RESEARCH ARTICLE OPEN ACCESS

Identification and Forensic Investigation of Network Intruders Based On Honeynet

Palika Jajoo*, Ganesh Singh**, Maninder Singh Nehra***
(Department of Computer Science & Engineering, Govt. Engineering College, Bikaner, India

ABSTRACT
In current modern world, internet is becoming the part of everyone's life and the use of internet is growing day by day. Thereby the security is becoming the main important aspect to protect the internet from unauthorized users and to protect the innocent end user of the internet. Cybercrime and network attacks are growing exponentially by the hacker's communities. There are numerous detection and prevention technologies like firewalls, IDS, antivirus etc but they don't provide complete security as there are certain shortcomings in these technologies. Since hackers and virus writers have come up with better ways to evade anti-virus technology throughout the years, the use of signature-based anti-virus software is proving to be less effective in putting a stop to malicious codes running in our computers. There is a need to find a way to analyze malicious activity without having to rely on the traditional signature based anti-virus tools but instead, complement what these tools can already do. For the development of network security model, network forensic is introduced which emphasize traditionally detection and prevention of attacks on networks. The power of various network forensic analysis tools available as open source can be integrated so that the investigator can have an edge over the attacker. In this paper, we discuss the network intruder's detection by forensically analysis of honeypot data. Network forensic can be integrated with IDS or firewalls but in our work we focused on forensic investigation of network data collected on honeynet to detect the intruders. Honeypot based system improve the defense mechanism as it is used to attract the attackers so that their process methodology can be observed and analyzed. The end result of this system is the collected information of network data which could further be analyzed forensically to get the intelligent information about the attackers and maintain the reports for network forensics.
Keywords – Honeypot, Honeynet, Network Security, IDS, Forensics

I. INTRODUCTION

Internet shortens the physical distance barrier, so that people can easily share information with each other in real time. The more applications in Internet, the more people rely on the actions. According to the Computer Crime and Security Survey [1] showed that 64% respondents of information security and information technology professionals in United States had dealt with malware events (50% in 2008), 29% dealt with denial of service events (21% in 2008), 23% dealt with bots events (20% in 2008), these statistics reflected the rising on cyber crime in 2009, even the serious is more than the past.

"Just as nuclear was the strategic warfare of the industrial era, cyber warfare has become the strategic war of the information era," says U.S. Secretary of Defence Leon Panetta. Cyber espionage and cyber sabotage are already a reality. Outside the realm of states and their proxies, corporate spies are using increasingly advanced techniques to steal company secrets or customer data for profit. Hactivists with political and anti business agendas are also busy.

The string of media revelations about security breaches this year suggests that the business world is just as vulnerable to attack as ever. Threats to online security have grown and evolved considerably in 2012. From the threats of cyber espionage and industrial espionage to the widespread, chronic problems of malware and phishing, we have seen constant innovation from malware authors [Symantec report].

Figure 1: Targeted attacks in numbers [source: Symantec threat report]

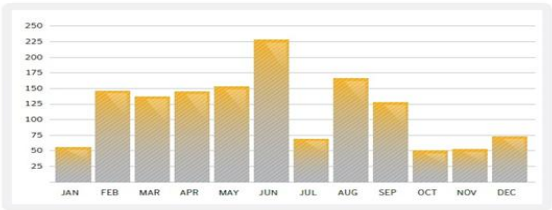

Figure 2: Targeted attack report by Symantec [source: Symantec report]

1.1 Network Forensic

The network forensic is defined as the activity of capturing, recording and analysis of network data in order to identify the patterns of attacks in that network data. The domain of network forensic is very vast which include capturing of network data, logging, identification of attack in those collected data. Network forensics is a comparatively new field of forensic science. The growing popularity of the Internet in homes means that computing has become network-centric and data is now available outside of disk-based digital evidence. Network forensics can be performed as a standalone investigation or alongside a computer forensics analysis (where it is often used to reveal links between digital devices or reconstruct how a crime was committed).

The concept of network forensics deals with the data found across a network connection mostly ingress and egress traffic from one host to another. Network forensics analyzes the traffic data logged through firewalls or intrusion detection systems or at network devices like routers. The goal is to trace back to the source of the attack so that the cybercriminals are prosecuted.

Network forensics is defined in [2] as "the use of scientifically proven techniques to collect, fuse, identify, examine, correlate, analyze, and document digital evidence from multiple, actively processing and transmitting digital sources for the purpose of uncovering facts related to the planned intent, or measured success of unauthorized activities meant to disrupt, corrupt, and or compromise system components as well as providing information to assist in response to or recovery from these activities".

Ranum [3] is credited with defining network forensics as "the capture, recording, and analysis of network events in order to discover the source of security attacks." Network forensics involves monitoring network traffic and determining if there is an anomaly in the traffic and ascertaining whether it indicates an attack. If it is so then the nature of the attack is also determined. Network traffic is captured, preserved, analyzed and an incident response is invoked immediately.

1.2 Technology used in Network Forensic

1.2.1 Intrusion Detection System

Intrusion detection is the process of monitoring computers or networks for unauthorized entrance or activity. IDS can also be used to monitor network traffic, thereby detecting if a system is being targeted by a network attack. There are two basic types of intrusion detection: host-based (HIDS) and network-based (NIDS). Each has a distinct approach to monitoring and securing data, and each has distinct advantages and disadvantages.

Host-based IDSs examine data held on individual computers that serve as hosts; they are highly effective for detecting insider abuses. Examples of host-based IDS implementations include Windows NT/2000 Security Event Logs, and UNIX Syslog. On the other hand, Network based intrusion detection systems analyze data packets that travel over the actual network. These packets are examined and sometimes compared with empirical data to verify whether they are of malicious or benign nature. An example of NIDS is Snort, which is an open source network intrusion detection system that performs real-time traffic analysis. It can be used to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, and OS fingerprinting attempts.

Also, they employ two main approaches to detect attacks. The first one is Signature-based, where detection is achieved by matching against a database of known attacks and the other one is Anomaly-based, in this approach, an IDS builds a model of "normal" activities of a system and when a deviation is detected it generate alerts. An IDS plays a valuable role in Network forensic system and works like a sensor that triggers the forensic system.

1.2.2 Honeypots

Lance Spitzner, Founder of Honeypot technology is given the authority of the definition of honeypot as "A honeypot is an information system resource whose value lies in unauthorized or illicit use of that resource**"** [7]**.** Honeypot refers to set of services, an entire operating system or even an entire network that is built to lure and contain the intruder. To collect known and unknown kind of attacks into any organization, honeypot places a significant role.

Honeypot is a security resource whose value lies in being probed, attacked or compromised [8]. Honeypot does not solve a specific security problem; therefore it is not a solution but a general technology which is unique in itself. Honeypot can be involved in various aspects of security such as detection, prevention and information gathering. Honeypot is highly flexible tool with applications in such areas as network forensics and intrusion detection. The motivation gain is to gather the information about the attacker (black-hat community) to learn the tools and techniques used by the attackers.

Types of Honeypots

Honeypots [8] can be classified on the basis of their purpose and interaction level with the attackers. Based on purpose, honeypots may be classified as:

1. Production honeypots
2. Research honeypots

1. Production Honeypots

The basic honeypot when comes to our mind it is the production honeypot. Many organizations use production honeypots for their protection and mitigating risks [9]. Their providing security to the production resources makes them valuable for any

organization. Production honeypots are much easy to build, deploy and maintain as compared to research honeypots. Even they require less functionality than the research honeypots. The source of attacks exploiting can be known by the help of production honeypot. It is difficult to know about attackers, how they organize attacks and what tools are used by them with the help of production honeypots but in recognizing attack patterns it is useful. Production honeypots are installed to mirror the production servers or any service for the intruder to work with. It also exposes any vulnerability present in the network. Administrator finds out attacks and vulnerabilities with the help of honeypots. These findings and warnings reduce risks of intrusion. On the basis of data provided by honeypot can be used for better defense and counter measures against future vulnerabilities. The production honeypot mostly deals with the bad guys for law enforcement.

Research Honeypots:

The Research honeypots used to gather information about the Blackhat community [9]. The associations like government/private agencies, universities/colleges, and defense organizations/institutions use honeypots for research purposes to collect information about latest vulnerabilities.

Protective measures can be taken on the basis of this information gathered by research honeypots. Ways and means used by attackers can be know and gathered by the research honeypot during an attack. Determination of actions, intentions and even knowing the attackers is possible with the help of information provided by research honeypot. This honeypot is very complex to deploy and to maintain. A large amount of data can be gathered by this. But, it is very time consuming for an administrator. Cyber threat study and extensive research can be done by the research honeypot. It can support constant monitoring of all the actions of an attacker as well as they can be recorded while they compromise any system. The most unique and advanced feature of research honeypot is its intelligence gathering. Research honeypots can lead to discovery of new worms. Research honeypots can be very useful in forensics. Honeypot functions by capturing attacker keystrokes and records all the activity of attack in the form of packet capturing data. Same is the case when any organization is using this honeypot as a production solution; definitely it is detecting the attack, blocking the attacker and perhaps even prosecuting the individuals involved. Whereas if the same honeypot is used by the organization as a research solution, it is more interested in what tools the attackers are using, where they are coming from, and their activities after they have compromised the honeypot. Thus same honeypot allows us to gather same information, only the difference is in its purpose or either production or research solution.

Based on level of interaction, honeypots may be classified as:

1. High-interaction honeypots
2. Medium-interaction honeypots
3. Low-interaction honeypots

1.3 Network Security using Honeynet

A special kind of high-interaction honeypot is known as Honeynet [13]. The concept of extending a single honeypot to a highly controlled network of honeypots is done by honeynet. All kind of system and network activity can be monitored and controlled with this kind of highly controlled network architecture. Then, within this network honeypots are placed. The Honeywall is a transparent gateway behind which honeypots are placed to form a basic honeynet. Honeywall is undetectable by the attackers as it acts as a lucid gateway. It keeps a track of all logging of network activities passing through honeypots. As per our study, honeynets are complex and time consuming to install and maintain.

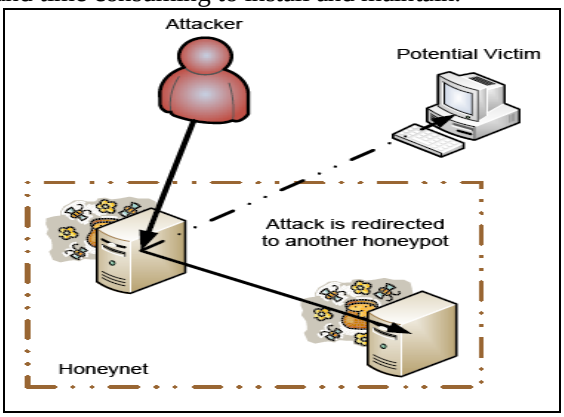

Figure 3: Honeynet

Requirements of the Honeynet

Data Control:

Data control is the repression of activity within the honeynet. Determination of ways of avoiding destructive and abusing other machines through the honeynet by the attacker can be done with the help of Data Control. As we require learning from the moves of an attacker, it demands great planning. We also have to restrict the attacker to use our resources like honeypot and bandwidth for attacking, damaging and abusing other hosts on the same or different subnets. Administrators have to take careful measures to study and make a policy for the attacker's freedom against containment. It is implemented in this way for achieving maximum data control and still not discovered/identified as a honeypot by the attacker. The process of security is implemented in layers

Data Capture:

All the logging, monitoring, and capturing of all threats and intruder can be done in the honeynet. Investigation of captured data gives an approach on the tools, method, techniques and aim of

the attackers. This idea is to attain maximum logging capability at all the system and the attacker does not know about the logging data on the honeypot. This type of silent logging is attained by installing up tools and mechanism on the honeypots to log all network/system actions and also have network data logging power at the Honeywall. All the logging information is vital in analysis the for understanding intruder whether its tcpdump packet, TCP port scan, remote and local exploits attacks, brute force attacks, malicious tools/ applications downloads by hackers, local/ global commands run, any type of information passed over the encrypted and unencrypted network(like IRC). This logged information is successfully sent over to a remote location to avoid any loss of data due to risk of system damage caused by attackers. Data masking techniques are used to avoid detection of this kind of activity from the attacker, such as encryption.

Data Analysis:

When data is captured, it is safely forwarded to a centralized data collection point which allows data captured from numerous. Honeynet sensors are to be centrally collected for analysis and archiving. Implementations may vary depending on the requirements of the organization. This latest implementations incorporate data collection at the Honeywall gateway.

1.4 Problem Statement

Network traffic analysis and investigation deals with the capturing of network traffic, log them and further analyze the network traces to find out the intrusions in the network logs to characterize the intrusion and misbehavior features in the network data. To detect the intrusion in the network traffic and to detect any kind of anomalous behavior, it is very important for forensic engineer to analyze the network data. The investigation of the captured data may lead to incident response towards the findings of the anomalies or suspicious behavior of the traffic. The network forensic or investigation of network data is not another name for network security, it is an extended phase of network security as the network data for forensic investigation and collected from various security products such as intrusion detection system, firewalls, routers etc. The data collected from various security products are further investigated for detection of the attacks in the network. During the course of these research implementations, we have used the honeynet technologies for data collection and data analysis to find out the anomalous bevaiour in the network data. With the help of the honeynet, the activities and behavior of the intruder can be observed and analyzed. Honeynet is a powerful tool to study the behavior of the attackers as there are not pre-defined set of signatures to detect the attacks. It is able to collect the known and unknown kind of attacks.

Overview: A honeypot refers to a set of resources which are built to lure the attackers so that they can attack on the honeypots resources and can be caught there. Although, honeypots are designed be compromised, they are in reality a tightly sealed compartment that is well controlled and monitored. Essentially, all honeypots share the same concept. They do not have any production value or any authorized activity. Thus, any attempt to interact with them is most likely malicious. Any interactions with the honeypots are considered as malicious in nature which can further studied and investigated for study of behaviour of the attackers. This is exactly we will implement during the research implementations. A combination of honeypots including low and high interaction are being implemented to collect the network logs and to study the behaviour of the intruders.

Network Forensics*:* From an investigative perspective, a honeypot is an ideal tool to closely study attackers and capture their tools, keystrokes, etc. Few studies have been proposed to adopt honeypots for forensics purposes. A notable example is the Honeynet Project, a voluntary research organization dedicated to study the tools, tactics, and motives of attackers.

1.5 Tools and Techniques used:

During the course of research implementation, we have used the open source tools to complete our study. Following open source tools we have used majorly in our implementation:

- Honeywall Roo
- SNORT
- TCPDUMP
- SNORTALOG
- Wireshark

1.6 Objectives of this study

During this research study and implementation, our main objective to collect the attack data based on implementation of honeynet infrastructure and forensically analyse the collected attack data on honeypot sensors. Keeping this main objective in mind the following objectives are stated:

- Network architecture design for deployment honeypot sensors
- Honeypot test bed creation
- Analyse the activities that will be logged by the honeypot.

The remainder of this paper is organized as follows – the next section gives the details about the Implementation and design. In Section 2 describes experimental results and attack data results after forensic investigation of the network traffic collected on honeypots. Section 3 consists the conclusion of the research work.

II. DESIGN AND IMPLEMENTATION DETAILS THE DESIGN

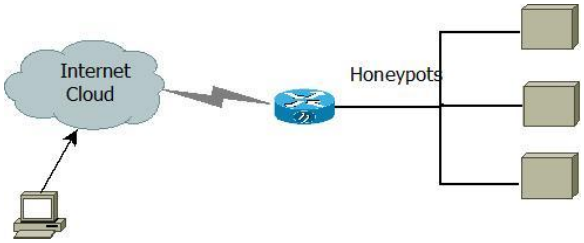

Figure 4: Network Design

Network Setup: Here we discuss the basic network design which can be configured as per the needs and motivations. More number of honeypots can be added in the network setup. Basically we have deployed the mixture of honeypots including both low interaction and high interaction honeypots. For high interaction honeypot, we have taken the window XP operating system in a virtualized environment whereas as low interaction we have taken the nepenthes honeypot. Low interaction honeypots which provide the emulated environment to attackers whereas high interaction honeypots provide the real environment to the attackers.

III. EXPERIMENTAL RESULTS

In this section we show the set-up of our system i.e. "Honeypot based on Network Forensic". In our system PCAP data is being logged and analyzed forensically. The collective PCAP data is submit directly to Snort Data Processing Engine and the attack data is being processed with the help of signatures into snort database.

Attack Data Classification on Honeypot

In this we describe the classification of attack data collected on Honeypot1, in which we show the distribution of attack methods, classification methods and event by destination port.

1. Distribution of attack methods

%	No	IP Destination	Attack	Severity
27.72	79	110.x.x.x	OS-WINDOWS DCERPC NCACN-IP-TCP srvsvc NetrPathCanonicalize overflow attempt {tcp}	high
17.89	51	110.x.x.x	OS-WINDOWS DCERPC NCACN-IP-TCP srvsvc NetrpPathCanonicalize path canonicalization stack overflow attempt {tcp}	high
11.93	34	x.x.x.x	FILE-IDENTIFY Portable Executable binary file magic detected {tcp}	low
9.82	28	x.x.x.x	OS-WINDOWS DCERPC NCACN-IP-TCP ISystemActivator RemoteCreateInstance attempt {tcp}	low
8.42	24	203.x.x.x	OS-WINDOWS DCERPC NCACN-IP-TCP ISystemActivator RemoteCreateInstance attempt {tcp}	low
6.67	19	x.x.x.x	MALWARE-OTHER lovegate attempt {tcp}	high
6.67	19	x.x.x.x	INDICATOR-SHELLCODE x86 OS agnostic xor dword decoder {tcp}	high
3.86	11	x.x.x.x	MALWARE-OTHER lovegate attempt {tcp}	high
3.16	9	x.x.x.x	MALWARE-CNC Trojan.Kbot variant outbound connection {tcp}	high
1.75	5	x.x.x.x	MALWARE-OTHER msblast attempt {tcp}	high
0.70	2	x.x.x.x	MALWARE-OTHER msblast attempt {tcp}	high
0.70	2	x.x.x.x	FILE-IDENTIFY download of executable content {tcp}	high
0.35	1	x.x.x.x	INDICATOR-COMPROMISE Microsoft cmd.exe banner {tcp}	high
0.35	1	x.x.x.x	INDICATOR-COMPROMISE Microsoft cmd.exe banner {tcp}	high

Table: Distribution of attack methods

2. Distribution of event by destination port

%	No	Destination Port
37.89	108	445
37.19	106	135
8.42	24	139
3.16	9	80
2.81	8	1046
2.46	7	1049
2.11	6	1043
1.75	5	1048
1.40	4	1044
1.05	3	1050
0.35	1	1051
0.35	1	11207
0.35	1	1154
0.35	1	2952
0.35	1	29239

Table: Port-wise distribution of attacks

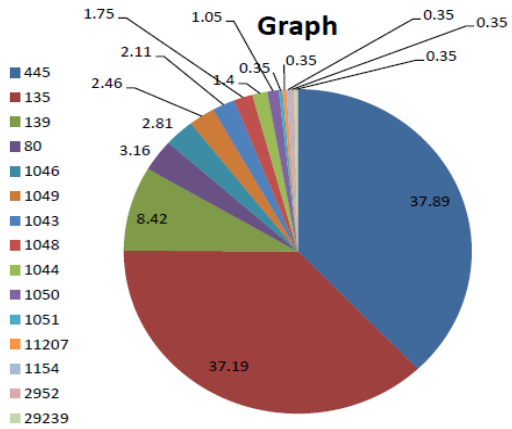

Figure 5: Distribution of events by destination port

IV. CONCLUSION

Network forensic prove as valuable investigative tools on collection of attacks. Network forensic system ensures investigation of the attacks by tracing the attack back to source and attributing the crime to a person, host or a network. Honeypots based model is useful to collect the attacker traces as anything coming on honeypot is malicious in nature. We have developed automated prototype network forensic system which incorporate signature based detection techniques with honeynets. The attack data collected on honeynet are analyzed by NIDS and processed by the SnortAlog tool. The categorization of these attacks has done with respect to attack type, port etc with statistical graphical distribution. Compared with other security mechanism found that honeypots are easy to use, effective in complex environment, collecting data and information relevant of a good value which can be later analyzed forensically.

With the developed solution, the deployment in distributed environment would lead to better and good volume of attack data which are always useful for investigation purpose. Scalability is one of major future work involved as it just our initial efforts to develop the network based forensic system. In future we can extend the analysis of malware in real time bases for both low interaction and high interaction honeypot with the implementation for the detection of malware on Smartphone android, iOS based platform.

V. ACKNOWLEDGEMENTS

During the course of this research work and implementations, I would like to thank Ganesh Singh, Assistant Professor, Department of Computer Science and Engineering, for his support and extremely useful guidance. Also thankful to Maninder Singh Nehra, Assistant Professor, Department of Computer Science and Engineering. without their guidance it was not possible to carry out this kind of research.

REFERENCES

[1] Computer Crime and Security Survey http://www.canberra.edu.au/cis/storage/Cyber Crime and Security Survey Report 2012.

[2] Palmer, G. 2001. "A Road Map for Digital Forensic Research", 1st Digital Forensic Research Workshop, New York, 15-30,2001.

[3] Ranum, M. "Network Flight Recorder", http://www.ranum.com/.

[4] Garfinkel, S. "Network Forensics: Tapping the Internet", http://www.oreillynet.com/pub/a/ Network/2002/04/26/ nettap.html.

[5] Sira,R. "Network Forensics Analysis Tools: An Overview of an Emerging Technology" GSEC (1.4), 2003.

[6] Emmanuel S.Pilli, R.C. Joshi and Rajdeep Niyogi "Generic Framework for Network Forensic International Journal of Computer Applications (0975 – 8887) Volume 1-No.11, 2010.

[7] Lance Spitzner "Honeypots: Definitions and Value of Honeypots" http://www.tracking-hackers.com Last Modified: 29 May, 2003.

[8] Iyatiti Mokube, Michele Adams, "Honeypots: Concepts, Approaches, and Challenges" ACM, in ACM-SE 45 Proceedings of the 45th annual southeast regional conference , pp. 321 – 326, North Carolina, 2007.

[9] Karthik, S., Samudrala, B. and Yang, A.T. "Design of Network Security Projects Using

Honeypots" Journal of Computing Sciences in Colleges, 20 (4).

[10] Sutton Jr., R.E. DTEC 6873 Section 01: "How to Build and Use a Honeypot".

[11] Berghel H."The Discipline of Internet Forensics", Digital Village, Communications of the ACM, Vol. 46, No. 8, pp. 15-20, August 2003.

[12] Provos, N. "Honeypot Background" http://www.honeyd.org/background.php.

[13] L.Spitzner, Honeynet Project "Know Your Enemy: Honeynet" http:// www.honeynet.org/ papers/honeynet Last Modified: 31 May, 2006. Peter Stephenson, Richard D. Walter " Toward Cyber Crime Assessment: Cyberstalking" Annual Symposium on Information Assurance (Asia), Albany, NY, June 7-8, 2011.

[14] Vasilios Katos, Peter M. Bednar "A cyber-crime investigation framework" Journal of Elsevier, 2007.

[15] P. Stephenson and R. Walter, "Cyber Crime Assessment", in Proc. HICSS, pp.5404-5413, 2012.

[16] Hanan Hibshi, Timothy Vidas and Lorrie Cranor "Usability of Forensics Tools: A User Study" Sixth International Conference on IT Security Incident Management and IT Forensics, pp. 81-91, IEEE 2011.

[17] Yanet Manzano and Alec Yasinsac, "Policies to Enhance Computer and Network Forensic" 2nd Annual IEEE Systems, Man, Cybernetic Information Assurance Workshop, June 2001.

[18] Hong-Ming Wang, Chung-Huang Yang "Design and Implementation of a Network Forensic System for Linux" Computer Symposium IEEE, pp. 390-395, 2010.