Design of Network Forensic System Based on Honeynet

Rajani Misra
Department of Computer Science and Engineering
National Institute of Technology, Jalandhar, Punjab, India.

Dr. Renu Dhir
Department of Computer Science and Engineering
National Institute of Technology, Jalandhar, Punjab, India.

Abstract- Network forensics deals with the capturing and analysis of the trace and logs of network intrusions from the multiple systems for providing the information to characterize intrusion or features. This paper demonstrates the internal working of implementation of server honeypot technology and network forensics. Honeypot based system is used to attract the attackers so that their process methodology can be observed and analyzed to improve defense mechanisms. Network Forensic allow administrators to monitor the networks, gather all the intelligent information about all the abnormal traffic, and helps to collect the attack evidence for network forensics. A prototype system have been developed to collect the network logs using honeynet infrastructure and analyze all the logged traffic, which is highly malicious in nature with large volume of attacker's information. The end result of the system is to collect network data which are highly malicious in nature and which can be used for further investigation to get the intelligent information about the attackers as evidence for Network Forensics.

Keywords – Network Forensics, NFATS, Honeypot, Honeynet, Honeyd, Finger Printing.

I. INTRODUCTION

Advent of internet has laid to cyber squatting (acquisition of a person's domain name in bad faith to profit, mislead, destroy the reputation and deprive others from registering the same). In spite of the availability of various security measures such as a firewall guarding the perimeter, an antivirus solution for workstations protection, a secure e-mail gateway, a web content manager, a network intrusion detection system and even a virtual private network for covering home users logging into the network. The structure can also include ingress and egress filtering at the router level, a syslog server for monitoring logs at the server level, and even a Linux machine running Nessus for vulnerability assessment at the enterprise level. But still to keep the situation under control the security administrators need to actively monitor their networks so as to be proactive in their security posture. Security administrator need to assiduously prevent all the system and network vulnerabilities before they are being exploited by any malicious user.

Since we know that no system is absolutely perfect, hence if any security breach occurs then there should be enough arrangement made available by the security administrator for evidence gathering, so as to punish offences such as those against the confidentiality, integrity and availability of computer data system, illegal access, illegal interception, data interference, system interference, and misuse of devices [1].

For this task Network Forensic Analysis Tools (NFATs) come into play which help administrators to monitor their environment for anomalous traffic, do forensic analysis and get a clear picture of their environment.

An approach for collection and analysis of evidences by combining honeypot with forensics was proposed [2]. The investigator's work load is reduced and hence the integrity of evidence could be protected due to the character of honeypot.

II. BACKGROUND AND RELATED WORK

The word "forensic" means "used in or suitable to courts of law." [5]. Network forensics is an important extension to the model of network security, and it focuses on the capture, recording, and analysis of network packets and events for investigative purposes [6]. Network forensics basic purpose is two-folds: a) Enhance the network security (Defence in depth) and b) Gather evidence for legal conviction of the culprit.Unlike other areas of digital forensics,

network investigations deal with large amounts of fast-flowing information. Here although not all the information captured or recorded will be useful for evidence or analysis, but exactly which information is not known before-hand. However, due to the increasing volume of network traffic in today's networks, it is infeasible to effectively store and query all the network information (packets) for extended periods of time in order to allow analysis of evidences. Therefore, current digital forensic tools should be capable enough to handle the large volumes of live forensic data and offline forensic data in an efficient manner.

2.1 Classification of Network Forensic System –

Based on various characteristics - Network forensic systems could be classified into two types: 'General Network Forensics' is to enhance network security and 'Strict Network Forensics' to get evidence satisfying legal principles and requirements) [7].

Collection of Traffic: 'Catch-it-as-you-can' systems where all packets passing through a particular traffic point are captured and analysis is subsequently done requiring large amounts of storage and **'Stop-look-and-listen'** systems where each packet is analyzed in memory and certain information is saved for future analysis requiring a faster processor. The network forensic system is an appliance with hardware and pre-installed software or exclusively a software tool.

2.2 Honeypot System –

Honeypot Systems are decoy servers or systems setup to gather information regarding an attacker or intruder into your system. It is important to remember that Honeypots do not replace the existing traditional Internet security systems; instead they are an additional level or system. Honeypots can be setup inside, outside or in the DMZ of a firewall design or even in all of the locations although they are most often deployed inside of a firewall for control purposes. Honeypot system are also called "Malware collection System". It enhances the thought of defence-in-depth by deceiving the intruder and gathering the attack information.

On the basis of level or frequency of intruder's interaction [8], honeypots can be classified as of three types: Low interaction honeypot (e.g. *Nepenthese)*, medium interaction and high interaction honeypot (e.g. *Capture-HPC)*. In functional point of view, it is divided into production honeypot and research honeypot. Finally, the hacker have two options to gain access to the honeypot; either by brute force or password guessing**.**

2.3 Honeynets –

Honeynet is a high-level interaction Honeyd. In fact Honeyd can hardly provide high-level interaction. The concept of Honeynet is quite simple: construct a network system and to monitor the network system when it is set up behind some kinds of access control equipment (Firewall). Attacker can infiltrate attack and use any system in honeynet and provide integrated operating system and applications for interaction.

2.4 Honeyd –

Honeyd is a background program for creating the hosts in virtual network, which could provide any service by configuration. Using personalized treatment, the hosts display that they run in a particular version of operating system [9]-[10]. Honeyd works in network layer. The intruder can only interact with the Honeyd in the network layer. Even if the honeyd is broken, the forever real system access is not obtained by the intruder.

2.5 Sniffer Tools –

Sniffer tools provide a mean to see all of the information or packets moving between the firewall and the Honey Pot system. Generally sniffers available now-a-days are capable of decoding common TCP packets such as Telnet, HTTP and SMTP. We can investigate packets in more detail by using a sniffer tool which allows us to determine what strategy the intruder is trying to use in much more detail than firewall or system logging alone. An bonus of using sniffer tools is that they can also create and store log files. The log files can then be stored and used for forensic purposes.

2.6 Malware Analysis –

The Goal of malware analysis is to gain understanding of how a specific piece of malware functions so that a defense mechanism could be built to protect an organization's network. Malware analysis could be performed in two ways by the professionals: Static (Code) malware analysis and dynamic(behavior) malware analysis.

Static analysis is a white-box method where we study a program without actually executing it. Thus it facilitates the security administrator to understand the malware without actually executing it. While performing static analysis, antivirus scanner such as ClamAV, AVIRA, and BitDefender must be used to analyze and define the categories of the threats.

Dynamic analysis is a black-box method where focus is only on the observables such as the external inputs, outputs, and their timing relationships and not on the internal structure. This is a fast and accurate method but with limitation of "what you see is all you get". Dynamic analysis tool such as Autoruns and Capture-BAT are used to monitor the action detail of the malware. Internally, it saves and access the file,
DLLs, registry, and API procedure call. Externally, it monitors the server access, malware comportment scanning, and malware downloading.

2.7 Fingerprinting –

There are two approaches to fingerprinting, namely active and passive. In the former approach, the tool sends out several "probes", i.e., specifically crafted network packets with a careful combination of flags and payload content, in order to force a reply from the target host, which is then analyzed for discrepancy with the expected behavior. On the other hand, passive tools do not generate any network traffic. As the name suggests, they passively collect network traffic and attempt to match the collected traces with a database of signatures.

III. Description Of Network Forensic Analysis Tools

Network Forensic Analysis Tools (NFATs) facilitates network monitoring by security administrators and thereby gather all information about anomalous traffic, to help in network forensics. NFATs synergizes with IDSs and firewalls making long term network traffic record preservation possible by allowing quick analysis of trouble spots identified by IDSs and firewalls. NFAT provides functionalities likes : Network traffic recording and analysis, Network performance evaluation, Data aggregation from multiple sources, Anomaly detection, Determination of network protocols in use, Detection of employee misuse of resources, Security investigations and incident response and Intellectual property protection.

3.1 NetIntercept –

It is an example of 'Catch-it-as-you-can' based analysis. It is a network traffic collection and analysis tool for real-time capture, distillation and analysis of network data, works with TCP and UDP streams, and complete data objects in addition to packets and bytes. NetIetercept recognizes and parses actual content on over 50 data stream types, including FTP, HTML, telnet, and email with attachments, allowing it to identify security threats that traditional packet oriented systems might miss. NetIntercept features include : Sophisticated search capabilities, GUI that allows users to: Browse through sets of NetIntercept results by selecting stream attributes, view bandwidth use by selected hosts and generate detailed reports, invisible to network users.

3.2 NetDetector –

NetDetector is the only security appliance that proactively detects both anomalies & signature-based intrusions. NIKSUN's NetDetector is a feature-packed analysis tool; an event viewer and an application reconstruction tool. These are quite helpful in analyzing how a breach occurred, what data were compromised and by whom, and what corrective measures can be taken to fix the breach. The solution also keeps track of the number of attacks launched by an attacker. The analysis tool facilitates the packet level decoding or investigation and analyzes the network security protocols that are in use. This enables the deepest and fastest mining. In order to prevent malicious attacks, NetDetector allows one to set user-generated rules and choose from NIKSUN edicts regarding IDS signatures.

3.3 SilentRunner –

Main feature of SilentRunner is to capture, detect, identify, correlate, analyze and report the network data. It is a passive network monitoring solution that visualizes network activity by creating a dynamic picture of communication flows, swiftly uncovering break-in attempts, weaknesses, abnormal usage, policy violations and misuse, and anomalies— before, during and after an incident. Operating like a surveillance camera, SilentRunner can play back events from thousands of communications to validate system threats and investigate security breaches. This dramatically enhances your ability to identify offenders, determine root cause, and mitigate the recurrence of the same security incident. In addition, it helps monitor infractions to regulatory controls and policy violations, providing supporting reports for auditing requirements and contributing to your ability to demonstrate compliance.

3.4 NetworkMiner –

Network traffic capture by live sniffing, performs host discovery, resembles transferred files, identifying rouge hosts and accesses how much data leakage was affected by an attacker. Network Miner is a good incident response NFAT which can extract files and certificates transferred over the network by parsing a PCAP file or by sniffing traffic directly from the network. This functionality can be used to extract and save media files (such as audio or video

files) which are streamed across a network from websites such as YouTube. Supported protocols for file extraction are FTP, TFTP, HTTP and SMB.

3.5 Iris –

Collects network traffic and reassembles it as its native session based format, reconstructs the actual text of the session, replays traffic for audit trial of suspicious activity, provides a variety of statistical measurements and has advanced search and filtering mechanism for quick identification of data[11].

3.6 EnCase –

EnCase Forensic also contains a full suite of analysis, bookmarking and reporting features. It gives investigators the ability to image a drive and preserve it in a forensic manner using the EnCase evidence file format (LEF or E01), a digital evidence container vetted by courts worldwide. The features include of EnCase : Intuitive User Interface, Powerful Automation, Unified Search, Simple E-Mail Review, Integrated Smartphone/Tablet Acquisition, Optimized & Integrated EnScript, Improved Evidence Management, Customizable Reports.

IV. NETWORK ANALYSIS TOOLS

4.1 NetFlow –

NetFlow efficiently provides a key set of services for IP applications, including network traffic accounting, usage-based network billing, network planning, security, Denial of Service monitoring capabilities, and network monitoring. NetFlow provides valuable information about network users and applications, peak usage times, and traffic routing. Cisco invented NetFlow and is the leader in IP traffic flow technology.

4.2 VisualRoute –

VisualRoute combines the tools Traceroute, Ping and Whois into an easy to use graphical interface that analyzers Internet connections to quickly locate where an outage or slowdown occurs. In addition, VisualRoute identifies the geographical location of IP addresses and Web servers on a global map – key information for security purposes to help identify network intruders and Internet abusers. Along with these few more exciting features offered are the reverse tracing and remote tracing via a web browser, port testing and application availability testing. A new report graph displays an instant picture of connection performance; tabbed display enables views of multiple test reports.

4.3 PyFlag –

Python Forensic Log Analysis GUI is an advanced forensic tool to analyze network captures in libpcap format while supporting a number of network protocols. It has the ability to recursively examine data at multiple levels and is ideally suited for network protocols which are typically layered. PyFlag parses the pcap files, extracts the packets and dissects them at low level protocols (IP, TCP or UDP). Related packets are collected into streams using reassembler. These streams are then dissected with higher level protocol dissectors (HTTP, IRC, etc.).

V. OPEN SOURCE NETWORK SECURITY AND MONITORING TOOLS

5.1 TCPDump/Libpcap/WinDump –

TCPDump: Tcpdump is the most used tool for network monitoring and data acquisition. It is a command-line packet sniffer and analyzer which intercepts and displays the packet being sent over the network. It captures, displays, and stores all forms of network traffic in a variety of output formats. It will print packet data like timestamp, protocol, source and destination hosts and ports, flags, options, and sequence numbers.
Libpcap (Packet Capture library): A portable C/C++ library for network traffic capture. libpcap is a system-independent interface for user-level packet capture. libpcap provides a portable framework for low-level network monitoring. Applications include network statistics collection, security monitoring, network debugging, etc.
Windump is a free version of tcpdump for Windows, the command line network analyzer for UNIX. WinDump is fully compatible with tcpdump and can be used to watch, diagnose and save to disk network traffic according to various complex rules. It can run under Windows 95, 98, ME, NT, 2000, XP, 2003 and Vista.

5.2 Nmap (Network Mapper) –

Nmap is used to discover computers and services on a computer network, thus creating a "map" of the network. Nmap is used for Host discovery, Port scanning, Version detection, OS detection, Scriptable interaction with the target.

5.3 P0f –

p0f is a versatile passive OS fingerprinting tool. p0f can identify the system on machines that connect to our box, machines we connect to, and even machines that merely go through or near our box even if the device is behind a packet firewall. It also checks masquerading and firewall presence, the distance to the remote system and its uptime, other guys' network hookup (DSL, OC3, avian carriers) and his ISP.

5.4 TCPstat –

Tcpstat is a simple c program used to monitor active TCP connections. Tcpstat reports certain network interface statistics. It gets its information by either monitoring a specific interface, or by reading previously saved tcpdump data from a file. It provides more than 15 different types of statistics including the number of packets passed through the interface, the average size of each packet, the standard deviation of the packet size and the bandwidth in bits per second. Tcpstat supports currently Linux, OpenBSD and OS X systems. Not all functionality is yet available on OpenBSD or OS X.

5.5 TCPtrace –

Tcptrace is a tool for analysis of TCP dump files. It can take as input the files produced by several popular packet-capture programs, including tcpdump, snoop, etherpeek, HP Net Metrix, and WinDump. Tcptrace can produce several different types of output containing information on each connection seen, such as elapsed time, bytes and segments sent and received, retransmissions, round trip times, window advertisements, throughput, and more. It can also reconstruct streams and produce a number of graphs for further analysis.

5.6 TCPflow –

Tcpflow is a program that captures data transmitted as part of TCP connections (flows), and stores the data in a way that is convenient for protocol analysis or debugging. A program like "tcpdump" shows a summary of packets seen on the wire, but usually doesn't store the data that's actually being transmitted. In contrast, tcpflow reconstructs the actual data streams and stores each flow in a separate file for later analysis. Tcpflow understands sequence numbers and will correctly reconstruct data streams regardless of retransmissions or out-of-order delivery. However, it currently does not understand IP fragments; flows containing IP fragments will not be recorded properly. Tcpflow is based on the libpcap and therefore supports the same rich filtering expressions that programs like tcpdump support.

VI. NETWORK FORENSICS ANALYSIS TOOLS LIMITATIONS

Like any other security tool, even NFATS suffers from few limitations. Commercial NFATs such as SilentRunner, NetDetect and NetIntercept are quite expensive apart from the extra overhead of training for how to use these products. Secondly, the drawback to NFATs being the fact that ample freeware tools are available that can perform similar forensic analysis for an environment. Although they don't exhibit less monitoring, analysis and visual capabilities but there lesser price attract many companies.

Another major drawback is that the most NFATS are unable to detect encrypted traffic such as SSL and SSH. Yet another limitation for Network Forensic Analysis Tools is that they are "mostly reactive, rather than proactive". The technology is designed to watch the network and alert the concerned person for any anomalous behavior. There is no technology interfere with network traffic because it is designed to be passive.

VII. CONCLUSION

Although there are several available security devices(Software and Hardware) available which safegaurd our network, but still the synergization of network forensic system based on honepot, combined with the existing IDS/IPS and firewall etc enormously enhance the security capabilities of the network.

Network forensics investigation ensures that the attacks are traced back to the source and hence attributing the crime to a person, host or a network. It has capabilities of future attack prediction by pattern matching and hence thereby, making the incident response to an attack much faster. The preparation of authentic evidence, admissible into a legal system, is also facilitated.

To implement this scenario, Network forensic tools (NFATs – both commercial and open source) can very efficiently simulate the network model by collection, documentation, examination and analysis of the network traffic. In future, we expect any intruder who tries to exploit the system/network vulnerabilities must have sense of awareness that he might be under surveillance and could be prosecuted in the court of law with enough evidence.

REFERENCES

[1] Online : www.crime-research.org/news/24.09.2012/3901/.

[2] McCarty B., "Honeypot forensics part I: analyzing the network" [EB/OL].

[3] Yasinsac and Yanet Manzano, “Honeytraps, a Network Forensic Tool”. Sixth Multi-Conference on Systemics, Cybernetics and Informatics, Orlando, Florida, USA , July 14-18, 2002.

[4] Raynal, F. Berthier , Y. Biondi, P. Kaminsky, D., “Honeypot Forensics”. Proceedings from the Fifth Annual IEEE SMC 10-11 June 2004 page(s): 22- 29.

[5] BLACK’S LAW DICTIONARY 721 (9th ed. 2009).

[6] A. Almulhem, and I. Traore, “Experience with engineering a network forensics system”, *Lecture Notes in Computer Science*, vol. 3391, pp. 62–71, Jan. 2005.

[7] Ren W and Jin H., “Modeling the network forensics behaviors”, In: Proceedings of the first international conference on security and privacy for emerging areas in communication networks (SecureComm 2005); Sept. 2005a, p. 1–8.

[8] H. Artaila, H. Safab, M. Sraja, I. Kuwatlya, and Z. Al-Masria, “A hybrid honeypot framework for improving intrusion detection systems in protecting organizational networks,” *Computers & Security*, Volume 25, Issue 4, pp, 274-288, June 2006.

[9] L. Corrado, M. Ken and D. Marc., “ScriptGen: An automated script generation tool for honeyd”. 21st Annual Computer Security Applications Conference, ACSAC 2005, pp: 203-214.

[10] C. Thomas M and B. John. “Design considerations for a honeypot for SQL injection attacks”. Proceedings - Conference on Local Computer Networks, LCN, pp: 915-921.

[11] V. Broucek and P. Turner, “Forensic computing: Developing a conceptual approach for an emerging academic discipline”, in 5th Australian Security Research Symposium, 2001.