to be an effective methodology for pre-analysis of network flaws and vulnerabilities of the systems.

The figures and tables below shows the generated attack graphs and its explanation for the two phases of experiments conducted. The explanation for each attack graph generated is given above.

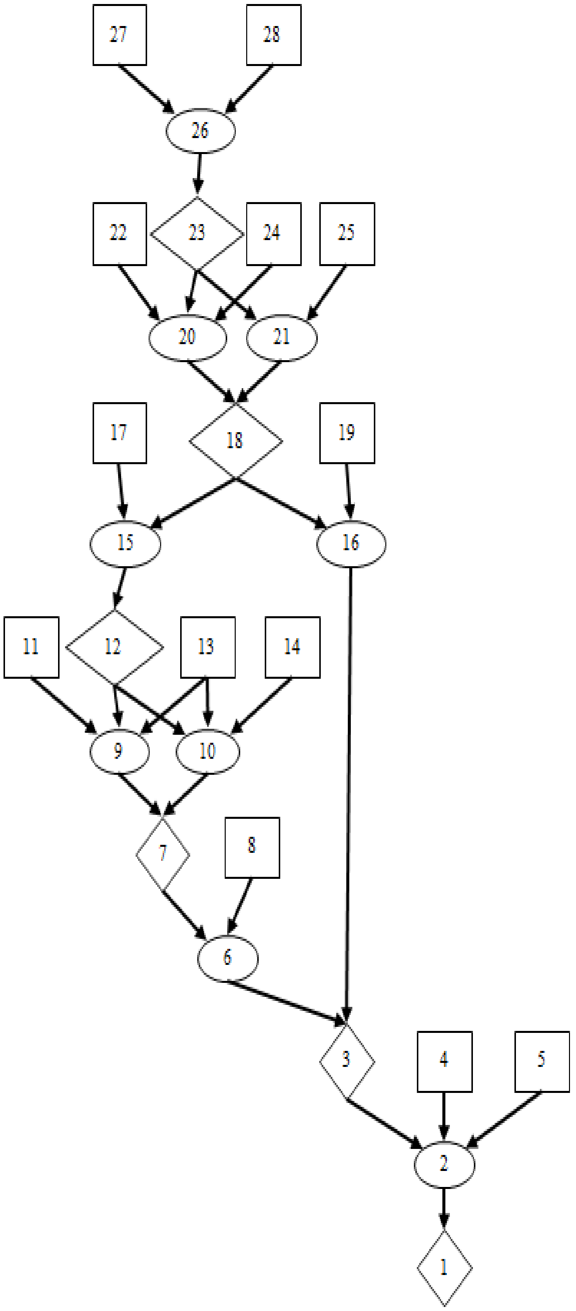


Figure 5.1 Attack graph for workstation “192.168.120.10”

Table 5.1. Attack graph for workstation “192.168.120.10”

Sl	Description
1	execCode(’192.168.120.10’,user)
2	RULE 2 (remote exploit of a server program):
3	netAccess(’192.168.120.10’,httpProtocol,httpPort)
4	networkServiceInfo(’192.168.120.10’, serverApplication,httpProtocol,httpPort,user)
5	vulExists(’192.168.120.10’,remoteVul_0, serverApplication,remoteExploit,privEscalation):
6	RULE 5 (multi-hop access):0
7	execCode(database,_) :0
8	hacl (database, ’192.168.120.10’ ,httpProtocol , httpPort) :1
9	RULE 2 (remote exploit of a server program):0
10	RULE 2 (remote exploit of a server program):0
11	24:vulExists(database,blindSQLinjection, mySQL,remoteExploit,privEscalation):1
12	netAccess(database,dbProtocol,dbPort):0
13	networkServiceInfo(database,mySQL,dbProtocol, dbPort ,_) :1
14	vulExists(database,’SQLinject ion’,mySQL,remoteExploi t ,privEscalat ion):1
15	RULE 5 (multi-hop access):
16	RULE 5 (multi-hop access):0
17	hacl(webserver,database,dbProtocol,dbPort):1
18	execCode(webserver,apache):0
19	hacl(webserver,’192.168.120.10’,httpProtocol,http Port):1
20	RULE 2 (remote exploit of a server program):0
21	19:RULE 2 (remote exploit of a server program):0
22	18:vulExists(webserver,inputvalidation, httpd, remoteExploit ,privEscalation) :1
23	netAccess(webserver,tcp,80):0
24	17:networkServiceInfo(webserver, httpd, tcp,80,apache) :1
25	20:vulExists(webserver,webInputCheck, httpd, remoteExploit ,privEscalation) :1
26	14:RULE 6 (direct network access):0
27	16:attackerLocated(internet):1
28	hacl(internet,webserver,tcp,80):1

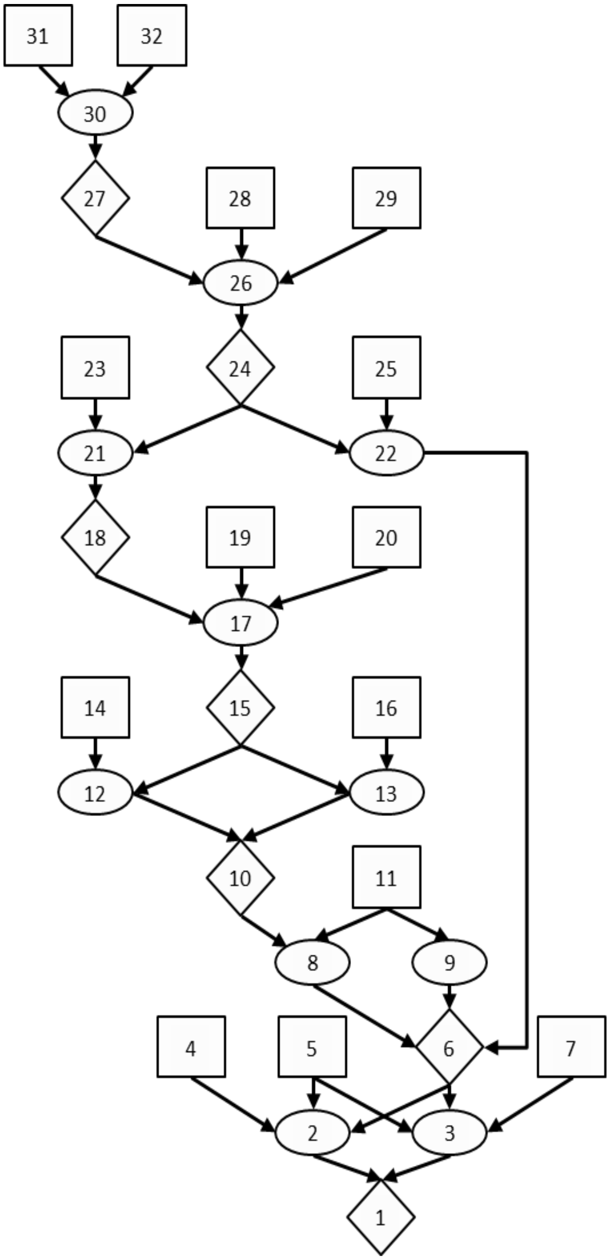


Figure 5.2 Attack graph for database using local exploits

Table 5.2 Attack graph for database using local exploits

Sl	Description
1	execCode(database,_)
2	RULE 2 (remote exploit of a server program)
3	RULE 2 (remote exploit of a server program)
4	vulExists(database,’SQLinjection’,mySQL,remoteExploit, privEscalation)
5	netAccess(database,dbProtocol,dbPort)
6	networkServiceInfo(database,mySQL,dbProtocol ,dbPort ,_)
7	vulExists(database,blindSQLinjection, mySQL,remoteExploit ,privEscalation)
8	RULE 5 (multi-hop access)
9	RULE 5 (multi-hop access)
10	execCode(’192.168.120.10’,root)
11	hacl(’192.168.120.10’,database,dbProtocol,dbPort)
12	RULE 1 (local exploit)
13	RULE 1 (local exploit)
14	vulExists(’192.168.120.10’,localVul_1,localApplication, localExploit,privEscalation)
15	execCode(’192.168.120.10’,user)
16	vulExists(’192.168.120.10’,localVul_0,localApplication, localExploit,privEscalation)
17	RULE 2 (remote exploit of a server program)
18	netAccess(’192.168.120.10’,httpProtocol,httpPort)
19	networkServiceInfo(’192.168.120.10’,serverApplication, httpProtocol,httpPort,user)
20	vulExists(’192.168.120.10’,remoteVul_1,serverApplication,remoteExploit,privEscalation)
21	RULE 5 (multi-hop access)
22	RULE 5 (multi-hop access)
23	hacl(webserver,’192.168.120.10’,httpProtocol,httpPort)
24	execCode(webserver,apache)
25	hacl(webserver,database,dbProtocol,dbPort)
26	RULE 2 (remote exploit of a server program)
27	netAccess(webserver,tcp,80)
28	networkServiceInfo(webserver,httpd,tcp,80,apache)
29	vulExists(webserver,inputvalidation,httpd,remoteExploit ,privEscalation)
30	RULE 6 (direct network access)
31	hacl(internet,webserver,tcp,80)
32	attackerLocated(internet)

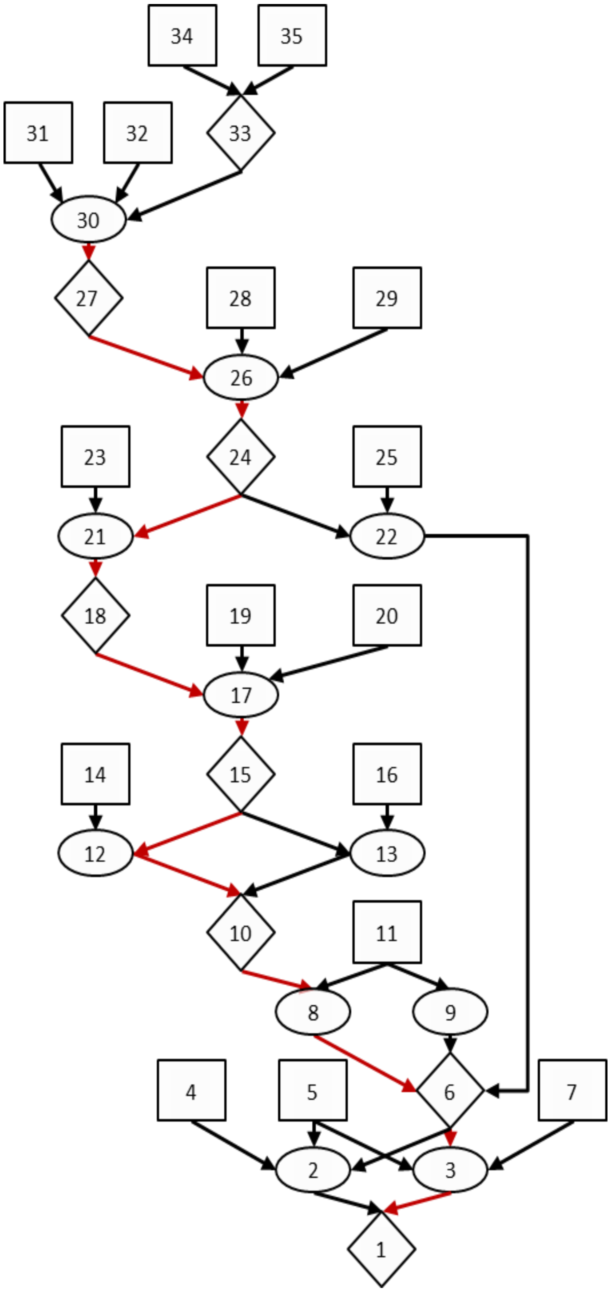


Figure 5.3 Attack graph integrating new nodes

Table 5.3 Attack graph integrating new nodes

Sl	Description
1	execCode(database,_)
2	RULE 2 (remote exploit of a server program)
3	RULE 2 (remote exploit of a server program)
4	vulExists(database,’SQLinjection’,mySQL,remoteExploit, privEscalation)
5	netAccess(database,dbProtocol,dbPort)
6	networkServiceInfo(database,mySQL,dbProtocol ,dbPort ,_)
7	vulExists(database,blindSQLinjection, mySQL,remoteExploit ,privEscalation)
8	RULE 5 (multi-hop access)
9	RULE 5 (multi-hop access)
10	execCode(’192.168.120.10’,root)
11	hacl(’192.168.120.10’,database,dbProtocol,dbPort)
12	RULE 1 (local exploit)
13	RULE 1 (local exploit)
14	vulExists(’192.168.120.10’,localVul_1,localApplication, localExploit,privEscalation)
15	execCode(’192.168.120.10’,user)
16	vulExists(’192.168.120.10’,localVul_0,localApplication, localExploit,privEscalation)
17	RULE 2 (remote exploit of a server program)
18	netAccess(’192.168.120.10’,httpProtocol,httpPort)
19	networkServiceInfo(’192.168.120.10’,serverApplication, httpProtocol,httpPort,user)
20	vulExists(’192.168.120.10’,remoteVul_1,serverApplication,remoteExploit,privEscalation)
21	RULE 5 (multi-hop access)
22	RULE 5 (multi-hop access)
23	hacl(webserver,’192.168.120.10’,httpProtocol,httpPort)
24	execCode(webserver,apache)
25	hacl(webserver,database,dbProtocol,dbPort)
26	RULE 2 (remote exploit of a server program)
27	netAccess(webserver,tcp,80)
28	networkServiceInfo(webserver,httpd,tcp,80,apache)
29	vulExists(webserver,inputvalidation,httpd,remoteExploit ,privEscalation)
30	RULE 6 (direct network access)
31	hacl(internet,webserver,tcp,80)
32	attackerLocated(internet)
33	Internet Access
34	Main Vulnerability
35	Source IP address (223.29.208.30)

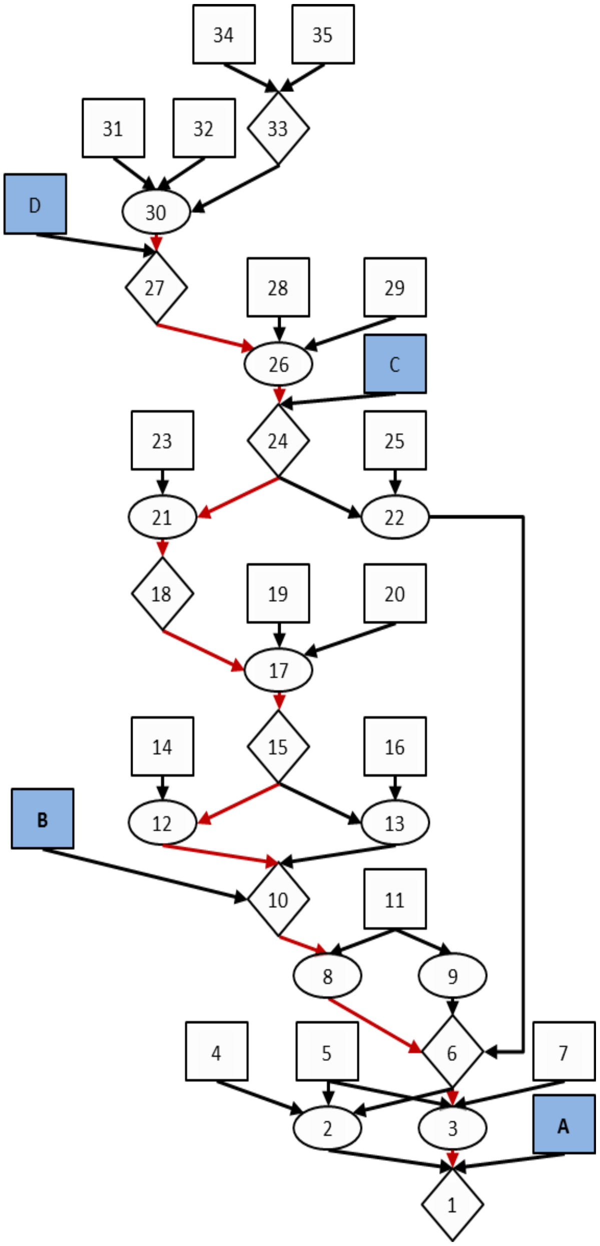


Figure 5.4. Attack graph with anti-forensic techniques

Table 5.4. Attack graph with anti-forensic techniques

Sl	Description
A	Delete file content
B	Delete log file
C	Disable event logging
D	Hide IP

Sl	Description
1	execCode(database,_)
2	RULE 2 (remote exploit of a server program)
3	RULE 2 (remote exploit of a server program)
4	vulExists(database,’SQLinjection’,mySQL,remoteExploit, privEscalation)
5	netAccess(database,dbProtocol,dbPort)
6	networkServiceInfo(database,mySQL,dbProtocol ,dbPort ,_)
7	vulExists(database,blindSQLinjection, mySQL,remoteExploit ,privEscalation)
8	RULE 5 (multi-hop access)
9	RULE 5 (multi-hop access)
10	execCode(’192.168.120.10’,root)
11	hacl(’192.168.120.10’,database,dbProtocol,dbPort)
12	RULE 1 (local exploit)
13	RULE 1 (local exploit)
14	vulExists(’192.168.120.10’,localVul_1,localApplication, localExploit,privEscalation)
15	execCode(’192.168.120.10’,user)
16	vulExists(’192.168.120.10’,localVul_0,localApplication, localExploit,privEscalation)
17	RULE 2 (remote exploit of a server program)
18	netAccess(’192.168.120.10’,httpProtocol,httpPort)
19	networkServiceInfo(’192.168.120.10’,serverApplication, httpProtocol,httpPort,user)
20	vulExists(’192.168.120.10’,remoteVul_1,serverApplication,remoteExploit,privEscalation)
21	RULE 5 (multi-hop access)
22	RULE 5 (multi-hop access)
23	hacl(webserver,’192.168.120.10’,httpProtocol,httpPort)
24	execCode(webserver,apache)
25	hacl(webserver,database,dbProtocol,dbPort)
26	RULE 2 (remote exploit of a server program)
27	netAccess(webserver,tcp,80)
28	networkServiceInfo(webserver,httpd,tcp,80,apache)
29	vulExists(webserver,inputvalidation,httpd,remoteExploit ,privEscalation)
30	RULE 6 (direct network access)
31	hacl(internet,webserver,tcp,80)
32	attackerLocated(internet)
33	Internet Access
34	Main Vulnerability
35	Source IP address (223.29.208.30)

5.3 Research Questions

From the literature review and review of similar studies in chapter 3, the main research question and secondary research questions were developed. In this section, the solution to the research question is described from the findings from the research in chapter 4. The discussion in the tables shown will provide a comparison for the pros and cons of the hypothesis/ sub-research questions. In conclusion, a concise summary of research question will be depicted.

5.3.1 Main Research Question and Associated Hypothesis

The derivation of the main research question postulates the key objective for different phases of experiments. The main research question portrayed was:

“Whether the effects of anti-forensic techniques can be reduced using the attack graph methodology?”

In order to find solutions to the main research question, different phases of experiments were proposed, experimental test bed was designed and conducted. Attack graph methodology was used for analysis of the network attacks in experiments. By finding the answers for the secondary questions, the solution to the main research question is derived.

Table 5.5 Secondary question 1 and solution

Secondary Question1: **“What are anti-forensic techniques and how it affects forensic procedure?”**
The literature review in the chapter 2 describes the anti-forensic techniques, its classification and tools for implementation of anti-forensics in attacks. Anti-forensics can be classified into mainly two kinds such as traditional anti-forensics and network anti-forensics. The traditional anti-forensics deals with deletion, destruction, and obfuscation of data and information from offline sources such as solid state drives, hard drives, external hard disks, USB and other portable storage devices. Network anti-forensics mainly deals with destruction, hiding and obfuscation of data and valuable information in network

packets and other network peripherals such as router and network drives. Routing table misconfiguration, proxy of IP address are some of the techniques of this type.

Effects of anti-forensic techniques in forensic procedure

The main phases of digital forensic process are evidence collection, identification of evidence and analysis. The collection of evidence is a crucial process in digital forensic process. Offline forensics collects evidence from static storage devices while on-line forensic process collects evidence from network traffics. When anti-forensic techniques are associated with attacks, the integrity of the evidence collected may change. There are anti-forensic techniques that even change the hash values of the evidence. For evidence collection, anti-forensic techniques misguide the forensic investigators in gathering incriminated evidence. Another challenge faced by the forensic investigators is that while performing forensic process, they are unaware that whether anti-forensic techniques have been incorporated by the attackers. Identification of anti-forensic techniques in evidence collected and on the crime detected is the main challenge. During the analysis phase of the forensic process, the effects of anti-forensic techniques hinder the process as it is time consuming for the forensic investigators to reduce their effects.

Suggested Solutions

The main solutions recommended are that the forensic procedure should incorporate another phase for identification of anti-forensic techniques and retrieve the evidence in original state. It should also include a phase for searching the presence of anti-forensic techniques.

Table 5.6 Secondary question 2 and its solution

Secondary Question 2**: "What are the key requirements for generation of attack graphs to identify the attack path?"**
The literature review describes the anti-forensics and its effects. The chapter 3 describes the research methodology and research design. For the purpose of answering the main research question, attack graph methodology is used. The related studies in chapter 3 explain the attack graphs and tools for generating the attack graphs. The key requirements for the generation of attack graphs are the network configurations of the network infrastructure, system configurations and vulnerabilities of the peripherals. Attack graphs generated shows the attack paths of all attacks with vulnerabilities exploited.

Table 5.7 Secondary question 3 and its solution

Secondary Question 3: **"How is the attack graph helpful in determining the occurrence of anti-forensic techniques in a particular attack and how it helps to improve the network security?"**
In order to find the answer to the research question developed, experimental methodology is utilized. Experiments are conducted to attain solutions to the secondary questions. Attack graphs are generated using the tool MULVAL. Four different experiments are conducted on different peripherals of the network infrastructure such as database server, web server and workstation. The experiments have mainly two phases which analyses the attacks using attack graphs. The attack graphs generated are analyzed manually. From the attack graph analysis in chapter 5 section 5.2, it can be concluded that the attack paths are identified from the attack graphs. From the attack graphs, the main attack strategies and vulnerabilities exploited.

The attack graphs are generated for attacks in database server and workstation which are mainly used for analysis of normal attacks and how attack propagates in a network. The introduction of new nodes in attack graphs for IP address and main vulnerability make the graph more precise and accurate which can be seen in the figure 5.3. Thus, it helps in identification of exact path from various paths generated. The introduction of anti-forensic techniques in network attacks is experimented in the second phase of the experiment. Attack graph generated conveys the application of anti-forensic techniques and gives exact location where they are applied. The figure 5.4 explains the attack graph generated with modified nodes.

The attack graph helps to identify the attack paths, modus of operation and strategy of the attacks. From the analysis of the graph, vulnerabilities of each peripheral can be identified and network professionals will be able to comprehend each stage of attack and take precautionary measures to defend. The key objective of the research question is to reduce the effect of anti-forensic techniques in network attacks. This is achieved using attack graph methodology. Penetration testing is one of the main testing strategies for network security improvement in corporations. This research helps the penetration tester to identify the network flaws with the help of this attack graphs. This also helps the network security professionals in collecting the exact evidence form exact location. They can also identify whether anti-forensic techniques are applied and has counterfeited the evidence.

5.4 Practical Implications and Justifications

From the analysis of anti-forensic techniques using attack graphs, it can be suggested that the methodology definitely conveys the solution to the main research question. The system is capable of providing an in-depth analysis of both normal attacks and anti-forensic techniques incorporated attacks. The survey of anti-forensic techniques in chapter 2 provides an exquisite study on the tools and techniques. The sections in the same provide survey of most kinds of network forensic tools and network monitoring systems.

In order to discover the effects of anti-forensic techniques in network attacks, experimental methodology using attack graphs are implemented on the research. During the first phase of the research, attack graphs are generated for normal attacks on database server and workstation. This helps to analyze the attack graphs and check whether the accurate paths are generated for the attacks implemented. Before the start of the second phase, an improvement in the attack graph is developed such as manual inclusion of additional node for the immediate IP address and the main vulnerability exploited. This helps to evaluate the attack graphs generated and improve the accuracy of the attack graph as one can easily find the exact path the attacker propagates. Thus it helps in locating the network flaws and vulnerabilities in a network.

For the future work, it is recommended that the generation of attack graph should be integrated with IDS systems and automated analysis of network flaws should be implemented. The research experiment conducted introduced new node by manual analysis of IDs alerts and logs. Development of simplified script for gathering information such as main vulnerability and the immediate IP address from where the attack occurred helps to improve the attack graph. If this code is developed in advanced stage such that automatic inclusion of these data gathered from the IDs alerts are integrated with MULVAL tool, more precise and accurate attack graphs can be generated. Thus, it helps in reducing the time of forensic process as well as penetration testers.

Chapter 6 Conclusions and Future Work

Security of network is one of the most concerned area any business corporation and industry. The main challenge of network security is to defend from the largest threat and attacks. In this current era of digital forensics, network forensics is one of the main challenging fields. Advancement in technology has strengthened the network security as well as the hackers. They develop complex tools and techniques to break security in networks to hack into systems. With the help of anti-forensics, counterfeiters are able to hide their source and misconfigure the system so that no evidence of their presence is identified during investigation.

At first, anti-forensics was confined only to storage devices and computer systems which help in hiding data in file systems, slack space and bad clusters. Network attacks incorporated with anti-forensic attacks has made the forensic investigators almost impossible to find the exact source of the attack and has become far more robust and intense way of attacking. Evidence collection, analysis and to find the trace route and source of attacks has become more challenging.

The anti-forensic techniques were then extended to computer networks which hides, deletes and obfuscate the evidence trace from the networks. The anti-forensic incorporated networks attacks are one of the most challenging to detect. The network security and forensic professionals trace down the source of the attacks using different tools. Once they trace down the IP address, it can be blocked. This happens only when an attack is detected. Tracing down the attacker becomes difficult due to anti-forensic techniques such as IP Proxy and Hide IP. The network forensic professionals may not be aware of the challenges and consequences of anti-forensic techniques. Thus, the thesis focuses on an in-depth survey of anti-forensic tools and techniques.

As the technology advances, network attacks have become more and more sophisticated. The analyses of network attacks are complex than forensic analysis of offline systems. Attack graphs provide a promising methodology to identify the potential attack paths using the vulnerabilities of system and network configurations. The current attack graphs generated by the tool MULVAL terminates, mentioning internet as the source of the attacker. In this section, we introduce additional nodes above the current attack graph for source IP address of the suspicious system and vulnerability is implemented. This introduction of main vulnerability node will helps in concrete and precise analysis of network attacks.

The research commences with the contextual literature review which explains the network forensic process and introduces the concept of anti-forensics. The concept of network anti-forensics and its techniques and tools are also known and understood from the literature review conducted on Chapter 2. The appendix A provides comparison of network security tools, network forensic tools and anti-forensic tools and techniques with their functions and features explained in detail. Identification of crucial evidence and network flaws in a particular network is the main focus of the research. The research gap is identified in the literature review with the help of approaches, methodologies and trends.

An in-depth survey focusing mainly about anti-forensic tools that is classified on the relevant techniques and on the algorithm they exploit was conducted. The survey not only dealt on combining anti-forensics with network attacks but also contained a review of common network attacks and network tools. Study of network attacks and collecting evidences are done with the help of network security and monitoring tools (NSMs and network forensics analysis tools (NFAT).

Validating the evidence is the main issue faced by the forensic investigators during the forensic process. Adding to that another issue is compromising on the integrity of the collected evidence. Hash analysis and signature analysis offer a level of support while examining the evidence at each stage. Hash collision techniques are helpful as well but they give an unclear picture to the investigators at times. The investigation process has to be carried out under a secure environment as Rootkits and compromised hosts can attack the process itself.

In order to discover about the vulnerabilities, a detailed study on the challenges and various issues on the tools and techniques has to be carried out. Unclear information can make anti-forensics techniques focus on vulnerabilities of digital forensic software. An in-depth investigation on anti-forensics techniques and network anti-forensics' has to be carried out in order to prevent those attacks.

The chapter 3 details the identified research problem and its related studies. The concept of network anti-forensics is explained in detail. From the related studies, the main research question and the sub questions are portrayed in the section 3.3. The research methodology and research design was proposed in order to find an appropriate and precise solution the research question identified. Experimental research methodology is chosen to refine valuable information with relevance to the hypothesis. The hypothesis developed from the research question is tested with a number of experiments. The experiments run on virtual simulation environments created on virtual machines. The associate data requirements and expected outcomes are also illustrated.

The solution to the research question is found from the experiments conducted. The main mode of approach for analysis of attacks on computer networks are network attack graphs. They provide valuable information regarding the path and mode of strategy of the attacks. The main aim of this approach is to find the preventive and precautionary measures in networks and cover the network flaws so that the effects of network attacks and anti-forensic techniques can be reduced and valid evidence can be collected. The main experimental structure and findings are explained in the chapter 4.

Chapter 5 details the main research analysis of the experiment conducted. The section 5.2 covers the attack graph analysis of the two phases of the experiment conducted. The answer to the research question and the significance of the analysis is presented in this chapter. This thesis identified a set of information relevance to the network security flaws and vulnerabilities. The thesis recommends extending the attack graph to the next level by addition of new nodes containing the immediate IP address and the main vulnerability exploited. The attack graph generated has shown many paths and to find the precise path, the main vulnerability exploited has to be identified. The attack graph optimization has to be carried out as the future work.

The main challenges of the research are that the experiments were conducted on a controlled environment and every time an attack is implemented, the original state of each and every peripheral has to be restored to conduct the next experiment. The research outlines the effects of anti-forensic techniques in attacks graphs generated from both phases. The chapter 5 finishes with the suggestions and recommendations for further research of anti-forensic tools and techniques. The thesis also recommends the further improvement of attack graphs on the minimization techniques to achieve greater precision on the attack path generated. The main limitations of the experiments are that the number of attacks utilized for analysis is confined to two. The experimentation of all anti-forensic techniques was not implemented and analyzed. One of the main limitations of the research is the manual comparison and correlation of IDS alert system with the vulnerability database to include the new nodes. Thus, it is recommended integration of attack graphs onto the IDS systems so that the network professionals would be aware of how and from where the attack or threat is coming and how it can be prevented.

Now-a-days most of the network attacks are incorporated with anti-forensic techniques which we define as network anti-forensics. In this thesis, we introduce network anti-forensic techniques and to the best of our knowledge this is the first time, network anti-forensics are analyzed using attack graphs. The network anti-forensic activity adversely affect the attack path and in a way making it profoundly complex. The main limitation of the research was the manual generation of attack graphs and the input parameters has to be fed manually. Implementation of a script code that collects necessary information form IDS alert logs and rules and insert these data to the input file of the MULVAL tool.

The future research should manipulate on active inclusion of anti-forensic techniques, it consequences and vulnerabilities exploited onto a database similar to NVD database. Addition of this database and implementing new rules helps in effective generation of attack graphs featuring anti-forensic techniques. Thus, Thesis shows that attack graphs are an effective methodology to analyze anti-forensic techniques. The contributions of the research help the network professionals to be forensically ready to analyze the major consequences of the anti-forensic techniques and adopt preventive and precautionary measures to reduce their effect and improve the network security and gather forensically sound evidence.

APPENDIX A

Network Forensic Analysis Tools

Table A shows the different network forensic tools used for network evidence analysis.

Network Forensic Tools	Functions	Features
NetDetector	Signature analyzing IDS is incorporated which detect known and unknown threats , analyzes network packets, provides email traffic monitoring, untrusted URL activity and helps to resolve sophisticated cyber security attacks, real time alerting on security and performance related events.	• Signature analysis tool • Event viewer • Application reconstruction tool. • Uses a Flash-based web interface.
Network Miner v1.0	Packet Capturing tool which collects data regarding operating systems and open ports. It is a passive sniffer and the. Files are extracted using parsing PCAP file.	• Offline Analysis • Supported protocols are FTO, HTTP, SMB and TFTP
Iris v5.1.065	Analyzes the network traffic and reassembles in its own format and reconstructs the session and packets. Also used for Electronic Discovery.	Service oriented architecture for packet capture Statistical measurement for packet size and protocol distribution Reconstruction of Email messages, Web Browsing Sessions and Instant Message Sessions.
Xplico v1.0.0	Network traffic Capturing and is a protocol analyzer which has multithreading, TCP reassembling and Reverse DNS look up option for better analysis and result is presented in a visual form.	Data capture Real time Acquisition Reverse DNS Look-up
Silent Runner	Network Packet capturing, analyzing, host detection and anomaly detection is the main function. Reverse engineering of events, actual network traffic and security incidents in the proper sequence are the main features..	Real Time Data Capture Incident Response Graphical Visualization of Result
Kismet	For 802.11 layer 2 wireless network capturing, analysis and intrusion detection system. Detects hidden networks, passive collection	802.11b, 802.11g, 802.11a, 802.11n sniffing Multi-card and channel hopping support

	of network packets (TCP, ARP, DHCP and UDP).	Runtime WEP decoding Tap virtual network interface drivers for real time export of packets Hidden SSID de-cloaking Distributed remote sniffing with Kismet drones and XML Logging
Solera Network DS Series Applications	Mainly used for Packet Capture, Network Forensics and Security Intelligence and Analytics The DeepSee forensic suite reconstructs network attributes such as web pages, pdf files and images	High speed data capture application for network traffic Reconstruction and sequencing

APPENDIX B

Network Security and Monitoring Tools

Table B below shows the main network security and monitoring tools used for the evidence collection and analysis.

Network Monitoring tools	Functions	Features
TCP Dump	Packet sniffer for Protocol debugging and acquisition of data. Used for trouble shooting network activity and diagnosis of DoS attacks and has the "Berkley Packet Filter" (BPF)	Command line tool a portable C/C++ library for network traffic
TCPFlow	Investigation and management of network traffic and data flow in TCP/IP network. Captured file stored separately and reconstructs the data stream.	Protocol Analysis Packet Capture
Nmap	Network Mapper used for security auditing. The GUI module is Zenmap. Raw Ip packets are used for various functionalities.	Port Scanning OS Detection
TCPDStat	Reads TCPdump files with the aid of the pcap library and finds the trace. Gives a vague idea of content of the trace. Output may include protocol breakdowns, source and destination address and number of packets.	Protocol Break Down PCAP Library High level traffic pattern monitoring
WireShark	Protocol Analyzer which provide in depth inspection of protocol, live capture, VOIP analysis.	Rich Display Filter Can run on multiple platforms such as Windows, LINUX and Solaris Supports more than 100 protocols
Ethereal	Open Source Packet Analyzer which has filter capabilities and works in both promiscuous and non-promiscuous mode.	Reconstructs TCP session Captures data from Ethernet, token ring and 802.11 wireless
Snort v2.9.3.1	It's an Open Source IPS/IDS which incorporates	Supports Unix and Windows platforms

	signature, anomaly-based and protocol inspection. Protocol analysis and content searching are the main function.	
Bro	Network analysis framework with IDS. In-depth analysis of protocols and can be used in high performance networks, focus on application level.	Protocol Analysis Semantic analysis and thorough activity logging

APPENDIX C

Anti-forensics Tools

The table C shows the features and functions of different anti-forensic tools.

Technique	Tools	Functions	Features
Data Destruction			
Physical	Magnetic fields	Degaussing the medium such as hard disks and other storage devices	
Logical			
	Drive Scrubber 3	Permanently and securely deletes data form drives. It also wipes free spaces	Wipes entire drive Clean and Restores Supports SATA, USB and SCSI.
	Active Eraser and Active Kill Disk v6.0	Destroys all the data securely. It erases partitions, unused space and logical drives. Supports all formats such as FAT and NTFS. Erases Internet Activities (temporary internet files, cookies, history, etc.) Wipes out drive's free space out of previously deleted data	*Securely overwrites and destroys all data on physical drive or logical partition *Supports IDE / ATA / SCSI hard disk, HDD / Floppies / Zip / FlashMedia drives disk eraser software *Supports large (more than 128GB) size drives *Data verification could be performed after erasing is completed *Scan drives and preview files on FAT, FAT32 and NTFS before erasing *Can be placed and run from USB Disk
	Disk Wipe2.3.1	Secure file wiping application which uses quick format before disk wiping for better performance and replaces the 0's and 1's with all zeros or ones new data	S-ATA (SATA), IDE, SCSI, USB and FIREWIRE interfaces are supported.
Data Hiding			
Slack space	Slacker	All these applications hide the data in slack space, bad cluster of NTFS file system, and rootkit	
	FragFS,		
	Rootkit		
Encryption	TrueCrypt	Tools are used to encrypt the drives for	Creates a virtual encrypted disk within a file and mounts it as a real

		protection and inaccessibility. Algorithms such as AES, RSA and Blowfish are mainly used. Encrypts an entire partition or storage device such as USB flash drive or hard drive. Encrypts a partition or drive where Windows is installed (pre-boot authentication).	disk. Encryption is automatic, real-time (on-the-fly) and transparent. Parallelization and pipelining allow data to be read and written as fast as if the drive was not encrypted. Encryption can be hardware-accelerated on modern processors. Provides plausible deniability, in case an adversary forces you to reveal the password:
Steganogra-phy	Steghide	Hides data files in images, audio and video files, especially pictures.	Compression of embedded data Encryption of embedded data Embedding of a checksum to verify the integrity of the extracted data Support for JPEG, BMP, WAV and AU files
	Stegdetect	Stegdetect can detecting hidden content in the file	Only reports images that are likely to have steganographic content. -h Only calculates the DCT histogram. Use the -d option to display the values. -n Enables checking of JPEG header information to suppresses false-positives. If enabled, all JPEG images that contain common fields will be treated as negatives. Out Guess checking will be disabled if the JFIF marker does not match version 1.1.
Network Steganography tools	Stegtunnel	Using covert channels for communication using HTTP GET request and TCP connection.	It can hide the data underneath real TCP connections, using real, unmodified clients and servers to provide the TCP conversation. In this way, detection of odd-looking sessions is avoided. It provides covert channels in the sequence numbers and IPIDs of TCP connections.
	Hcovert		Latest version added a reliable file transfer mode using Hamming-style error correction, and removes the requirement for a proxy IP address on some operating systems.
	Socat	Socat is a command	It supports broadcasts and multicasts,

		line tool which creates packets for IP6, IP4, TCP and UDP protocols.	abstract Unix sockets, Linux tun/tap, GNU readline, and PTYs. It provides forking, logging, and dumping and different modes for interprocess communication. Many options are available for tuning socat and its channels. Socat can be used, for example, as a TCP relay (one-shot or daemon), as a daemon-based socksifier, as a shell interface to Unix sockets, as an IP6 relay, or for redirecting TCP-oriented programs to a serial line.
	OpenPuff	OpenPuff supports many carrier formats such as images, audio and video.	-*lets users hide data in more than a single carrier file. When hidden data are split among a set of carrier files you get a carrier chain, with no enforced hidden data theoretical size limit (256MB, 512MB, ... depending only on the implementation) *implements 3 layers of hidden data obfuscation (cryptography, whitening and encoding) *extends deniable cryptography into deniable steganography
Hide IP	A4 Proxy	Anonymity 4 Proxy is mainly used for active hiding of IP address while surfing. Generates fake IP address, block cookies and modifies HTTP variables. Also used for sharing internet connection with other users over a LAN.	Confuse the websites further by sending them a fake IP address along with your requests Download files with programs like GetRight and other download managers staying anonymous to the sites from which you download Learn more about the inside of the Internet and how it works Thoroughly check the anonymity status of proxy servers and their performance Choose to use only those proxies that meet particular anonymity requirements *A4Proxy supports HTTP (websites), Secure HTTP (HTTPS, SSL - secure websites) and FTP protocols. Use a different anonymous proxy server for each request Block cookies, and selectively modify any information sent out by your browser. Find the anonymous proxy server

			which is the fastest for your location or the fastest for a particular URL (ftp server or website) Simulate ordinary requests, as if they are made not through a proxy but directly *Simulate non-anonymous requests from proxy servers with randomly-selected IP addresses Redirect and modify HTTP-requests to anonymous proxy servers according to the rules defined by yourself Use Stop-Lists for sites and network clients Associate each computer in your LAN with its own anonymous proxy server
Data/ Trail Obfuscation			
IP spoofing, MAC Spoofing, SMTP Proxies, Log Cleaners	Obfuscate payload	Obfuscate pay load to bypass the SNORT IDS	
Others	Back Track 5 R2 – OS	The latest version of this Linux OS contains more than 150 anti-forensic tools. This is one of the best OS to carry out the experiments with the tools and techniques.	
	Metaslpoit framework SamJuicer Slacker Timestomp	Sam Juicer — acquires the hashes from the NT Security Access Manager (SAM) files without changing the data on the hard disk, Slacker — hides files within the slack space of the NT file system (NTFS) Time stomp — alters all four NTFS file times: modified, access, creation, and file entry update.	

	Evidence Eliminator	In-depth wiping of data from storage devices. Deletes all the files including plug-in modules, slack space. It deletes and modifies the date and time of all files including the windows registry and log files.	This software deletes files so effectively that they can’t be recovered by any of the current commercial or government recovery methods. Remove the traces of files and your internet history so that they can’t be recovered. Removal tools for both your online activity and offline

References

Albanese, M., Jajodia, S., Pugliese, A., & Subrahmanian, V. S. (2011). Scalable Analysis of Attack Scenarios. In V. Atluri & C. Diaz (Eds.), *Computer Security – ESORICS 2011* (Vol. 6879, pp. 416-433): Springer Berlin Heidelberg. doi:10.1007/978-3-642-23822-2_23

Almulhem, A. (2009). Network Forensics: Notions and Challenges. Symposium conducted at the meeting of the IEEE International Symposium on Signal Processing and Information Technology (ISSPIT), 2009 doi:10.1109/isspit.2009.5407485

Ammann, P., Wijesekera, D., & Kaushik, S. (2002). Scalable, graph-based network vulnerability analysis *ACM.* Symposium conducted at the meeting of the Proceedings of the 9th ACM conference on Computer and communications security, Washington, DC, USA. doi:10.1145/586110.586140

Anming, X., Zhuhua, C., Cong, T., Jianbin, H., & Zhong, C. (2009). Evaluating Network Security With Two-Layer Attack Graphs Symposium conducted at the meeting of the Annual Computer Security Applications Conference, 2009. ACSAC '09. doi:10.1109/acsac.2009.22

Arnold, T., & Yang, T. A. (2011). Rootkit attacks and protection: A case study of teaching network security. *Journal of Computing Sciences in Colleges, 26*(5), 122-129.

Azadegan, S., Yu, W., Liu, H., Sistani, M., & Acharya, S. (2012). Novel Anti-forensics Approaches for Smart Phones. *45th Hawaii International Conference on System Science (HICSS), 2012* 5424-5431. doi:10.1109/hicss.2012.452

Baier, H., & Breitinger, F. (2011). Security Aspects of Piecewise Hashing in Computer Forensics. Symposium conducted at the meeting of the Sixth International Conference on IT Security Incident Management and IT Forensics (IMF), 2011 doi:10.1109/imf.2011.16

Barford, P., Kline, J., Plonka, D., & Ron, A. (2002). A signal analysis of network traffic anomalies. *ACM.* Symposium conducted at the meeting of the

Proceedings of the 2nd ACM SIGCOMM Workshop on Internet measurment, Marseille, France. doi:10.1145/637201.637210

Barnes, J. A., & Harary, F. (1983). Graph theory in network analysis. *Social Networks, 5*(2), 235-244. doi:10.1016/0378-8733(83)90026-6

Benjamin, T., & Jill, S. (2007, Jan. 2007). Wireless Forensic Analysis Tools for Use in the Electronic Evidence Collection Process. Symposium conducted at the meeting of the 40th Annual Hawaii International Conference on System Sciences, 2007. HICSS 2007. doi:10.1109/hicss.2007.617

Berghel, H. (2003). The discipline of Internet forensics. *Communications of the ACM, 46*(8), 15-20.

Berghel, H. (2007). Hiding data, forensics, and anti-forensics. *Communications of the ACM, 50*(4), 15-20.

Beverly, R., Garfinkel, S., & Cardwell, G. (2011). Forensic carving of network packets and associated data structures. *Digital Investigation, 8, Supplement*(0), S78-S89. doi:10.1016/j.diin.2011.05.010

Boran, S. (1999). *An Overview of Corporate Information Security*. Retrieved April, 2012, from http://boran.com/security/sp/security_space.html

Bosheng, Z., Marshall, A., Wenzhe, Z., & Kun, Y. (2008, 19-23 May 2008). A Random Packet Destruction DoS Attack for Wireless Networks Symposium conducted at the meeting of the IEEE International Conference on Communications, 2008. ICC '08. doi:10.1109/icc.2008.320

Bosschert, T. (2007). Battling Anti-Forensics: Beating the U3 Stick. *Journal of Digital Forensic Practice, 1*(4), 265-273. doi:10.1080/15567280701417975

Bursztein, E., & Mitchell, J. (2011). Using Strategy Objectives for Network Security Analysis. In F. Bao, M. Yung, D. Lin, & J. Jing (Eds.), *Information Security and Cryptology* (Vol. 6151, pp. 337-349): Springer Berlin Heidelberg. doi:10.1007/978-3-642-16342-5_25

Caloyannides, M. A. (2009). Forensics Is So "Yesterday". *Security & Privacy, IEEE, 7*(2), 18-25. doi:10.1109/msp.2009.37

Cao, G., Zhao, Y., Ni, R., & Tian, H. (2010). Anti-forensics of contrast enhancement in digital images. *ACM.* Symposium conducted at the meeting of the Proceedings of the 12th ACM workshop on Multimedia and security, Roma, Italy. doi:10.1145/1854229.1854237

Catania, C. A., & Garino, C. G. (2012). Automatic network intrusion detection: Current techniques and open issues. *Computers & Electrical Engineering, 38*(5), 1062-1072. doi:10.1016/j.compeleceng.2012.05.013

Chan, E., Venkataraman, S., Tkach, N., Larson, K., Gutierrez, A., & Campbell, R. H. (2011). Characterizing data structures for volatile forensics. Symposium conducted at the meeting of the Sixth International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE), IEEE , 2011

Chandankhede, P. H., & Nimbhorkar, S. U. (2012). Autonomous Network Security for Detection of Network Attacks. *International Journal of Science and Research Publications, 2*(1).

Changwei, L., Singhal, A., & Wijesekera, D. (2012, 20-24 Aug. 2012). Using Attack Graphs in Forensic Examinations Symposium conducted at the meeting of the Seventh International Conference on Availability, Reliability and Security (ARES), 2012 doi:10.1109/ares.2012.58

Cheng, F., Roschke, S., & Meinel, C. (2011). An Integrated Network Scanning Tool for Attack Graph Construction. In J. Riekki, M. Ylianttila, & M. Guo (Eds.), *Advances in Grid and Pervasive Computing* (Vol. 6646, pp. 138-147): Springer Berlin Heidelberg. doi:10.1007/978-3-642-20754-9_15

Chris B. Simmons, Danielle L. Jones, & Lakisha L. Simmons. (2011). A Framework and Demo for Preventinf Anti-Computer Forensics. *Issues in Information Systems, 12*(1), 366-372.

Cohen, F. (2009). Bulk Email Forensics In G. Peterson & S. Shenoi (Eds.), (Vol. 306, pp. 51-67): Springer Boston. doi:10.1007/978-3-642-04155-6_4

Dahbur, K., & Mohammad, B. (2011). The anti-forensics challenge *ACM.* Symposium conducted at the meeting of the Proceedings of the 2011 International Conference on Intelligent Semantic Web-Services and Applications Amman, Jordan. doi:10.1145/1980822.1980836

Dahbur, K., & Mohammad, B. (2011). Toward Understanding the Challenges and Countermeasures in Computer Anti-Forensics. *International Journal of Cloud Applications and Computing (IJCAC), 1*(3), 22-35.

Diamah, A., Mohammadian, M., & Balachandran, B. (2012). Network Security Evaluation Method via Attack Graphs and Fuzzy Cognitive Maps. In J. Watada, T. Watanabe, G. Phillips-Wren, R. J. Howlett, & L. C. Jain (Eds.), *Intelligent Decision Technologies* (Vol. 16, pp. 433-440): Springer Berlin Heidelberg. doi:10.1007/978-3-642-29920-9_44

Ding, X., & Zou, H. (2011). Time based data forensic and cross-reference analysis. *ACM.* Symposium conducted at the meeting of the Proceedings of the 2011 ACM Symposium on Applied Computing, TaiChung, Taiwan. doi:10.1145/1982185.1982227

Distefano, A., Me, G., & Pace, F. (2010). Android anti-forensics through a local paradigm. *Digital Investigation, 7, Supplement*(0), S83-S94. doi:10.1016/j.diin.2010.05.011

Eggendorfer, T. (2008). Methods to identify spammers. *ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering).* Symposium conducted at the meeting of the Proceedings of the 1st international conference on Forensic applications and techniques in telecommunications, information, and multimedia and workshop, Adelaide, Australia.

Endicott-Popovsky, B., & Frincke, D. (2007). Embedding Hercule Poirot in Networks: Addressing Inefficiencies in Digital Forensic Investigations In D. Schmorrow & L. Reeves (Eds.), *Foundations of Augmented Cognition* (Vol. 4565, pp. 364-372): Springer Berlin / Heidelberg. doi:10.1007/978-3-540-73216-7_41

Fairbanks, K. D., Lee, C. P., Xia, Y. H., & Owen, H. L. (2007). TimeKeeper: A Metadata Archiving Method for Honeypot Forensics. *Information Assurance and Security Workshop, 2007. IAW '07. IEEE SMC*, 114-118. doi:10.1109/iaw.2007.381922

Fen, Y., Xinchun, Y., & Hao, H. (2012). An Network Attack Modeling Method Based on MLL-AT. *Physics Procedia, 24, Part C*(0), 1765-1772. doi:10.1016/j.phpro.2012.02.260

Forte, D. (2008). Dealing with forensic software vulnerabilities: Is anti-forensics a real danger? *Network Security, 2008*(12), 18-20. doi:10.1016/s1353-4858(08)70143-0

Forte, D., & Power, R. (2007). A tour through the realm of anti-forensics. *Computer Fraud &amp; Security, 2007*(6), 18-20. doi:10.1016/s1361-3723(07)70079-9

Goodall, J. R., Lutters, W. G., Rheingans, P., & Komlodi, A. (2006). Focusing on Context in Network Traffic Analysis. *IEEE Computer Graphics and Applications, 26*(2), 72-80. doi:10.1109/mcg.2006.31

Gorodetski, V., & Kotenko, I. (2002). Attacks against Computer Network: Formal Grammar-Based Framework and Simulation Tool. In A. Wespi, G. Vigna, & L. Deri (Eds.), *Recent Advances in Intrusion Detection* (Vol. 2516, pp. 219-238): Springer Berlin / Heidelberg. doi:10.1007/3-540-36084-0_12

GS Dardick, & Roche, C. L. (2007). BLOGS: Anti-Forensics and Counter Anti-Forensics. Symposium conducted at the meeting of the Australian Digital Forensics Conference

Harbort, Z., Louthan, G., & Hale, J. (2011). Techniques for attack graph visualization and interaction *ACM.* Symposium conducted at the meeting of the Proceedings of the Seventh Annual Workshop on Cyber Security and Information Intelligence Research, Oak Ridge, Tennessee. doi:10.1145/2179298.2179383

Harris, R. (2006). Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem. *Digital Investigation, 3, Supplement*(0), 44-49. doi:10.1016/j.diin.2006.06.005

Harshbarger, B. (2010). Social Networking Websites as a Tool for Investigators. *Journal of Network Forensics*, 25.

Hart, C. (2013). Graph Theory Topics in Computer Networking.

Hartley, W. M. (2007). Current and Future Threats to Digital Forensics. *ISSA Journal*.

Heydari, S., Martin, M. V., Rjaibi, W., & Lin, X. (2010). *Emerging trends in network forensics*: IBM Corporation.

Hilley, S. (2007). Anti-forensics with a small army of exploits. *digital investigation*, *4*(1), 13-15. doi:10.1016/j.diin.2007.01.005

Homer, J., Varikuti, A., Ou, X., & McQueen, M. (2008). Improving Attack Graph Visualization through Data Reduction and Attack Grouping. In J. Goodall, G. Conti, & K.-L. Ma (Eds.), *Visualization for Computer Security* (Vol.

5210, pp. 68-79): Springer Berlin Heidelberg. doi:10.1007/978-3-540-85933-8_7

Hunt, R., & Slay, J. (2010, 17-19 Aug. 2010). Achieving critical infrastructure protection through the interaction of computer security and network forensics Symposium conducted at the meeting of the Eighth Annual International Conference on Privacy Security and Trust (PST), 2010 doi:10.1109/pst.2010.5593243

Idika, N., & Bhargava, B. (2012). Extending Attack Graph-Based Security Metrics and Aggregating Their Application. *IEEE Transactions on Dependable and Secure Computing, 9*(1), 75-85. doi:10.1109/tdsc.2010.61

Ingols, K., Chu, M., Lippmann, R., Webster, S., & Boyer, S. (2009, 7-11 Dec. 2009). Modeling Modern Network Attacks and Countermeasures Using Attack Graphs Symposium conducted at the meeting of the Computer Security Applications Conference, ACSAC doi:10.1109/acsac.2009.21

Jantan, A., Rasmi, M., Ibrahim, M., & Rahman, A. A. (2012). A Similarity Model to Estimate Attack Strategy Based on Intentions Analysis for Network Forensics. In *Recent Trends in Computer Networks and Distributed Systems Security* (Vol. 335, pp. 336-346): Springer Berlin Heidelberg. doi:10.1007/978-3-642-34135-9_34

Jha, S., Sheyner, O., & Wing, J. (2002). Two formal analyses of attack graphs Symposium conducted at the meeting of the 15th IEEE Proceedings Computer Security Foundations Workshop doi:10.1109/csfw.2002.1021806

Jian, B., Chang-peng, J., & Mo, G. (2010, 22-24 Oct. 2010). Research on network security of defense based on Honeypot. Symposium conducted at the meeting of the International Conference on Computer Application and System Modeling (ICCASM), 2010 doi:10.1109/iccasm.2010.5622780

Jiang, D., & Shuai, G. (2011). Research on the clients of network forensics. Symposium conducted at the meeting of the 3rd International Conference on Computer Research and Development (ICCRD), 2011 doi:10.1109/iccrd.2011.5764059

Jing, D., Han, R., & Mishra, S. (2004). Intrusion tolerance and anti-traffic analysis strategies for wireless sensor networks. Symposium conducted at the meeting of the International Conference on Dependable Systems and Networks, 2004 doi:10.1109/dsn.2004.1311934

Johansson, C. (2002). Forensic and Anti-Forensic Computing.

Katipally, R., Yang, L., & Liu, A. (2011). Attacker behavior analysis in multi-stage attack detection system. *ACM.* Symposium conducted at the meeting of the Proceedings of the Seventh Annual Workshop on Cyber Security and Information Intelligence Research

Kessler, G. C. (2007). Anti-forensics and the digital investigator

Khaitan, S., & Raheja, S. (2011). Finding optimal attack path using attack graphs: a survey. *International Journal of Soft Computing and Engineering, 1*(3), 2231-2307.

Kiley, M., Dankner, S., & Rogers, M. (2008). Forensic Analysis of Volatile Instant Messaging. In I. Ray & S. Shenoi (Eds.), *Advances in Digital Forensics IV* (Vol. 285, pp. 129-138): Springer US. doi:10.1007/978-0-387-84927-0_11

Kotenko, I., & Stepashkin, M. (2006). Attack Graph Based Evaluation of Network Security. In H. Leitold & E. Markatos (Eds.), *Communications and Multimedia Security* (Vol. 4237, pp. 216-227): Springer Berlin Heidelberg. doi:10.1007/11909033_20

Krawetz, N. (2004). Anti-honeypot technology. *Security & Privacy, IEEE, 2*(1), 76-79. doi:10.1109/msecp.2004.1264861

Levi, A., & Güder, C. B. (2009). Understanding the limitations of S/MIME digital signatures for e-mails: A GUI based approach. *Computers & Security, 28*(3–4), 105-120. doi:10.1016/j.cose.2008.09.003

Lewthwaite, J., & Smith, V. (2008). Limewire examinations. *Digital Investigation, 5, Supplement*(0), S96-S104. doi:10.1016/j.diin.2008.05.017

Li, Z.-t., Lei, J., Wang, L., & Li, D. (2007). A data mining approach to generating network attack graph for intrusion prediction *IEEE.* Symposium conducted at the meeting of the Fourth International Conference on Fuzzy Systems and Knowledge Discovery, 2007. FSKD 2007.

Lubacz, J., Mazurczyk, W., & Szczypiorski, K. (2012). Principles and Overview of Network Steganography. *ArXiv e-prints*.

Mansfield-Devine, S. (2010). Fighting forensics. *Computer Fraud and Security, 2010*(1), 17-20. doi:10.1016/s1361-3723(10)70112-3

Meghanathan, N., Allam, S. R., & Moore, L. A. (2009). Tools and Techniques For Network Forensics. *International Journal of Network Security & Its Applications, 1*(1).

Nikkel, B. J. (2006). Improving evidence acquisition from live network sources. *Digital Investigation, 3*(2), 89-96.

Nilsson, D. K., & Larson, U. E. (2008). Conducting forensic investigations of cyber attacks on automobile in-vehicle networks. *ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering).* Symposium conducted at the meeting of the Proceedings of the 1st international conference on Forensic applications and techniques in telecommunications, information, and multimedia and workshop, Adelaide, Australia.

Ou, X., Boyer, W. F., & McQueen, M. A. (2006). A scalable approach to attack graph generation *ACM.* Symposium conducted at the meeting of the Proceedings of the 13th ACM conference on Computer and Communications Security

Ou, X., Govindavajhala, S., & Appel, A. W. (2005). MulVAL: a logic-based network security analyzer*USENIX Association.* Symposium conducted at the meeting of the Proceedings of the 14th conference on USENIX Security Symposium, Baltimore, MD.

Ou, X., & Singhal, A. (2011). Attack Graph Techniques. In *Quantitative Security Risk Assessment of Enterprise Networks* (pp. 5-8): Springer New York. doi:10.1007/978-1-4614-1860-3_2

Pajek, P., & Pimenidis, E. (2009). Computer Anti-forensics Methods and Their Impact on Computer Forensic Investigation Global Security, Safety, and Sustainability. In H. Jahankhani, A. G. Hessami, & F. Hsu (Eds.), (Vol. 45, pp. 145-155): Springer Berlin Heidelberg. doi:10.1007/978-3-642-04062-7_16

Panko, R. R. (2010). *Corporate computer and network security* (2nd ed.). Boston: Prentice Hall.

Peron, C. S. J., & Legary, M. (1995). Digital Anti-Forensics: Emerging trends in data transformation techniques.

Pietro Albano, Aniello Castiglione, Giuseppe Cattaneo, & Alfredo De Santis. (2011). A Novel Anti-forensics Technique for the Android OS. Symposium conducted at the meeting of the International Conference on Broadband and Wireless Computing, Communication and Applications

Pilli, E. S., Joshi, R. C., & Niyogi, R. (2010). Network forensic frameworks: Survey and research challenges. *Digital Investigation, 7*(1-2), 14-27. doi:10.1016/j.diin.2010.02.003

Pollitt, M. (2008). Applying Traditional Forensic Taxonomy to Digital Forensics. . In I. Ray & S. Shenoi (Eds.), *Advances in Digital Forensics IV* (Vol. 285, pp. 17-26): Springer US. doi:10.1007/978-0-387-84927-0_2

Rasmi, M., & Jantan, A. (2011). Attack Intention Analysis Model for Network Forensics. . In J. M. Zain, W. M. b. Wan Mohd, & E. El-Qawasmeh (Eds.), *Software Engineering and Computer Systems* (Vol. 180, pp. 403-411): Springer Berlin Heidelberg. doi:10.1007/978-3-642-22191-0_35

Rekhis, S., & Boudriga, N. (2010a). Formal Digital Investigation of Anti-forensic Attacks. Symposium conducted at the meeting of the Fifth IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE), 2010 doi:10.1109/sadfe.2010.9

Rekhis, S., & Boudriga, N. (2010b). Formal Digital Investigation of Anti-forensic Attacks. Symposium conducted at the meeting of the Fifth IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE), 2010 doi:10.1109/sadfe.2010.9

Rekhis, S., & Boudriga, N. (2012). A System for Formal Digital Forensic Investigation Aware of Anti-Forensic Attacks. *IEEE Transactions on Information Forensics and Security, 7*(2), 635-650. doi:10.1109/tifs.2011.2176117

Roschke, S., Cheng, F., Schuppenies, R., & Meinel, C. (2009). Towards Unifying Vulnerability Information for Attack Graph Construction. In *Information Security* (pp. 218-233): Springer.

Roschke, S., Feng, C., & Meinel, C. (2010). Using vulnerability information and attack graphs for intrusion detection. Symposium conducted at the meeting of the Sixth International Conference on Information Assurance and Security (IAS) doi:10.1109/isias.2010.5604041

Saad, S., & Traore, I. (2010). Method ontology for intelligent network forensics analysis. *IEEE.* Symposium conducted at the meeting of the Eighth Annual International Conference on Privacy Security and Trust (PST), 2010

Samalekas, K. (2010). *Network Forensics: Following the Digital Trail in a Virtual Environment* University of Gothenburg.

Sang Su, L., Ku-Young, C., Deokgyu, L., & Do won, H. (2007). A New Anti-Forensic Tool Based on a Simple Data Encryption Scheme Symposium conducted at the meeting of the Future Generation Communication and Networking (FGCN 2007) doi:10.1109/fgcn.2007.21

Sartin, B. (2006). Anti-Forensics – Distorting the evidence. *Computer Fraud and Security, 2006*(5), 4-6. doi:10.1016/s1361-3723(06)70354-2

Schlicher, B. (2008). Emergence of cyber anti-forensics impacting cyber security *ACM.* Symposium conducted at the meeting of the Proceedings of the 4th annual workshop on Cyber security and information intelligence research: Developing strategies to meet the cyber security and information intelligence challenges ahead, Oak Ridge, Tennessee. doi:10.1145/1413140.1413166

Shanmugam, K., Powell, R., & Owens, T. (2011). An Approach for Validation of Digital Anti-Forensic Evidence. *Information Security Journal: A Global Perspective, 20*(4-5), 219-230. doi:10.1080/19393555.2011.604667

Shaojun, Z., Lan, L., Jianhua, L., Shanshan, S., & Xiuzhen, C. (2009). Using attack graphs and intrusion evidences to extrapolate network security state. Symposium conducted at the meeting of the Fourth International Conference on Communications and Networking in China, 2009. ChinaCOM 2009. doi:10.1109/chinacom.2009.5339841

Sheyner, O., Haines, J., Jha, S., Lippmann, R., & Wing, J. M. (2002). Automated generation and analysis of attack graphs. Symposium conducted at the meeting of the IEEE Symposium on Security and Privacy, 2002. Proceedings. doi:10.1109/secpri.2002.1004377

Sheyner, O., & Wing, J. (2004). Tools for Generating and Analyzing Attack Graphs. In F. Boer, M. Bonsangue, S. Graf, & W.-P. Roever (Eds.), *Formal Methods for Components and Objects* (Vol. 3188, pp. 344-371): Springer Berlin Heidelberg. doi:10.1007/978-3-540-30101-1_17

Singhal, A., & Ou, X. (2012). Quantitative Security Risk Assessment of Enterprise Networks. *SpringerBriefs in Computer Science*. doi:10.1007/978-1-4614-1860-3_3

Smith, A. (2007). Describing and Categorizing Disk-Avoiding Anti-Forensics Tools. *Journal of Digital Forensic Practice, 1*(4), 309-313. doi:10.1080/15567280701418155

Suhyung, J., & Dowon, H. (2008, 14-17 Oct. 2008). Defense technology of anti forensic Symposium conducted at the meeting of the International Conference on Control, Automation and Systems, 2008. ICCAS 2008. doi:10.1109/iccas.2008.4694617

Sy, B. K. (2009). Integrating intrusion alert information to aid forensic explanation: An analytical intrusion detection framework for distributive IDS. *Information Fusion, 10*(4), 325-341. doi:10.1016/j.inffus.2009.01.001

Szczypiorski, K. (2009). A Performance Analysis of HICCUPS--A Steganographic System for WLAN. *International Conference on Multimedia Information Networking and Security, 2009. MINES '09. , 1*, 569-572. doi:10.1109/mines.2009.248

Taylor, M., Haggerty, J., Gresty, D., & Berry, T. (2011). Digital evidence from peer-to-peer networks. *Computer Law & Security Review, 27*(6), 647-652.

Vasiliadis, G., Antonatos, S., Polychronakis, M., Markatos, E., & Ioannidis, S. (2008). Gnort: High Performance Network Intrusion Detection Using Graphics Processors. . In R. Lippmann, E. Kirda, & A. Trachtenberg (Eds.), *Recent Advances in Intrusion Detection* (Vol. 5230, pp. 116-134): Springer Berlin / Heidelberg. doi:10.1007/978-3-540-87403-4_7

Velupillai, H., & Mokhonoana, P. (2008). Evaluation of Registry Data Removal by Shredder Programs. . In I. Ray & S. Shenoi (Eds.), *Advances in Digital Forensics IV* (Vol. 285, pp. 51-58): Springer US. doi:10.1007/978-0-387-84927-0_5

Wang, L., Liu, A., & Jajodia, S. (2006). Using attack graphs for correlating, hypothesizing, and predicting intrusion alerts. *Computer Communications, 29*(15), 2917-2933.

Wang, L., Noel, S., & Jajodia, S. (2006). Minimum-cost network hardening using attack graphs. *Computer Communications, 29*(18), 3812-3824. doi:10.1016/j.comcom.2006.06.018

Wang, L., Singhal, A., & Jajodia, S. (2007a). Measuring the Overall Security of Network Configurations Using Attack Graphs. . In S. Barker & G.-J. Ahn (Eds.), *Data and Applications Security XXI* (Vol. 4602, pp. 98-112): Springer Berlin Heidelberg. doi:10.1007/978-3-540-73538-0_9

Wang, L., Singhal, A., & Jajodia, S. (2007b). Toward measuring network security using attack graphs. *ACM.* Symposium conducted at the meeting of the Proceedings of the 2007 ACM workshop on Quality of protection, Alexandria, Virginia, USA. doi:10.1145/1314257.1314273

Wang, W., & Daniels, T. E. (2008). A Graph Based Approach Toward Network Forensics Analysis. *ACM Transactions on Informations and System Security, 12*(1), 1-33. doi:10.1145/1410234.1410238

Weihan, G., Peng Chor, L., & Chai Kiat, Y. (2009). A Trusted Platform Module Based Anti-Forensics System. *International Conference on Network and Service Security.*, 1-5.

Xie, A., Wen, W., Zhang, L., Hu, J., & Chen, Z. (2009). Applying Attack Graphs to Network Security Metric. *IEEE.* Symposium conducted at the meeting of the International Conference on Multimedia Information Networking and Security

Zheng, W., Yang, O., & Yujun, L. (2011). A Taxonomy of Network and Computer Attacks Based on Responses. Symposium conducted at the meeting of the International Conference on Information Technology, Computer Engineering and Management Sciences (ICM), 2011 doi:10.1109/icm.2011.363