International Journal of

Emerging Research in Management &Technology

Research Article | January 2014

A Study on Network Intrusion Detection Based on Proactive Mechanism

Munish Sharma
M.Tech Scholar
PTU Regional Center(SBBSIET), India

Er. Tajinder Kaur
Assistant Professor
SBBSIET Padhiana(Jalandhar), India

Abstract :

In the current internet world where peoples are connected through communication channel and most of their data is hosted on the internet connected resources. Therefore the security is the major concern of this internet community to protect the resources and to protect the data hosted on these networks. In current trends, most of the end user are relying on the end security products such as Anti-viruses, Intrusion detection system, firewall etc. In this paper, we present the tools and techniques used to protect the networks and its associated resources and requirements for the proactive network intrusion detection mechanism which should be placed in line with the current intrusion detection system to protect the entire network. During this research, we will implement and design the proactive network security mechanism which will help to collect the attack traces. Further those collected attack traces can be used to strengthen the signature based detection mechanism.

Keywords–Network Intrusion detection, SNORT, Network Security, Proactive Network Security, Firewall

1. INTRODUCTION

The volumes of internet users are increasing in exponential manner which enable the concerns of network security. It is increasingly becoming difficult to secure computer networks due to largely increase in the activities of e-commerce over the internet. Today, information is a vital element in every aspect of life. Up-to-date and correct information are the key to any successful businesses, academia, government, personal finances or leisure activities. While this has been true for hundreds of years, it has never been as true as in the last half of the 20th century with the invention of the modern digital computer. The size of the internet has significantly increased in past few years as well as applications hosted on internet are increasing exponentially. Internet has become the most popular medium of communication and global information reservoir. With the increasing popularity of public social networking sites, the whole universe seems to congregate around internet to get his/her share of web. Though the general impression is the growing cyber security awareness among the masses, but the advanced hacker techniques and sophistication seems to counter the defensive mechanisms easily and befool the users. The malwares propagating in network have become the biggest threat to the increasing internet.

1.1. Introduction to Proactive Network Security

Countermeasures like firewalls or anti-anything (antivirus, anti-spam, anti-spyware, etc.) are all reactive security tools. They are necessary countermeasures and a part of a comprehensive security system, but you must also take action, be proactive, to ensure the highest level of network security. Daily vigilance is key. But it's nearly impossible to watch your network all the time.

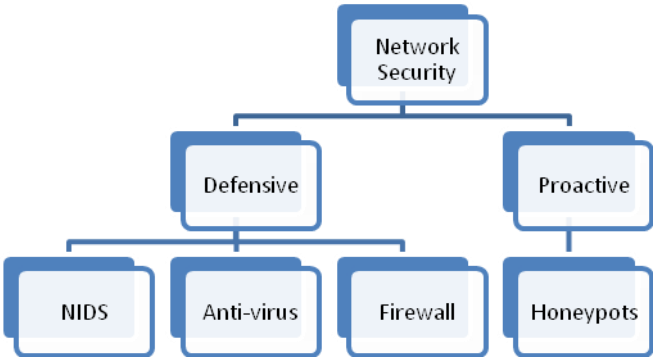

Figure1: Detection techniques

Before you pursue proactive network security, you need to understand the commonly used four pillars of network security. These pillars are firewalls, VPNs, antivirus software, and intrusion detection systems (IDS). Firewalls inspect packets and attempt to block bad packets, but they cannot recognize an attack or may block legitimate access. VPNs create secure tunnels between insecure computers, but they don't protect network assets. Antivirus has its role and, vital as it is, it cannot close the vulnerabilities that would prevent an attack. Finally, intrusion detection systems (IDS) are purely reactive, dealing with an attack after it has occurred.

While these four pillars of network security are critical to your organization, the fact is, a single enterprise can spend thousands on firewalls, VPNs, antivirus and IDS systems, while the real network security culprits, "Common Vulnerabilities and Exposures" (CVEs), go largely undetected. CVEs are essentially holes in applications that can be attacked by hackers and cyber terrorists to steal information or bring down networks. CVEs are a real problem and according to the 2004 E-Crime Survey are the systemic cause of over 90 percent of all network security breaches.
Proactive network security is the act of managing the four pillars of network security so that you get the most performance from them while at the same time augmenting your system with a vulnerability management system. A more effective firewall is going to block the right traffic. A more effective antivirus program is going to have less work to do, because viruses will have fewer opportunities to attack your systems. The IDS will become a backup system, rarely forced to sound an alarm that someone has actually gotten past your secure threshold. But preventing the attack with a vulnerability management system to eliminate CVEs is the most important component.
A proactive network security system to protect against hackers for the proactive automated defense against hackers by automatically finding, reporting, communicating with countermeasures about and removing the common vulnerabilities and exposures (CVEs) that they exploit

1.2 Statement of the problem

Hackers and malware writers have come with better ways to evade the network security devices such anti-virus technology throughout the years, therefore the significance of working capability of these security devices is proving to be less effective to stop and to prevent the malicious code running in our computers. There is a need to put the place a security mechanism to analyse malicious activity without having rely on the traditional signature based tools. To strengthen these signatures based tools and to manage these tools, there is a need to react proactively so that the analysis of the malicious codes can be performed and signatures for the security can be performed.

1.3 Significance of the problem

Based the study of the security devices and their working capability, it is necessary to put the proactive security mechanism instead of the signature based techniques such as firewall, Network Intrusion Detection System(NIDS), etc. Because the detection algorithm of these network intrusion detection system is based on the how signature based anti-virus tools detect malicious activities. All these signature based devices are rely on the pre-determined rule sets in the form of attack database that already been detected and recorded. This leaves in the state of known as unknown attacks. Therefore they will not be able to detect the unknown attacks which compromise the computer system.
Based on the above mentioned techniques, there is a requirement to put in place a proactive based security tested that would be able study the entire network and at the same time collect the attack traces which is known and unknown to them. The unknown attack traces can be used to strengthen the network intrusion detection system, prevent intrusions from exposing and exploiting the vulnerabilities of the said network. One of such proactive network security mechanism is in the form of honeypots. Since honey pots are deceptive systems, it will be very useful in hiding the real value of the data that pass over the network.
This research will explain the use of proactive security defence mechanism based on different tools and techniques which help in the creation of a tested that would help in testing and identifying the weakness of a network.
The format of the remaining paper is: section 2, defines and explains the technology that has been employed and discusses the background and motivation in brief and other detection approaches. Section 3 deliberates the proactive detection tools and techniques as well as requirement of implementation of proactive mechanism. Section 4 discusses conclusion and future work of the research problem.

2. BACKGROUND AND MOTIVATION

In 2001, when Code Red [5] was detected on the internet, Liston had the idea of a sticky honey pot [6], [7]. Thus, theLaBreaTarpit was born. The LaBreaTarpit uses unused IP addresses and creates virtual servers on them. These virtual servers respond to connection attempts that are made by attackers. This action delays the attackers until they get stuck for a period of time. This is why it is called a tar pit.[Network Intrusion tested through honey pot]
Network-based detection refers to methods used to help detect malicious entities by studying network traffic [8]. Szor[9] proposed to update and maintain a list of hosts or network segments that are allowed to access the resources of a network. Through this, packets from intruders are simply not allowed to enter the network. Although this is an effective method, address spoofing may be used to imitate or use the address of a host that has access to the network.

2.1 Malware & its types

Malware can be defined as “a set of instructions that run on your computer and make your system do something that an attacker wants it to do” [3]. Once a malicious web page attacks the user’s system, then it is able to download malware including the following, as described by Provos, et al. [4] and [5]:

- Virus
- Worm
- Trojans
- Spyware
- Adware
- Root kits

2.2 Security of Operating System

Operating system is the platform on which all other user applications run and resembles the foundation of building. Microsoft is the dominant player in operating system market and has a total share of 94 percent of all operating systems in use. While its latest operating system, Windows 7 is the most stable and most secure operating system, its slow adaptation in home users and corporations has led to wide spread use of older operating systems. According to statistics of the last three month (Nov-Dec-Jan 2010), Windows XP, a popular but vulnerable operating system has a 50% market share while windows Vista owns 15% followed by Widows 7, 28%. Microsoft provides constant updates for these operating systems; it is up to the user to install these updates. A quick look at the operating system security however, confirms that even with constant update and release of service packs, the number of discovered vulnerabilities have not decreased dramatically. Based on the report be Secunia, 75 vulnerabilities were discovered in Windows 7 alone in 2010. Windows Vista follows by 89 followed by Windows XP 97 [12].

2.3 Client Firewall

Most recent operating systems come with built in and "enabled by default" firewall package. Starting with Windows XP service pack 2 and since, firewall has been enabled by default on all Microsoft operating systems. This provides basic protection for an average home user. Based on a latest study in European Union countries in 2010 [Internet usage in 2010 – Households and Individuals], less than 50 percent of the users had their firewalled enabled. Users decide to disable windows firewall because of compatibility issues with other programs. This results in significant threat to the security of the host system.

2.4 Antivirus

Antivirus software is the basic security tool installed in end user computer. They mostly rely on signature based detection where executable files are matched against a signature database of known viruses. New versions have run-time scanning feature that scans the file in real time and avoids execution, if a threat is detected. Signature based detection however results in the antivirus engine failing to detect variants of known viruses, therefore a constant update of antivirus signature database is essential to provide basic protection. Although an antivirus is fairly effective in detection of known attacks if updated regularly, they are unable to protect users from remote port attacks or attacks directed at user applications from internet. Latest survey shows that, 25 % of users disabled their antivirus software because they believe this software have negative impact on their PCs' performance [13].While another study by a research group had similar results showing around 23% had absolutely no active security software installed. Rightfully assuming that every computer without any active protection would be infected with one type of virus or malware, 23% makes a huge impact not only on the infected computers but overall security of the internet as these infected hosts will be used to attack other hosts across the internet, be a part of DDoS attacks or exploited to deliver Spam [14].

3. STUDY OF VARIOUS HONEYPOT SOLUTIONS

Traditionally, Maintaining Network Security Has Involved Acting Defensively, Using Network-Based Defense Techniques Like Firewalls, Intrusion Detection Systems And Encryption. Now More Than Ever, Proactive Techniques Are Needed To Detect, Deflect And Counteract Attempts At Unauthorized Use Of Information Systems. The Use Of Honey Pots Is A Proactive, Promising Approach To Fighting Off Network Security Threats. Knowledge Center Contributors Nielsprovos And Thorsten Holz Explain What Honey Pots Are, And How Honey Pots Can Help You Improve Your Network Security. Traditionally, the area of information security has been purely defensive. Classic examples of the defensive mechanisms used to protect communication networks include firewalls, encryption and intrusion detection systems. The strategy follows the classical security paradigm of "Protect, Detect and React." In other words, try to protect the network as best as possible, detect any failures in that defense, and then react to those failures.

The problem with this approach is that the attacker has the initiative, always being one step ahead. For example, traditional, signature-based anti-virus solutions have a hard time keeping up with the flood of new malware appearing each day (since the attackers can test new malware samples before releasing them into the wild). In the last few years, it has become more and more clear that these traditional, network-based defense techniques have severe limitations.

Thus, we need new techniques to improve network defenses. One promising approach is the use of honey pots, a closely monitored computing resource that we want to have probed, attacked or compromised. More precisely, a honey pot is "an information system resource whose value lies in monitoring unauthorized or illicit use of that resource"

3.1 The Value of a Honey pot

The value of a honey pot is weighed by the information that can be obtained from it. Monitoring the data that enters and leaves a honey pot lets us gather information that is not available to an IDs. For example, we can log the keystrokes of an interactive session even if encryption is used to protect the network traffic. To detect malicious behaviour, IDS requires signatures of known attacks and often fails to detect compromises that were unknown at the time it was deployed.

On the other hand, honey pots can detect vulnerabilities that are not yet understood, so-called "zero-day attacks." For example, we can detect compromises by observing network traffic leaving the honey pot, even if the means of the exploit has never been seen before.

Honey pots can run any operating system and any number of services. The configured services determine the vectors available to an adversary for compromising or probing the system. A so-called "high-interaction honey pot" provides a

real system with which the attacker can interact. In contrast, a "low-interaction honey pot" simulates only some parts; for example, the low-interaction honey pot "Honeyed" simulates the network stack of arbitrary systems.
Here we discuss the various honey pots solutions which act as defense mechanism proactively to protect the network.A honey pot is a computer which has been configured to some extent to seem normal to an attacker, but actually logs and observes what the attacker does. Thanks to these modifications, accurate information about various types of attacks can be recorded. The term honey pot was first presented by Lance Spitzner in 1999 in a paper titled To Build a Honey pot [20].
Honey pots are unique because they allow a security researcher to see and record what actions a malicious user takes on a compromised computer without necessarily interfering or revealing to the attacker that they are being monitored. Because of this invisibility, valuable intelligence can be gathered about the actual strategies of an attacker. A honey pot can be configured to be either proactive or reactive to attacks, depending on the needs of the person who set it up.
There are several possible ways to classify honeypots. Some of the more popular are by the level of interaction available to the attacker, the type of data collected, and the type of system configuration [2, 19, and 27].

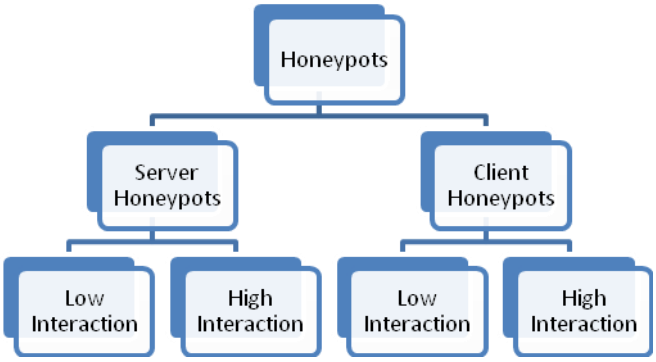

Figure 2: Classification of Honey pots

Honey pots can be classified into two main categories. Firstly, they can be based upon their level of interaction with an attacker. This can be further categorized as:

- Low-interaction: Emulate a variety of host services. These mimic real services but are implemented as a sandbox environment and run as an application. E.g. honeyd [Provos, N and Holz, T (July 26, 2007). Virtual Honeypots: From Botnet Tracking to Intrusion Detection. US: Addison-Wesley Professional.] And nepenthes.
- High Interaction: Attacker is given the freedom to interact with a real operating system and their every attempt is logged and accounted for.

The second Honey pot category is identified by the way they are deployed in a network. This includes:

- **Production Honeypots:** They are placed within an organization's production network for the purpose of detection. They extend the capabilities of intrusion detection systems. Such Honeypots are developed and configured to integrate with the organization's infrastructure. They are usually implemented as low-interaction Honeypots sitting within the server farm, but implementations may vary depending on available funding and requirements of the organization.

- **Research Honeypots**: These are deployed by network security researchers – the *white hat hackers*. They allow complete freedom for the attacker and, in the process; it is possible to learn their tactics. Using Research Honeypots zero day exploits, Worms, Trojans and viruses propagating in the network can be isolated and studied. Researchers can then document their findings and share them with system programmers, network and system administrators, various system and anti-virus vendors. They provide the raw material for the rule engines of IDS, IPS and firewall systems.

Table: Summary of Honeypots

Name of Solution	**Type**	**Category**
Dionaea [ref]	Low Interaction	General Purpose Honeypots
Nepenthes	Low Interaction	General Purpose Honeypots

Honeyd	Low Interaction	General Purpose Honeypots
Dshield	Low Interaction	Web Application Honeypots
Glastopf	Low Interaction	WAH
Argos	High Interaction Server Honeypot	Server Side Honeypot
HiHAT	High Interaction Server Honeypot	Server Side Honeypot
HoneyBOW	High Interaction Server Honeypot	Server Side Honeypot
Sebek	High Interaction Server Honeypot	Server Side Honeypot
Qebek	High Interaction Server Honeypot	Server Side Honeypot
HoneyC	Low Interaction Client Honeypot	Low Interaction client side Honeypot
PhoneyC	Low Interaction Client Honeypot	Low Interaction client side Honeypot
Monkey-Spider	Low Interaction Client Honeypot	Low Interaction client side Honeypot
CaptureHPC	High Interaction Client Honeypot	High Interaction Client side
Shelia	High Interaction Client Honeypot	High Interaction Client Side

4. METHODOLOGY

Based on the previous study, here we discuss the test bed creation using honey pot as deception mechanism which will be further useful for collection of attack trace. With the help of collected attack traces, a security researched can generate the network intrusion signature to tighten the network intrusion detection system [NIDS].

4.1 The design of deployment:

Deployment of Honeypots: Below figure depicts the one of the deployment scenario of honeypot which is placed with direct interface to the internet.

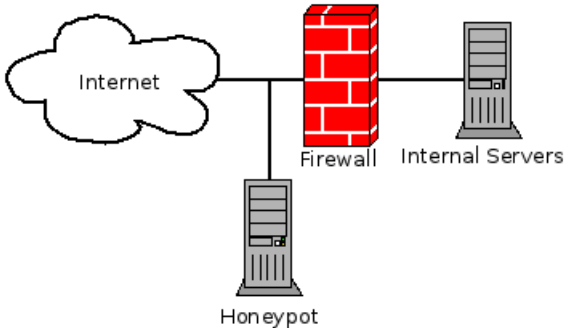

Figure3: Deployment of Honeypot

4.2 Process Methodology:

The purposed work completes through the following steps in order to analyze the network attacks.

- Platform creation using virtualization and installation of Linux operating system as based operating system
  - Installation of Virtual Box tools to create multiple operating system on a single base machine
  - Installation of unmatched operating system with latest vulnerabilities.

  - Configuration development to record the activities of invader.
- Network configuration and accessibility on base machine as well as virtual machines (depend no of honeypots).
  - IP address setting and assignments.
  - Network port configurations.
  - Application bind with specific port (depending upon requirement)
- Design and Implementation of Honeyed: a low interaction honeypots
- Development of automated scripts to simulate the Operating systems and services.
- Incorporation of Signature Based Detection Techniques with Honeypot.
- Network Attack capturing through honeypot and storage of attack data.
- Signature based classification through data processing engine
- Statistical report generation.
  - Port wise distribution
  - Attack wise distribution.
  - Percentage Distribution of attacks.
  - Pie charts of attacks
  - Bar charts of attacks etc.
- Distribution of collected attacks based on SNORT (Intrusion detection system) alerts.

Process Flow:

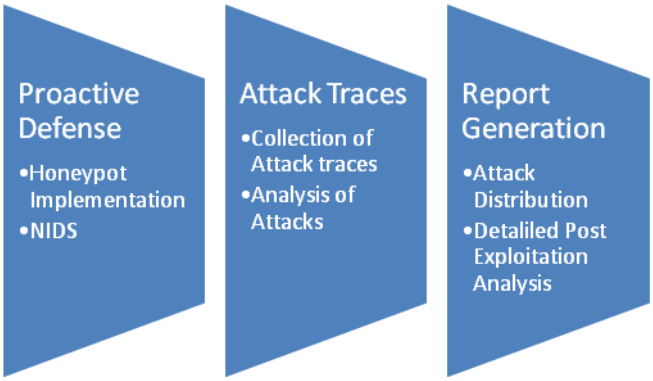

Fig 4: Process flow

As shown in the above figure, attack data capturing will be performed with the help of various types of honeypot implementation such as low interaction and high interaction honeypots. The data captured through honeypots will further be analyzed to get detailed post-exploitation analysis of attack traces.

5. CONCLUSION

In this paper, we only present the literature study of the existing solution of proactive defense mechanism for detection of malicious codes and found that most of the solution is either not available for public users and closely bound, thereby we propose the system which is able to detect the malware programs with the help of honeypot as well as by applying the intelligent forensic investigation of the collected network PCAP data.

ACKNOWLEDGEMENTS

We would like to sincerely thank Er.Tajinder Kaur (Assistant Professor) for her contribution and help in writing this paper.

References

[1] R. Danford, ―2nd Generation Honeyclients‖, SANS InternetStorm Center,2006 http://handlers.dshield.org/rdanford/pub/Honeyclients_Danford_SANS 06.pdf
[2] Cheswick, B. (1990), An Evening with Berferd in which a cracker is Lured, Endured, and Studied: *Citeseer*.
[3] Ramaswamy, C. and R. Sandhu. (1998), Role-based access control features in commercial database management systems: *Citeseer*.
[4] Skoudis, E., and Zeltser, L., *"Malware: Fighting Malicious Code"*, Prentice Hall,2003, Page 3, ISBN = 978-0131014053.
[5] [Provos, N., McNamee, D., Mavrommatis, D. W., K and Modadugu, N., *the Ghost In The Browser Analysis of Web-based Malware*. 2007. [Online]. Available at:http://www.usenix.org/events/hotbots07/tech/full_papers/provos/provos.pdf [Accessed 11 Feb 2009]
[6] Secure Browsing | Malware Protection | Secunia. (2010), "Secunia Yearly Report - 2010". Available from:secunia.com/gfx/pdf/Secunia_Yearly_Report_2010.pdf.

[7] Secunia. (2010), "Research Reports, Factsheet by Browser - 2010". [Cited 2011 5 - January]; Available from: http://secunia.com/resources/factsheets/2010_browsers/.
[8] VirtualBox. (2004). Sun VirtualBox® User Manual. Available:http://www.virtualbox.org/manual/UserManual.htmlLast accessed 20 July 2008.
[9] Sanjeev Kumar, at al, Hybrid Honeypot Framework for Malware Collection and Analysis, ICIIS-2012, IIT Chennai
[10] www.honeyclient.org
[11] en.wikipedia.org/wiki/Client_honeypot
[12] www.honeynet.org
[13] Trustwavehttps://www.trustwave.com/securebrowsing/
[14] Detection and Analysis of Drive-by-Download Attacks and Malicious JavaScript Code www.cs.ucsb.edu/~vigna/.../2010_cova_kruegel_vigna_Wepawet.pdf
[15] Prophiler: A Fast Filter for the Large-Scale Detection of Malicious Web Pages www.cs.ucsb.edu/.../2011_canali_cova_kruegel_vigna_Prophiler.pdf
[16] Xiaoyan Sun, Yang Wang, JieRen, Yuefei Zhu and Shengli Liu, "Collecting Internet Malware Based on Client-side Honeypot", 9th IEEE International Conference for Young Computer Scientists (ICVCS 2008), pp. 1493 – 1498, 2008.
[17] Secunia. (2010), "Factsheets by Windows Operating System - 2010". 20 - March - 2011]; Availablefrom: http://secunia.com/resources/factsheets/2010_win_os/.
[18] PcPitstop. (2010), "The State of PC Security". 20 - December 2010]; Available from:http://techtalk.pcpitstop.com/2010/05/13/the-state-of-pc-security/.
[19] YaserAlosefer, Analysing Web-based Malware Behaviour through Client HoneypotsCardiff University School of Computer Science & Informatics, Feb-2012