Design and Implement the High Interaction Honeypot for a Campus Network

Thesis submitted in partial fulfillment of the requirements
for the award of degree of

Master of Engineering
in
Software Engineering

Submitted By
Kapil Madan
(Roll No. 801031015)

Under the supervision of:

Dr. Maninder Singh
Associate Professor, CSED

Mr. Sumit Miglani
Assistant Professor, CSED

COMPUTER SCIENCE AND ENGINEERING DEPARTMENT
THAPAR UNIVERSITY
PATIALA – 147004

June 2012

Certificate

I hereby certify that the work which is being presented in the thesis report titled, **"Design and Implement the High Interaction Honeypot for a Campus Network"**, in partial fulfillment of the requirements for the award of degree of Master of Engineering in *Software Engineering submitted* in Computer Science and Engineering Department of Thapar University, Patiala, is an authentic record of my own work carried out under the supervision of Mr. Maninder Singh & Mr. Sumit Miglani and refers other researcher's work which are duly listed in the reference section.

The matter presented in the thesis has not been submitted for award of any other degree of this or any other University.

Kapil Madan
(Kapil Madan)

This is to certify that the above statement made by the candidate is correct and true to the best of my knowledge.

(Dr. Maninder Singh)
Associate Professor
CSED, Thapar University

(Mr. Sumit Miglani)
Assistant Professor
CSED, Thapar University

Countersigned by

(Dr. Maninder Singh)
Associate Professor & Head
Computer Science and Engineering Department
Thapar University, Patiala

(Dr. S. K. Mohapatra)
Dean (Academic Affairs)
Thapar University
Patiala

i

Acknowledgement

No volume of words is enough to express my gratitude towards my thesis supervisor **Dr. Maninder Singh & Mr. Sumit Miglani** Department of Computer Science & Engineering, Thapar University, Patiala, whose guidance, wisdom and invaluable help has aided me in the completion of thesis. He has helped me to explore numerous topics related to the thesis in an organized and methodical manner and provided me with many valuable insights into various technologies.

I would also like to thank **Mr. Brett Ussher** and classmates who were always there at the need of the hour and provided with all the help and facilities, which I required, for the completion of my thesis work.

Most importantly, I would like to thank my Papa, Mummy and the Almighty for showing me the way and encouraging me through the difficult times I encountered during the completion of my thesis work.

Kapil Madan

Abstract

High interaction honeypots provide a valuable source of information about the techniques, tactics and motives of attackers in the internet. In high interaction honeypots has more information which is correct as compared to low interaction honeypots. Low interaction honeypots has more false information and does not provide detailed information.

In this thesis the concept of self contained virtual **High Interaction Honeypot** is discussed and a new honeynet solution is developed using CDROM roo 1.4 which is 3rd generation honeypots. Self contained means whole honeynet is embedded in the single system.eg install honeynet in the laptop. Honeywall has installation and configuration issues. In this thesis the whole scenario is considered with proper diagram, explain properly how to install and configure the honeywall and administration of high interaction honeynet remotely through walleye. Detect the various types of attack by attacker such as banner grabbing, netcat (Swiss army knife), port scanning, packet craft, DDOS Attack, Operating system fingerprinting and study how an attacker exploit the vulnerability existing in the honeypots system using metasploit framework. A case study of MS08-067 vulnerability in vnc server that allow remote code execution with the help of metasploit exploit and detect the backdoor installation using honeywall.

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Network Security

Network security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users are assigned an ID and password that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs conducting transactions and communications among businesses, government agencies and individuals [1].

1.2 Growth of Internet

Despite its humble beginnings in the labs of DARPA the Internet today has become the backbone of today's economy. Today most the computers of the world are interconnected using networks and the Internet is a collection of such networks. The primary building blocks of the Internet are the Local Area Networks (LANs). Although the principle method of communication on Internet is TCP/IP (Transport Control Protocol/ Internet Protocol) protocol suite but the Internet is fast becoming the environment with multiple protocols.

1.3 Essential Terminology

Hack Value

Hack Value is notion among the hackers that something is worth or interesting.

Target of evaluation

An IT system that is identified or subjected to required security evaluation.

Attack

An assault on the system security derived from an intelligent threat.

Threat

Threat is an action or event that might prejudice security. A threat is a potential violation of security.

Vulnerability

Vulnerability is the existence of weakness, design or implementation error that can lead to an unexpected, undesirable event compromising the security of the system.

Exploit

Exploit is a defined way to breach the security of systems through vulnerability.

Ethical Hacker

The term Ethical Hacker refers to security professionals who apply their skills for good.

A zero day

A computer threat that tries to exploit computer application vulnerabilities that are unknown to others or undisclosed to software engineer.

Daisy chaining

Hackers who get away with database theft usually complete their task, and then backtrack to cover their tracks by destroying logs.

1.4 Elements of Information security

1.4.1 Confidentiality

Assurance that the information is accessible only to those authorized to access Confidentiality breaches may occur due to improper data handling.

1.4.2 Integrity

Integrity refers to the trustworthiness of data or resources in terms of preventing improper and unauthorized changes. In information security, integrity means that data cannot be modified undetectably. Integrity is violated when a message is actively modified in transit. Information security systems typically provide message integrity in addition to data confidentiality.

1.4.3 Availability

Availability refers to the ability to use the information or resources desired. For any information system to serve its purpose, the information must be available when it is needed. This means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly. High availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades. Ensuring availability also involves preventing denial-of service attacks.

1.5 Security Triangle

A good security professional try to have the highest level of security in his infrastructure (ideal situation). Unfortunately, too much security controls may have a bad impact on the users, preventing them to perform their work in good conditions. Security Triangle helps to find the right balance between security, ease of use, functionality.

1) Security
2) Functionality
3) Ease of use

The Security Triangle is shown in Figure 1.1. In an ideal situation, the black point must stay at the center of the triangle, this is the best balance. If one of the components is increased, the two are affected. If security is increased (move the point nearby the top corner), the distance of circle from with functionalities and ease of use will increase. Same for the ease of use. By adding nice features to the project, security is decreased.

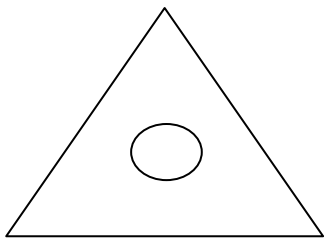


Figure 1.1 Security triangle

1.6 Classes of hackers

Several subgroups of the computer underground with different attitudes and aims use different terms to demarcate themselves from each other, or try to exclude some specific group with which they do not agree. The hackers can be broadly divided into following classes.

1.6.1 Black hat hackers

These are the individuals with extraordinary computing skills, resorting to malicious or destructive activities. They are also known as Crackers. A Black Hat Hacker is a hacker who violates computer security for little reason beyond maliciousness or for personal gain. Black Hat Hackers are the epitome of all that the public fears in a computer criminal. Black Hat Hackers break into secure networks to destroy data or make the network unusable for those who are authorized to use the network.

1.6.2 White hats hackers

These are individuals professing hacker skills and using them for defensive purposes. They are also known as Security Analysts. A white hat hacker breaks security for non-malicious reasons, for instance testing their own security system. This classification also includes individuals who perform penetration tests and vulnerability assessments within a contractual agreement. This type of 'white hat' hacker is called an ethical hacker.

1.6.3 Grey hats hackers

There are individuals who work both offensively and defensively at various times. A grey hat hacker is a combination of a Black Hat and a White Hat Hacker. A Grey Hat Hacker may surf the internet and hack into a computer system for the sole purpose of notifying the administrator that their system has been hacked e.g. they may offer to repair their system for a small fee.

1.6.4 Suicide hackers

Individuals who aim to bring down the critical infrastructure for a cause and are not worried about punishment for their actions.

1.7 Risk to Network security

Many methods and tools exist for locating vulnerabilities, running exploits, and compromising systems. Once vulnerabilities are found in a system, a hacker can exploit

that vulnerability and install malicious software. In Figure 1.2 show the internet crime report by ic3.gov [5]. Trojans, backdoors, and root kits are all forms of malicious software, or malware. Malware is installed on a hacked system after vulnerability has been exploited. Buffer overflows and sql injection are two other methods used to gain access into computer systems. Buffer overflows and sql injection are used primarily against application servers that contain databases of information. Most hacking tools exploit weaknesses in one of the following four areas:

1) Operating systems many system administrators install operating systems with the default settings, resulting in potential vulnerabilities that remain unpatched.

2) Applications usually aren't thoroughly tested for vulnerabilities when developers are writing the code, which can leave many programming flaws that a hacker can exploit. Most application development is "feature-driven," meaning programmers are under a deadline to turn out the most robust application in the shortest amount of time. Shrink-Wrap Code Many off-the-shelf programs come with extra features the common user isn't aware of and these features can be used to exploit the system. The macros in Microsoft Word, for example, can allow a hacker to execute programs from within the application.

3) Misconfigurations systems can also be misconfigured or left at the lowest common security settings to increase ease of use for the user. This may result in vulnerability and an attack.

4) Hackers use many different methods to breach an organization's security during a simulated attack or penetration test. Most hackers have a specialty in one or a few of the following attack methods.

1.7.1 Common entry points for an attack

1) Remote network: - A remote network hack attempts to simulate an intruder launching an attack over the Internet. The hacker tries to break or find vulnerability in the outside defenses of the network, such as firewall, proxy, or router vulnerabilities. The Internet is thought to be the most common hacking vehicle, while in reality most organizations have strengthened their security defenses sufficient to prevent hacking from the public network.

2) Remote Dial-Up Network: - A remote dial-up network hack tries to simulate an intruder launching an attack against the client's modem pools. War dialing is the process of repetitive dialing to find an open system and is an example of such an attack. Many organizations have replaced dial-in connections with dedicated internet connections so this method is less relevant than it once was in the past.

3) Local Network: - A local area network (LAN) hack simulates someone with physical access gaining additional unauthorized access using the local network. The hacker must gain direct access to the local network in order to launch this type of attack. Wireless LANs (WLANs) fall in this category and have added an entirely new avenue of attack as radio waves travel through building structures. Because the WLAN signal can be identified and captured outside the building, hackers no longer have to gain physical access to the building and network to

perform an attack on the LAN. Additionally, the huge growth of WLANs has made this an increasing source of attack and potential risk to many organizations.

4) Stolen Equipment: - A stolen-equipment hack simulates theft of a critical information resource such as a laptop owned by an employee. Information such as usernames, passwords, security settings, and encryption types can be gained by stealing a laptop. This is usually a commonly overlooked area by many organizations. Once a hacker has access to a laptop authorized in the security domain, a lot of information, such as security configuration can be gathered. Many times laptops disappear and are not reported quickly enough to allow the security administrator to lock that device out of the network.

5) Social Engineering: - A social-engineering attack checks the security and integrity of the organization's employees by using the telephone or face-to-face communication to gather information for use in an attack. Social-engineering attacks can be used to acquire usernames, passwords, or other organizational security measures. Social-engineering scenarios usually consist of a hacker calling the help desk and talking the help desk employee into giving out confidential security information.

6) Physical Entry: - A physical-entry attack attempts to compromise the organization's physical premises. An ethical hacker who gains physical access can plant viruses, Trojans, root kits or hardware key loggers (physical device used to record keystrokes) directly on systems in the target network. Additionally, confidential documents that are not stored in a secure location can be gathered by the hacker. Physical access to the building would allow a hacker to plant a rogue device such as a wireless access point on the network. These devices could then be used by the hacker to access the LAN from a remote location.

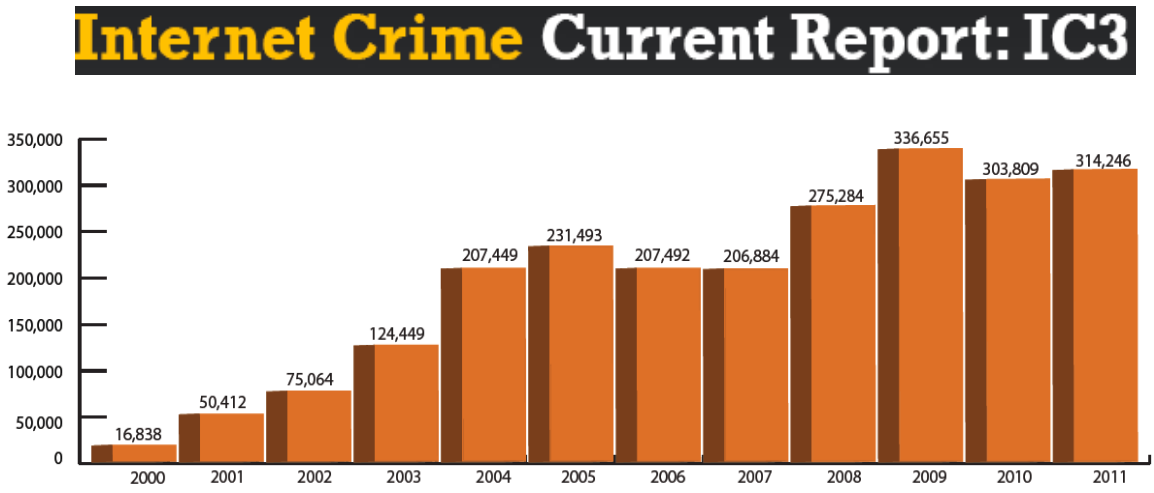


Figure 1.2 Internet crime report by IC3.gov [5]

1.8 Proactive approach

A proactive system constantly tests the organization's network for vulnerabilities and exposures. It then assesses and prioritizes those vulnerabilities and exposures and manages the process by which those vulnerabilities and exposures are addressed. All ip devices attached to the network are periodically or continuously scanned and profiled for changes, violations to policy, and vulnerabilities and exposures. Analytics are applied so that the administrators and business owners are presented with actionable intelligence relative to the risk to their business. The defect is then corrected, before security can be breached. In contrast to reactive systems, proactive systems have the advantage of providing valuable intelligence about an organization's network and networked devices even when they are not under attack. Of course, proactive systems work best when complemented with appropriate reactive systems. This provides organizations with a layered approach to network security where vulnerabilities are detected and deal with on multiple levels.

1.9 Hacktivist

A hacktivist is a hacker who utilizes technology to announce a social, ideological, religious, or political message. In general, most hacktivism involves website defacement or denial-of-service attacks.

1.10 Phases of Hacking

Hackers typically approach an attack using five common phases. It is important to understand these phases of hacking attacks in order to better defend against them. Figures 1.3 show the phases of hacking [4].

1.10.1 Reconnaissance

Before hacking online business or corporate infrastructure, hackers first perform routine and detailed reconnaissance. Hackers must gather as much information about business and networks as possible. Anything they discover about their target can be valuable during their attack phases. Strategies for hacking rely on a foundation of knowledge and understanding, arising initially from whatever the hacker can learn about their targets. Methods of reconnaissance include dumpster diving, social engineering, google searching, google hacking and work their way up to more insidious methods such as infiltrating employee's environments from coffee shops to simply walking in and setting up in a cubicle and asking a lot of questions. Whatever methods are used to perform reconnaissance, hackers will usually collect a large amount of information varying from trivial to sensitive, all of which may be useful during their attacks.

1.10.2 Network and System Scanning

Probing a target's network can reveal vulnerabilities that create a hit list for hackers to work through. Hackers may be either general hackers or specialized hackers such as phreakers, but their intent is same i.e. to access information and services that they should

not gain access to. Much of the information gathered during the hacker's reconnaissance phase now comes into play. This phase of network scanning is an extension of the reconnaissance phase. Hackers want to learn more about network mapping, phone system structure and internal informational architecture. Learning what routers, firewalls, IDS systems and other network components exist can lead hackers to beneficial hacking information by researching known vulnerabilities of known network devices. Typically, hackers perform port scans and port mapping, while attempting to discover what services and versions of services are actively available on any open or available ports.

1.10.3 Gaining Access

Open ports can lead to a hacker gaining direct access to services and possibly to internal network connections. This phase of attack is the most important and the most dangerous. Although some hack attacks do not need direct network access to damage target's business such as Denial of Services (DOS). Simple methods of attack are available to network-connected hackers including session hijacking, stack-based buffer overflow and similar security exploits. Smurf attacks try to get network users to respond and the hacker uses their real IP Addresses to flood them with problems. Whether the hacker is successful attacking an internal system has much to do with how vulnerable the specific system is, which is related to system configurations and architecture [2].

1.10.4 Maintaining Access

Hackers may choose to continue attacking and exploiting the target system, or to explore deeper into the target network and look for more systems and services. Not all attackers remain connected to the exploited network, but from a defensive strategy it must be expected. Hackers may deploy programs to maintain access by launching vnc clients from within target's network, providing access to external systems, opening telnet sessions and similarly serious services like FTP and SSH, or upload root kits and Trojans to infiltrate and exploit target's network and systems to the point where they have complete root level control. Hackers can continue to sniff network looking for more

information to use against the target. Trojans can export sensitive information to hackers, such as credit card records, usernames and passwords [2].

Figure 1.3 Phases of Hacking [4]

1.10.5 Covering Tracks

Most hackers will attempt to cover their footprints and tracks as carefully as possible. Although not always the case, removing proof of a hacker's attacks is their best defense against legal and punitive action. It is most likely that hackers and newbie hackers will get caught at a much higher rate than expert level hackers who know how to remain hidden and anonymous. Gaining root level access and administrative access is a big part of covering one's tracks as the hacker can remove log entries and do so as a privileged administrator as opposed to an unknown hacker. Placing programs inside target's network to continually send sensitive information out to anonymous drop-off points allows hackers to cover their tracks while maintaining access. Steganography allows hackers to hide information inside objects that are not obvious, such as image headers

and meta tags. Tunneling allows hackers to perform their insidious work through one service that is carried over another service, to increase the difficulty of finding them. As shown in Figure 1.3 these five phases of a hacker's attack loop back to the beginning. A successful attack with maintained access often results in continuing reconnaissance. The more the hacker learns about a target's internal operations means the more likely he will be back to intrude and exploit more network systems, internal services and business resources [2].

Chapter 2

Literature Survey

2.1 The Internet

The Internet is growing fast and doubling its number of websites every 53 days and the number of people using the internet is also growing. Hence, global communication is getting more important every day. At the same time, computer crimes are also increasing. Countermeasures are developed to detect or prevent attacks most of these measures are based on known facts, known attack patterns. Countermeasures such as firewalls and network intrusion detection systems are based on prevention, detection and reaction mechanism. But is there enough information about the enemy. As in the military, it is important to know, who the enemy is, what kind of strategy does he use, what tools he utilizes and what he is aiming for. Gathering this kind of information is not easy but important. By knowing attack strategies, countermeasure scan be improved and vulnerabilities can be fixed. To gather as much information as possible is one main goal of a honeypots. Generally, such information gathering should be done silently, without alarming an attacker. All the gathered information leads to an advantage on the defending side and can therefore be used on productive systems to prevent attacks.

2.2 Honeypot

It is the system which has the various vulnerability embedded in it so that it can lure the attacker to attack on vulnerable system. The attacker attacks on honeypots by its different technique. A more practical, but more limiting, definition is given by pcmag.com. “A server that is configured to detect an intruder by mirroring a real production system. It appears as an ordinary server doing work, but all the data and transactions are phony.

Located either in or outside the firewall, the honeypot is used to learn about an intruder's techniques as well as determine vulnerabilities in the real system".

2.3 History of Honeypot

The concept of Honeypot was first described by Clifford Stoll in 1990 [3]. The book is a novel based on a real story which happened to Stoll. He discovered a hacked computer and decided to learn how the intruder gained access to the system. To track the hacker back to his origin, Stoll created a faked environment with the purpose to keep the attacker busy. The idea was to track the connection while the attacker was searching through prepared documents. Stoll did not call his trap a honeypot. He just prepared a network drive with faked documents to keep the intruder on his machine. Then he used monitoring tools to track the hacker's origin and find out how he came in.

Gen I are the first honeynet architecture used by the honeynet project. The Honeynet Project is a non-profit research organization of security professionals dedicated to information security. They mainly use iptables and Snort IDS for data control and data capture. Gen II tries to improve the data control and data capture modules [6]. In addition to the Gen I iptables firewall layer and Snort IDS layer, Gen II adds another data capture layer where data is captured in the honeypot hosts using sebek and syslogd to capture more information and address the problem of encryption [9]. In terms of data control, Gen II improves Gen I by adding another layer that uses Intrusion Prevention System, Snort-Inline operating in packet drop mode and packet replace mode to try and mitigate the risks that may be caused by those outbound packets allowed to pass by the iptables.

In 1999 that idea was picked up again by the honeynet project lead and founded by Lance Spitzner [19]. During years of development the Honeynet project created several papers on honeypot and introduced techniques to build efficient honeypot. Attempts were made to make honeynet easier to deploy. This first began with pre-built tools, such as an rc.firewall script, making it easier to build and

deploy a honeynet. In May 2003, the first Honeywall CDROM was released, called Eeyore. The intent was to automate Gen II honeynet deployments by bringing all the tools and requirements into a single CDROM. This solution was considered a beta concept, and had several weaknesses. In September, 2004 team members got together to design, architect and develop a new solution, which is roo. This release is considered a Gen III technology, as it has radical new improvements. It contains the core Gen II Data Control and Data Capture functionality, but also now has remote GUI administration, data analysis integration, support for the Sebek 3.x branch, robust OS base, automated updating, and much more. It provides a solution that any security professional could easily use and maintain. Gen III offers a way of analyzing data from different sources without the person having to manually go through different data sources and try to determine the relationships themselves [17].

Honeypot can be made by installing unpatched operating system which has known vulnerability e.g. windows xp sp2 without current patches, hosting a website on web server which is not properly configured. In this way attacker attacks on honeypot.

2.4 Classification of honeypots

2.4.1 Classification according to purpose

2.4.2 Classification according to interaction

2.4.1.1 Production honeypots

Production honeypots are the computer system placed in the production system to protect the network from attacker. Production honeypots are generally low level honeypot which are easy to deploy. It helps in protecting the others production system. Attackers are busy in exploiting honeypot. The purpose of production honey pot is to protect network from attack [28]. It is much more difficult to use a production honeypot to attack and harm

other systems. But Production honeypot gives less detailed information rather than Research honeypot and provide a safeguard against the original production system.

2.4.1.2 Research honeypots

Research honeypots are the honeypots whose purpose is to find the new tools and technique used by the black hat community to attack the system. These honeypots are deployed for the purpose of finding the zero day attack. These are the nonprofit organization whose purpose is to do some research. Honeypot provides the detailed information about the attack such as how attacks happen, what are the tools used, how does attacker communicate and their intension. Research honeypots have risk that more allow the attacker and get more information about the attacker technique. There is possibility that attacker use research honeypots to attack on the production system. There is need to balance between what amount of freedom is given to attackers such that research honeypots cannot be misused [28].

2.4.2 Classification according to interaction

2.4.2.1 Low Interaction honeypots

Low-Interaction honeypots are system which emulates the services and easy to setup, config and deploy. The information is provided is not accurate and can be false. It helps to detect known vulnerability and measure how often attackers do the attack low-interaction honeypots are not suitable for detecting the zero day attack. They are easily detectable by an attacker e.g. PHPHOP, googlehack, honeyd [28].

2.4.2.2 Medium Interaction honeypots

A medium-interaction honeypots might more fully implement the http protocol to emulate a well-known vendor's implementation, such as internet information services server. Medium interaction honeypots provide more interaction to attacker as compared to low level Honeypots e.g. suppose an automatic script is propagated in internet to find the vulnerability in the network where it finds web server internet information services vulnerability in the system and try to exploit the web server then honeypots come to

know about the techniques of the hacker. Medium interaction honeypots have emulated services rather than a complete operating system e.g. Medium Interaction honey pot is kippo Medium interaction honeypots provide less interaction as compared to High interaction honeypots.

2.4.2.3 High Interaction Honeypots

High interaction honeypots offer full operating system rather than emulating services Attacker interact with Operating System and has more interaction with the system. The information gathered during interaction is more accurate and know more about the attacker tools and techniques. It has more risk associated to harm the production network system. Attacker hack the honeypot and used for its own use such as distributed denial of service attack, spamming, key logging, make the system as bot to attack on other machine, DHCP starvation attack etc. High interaction honeypot should be properly configured and deployed so that it doesn't harm the production system e.g. Honeynet and High Interaction Honeypots Analysis Toolkit (HIHAT) [34].

2.4.3 Honeynet

Honeynet is collection of honeypots which is high interaction honeypots. Honeynet is used where single honeypot does not provide the sufficient information for various technique used by attacker. Network is large and to secure the whole network. There is need of honeypots that are established at different location. This type of network provide real time system to interact with attacker and it helps the network administrator to know about the vulnerability exist in the network and compromise within the network. Honeynet has no production activity, no authorized services, any interaction with honeynet implies unauthorized activity or an attack preparation technique. There are two types of honeynet according to their implementation [10].

2.4.3.1 Physical Honeynet

Physical Honeynet is the real machine on the network which has an ip address assigned to it. Suppose honeynet contain 15 physical honeypots implies 15 computers are required to implement the honeynet. This technique is high interaction honeypots in which

attacker interact direct with the machine not with the emulating devices. This technique is expensive and difficult to maintain. For large network it is impractical to deploy the physical honeynet [10].

2.4.3.2 Virtual Honeynet

Virtual Honeynet is a solution that allows you to run everything you need on a single computer. Use the term virtual means all the different operating systems have the appearance to be running on their own, independent computer. These solutions are possible because of virtualization software that allows running multiple operating systems at the same time, on the same hardware. Virtual honeynet are not a radically new technology, they simply take the concept of honeynet technologies, and implement them into a single system. Virtual honeynet has advantage easy to deploy, less cost and are limited to what types of operating system [11].

1) Most virtual honeynet are based on the Intel X86 chips, so it is limited to operating systems based on that architecture. It cannot deploy a VAX, or cray computer within a virtual honeynet [26].

2) Virtual Honeynet come with a risk. An attacker may be able to compromise the virtualization software and take over the entire honeynet, giving them control over all the systems [26].

3) There is the risk of fingerprinting. Once the bad guys have hacked the systems within the virtual Honeynet, they may be able to determine the systems are running in a virtual environment.

Virtual Honeynet into two categories: - Self-contained and Hybrid.

2.4.3.2.1 Self contained honeynet

Self Contained is type of virtual honeynet in which one system contain the whole honeynet in itself [14]. A self contained honeynet network typically consists of a firewall gateway for data control and data capture, and the honeypots within the honeynet in the single system as shown in Figure 2.1 [11].

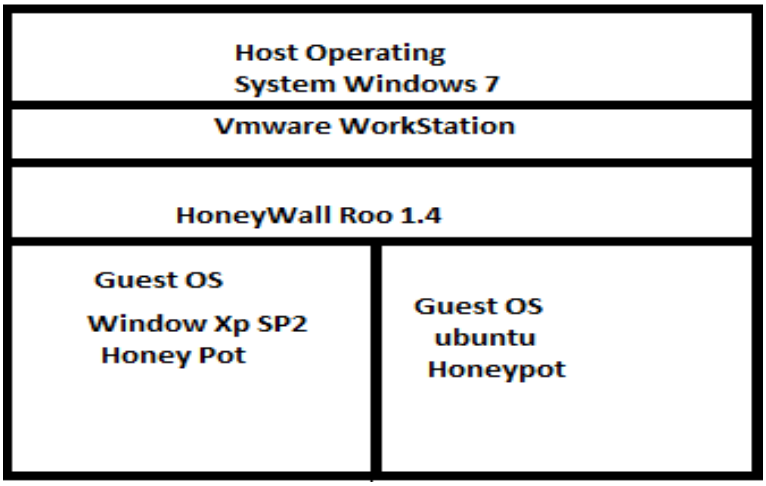


Figure 2.1 Self contained virtual honeynet architecture

2.4.3.2.2 Hybrid virtual honeynet

A Hybrid virtual honeynet is a combination of the classic honeynet and virtualization software. Data capture such as tcpdump, snort, sebek and data control such as rate limiting, iptables are on a separate isolated system. This isolation reduces the risk of compromise [14]. All the honeypots are virtually run on a single system as shown in Figure 2.2.

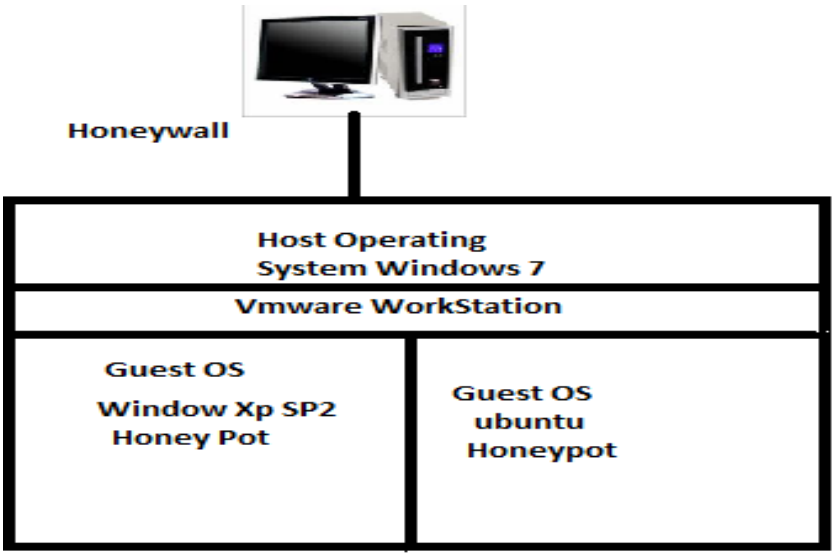


Figure 2.2 Hybrid virtual honeynet architecture

2.5 Honeywall CDROM Roo architecture

The Honeywall CDROM is a bootable CDROM that installs all of the tools and functionality necessary to quickly create, easily maintains and effectively analyze a third generation honeynet. Honeywall cdrom roo is the second version of our CDROM series, released in May, 2005. The first Honeywall CDROM Eeyore was released in May, 2003, but is now considered out of date and is no longer maintained [12].

2.5.1 Data Capture

The purpose of Data Capture is to log all of the attacker's activity. This is the whole purpose of the Honeynet, to collect information. Without Data Capture, Honeynet has no value. The key to Data Capture is collecting information at as many layers as possible [6]. No single layer tells us everything. What happens when the attacker launches a tool, how will you know what the tool does if you do not capture the network traffic. The Honeynet Project has identified three critical layers of Data Capture firewall logs, network traffic, and system activity. Chapter 4 contains the implementation of high interaction honeypot [9].

2.5.1.1 Sebek

Sebek is a tool for monitoring high interaction honeypot. It is basically a root kit-style kernel module or patch and supports Linux, centos, win32 platforms. It hooks system read/write calls to capture attacker's keystrokes, file access and other input/output activity. This data is then exported over the network via udp packets, so another function of Sebek is to hide this monitoring traffic from the attacker as well as hiding its own presence on the machine. Host level data capture capabilities are particularly useful when encryption technologies would otherwise result in attacker activity going undetected by plain text network based IDS devices or packet capture based solutions [13].

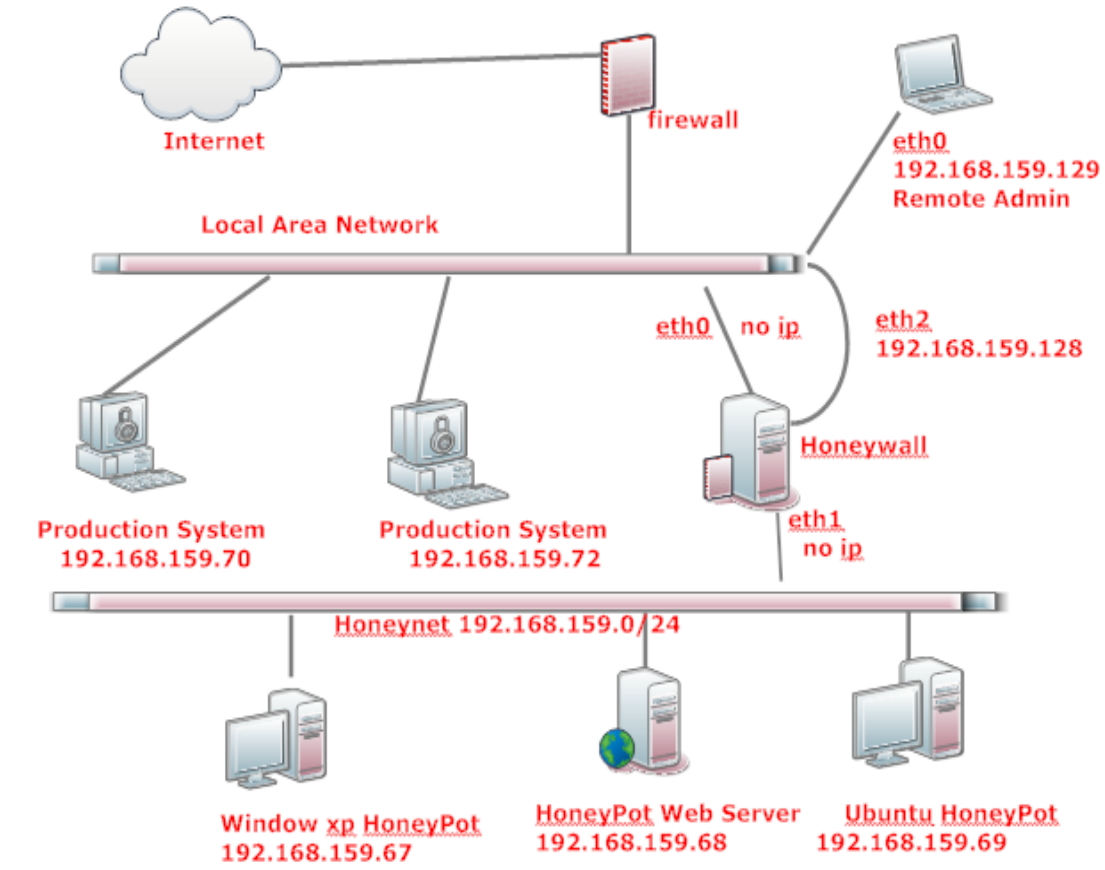


Figure 2.3 Honeynet Architecture Diagram

2.5.1.2 P0f

A passive network fingerprinting utility for use in honeypots environments. An operating system fingerprinting utility that is very versatile and fast. It is useful in monitoring trac coming into a honeynet since it can help identify ip addresses where the host OS is changing. The information from p0f is correlated with argus and snort for a clearer picture of the known flow information [8],[14].

2.5.2 Data Control

The purpose of data control is to prevent attackers using the honeynet to attack or harm other non-honeynet systems. Data control mitigates risk, it does not eliminate it [6]. With Data Control how much outbound activity do you control or allowed. The more allow the

attacker to do, the more administrators can learn. However, the more the honeywall allow the attacker to do, the more harm they can potentially cause. So, allow to such an extent such that contain their activity enough so they can't harm other production system, to learn allow the attacker to do tasks. How much administrator allows an attacker to do ultimately depend on how much risk you are willing to assume. To accomplish this there are two technologies connection counting and NIPS. Connection counting is limit how many outbound connections a honeypot can initiate. NIPS (Network Intrusion Prevention System) can block known attacks. Combined, these two technologies make a redundant and flexible data control mechanism and implement Data Control on the gateway. To implement connection limiting, there should be limit on how many outbound connections an attacker can initiate from a honeypot. The purpose here is to count outbound connections, and when a certain limit has been met, block any more connections. This is primarily used to reduce the risk of mass scanning, attacking, or denial of service attacks, activity that requires many outbound connections as shown in Figure 4.11.1.

2.5.2.1 Iptables

For data control iptables is used which is a firewall implementing certain rule on inbound and outbound traffic. Its purpose is to have the unique aspect of providing the appearance of a secure network. Iptables allow the traffic from eth0, eth1 and contain very less rule and allow the attacker to attack on machine. When it comes to the management interface, it does maintain the traditional role of a firewall by allowing access only to honeywall users and admins. This is done by restricting ip addresses and networks that can access the management interface and only allowing specific types of traffic out such as TCP port 443.

2.5.2.2 Snort IDS and Snort-inline IPS

Snort as an Intrusion Detection and Prevention System is integrated into Honeywall 1.4. It is an open source IDS, rule and signature based engine that can be run in one of the following modes:

1) Sniffer Mode:-In this mode Snort is used as packet sniffer and displays IP headers on the screen [35].

2) Logger Mode:-All packets are logged into the file and can be used for further analysis. Snort logs are saved in /var/log /message as shown in Figure 4.35.

3) Network Intrusion Detection Mode: - The core mode of Snort in which all incoming packets will be analyzed based on the user defined rules and signatures. Snort will log, detect and alert if there is any anomaly detection in the packets then inline mode. In this mode, Snort acts as an Intrusion Prevention System (IPS) which is called Snort-inline. It resides on the honeywall where the packets are analyzed and monitored using iptables in order to control outgoing packets from the honeypot. If the honeypots are compromised by worm, Snort Inline will prevent the attackers from compromising other machines in the same network. By using inline mode, Snort is able to perform the modify, reject, ignore actions against the packets which content matches the known attack. Modify action is very important for a honeynet. It allows modifying the content of the attack packets and rendering them harmless. In this case intruders cannot be aware of the changes in the packet.

2.5.3 Data Analysis

2.5.3.1 Walleye

Walleye web interface: - A web based interface for honeywall configuration, administration and data analysis. Walleye is used for analysis the inbound and outbound traffic through a web browser client by typing https://192.168.159.128/. For security reason, this interface is accessible over port 443 [18]. Walleye has two main functionalities.

2.5.3.1.1 Data Analysis

The Data Analysis is used for analyzing real time flows, overview of incoming and outgoing flows, Sebek based data, alert flows by the Snort IDS, who is capability, and activity summary per day. Walleye also provides downloading the packet data in pcap

format which we used for further analysis with wireshark on our remote management machine. System administration allows remote honeywall administration, provides access to the honeywall configuration, thus all the settings can be updated from this interface. With walleye see the examination of all connections for one day aggregated connections to each honeypot per day, number of IDS events, and most connected destination and source IP addresses and ports. Walleye helps in analyzing one connection in detail for the particular IP address. In Walleye, one is able to drill down through a particular data flow by date and time of day. If the logs grow too large, then Walleye will timeout while trying to display them and stopped functioning. Make a proper screenshot of the machine so that functioning does not interrupt if the walleye is not working.

2.5.3.1.2 System administration

With the help of walleye system administration is possible remotely as show in chapter 4 in detail such manage configuration files, Emergency lock down restart honeywall process remotely shown in Figure 4.36 to 4.38.

2.5.4 Honeywall tools

2.5.4.1 HWCTL

This is a powerful command line utility that allows you to configure the system variables used by various programs, and the ability to start/stop services. The advantage with this tool is you can simply modify the behavior of the system at the command line via local. It allows automated scripts to connect to remote system and change the system configuration, a feature critical for distributed environments [15].

2.5.4.2 Dialog Menu

Like the hwctl utility, it can be used with local access. It is graphic based, but its capabilities are limited. To use dialog menu use menu command with root privilege [15].

2.6 Honeynet Advantage

2.6.1 Zero day attack

Honeynet helps in finding zero day attack. A zero day (or zero hour or zero day) attack or threat is a computer threat that tries to exploit computer application vulnerabilities that are unknown to others or the software developer. Zero day exploits (actual software that uses a security hole to carry out an attack) are used or shared by attackers before the developer of the target software knows about the vulnerability [32].

2.6.2 Small data sets of high value

Honeypots collect small amounts of information. Instead of logging a one GB of data a day, they can log only one MB of data a day. Instead of generating 10,000 alerts a day, they can generate only 10 alerts a day. Honeypots only capture bad activity, any interaction with a honeypots are most likely unauthorized or malicious activity. As such, honeypots reduce noise by collecting only small data sets, but information of high value, as it is only the bad guys. This means it's much easier to analyze the data, honeypot collects and derive value from it.

2.6.3 New tools and tactics

Honeypots are designed to capture anything thrown at them, including tools or tactics never seen before.

2.6.4 Minimal resource

Honeypots require minimal resources, they only capture bad activity. An old Pentium computer with 128MB of RAM can easily handle an entire class B network.

2.6.5 Information and Simplicity

Honeypots can collect in depth information. Honeypots are conceptually very simple. There are no fancy algorithms to develop, state tables to maintain, or signatures to

update. The simpler a technology, the less likely there will be mistakes or misconfigurations.

2.6.6 Improve the security of the network

Honeypots help in protecting the production system from attack and improve the security of the network and complements the firewall, IDS.

2.7 Honeynet Risks and Issues

Any technology developed by man can also be defeated by man risk means different things to different organizations. There is need to identify what risks are important to the organization. Organizations have different thresholds for risk. Administrator cannot determine what is right and wrong for the organization. The organization will have to make those policy decisions for it. There are four general areas harm, detection, disabling and violation [33].

2.7.1 Harm

Harm is when a honeynet is used to attack or harm other, non honeynet systems. For example, an attacker may break into a honeynet, and then launch an outbound attack never seen before, successfully harming or compromising its intended victim. Data Control is the primary means of mitigating this risk. Multiple layers of Data Control are put in place to make it more difficult for the attacker to cause damage. However, there is no guaranteed method to ensure that a honeynet cannot used to attack or harm someone else. No matter what mechanisms are put in place, an attacker can eventually bypass them.The Organization will have to decide how much risk it is willing to assume. For low risk organizations, It does not allow outbound activity (count to zero). For organizations with greater risk thresholds, It allows greater outbound activity.

2.7.2 The risk of detection

Once the true identity of a honeynet has been identified, its value is dramatically reduced. Attackers can ignore or bypass the honeynet, eliminating its capability for capturing information. Perhaps even more dangerous is the threat that once identified, an attacker can introduce false or bogus information into a honeynet, misleading your data analysis. For example, with local access to the honeynet, an advanced attacker, or an attacker armed with proper tools, can potentially identify that a honeynet is in place and may even identify the honeynet data control.

2.7.3 Disabling honeynet functionality

This could be an attack against either Data Control or Data Capture routines. Attackers may want to not only detect a honeynet's identity, but disable its Data Control or Data Capture capabilities, potentially without the honeynet administrator knowing that functionality has been disabled e.g. an attacker may gain access to a honeypots within the honeynet, and then disable Data Capture functionality on the honeypots. The attacker could then feed the honeypots with bogus activity, making administrators think. Data Capture is still functioning and recording activity. Having multiple layers of Data Control and Data Capture helps to mitigate this risk, as there is no single point of failure.

2.7.4 Catch all of remaining risk

Attackers may attempt criminal activity from the compromised honeynet without actually attacking anyone outside your honeynet. One example is an attacker using a honeypots to upload, and then distribute illegal material, such as illegal copies of movies, music, stolen credit cards, or child pornography. This individual broke into the system on their own initiative. If detected, this illegal activity would be attributed (at least initially) to organization by way of it being on the organization system. Organization may then have to prove to that it was in fact not organization system who was responsible for this activity.

2.8 Solution

2.8.1 Human monitoring

By human monitoring, mean organization have a trained professional monitoring and analyzing the honeynet in real time. This gives the ability to detect a failure in the system, a failure that automated mechanisms may fail to detect or react to. By having a human analyzing honeynet activity, instead of just depending on automated techniques, It helps to protect the organization against new or unknown attacks, honeynet countermeasures.

2.8.2 Customization

All honeynet technologies, including the Honeywall CDROM are Open Source and publicly available. This means that anyone has access to this information, including the black hat community, which are actively reading this and developing countermeasures. To help reduce risk there is a need to modify the honeynet from any default settings or normal behavior. The more the honeynet differs from standard or default configurations, the more difficult it will be others for detect or attack it. However, it's critical that understand that no matter what measures an administrator takes, risk is not eliminated, only mitigated. Honeynets are a form of a high-interaction honeypots. Their primary advantage is their ability to gather extensive information. A honeynet is architecture. Within this architecture Organization can deploy any type of system or application desire. The critical requirements for this architecture are Data Control, Data Capture, Data Analysis and Data Collection, with Data Control taking the priority. While very powerful, honeynet present unique risks. Mechanisms can be put in place to mitigate these risks, but there is no way to eliminate all risk, it is critical to understand this.

2.8.3 Fingerprinting

Fingerprinting may be possible to fingerprint the VMware software on a honeypots, especially if the VMware tools are installed on the systems. VMware workstation does have options that can make fingerprinting more difficult, such as the ability to set the MAC address for virtual interfaces.

Chapter 3

Problem Statement

3.1 Problem definition

In the college campus there is a lot of attacks by attacker either from outside as well as inside. In campus attackers who have good knowledge in computer domain are doing the attack. The attack techniques are arp spoofing, ip spoofing, dynamic filtering, ddos, packet craft, and operating system fingerprinting to exploit the simple user. External attacker tries the new techniques to exploit the network using the different technique. Some of the attacks are new techniques are called zero day attack technique. Using honeypots, an administrator came to know about the new type attacks and write their signatures of attack and take the prevention action. To prevent the user and network from these threats. There is a need of security mechanism to handle this scenario. The solution is honeypots.

Honeypots are designed for corporate environment, are not free and customization of honeypots are difficult. Honeypots should be monitored remotely, but simple honeypot doesn't provide this functionality, those honeypots that provide this functionality are difficult to install, configure and maintain. Free honeypots have outdated documentation for new version of that honeypots and their forums contain only question and not the answers.

Objective

1. To design & implement IIIrd generation honeynet architecture using High Interaction honeypots for proactive monitoring of Campus network.
2. To detect the attacker's technique used for attacking the honeypots.
3. To validate the vnc server vulnerability of honeypot using MS08-067.

Chapter 4

Implementation and Results

4.1 Self contained virtual high interaction honeynet

Self contained virtual honeynet integrate the whole network into only one physical system. These kinds of virtual honeynet have several advantages.Self contained virtual honeynet has central management in which administrator has one physical system from where he can manage very easily. As for honeynet there is one physical system is enough. It has low cost as only one machine is required. Self contained virtual honeynet is portable, if installed on a laptop. Take this laptop in any network, become the part of network and then leave the honeypots to alive to find the attackers tools and technique. Honeynet is easier to deploy and only one system needs to be implemented, connected and work is done.

Limitations should also be kept into account when using self contained virtual honeynet. First limitation is VMware only supports x86 platforms. This limits the software that can be used in the honeynet. Second problem is with the hardware would affect the entire honeynet. Third is a powerful system is needed, depending of the kind and number of guest os used. Fourth is the virtualization software is susceptible to being compromised by an attacker that could take control over the entire honeynet and an expert attacker inside a compromised honeypots can easily determine if it is a virtual environment.

4.2 Tools necessary for the high interaction honeynet

1. VMware workstation 6.5
2. Honeywall cdrom roo1.4
3. Window xp sp2
4. Ubuntu 11.04

5. Backtrack 5 kde

6. Nmap

7. Wireshark

4.3 VMware Workstation

VMware is virtualization software that allows the running of multiple operating systems at the same time on Intel x86 architectures. It was developed by VMware Inc. and it has three product lines, namely Workstation, GSX, and ESX. Here the Workstation version is used. Install the VMware workstation 6.5. Create three types of network interfaces for Honeywall as shown in Figure 4.2.

1. VMnet 0 - bridged with the host OS Ethernet connection.

2. VMnet 1 - host –only connection. The devices connected to this are in the same network with the host operating system.

3. VMnet 8 – NAT. This is used for the remote management interface of honeywall.

4.3.1 Features of Vmware

VMware products also have some nice features like the ability to suspend a virtual machine. Pause the vmware, and take it out of suspension, all the processes go on like nothing happened. Once a system was compromised and the intruder started an attack. To prevent this attack cut the connection means lose valuable information. Solution is suspend the vmware, adjusted the firewall to block the attack, then brought the vmware back up. An interesting use of vmware is the ease and speed of bringing up. Once a honeynet is compromised, and learn as much as from it. Another feature of vmware Workstation is the ability to run several networks behind the host operating system. For a single machine a honeynet and personal computers all on the one system without worrying about data pollution [7].

4.4 Installing and configuring the honeywall

Configuring the honeywall is the most important step in setting up honeynet. Honeywall acts a gateway between the external network and the network of honeypots. Before configuring the honeywall assign valid IP address to all the honeypots, honeywall and remote machine. Figure 4.1 show the screenshot of the installation of honeywall cdrom roo [15].

Figure 4.1 Installing honeywall cdrom roo gateway

After installation add three network interfaces and configuring according to Figure 4.2. Honeywall is a gateway device that separates the honeypot from the rest of the world. Any traffic going to or from the honeypots must go through the honeywall. This gateway is traditionally a layer 2 bridging device, meaning the device should be invisible to anyone interacting with the honeypots. Honeywall has 3 interfaces. The first 2 interfaces (eth0 and eth1) are separate the honeypots from everything else, these are bridged interfaces that have no IP stack. The 3rd interface (eth2, which is optional) has an IP

stack allowing for remote administration and assign ip address to eth2 as shown in Figure 4.3.

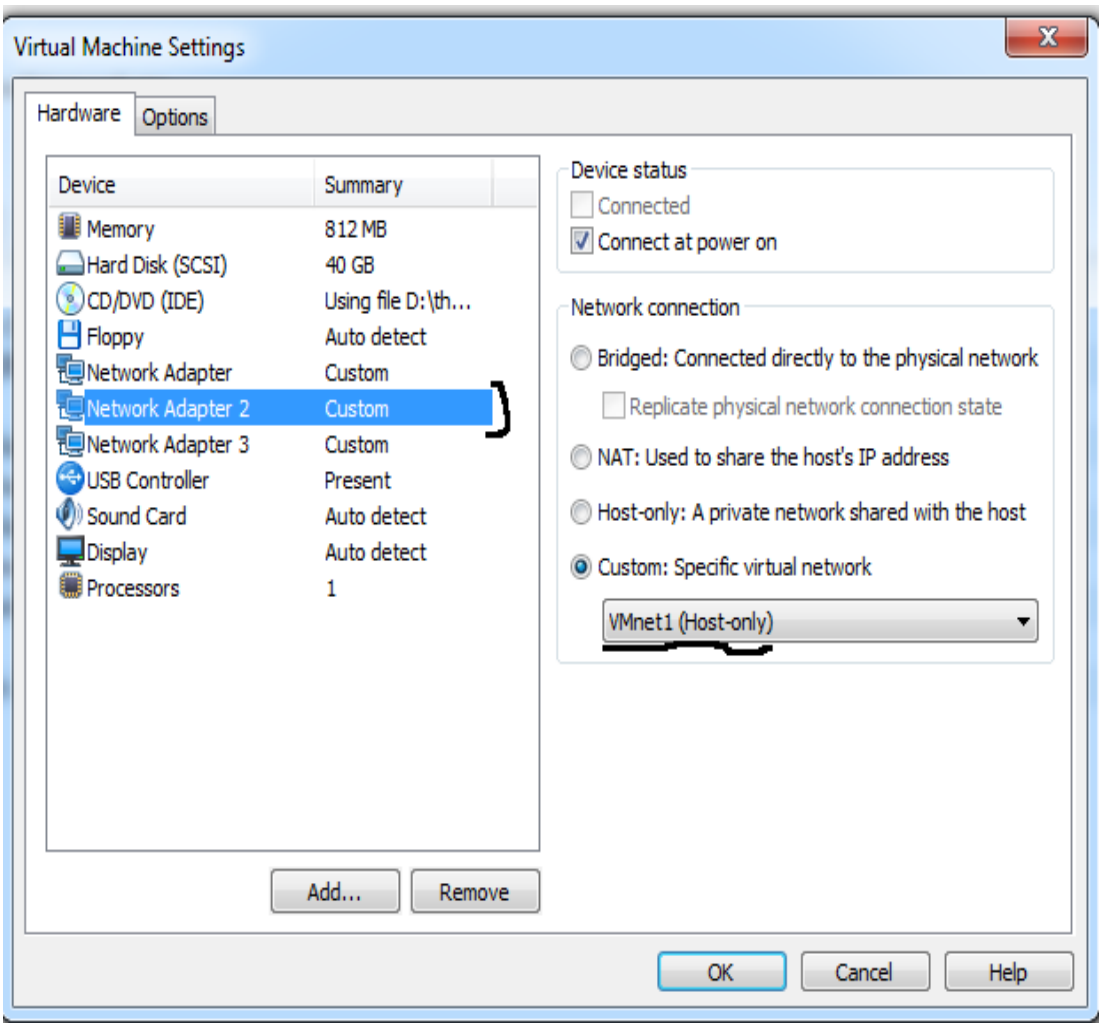


Figure 4.2 Honeywall gateway network adapter2 settings

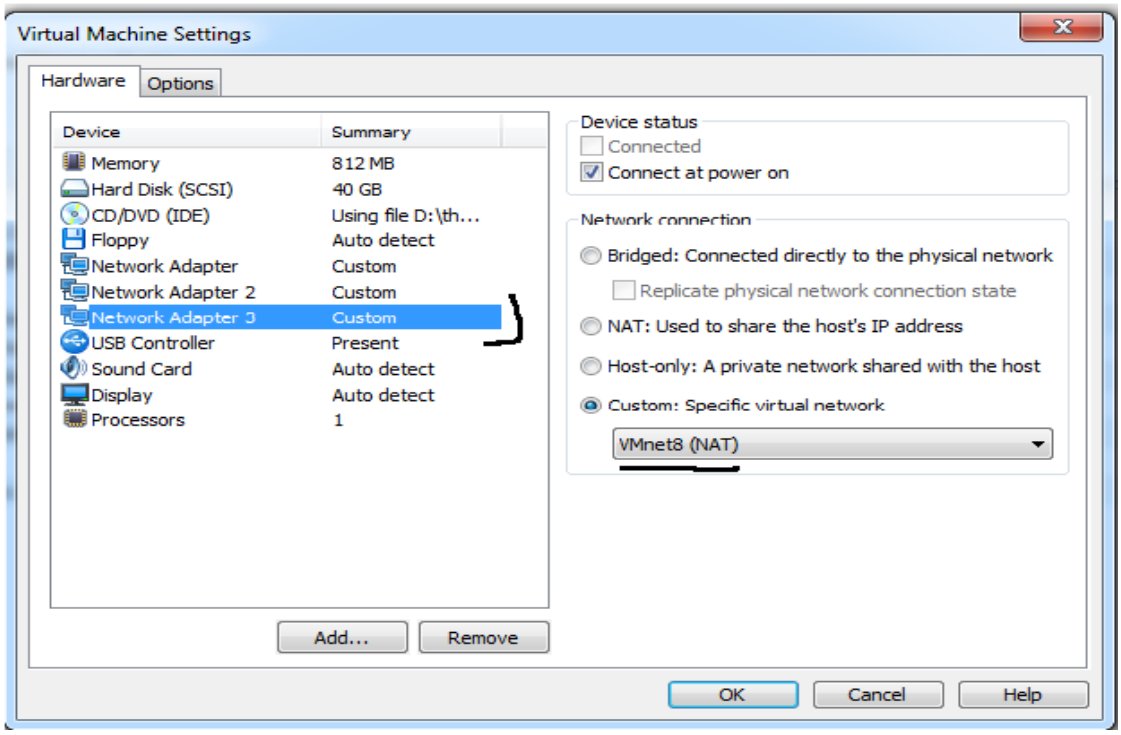


Figure 4.2.1 Honeywall gateway network adapter 3 settings

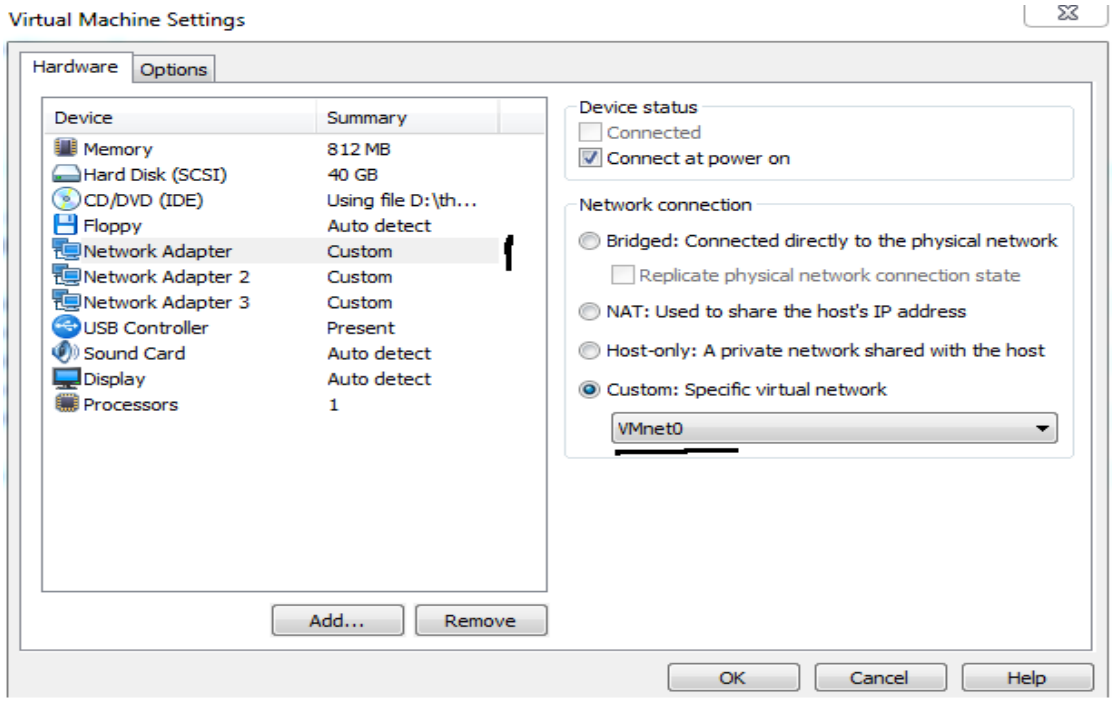


Figure 4.2.2 Honeywall gateway network adapter settings

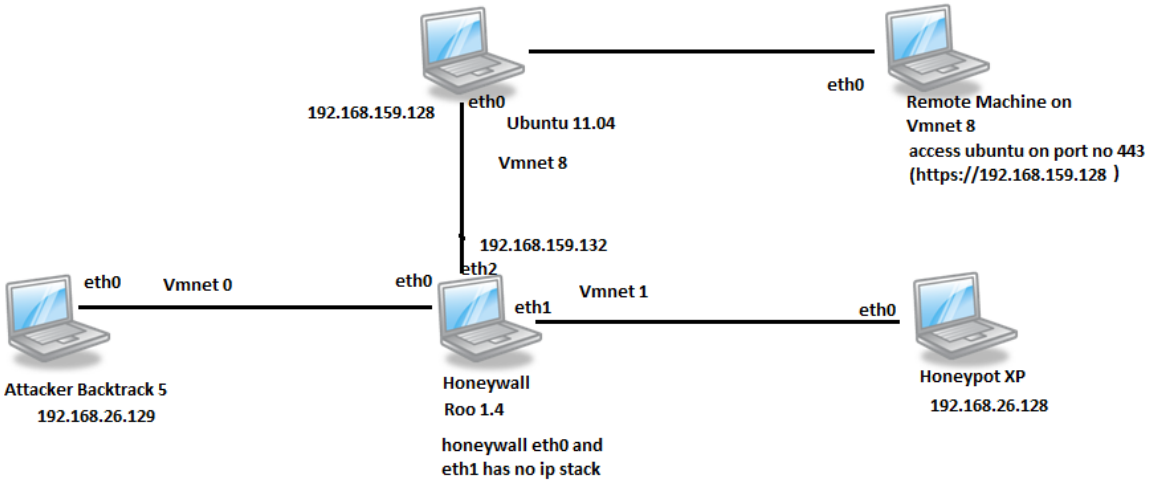


Figure 4.3 Honeynet architecture for high interaction honeynet with their ip addresses

4.5 Installation details

In this architecture honeywall has three network interfaces eth0 is in vmnet 0 and connects to the virtual ethernet device of the vmware. The second network adapter eth1 is used to connect the honeywall system to the honeypots. The third network interface Adapter eth2 is used for management purposes. The following sections describe how to setup and configure the system to create a virtual honeynet in vmware.

The steps to setup a virtual honeynet:

1. Install vmware 6.5 in the host windows 7 operating system.

2. Install honeywall cdrom roo 1.4 and its name is honeywall and the install windows xp as a honeypot in the virtual machine named as XP.

3. Install ubuntu 11.04 for management purposes and named as ubuntu 11.04.

4. Install window xp for remotely access the management interface eth2 and named it as window xp.

5. Install backtrack 5 for attacking on Honeypots and named as BT.

6. Assign ip address to XP, ubuntu, BT, window xp according to Figure 4.3.

7. In honeywall add three network interfaces in the honeywall operating system. The setup vmware networking according to design as shown in above Figure 4.3, see the Figure 4.2,4.2.1,4.2.2 and assign ip to eth2 interface, whereas eth0 and eth1 has no ip stack.

8. In Honeywall eth0 has on virtual network Vmnet0 which is in bridge mode by default. Second network interface eth1 has on virtual network Vmnet1 which is in Host only mode. Third network interface on eth2 has on virtual network Vmnet 8 which is NAT.

4.6 Prerequisite for honeywall configuration in vmware

1) All honeypots, remote machine and attacker have valid IP address as shown in Figure 4.3 and has subnet as according to design. Check the ip address by ipconfig in windows, for ubuntu, roo use ifconfig and write down ip address and mac address corresponding to those machines. It will help in understanding the analysis of attack and scenario [28][21].

2) Take a printout of Figure 4.3 to understand the topology, check the configuration with this printout so that any mistake can be corrected.

4.7 Configuring Honeywall

1) Power on the honeywall and use the roo account to login with password honey and then use su - command to get the root privileges in order to configure honeywall or perform other administrative tasks, check your directory by using pwd command if it shows /root means you have privileges as shown in Figure 4.4 [22].

2) Activate yum repository

By default, centos have its repositories turned off. This means that centos servers do not receive software updates by default. Since honeywall is built on centos in order to update the software in honeywall, some of the repositories have to be activated. Normally this is done by editing ASCII files found in /etc/yum.repos.d/. The honeywall project has simplified this by making a useful tool called hwrepoconf, which requires root access. Use the command to enable the repository.

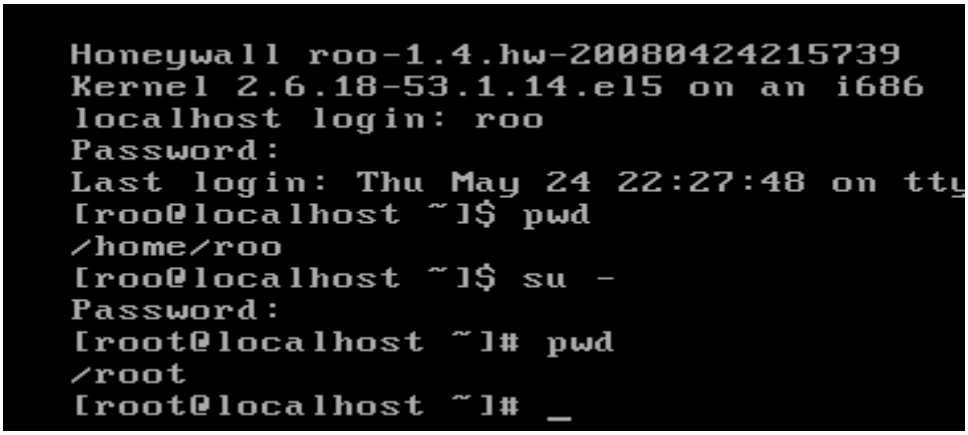


Figure 4.4 Honeywall login with username roo and password honey

hwrepoconf --enable epel os-base os-extras os-updates

hwrepoconf – show

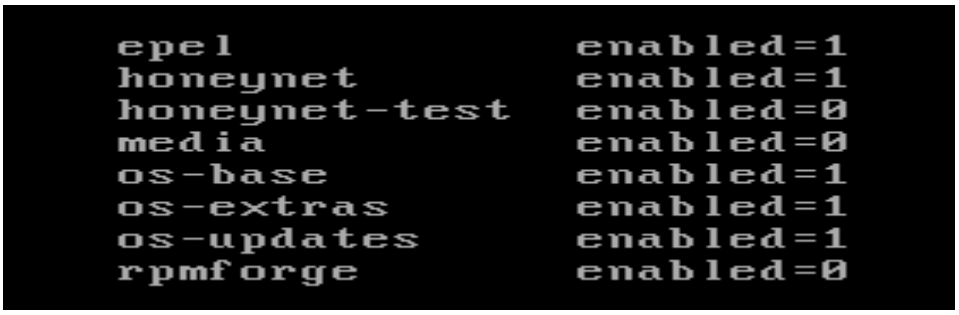


Figure 4.5 Activate the yum repository by using hwrepoconf

To enable the repository such as epel, os-base, os-extras, os-updates. It shows the output as shown in Figure 4.5

4.8 Honeywall.conf file

1) Open vim /etc/honeywall.conf file and assign these values to the corresponding parameters [18].

Parameters	Values
HwWALLEYE	Yes
HwMANAGER	192.168.159.0/24
HwTIME_SVR	blank
HwHEADLESS	No
HwMANAGE_IP	192.168.159.128
HwMANAGE_DNS	Blank
HwMANAGE_IFACE	eth2
HwHONEYWALL_RUN	Yes
HwMANAGE_DIALOG	Yes
HwMANAGE_NETMASK	255.255.255.0
HwALLOWED_TCP_IN	443
HwMANAGE_GATEWAY	192.168.159.132
HwMANAGE_STARTUP	Yes
HwALLOWED_TCP_OUT	443

Table 4.1 Honeywall.conf file parameter for management interface

2) The honeywall.conf file has been properly configured, the next step is to open a web browser in remote machine whose ip is 192.168.159.135 and navigate to the ip address assigned to management machine. This is a secure connection on port 443, so use https://192.168.159.128/ in the URL. Once the webpage loads, a login prompt will appear

in the middle of the page. Use roo for the user and honey for the password. Upon a successful login, following screen shot help in configuring the honeywall [18].

4.9 Honeywall configuration through walleye

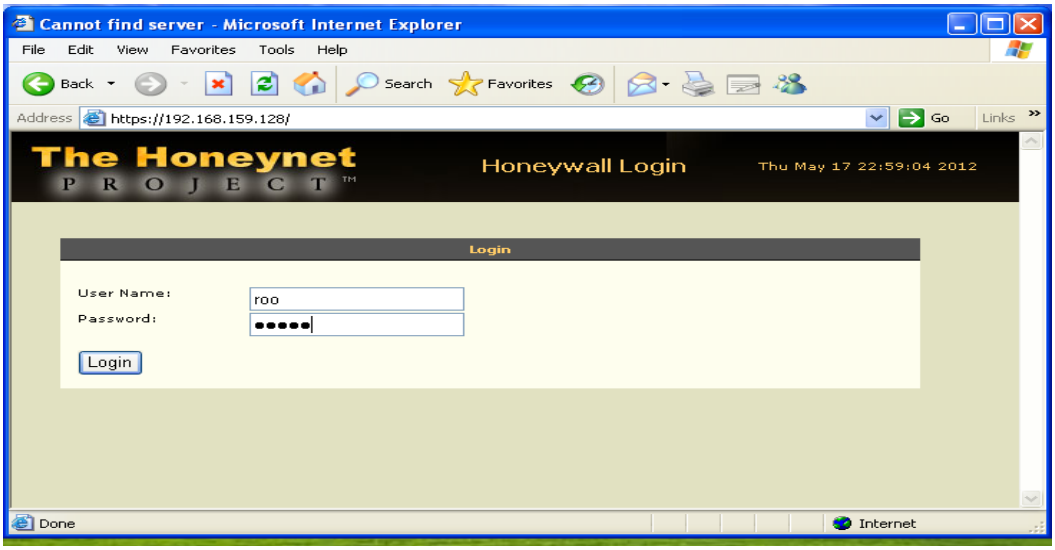


Figure 4.6 Walleye login page roo username and password honey [23]

Figure 4.7 Change the roo password

4.9.1 Honeywall filtered page

After successful login there is a data analysis section which contains the detailed information when apply the filters. This page shows a various filters of the honeywall. The purpose of the page is to give an overview of honeywall activity. Anything listed as bidirectional is defined as any flow for which data is sent in both directions from Client to Server and Server to Client. Total includes both bidirectional and unidirectional flows. In addition it shows network traffic. Anything in blue you can click on for more information. Click on the identification number of your honeywall sensor, get a more detailed overview of all the activity on that sensor. The sensor detail section provides administrative summary data about the honeywall and a top talkers report for the last 24 hours. The admin summary is geared towards distributed environments and provides a description of the geographic and organizational location of the honeywall. The top talker's reports show the 25 most active sources for and destinations of network connections. This page is a menu for querying specific IP based information. Its relatively self explanatory and search based on time/date, IP address and ports[20] [21].

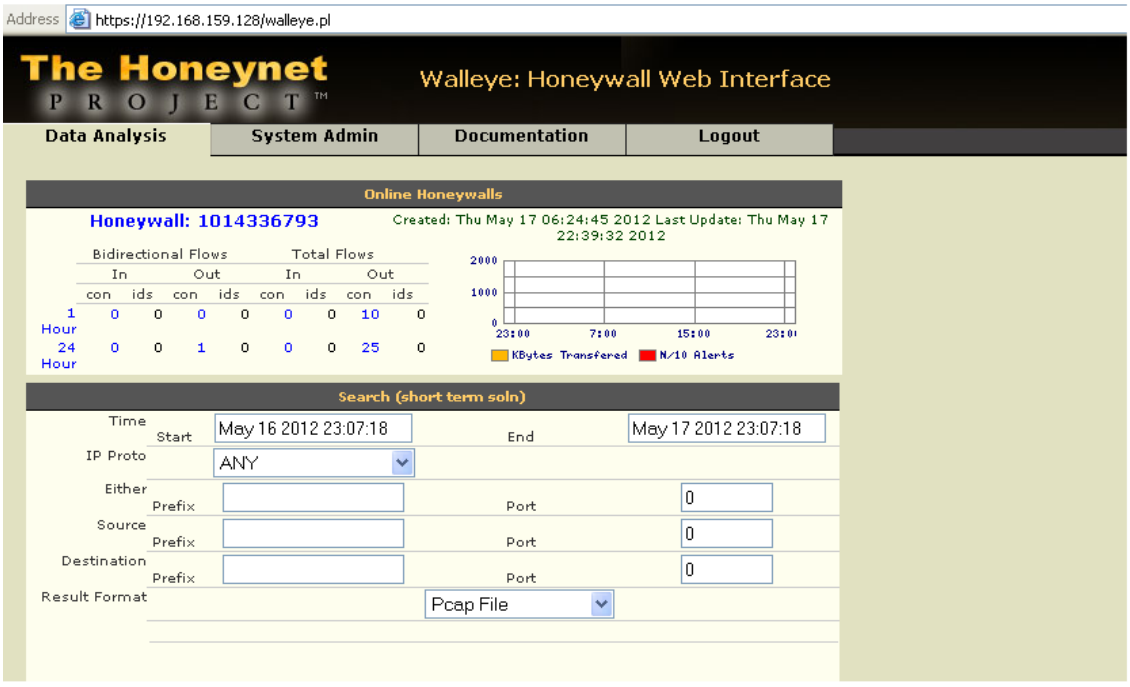


Figure 4.8 Walleye filtered page with sensor id 1014336793

4.9.2 **Manage User**

Add user for walleye who has the rights to analyze and see all the log and attack details of honeynet.

Figure 4.9 Create new administrators for walleye

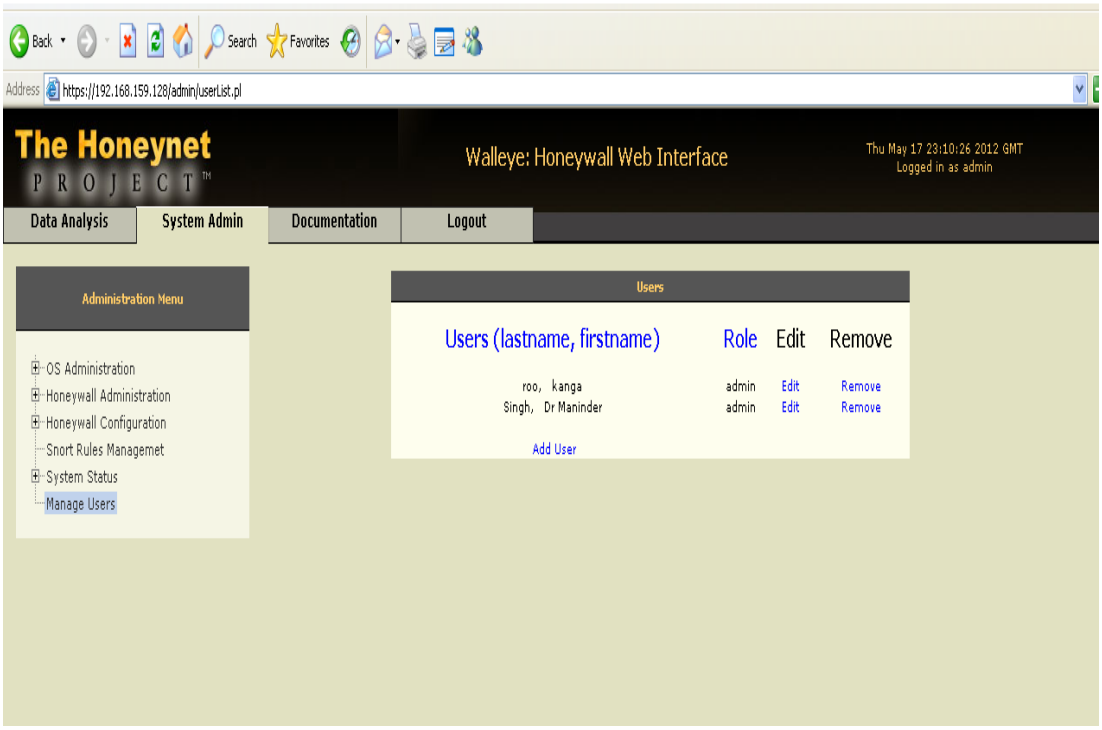


Figure 4.10 Walleye user list and add more users

4.9.3 Honeywall Configuration

4.9.3.1 Honeypots ip address

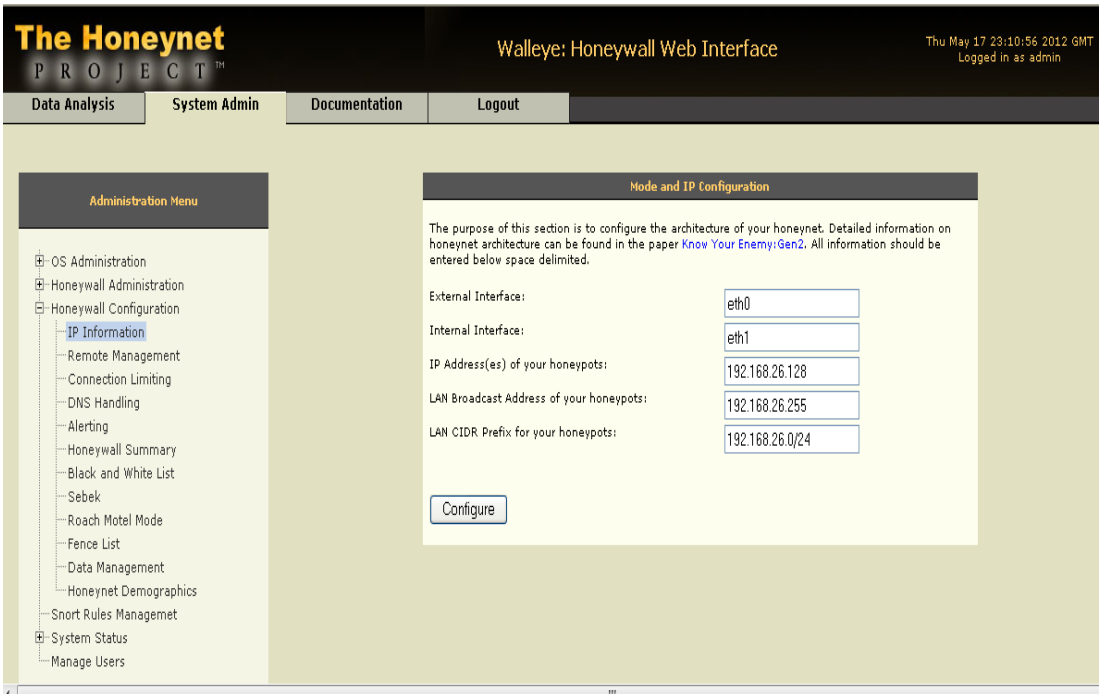


Figure 4.11 Assign the ip address of honeypot

4.9.3.2 Connection limiting

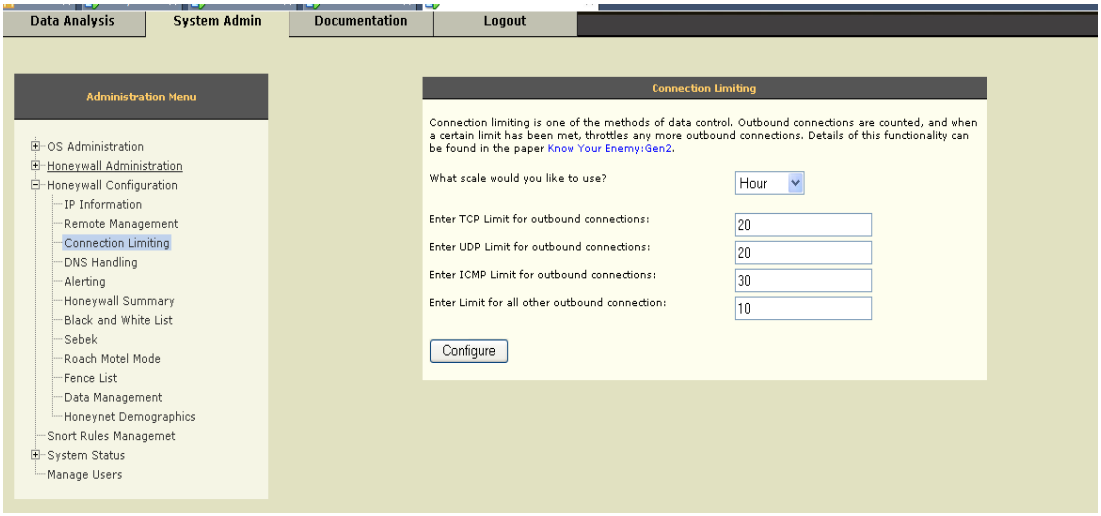


Figure 4.11.1 Limiting the outbound connection for honeypot

4.9.3.3Alerting

Email alert is the most important technique to alert the administrator to check the attack on honeypot.

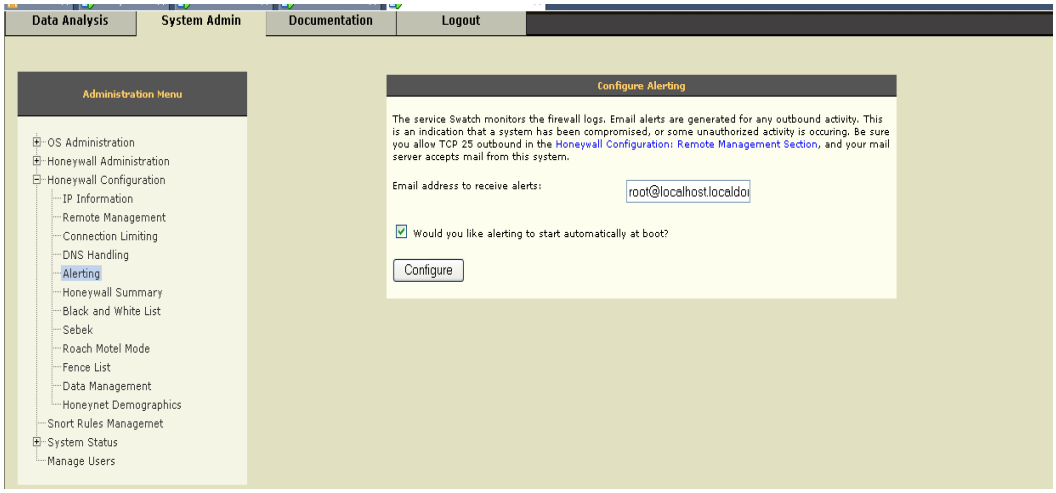


Figure 4.12 Email alert to administrator for outbound activity from Honeypot

4.9.3.4 Sebek configuration

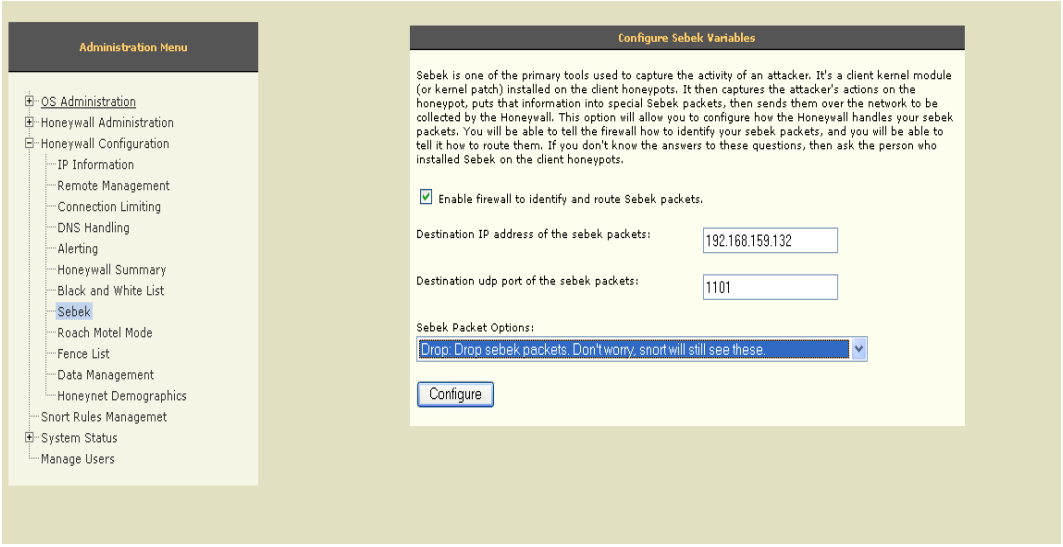


Figure 4.13 Sebek configurations setting to destination port 1101

4.9.3.5 Data Management

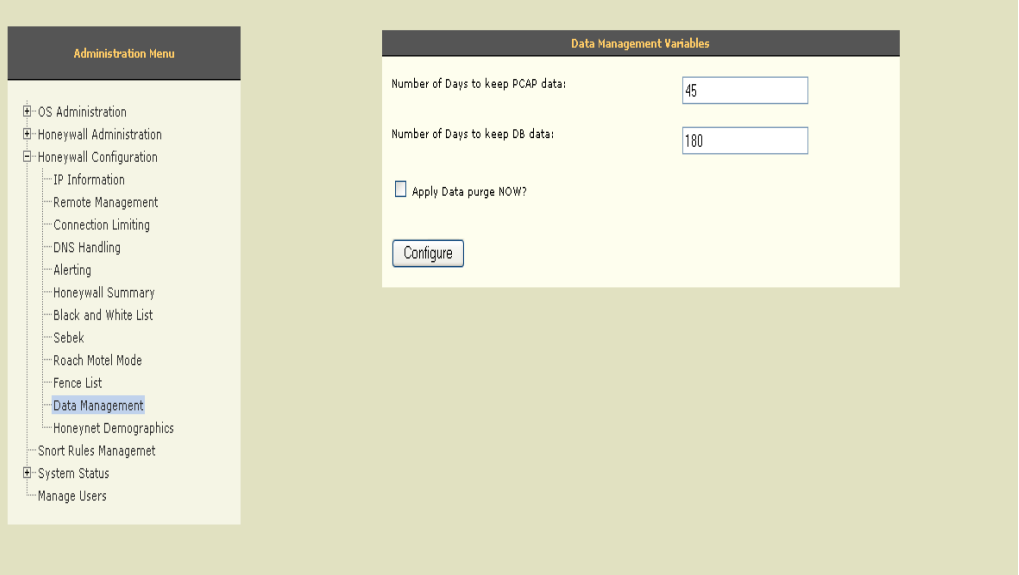


Figure 4.14 Data management to keep the data for certain days

The sensor section provides an overview of the activity the honeywall sees. Sensor identification is based on the management IP address of the honeywall. If IP address of the honeywall is changed, It will have multiple sensors listed (there is no way to delete old ones) as shown in Figure 4.15.

4.9.3.6 Honeynet Demographics

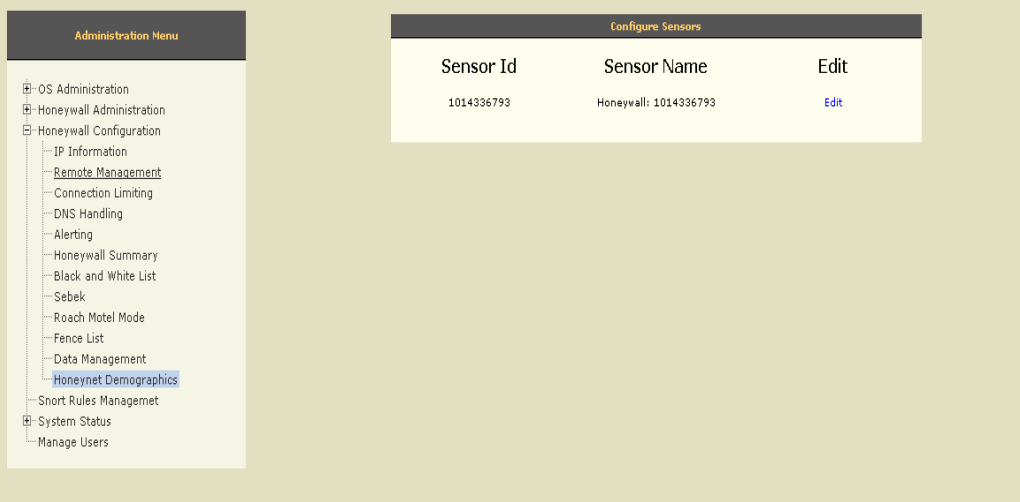


Figure 4.15 Honeynet demographics sensor id details

4.9.3.7 Snort rule management

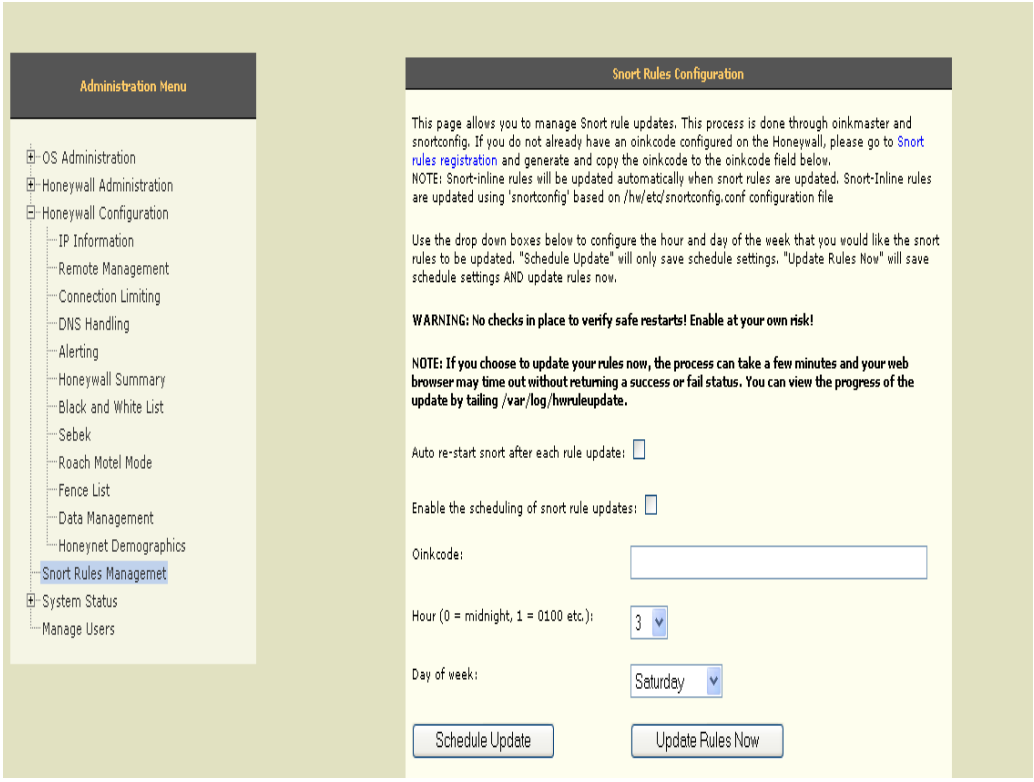


Figure 4.16 Timing of snort rules updates

4.10 Attack on the honeypots

Honeywall provide two ways to analyze the attacker activity either pcp file and walleye graphical representation [24].

4.10.1 Pcap file

4.10.1.1 Banner grabbing

Honeywall detect the attacker at this ip address 192.168.126.129 try to grab the banner of http, telnet, ftp of the honeypots.

1) Attacker send telnet syn packet to honeypots and honeypots send RST and ACK flag to the attacker as shown in Figure 4.17.

2) When the attacker send http SYN packet to honeypots, honeypots replies with SYN and ACK flag with banner information.

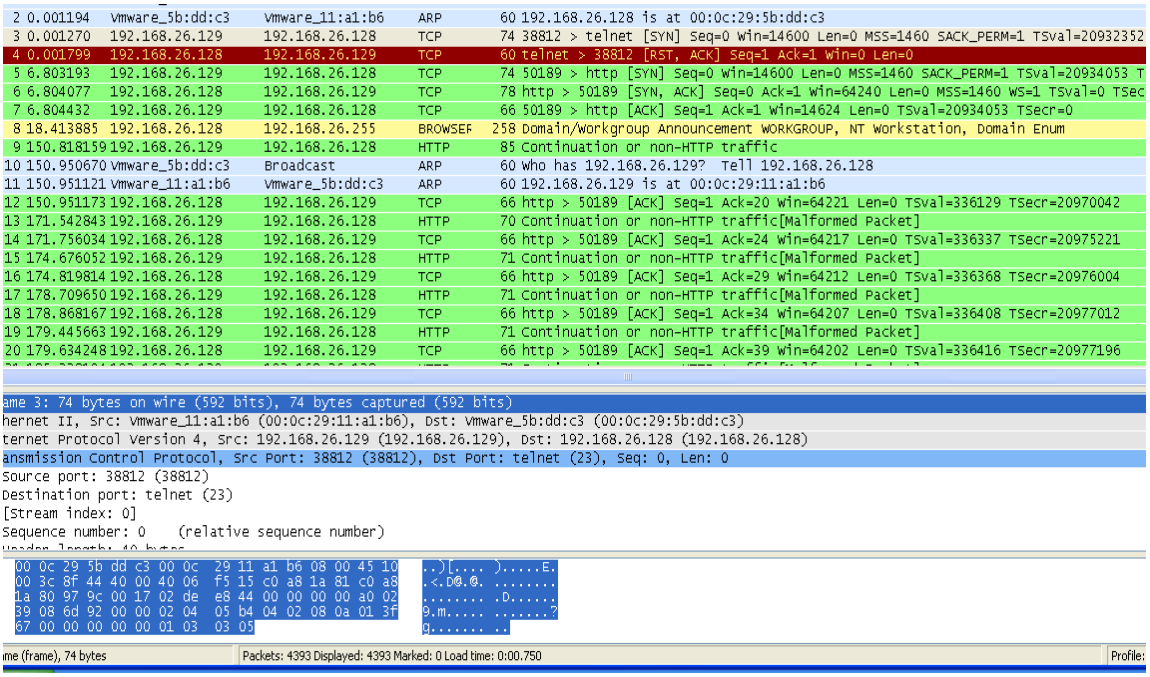


Figure 4.17 Attacker's technique to grab the banner

4.10.1.2 Netcat (Swiss army knife)

Netcat is a tool that can read and write to TCP and UDP ports. This dual functionality helps the netcat runs in two modes client and server.

1) Netcat is a computer networking service for reading from and writing network connections using TCP or UDP.

2) Netcat is designed to be a dependable "back end" device that can be used directly or easily driven by other programs and scripts.

3) Netcat is often referred to as a "Swiss army knife for TCP/IP."

   Now honeypots port scanning is done. Attacker uses the netcat tool to exploit the system as shown in Figure 4.19.

4.10.1.3 Port scanning

1) Attacker attack on honeypots for scanning the open port using netcat with –z options with attacker ip address and port range as shown in Figure 4.18.

Figure 4.18 Port scanning by attacker on honeypots using netcat

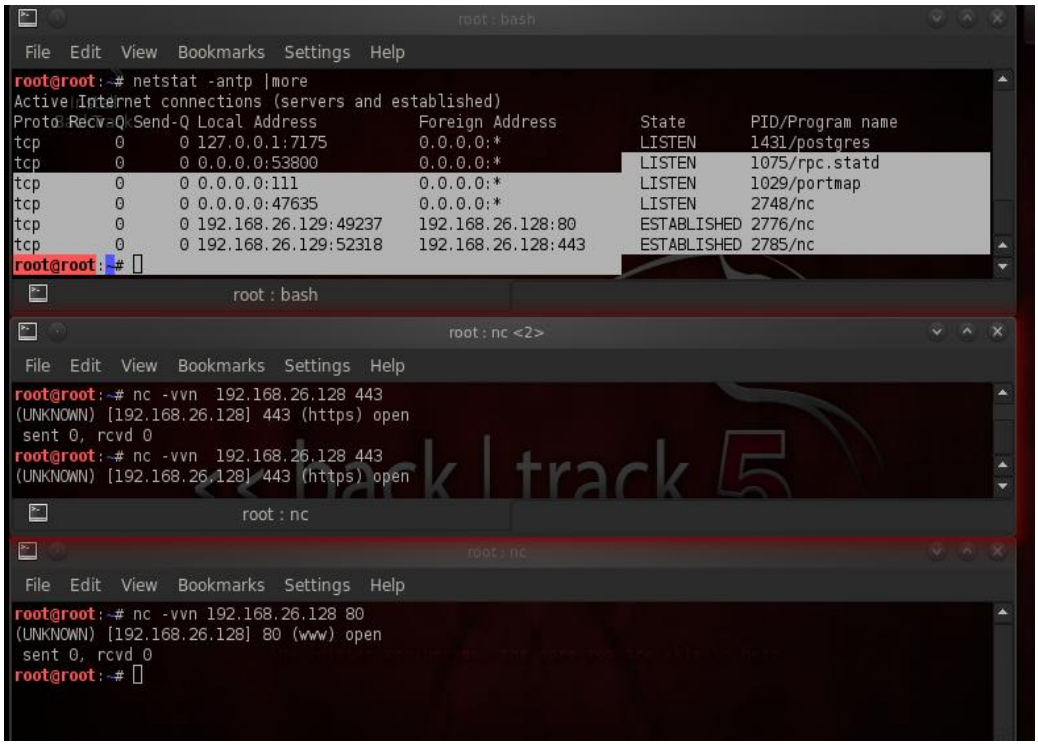


Figure 4.19 Attacker attack on listening port 80 and 443

Honeywall detect that attacker is tried to make the connection on port 80 and 443 by sending SYN flag, FIN and ACK flag to access the honeypots. Using port 80 and 443 as shown in Figure 4.20

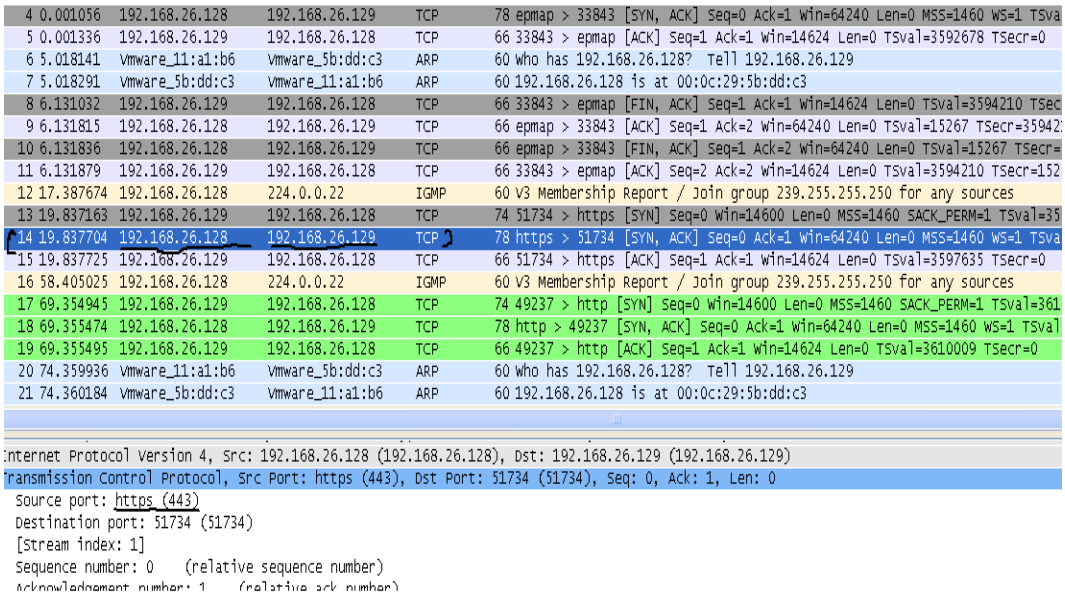


Figure 4.20 Capture the attacker interaction with honeypots using netcat

4.10.1.4 Packet Craft

Honeywall capture the this pcap file. An administrator can analyze this pcap file and try to know the technique of attacker. Attacker craft a packet with fin flag to honeypot and try to confuse the system to response for unexpected type of packet. Honeypot send the response which contains some useful information helpful to attacker.

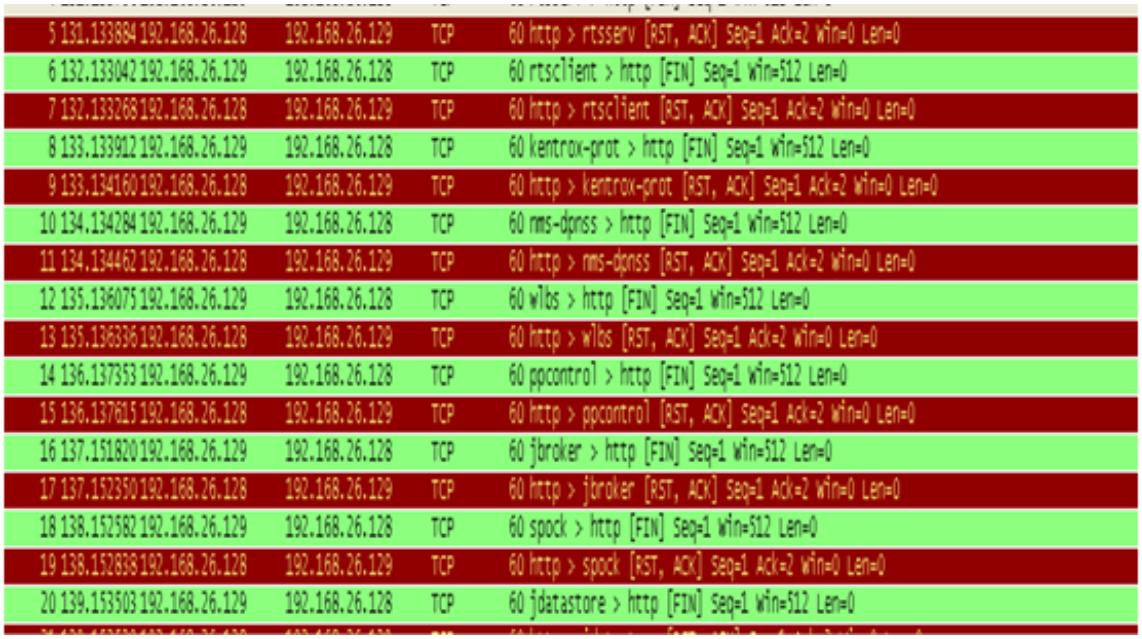


Figure 4.21 Attacker craft the anonymous packet with fin flag set

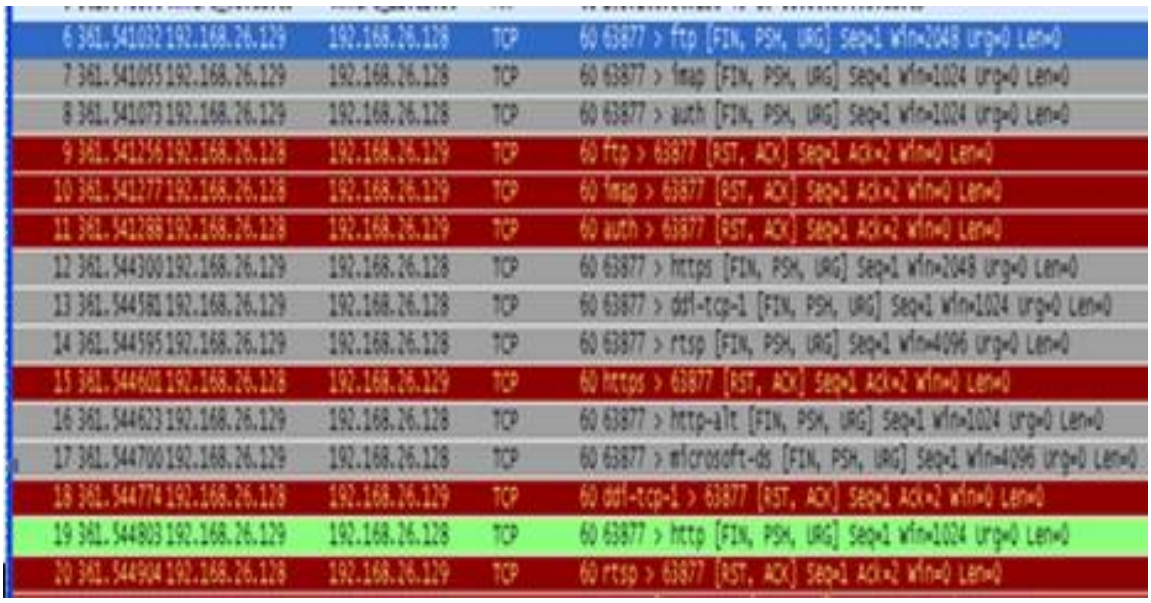


Figure 4.22 Attacker craft the packet FIN, PSH, URGENT flag set on different port 80, 443, 25

4.10.1.5 Nmap fingerprinting

Figure 4.23 Operating system fingerprinting using nmap by attacker [16].

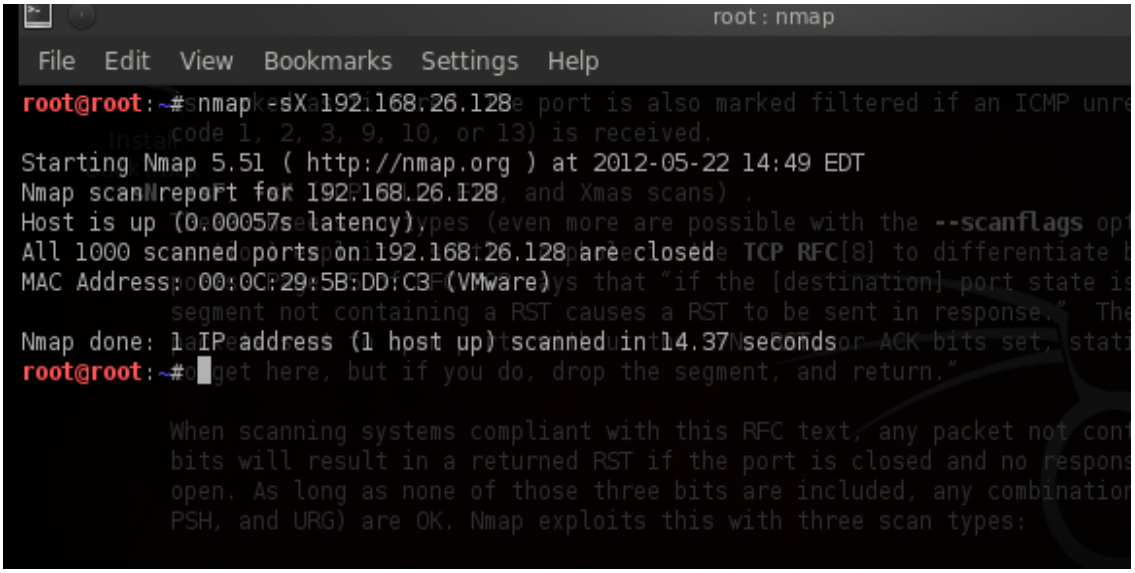


Figure 4.24 Nmap the honeypot with xmas Scan by attacker [16]

Attacker attack on the system by changing mac address with same ip address with small interval

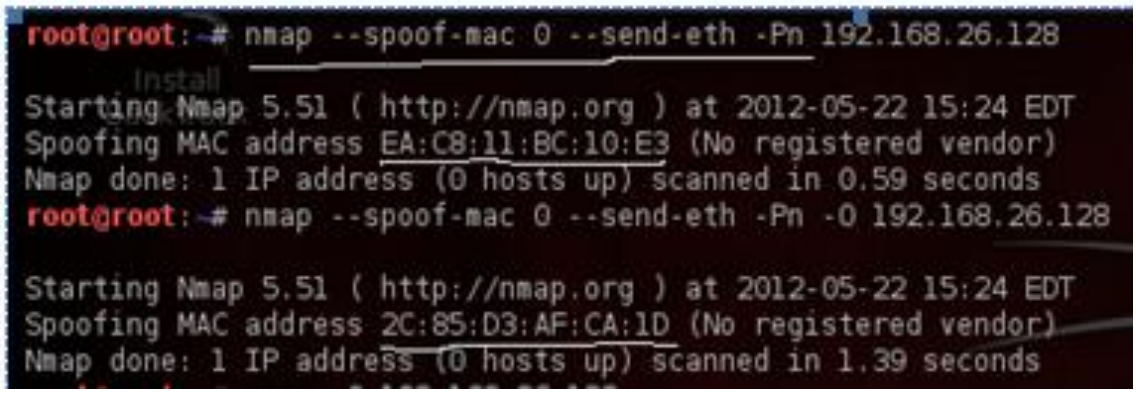
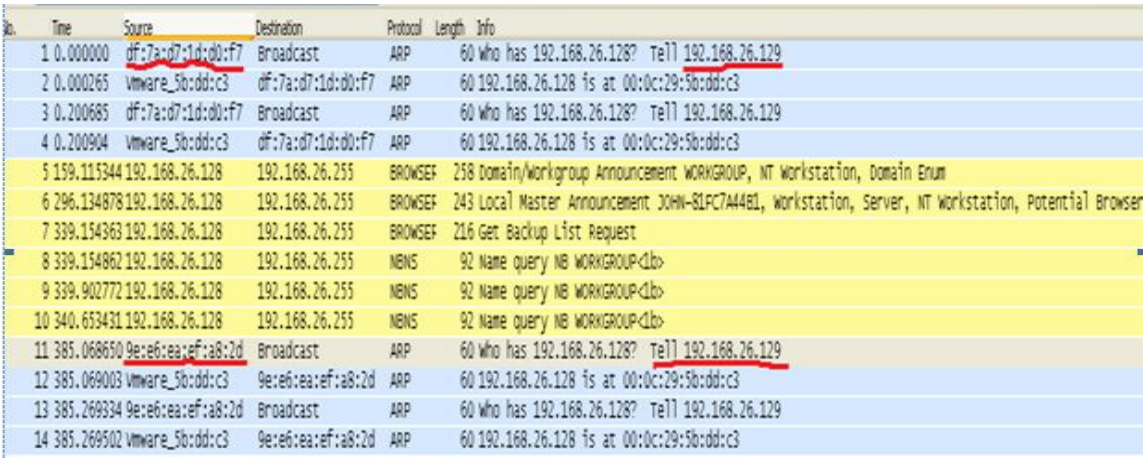


Figure 4.25 Attacker spoof the mac address with nmap

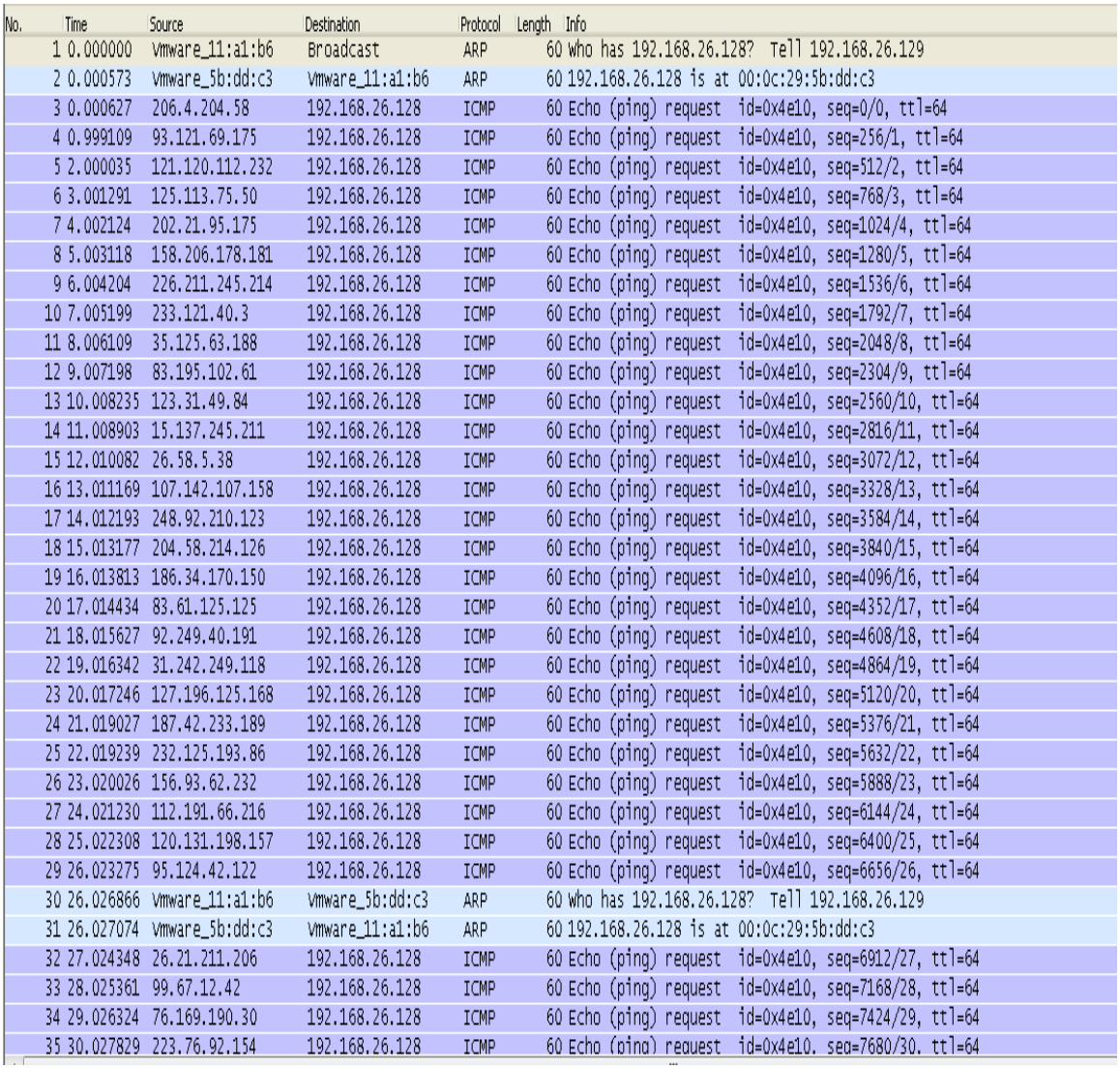


No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	df:7a:d7:1d:d0:f7	Broadcast	ARP	60	Who has 192.168.26.128? Tell 192.168.26.129
2	0.000265	Vmware_5b:dd:c3	df:7a:d7:1d:d0:f7	ARP	60	192.168.26.128 is at 00:0c:29:5b:dd:c3
3	0.200685	df:7a:d7:1d:d0:f7	Broadcast	ARP	60	Who has 192.168.26.128? Tell 192.168.26.129
4	0.200904	Vmware_5b:dd:c3	df:7a:d7:1d:d0:f7	ARP	60	192.168.26.128 is at 00:0c:29:5b:dd:c3
5	159.115344	192.168.26.128	192.168.26.255	BROWSER	258	Domain/Workgroup Announcement WORKGROUP, NT Workstation, Domain Enum
6	296.134878	192.168.26.128	192.168.26.255	BROWSER	243	Local Master Announcement JOHN-81FC7A4481, Workstation, Server, NT Workstation, Potential Browser
7	339.154363	192.168.26.128	192.168.26.255	BROWSER	216	Get Backup List Request
8	339.154862	192.168.26.128	192.168.26.255	NBNS	92	Name query NB WORKGROUP<1b>
9	339.902772	192.168.26.128	192.168.26.255	NBNS	92	Name query NB WORKGROUP<1b>
10	340.653431	192.168.26.128	192.168.26.255	NBNS	92	Name query NB WORKGROUP<1b>
11	385.068650	9e:e6:ea:ef:a8:2d	Broadcast	ARP	60	Who has 192.168.26.128? Tell 192.168.26.129
12	385.069003	Vmware_5b:dd:c3	9e:e6:ea:ef:a8:2d	ARP	60	192.168.26.128 is at 00:0c:29:5b:dd:c3
13	385.269334	9e:e6:ea:ef:a8:2d	Broadcast	ARP	60	Who has 192.168.26.128? Tell 192.168.26.129
14	385.269502	Vmware_5b:dd:c3	9e:e6:ea:ef:a8:2d	ARP	60	192.168.26.128 is at 00:0c:29:5b:dd:c3

Figure 4.26 Honeywall analyze the packet and find the attacker using fake mac address

4.10.1.6 DDOS Attack

After analysis of Figure 4.27 one ip address 192.168.26.129 use ARP command to find the mac address and other ip such as 93.121.69.175 send directly ping requests without knowing mac address. After analysis with this pcap file this is ddos attack done by attacker on honeypot to interrupt their services [30].



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	vmware_11:a1:b6	Broadcast	ARP	60	who has 192.168.26.128? Tell 192.168.26.129
2	0.000573	vmware_5b:dd:c3	vmware_11:a1:b6	ARP	60	192.168.26.128 is at 00:0c:29:5b:dd:c3
3	0.000627	206.4.204.58	192.168.26.128	ICMP	60	Echo (ping) request id=0x4e10, seq=0/0, ttl=64
4	0.999109	93.121.69.175	192.168.26.128	ICMP	60	Echo (ping) request id=0x4e10, seq=256/1, ttl=64
5	2.000035	121.120.112.232	192.168.26.128	ICMP	60	Echo (ping) request id=0x4e10, seq=512/2, ttl=64
6	3.001291	125.113.75.50	192.168.26.128	ICMP	60	Echo (ping) request id=0x4e10, seq=768/3, ttl=64
7	4.002124	202.21.95.175	192.168.26.128	ICMP	60	Echo (ping) request id=0x4e10, seq=1024/4, ttl=64
8	5.003118	158.206.178.181	192.168.26.128	ICMP	60	Echo (ping) request id=0x4e10, seq=1280/5, ttl=64
9	6.004204	226.211.245.214	192.168.26.128	ICMP	60	Echo (ping) request id=0x4e10, seq=1536/6, ttl=64
10	7.005199	233.121.40.3	192.168.26.128	ICMP	60	Echo (ping) request id=0x4e10, seq=1792/7, ttl=64
11	8.006109	35.125.63.188	192.168.26.128	ICMP	60	Echo (ping) request id=0x4e10, seq=2048/8, ttl=64
12	9.007198	83.195.102.61	192.168.26.128	ICMP	60	Echo (ping) request id=0x4e10, seq=2304/9, ttl=64
13	10.008235	123.31.49.84	192.168.26.128	ICMP	60	Echo (ping) request id=0x4e10, seq=2560/10, ttl=64
14	11.008903	15.137.245.211	192.168.26.128	ICMP	60	Echo (ping) request id=0x4e10, seq=2816/11, ttl=64
15	12.010082	26.58.5.38	192.168.26.128	ICMP	60	Echo (ping) request id=0x4e10, seq=3072/12, ttl=64
16	13.011169	107.142.107.158	192.168.26.128	ICMP	60	Echo (ping) request id=0x4e10, seq=3328/13, ttl=64
17	14.012193	248.92.210.123	192.168.26.128	ICMP	60	Echo (ping) request id=0x4e10, seq=3584/14, ttl=64
18	15.013177	204.58.214.126	192.168.26.128	ICMP	60	Echo (ping) request id=0x4e10, seq=3840/15, ttl=64
19	16.013813	186.34.170.150	192.168.26.128	ICMP	60	Echo (ping) request id=0x4e10, seq=4096/16, ttl=64
20	17.014434	83.61.125.125	192.168.26.128	ICMP	60	Echo (ping) request id=0x4e10, seq=4352/17, ttl=64
21	18.015627	92.249.40.191	192.168.26.128	ICMP	60	Echo (ping) request id=0x4e10, seq=4608/18, ttl=64
22	19.016342	31.242.249.118	192.168.26.128	ICMP	60	Echo (ping) request id=0x4e10, seq=4864/19, ttl=64
23	20.017246	127.196.125.168	192.168.26.128	ICMP	60	Echo (ping) request id=0x4e10, seq=5120/20, ttl=64
24	21.019027	187.42.233.189	192.168.26.128	ICMP	60	Echo (ping) request id=0x4e10, seq=5376/21, ttl=64
25	22.019239	232.125.193.86	192.168.26.128	ICMP	60	Echo (ping) request id=0x4e10, seq=5632/22, ttl=64
26	23.020026	156.93.62.232	192.168.26.128	ICMP	60	Echo (ping) request id=0x4e10, seq=5888/23, ttl=64
27	24.021230	112.191.66.216	192.168.26.128	ICMP	60	Echo (ping) request id=0x4e10, seq=6144/24, ttl=64
28	25.022308	120.131.198.157	192.168.26.128	ICMP	60	Echo (ping) request id=0x4e10, seq=6400/25, ttl=64
29	26.023275	95.124.42.122	192.168.26.128	ICMP	60	Echo (ping) request id=0x4e10, seq=6656/26, ttl=64
30	26.026866	vmware_11:a1:b6	vmware_5b:dd:c3	ARP	60	who has 192.168.26.128? Tell 192.168.26.129
31	26.027074	vmware_5b:dd:c3	vmware_11:a1:b6	ARP	60	192.168.26.128 is at 00:0c:29:5b:dd:c3
32	27.024348	26.21.211.206	192.168.26.128	ICMP	60	Echo (ping) request id=0x4e10, seq=6912/27, ttl=64
33	28.025361	99.67.12.42	192.168.26.128	ICMP	60	Echo (ping) request id=0x4e10, seq=7168/28, ttl=64
34	29.026324	76.169.190.30	192.168.26.128	ICMP	60	Echo (ping) request id=0x4e10, seq=7424/29, ttl=64
35	30.027829	223.76.92.154	192.168.26.128	ICMP	60	Echo (ping) request id=0x4e10, seq=7680/30, ttl=64

Figure 4.27 Honeywall detect the ddos attack on honeypot

4.11 Snort Rule

Snort rule are saved in /var/log /message .snort rule tell the system modification activities are done as shown in Figure 4.28 [35].

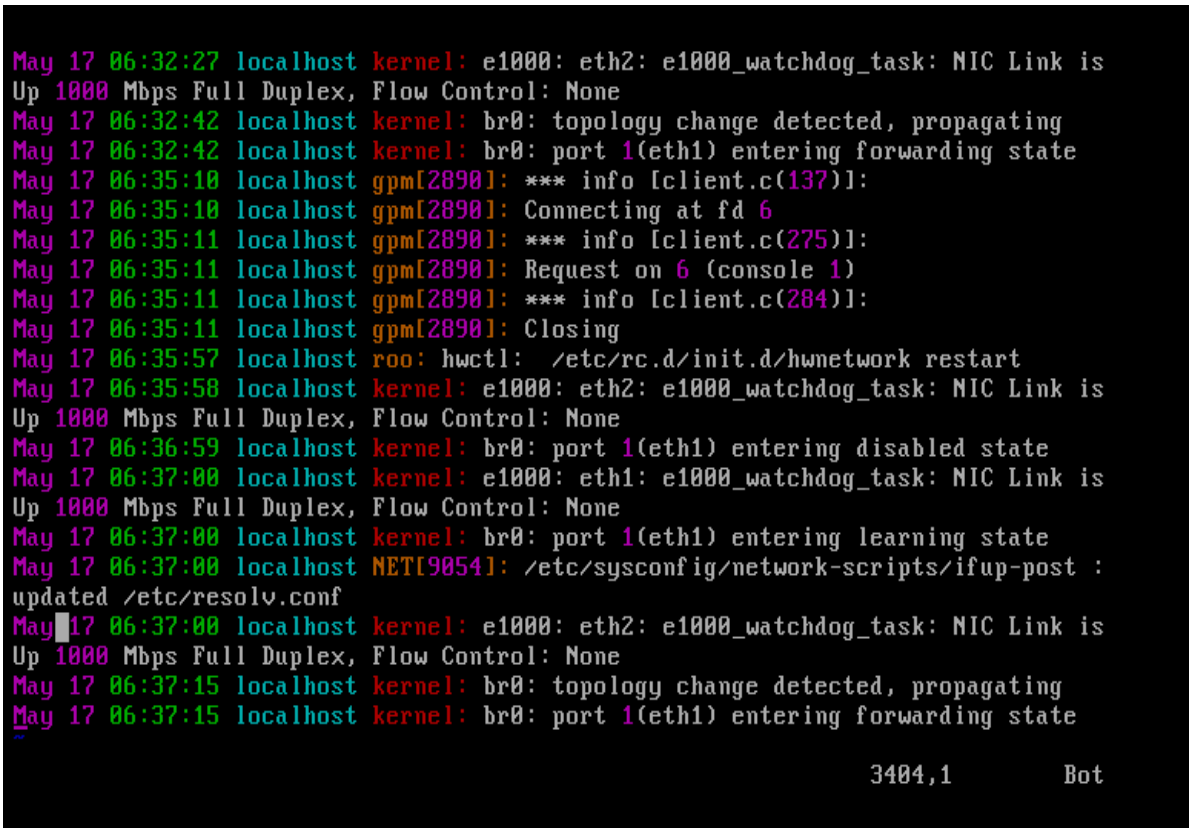


Figure 4.28 Snort alert message to administrator

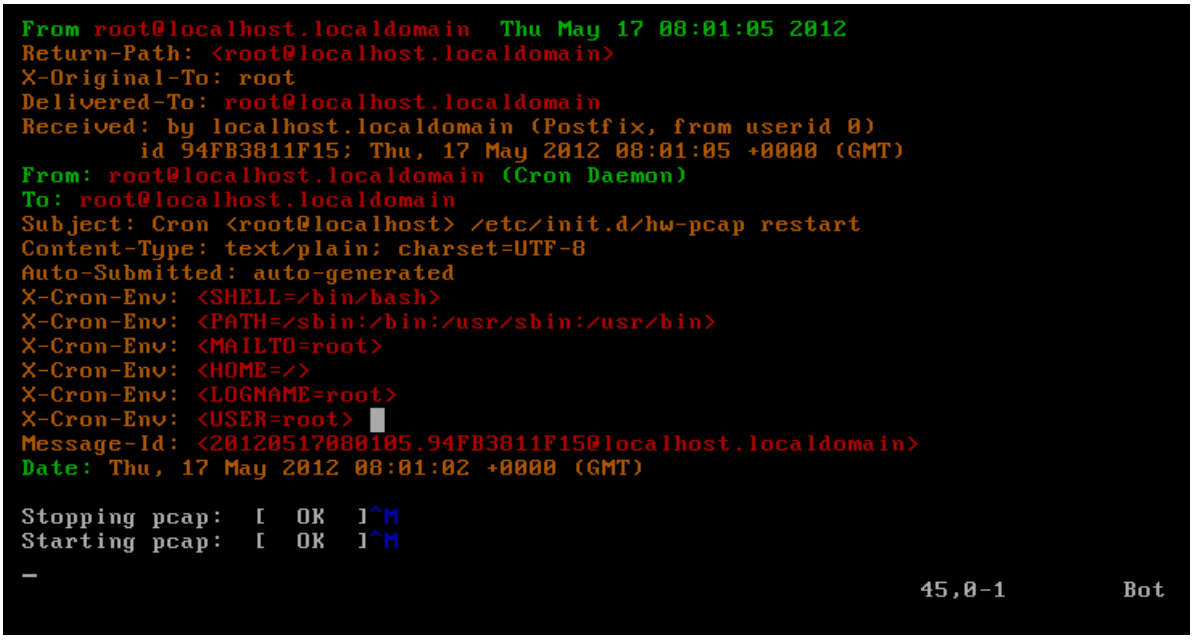


Figure 4.29 Email alert to the administrator

4.12 Email Alert

Honeywall alert the administrator when there is some major issue is there it sends alert message to administrator with Subject and its details. This email is saved in honeywall at /var/spool/Email/root as shown in Figure 4.29.

4.13 System status

4.13.1 Firewall rules

Firewall rules that are added to honeywall as explain in section 2.5.2.1 iptables as shown in Figure 4.30.

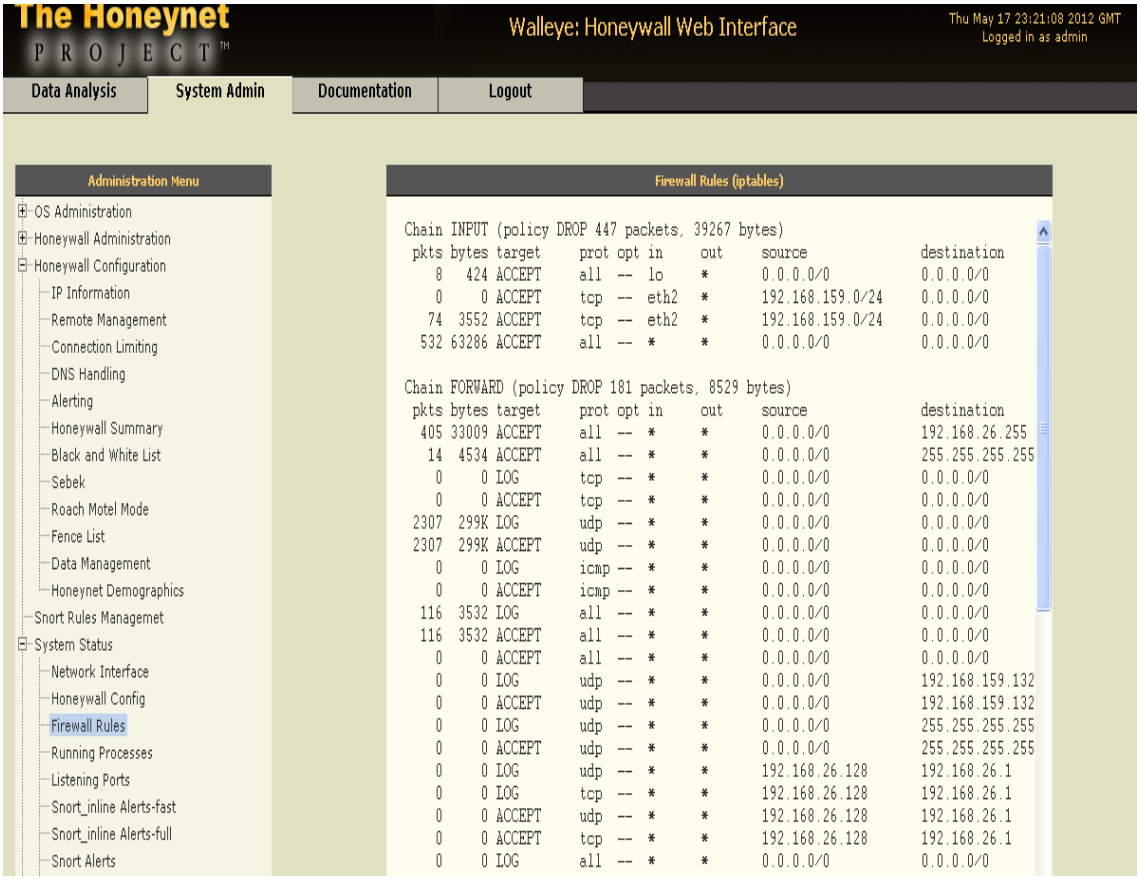


Figure 4.30 Firewall rules for honeywall with source and destination ip address

4.13.2 Listening ports

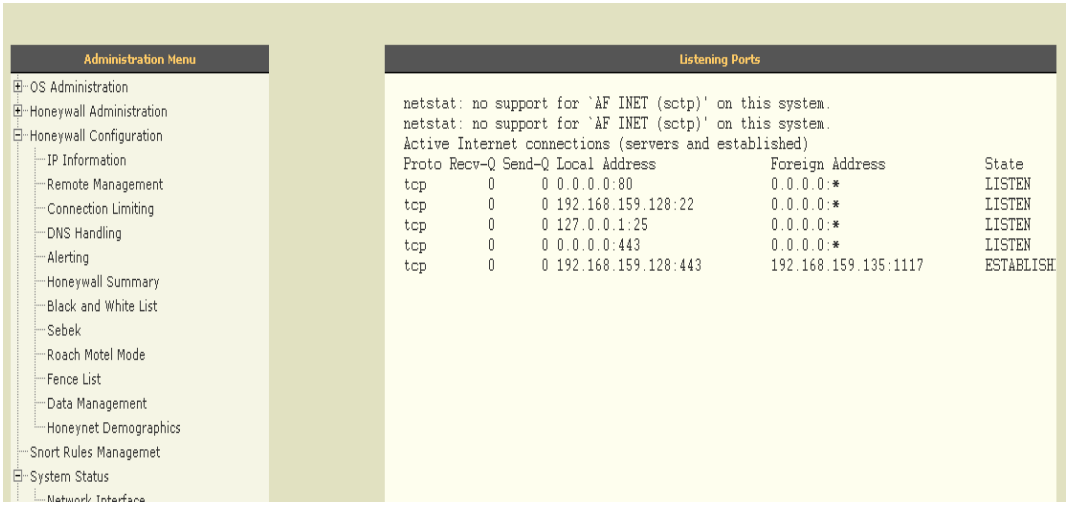


Figure 4.31 Active internet connections of management interface with remote host

4.13.3 Aggregated flow by calendar wise

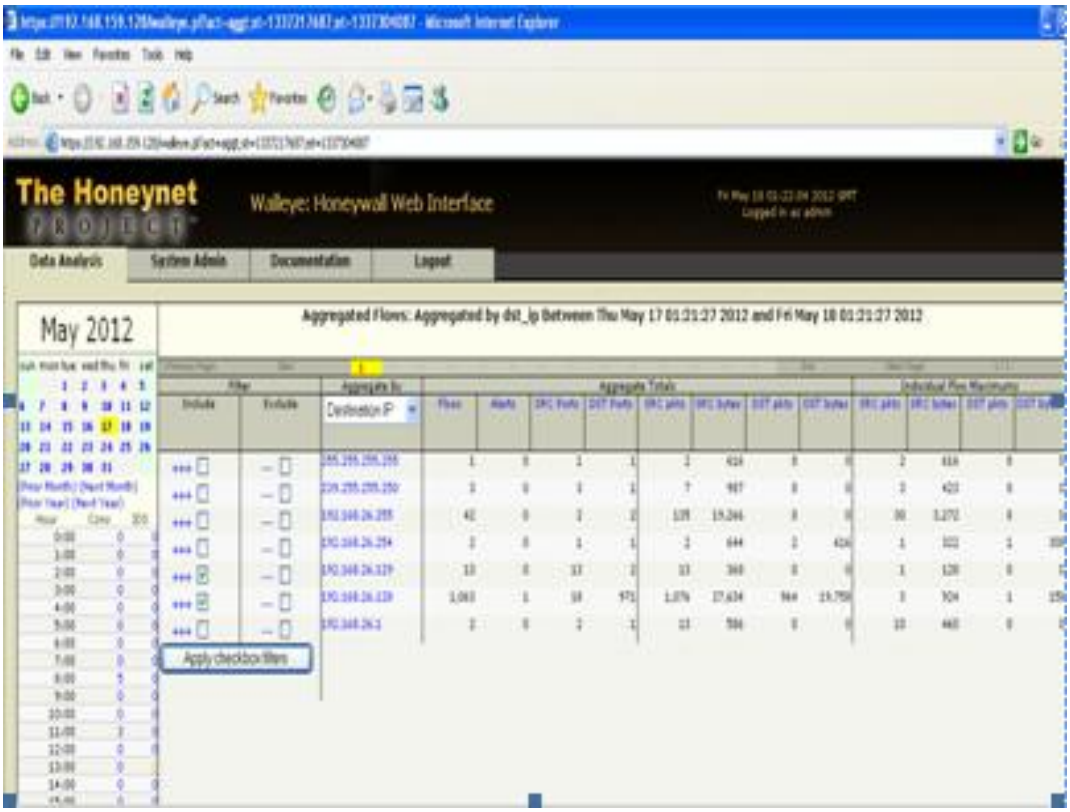


Figure 4.32 Calendar wise honeypots activity details

Figure 4.33 Graphical Representation of Attacker Connection to honeypots

4.13.4 Tcpdstat traffic statistics

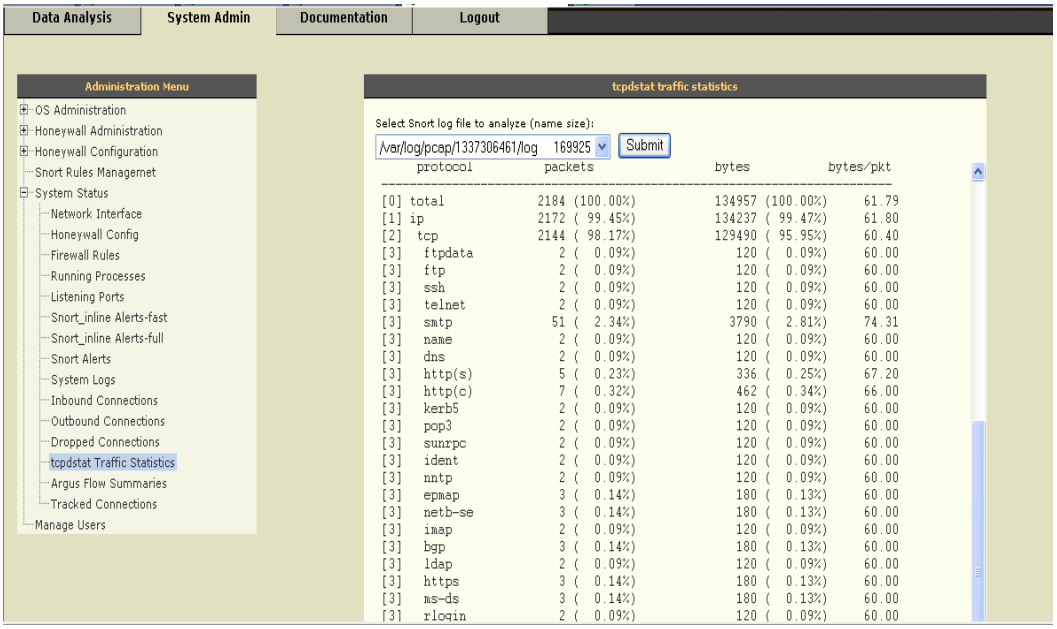


Figure 4.34 Statistics of tcpdstat protocol wise

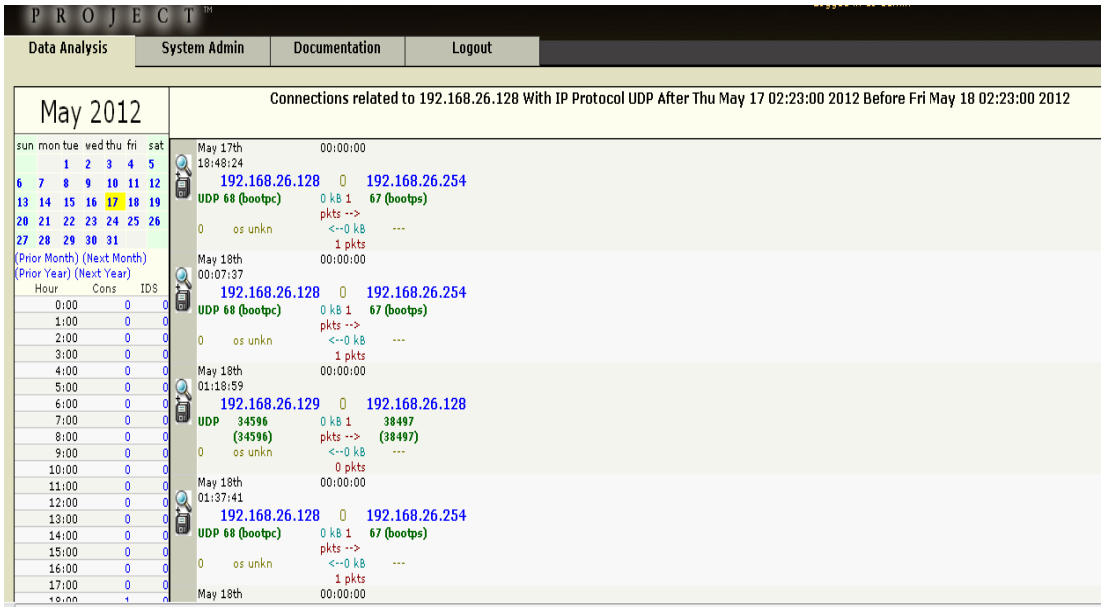


Figure 4.35 Connection related to udp protocol

4.13.5 Honeywall Administration

4.13.5.1 Manage configuration files

Figure 4.36 Remotely update the Configuration files

4.13.5.2 Emergency Lockdown

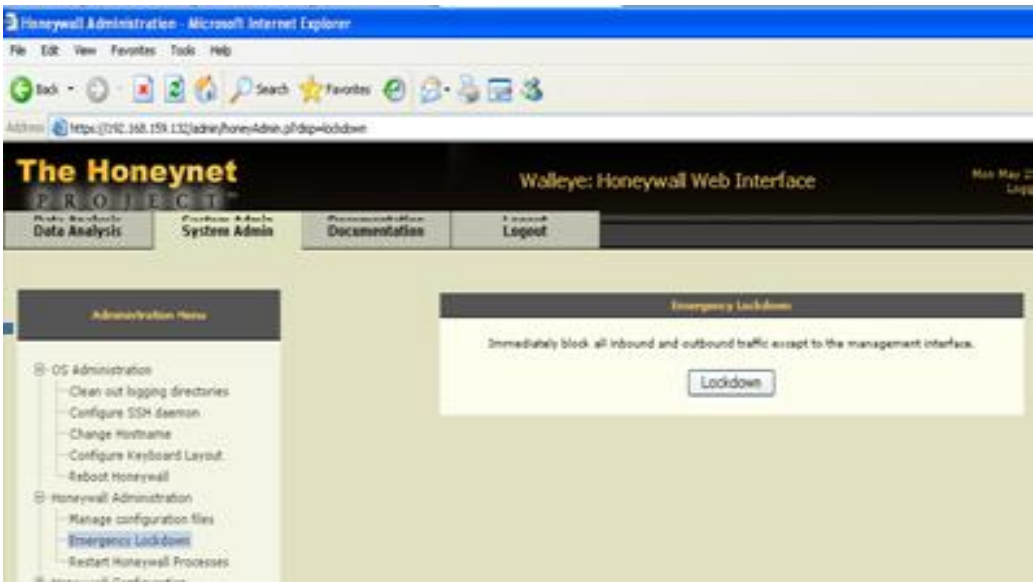


Figure 4.37 Emergency lockdown of all traffic except management interface

4.13.5.3 Restart Honeywall Processes

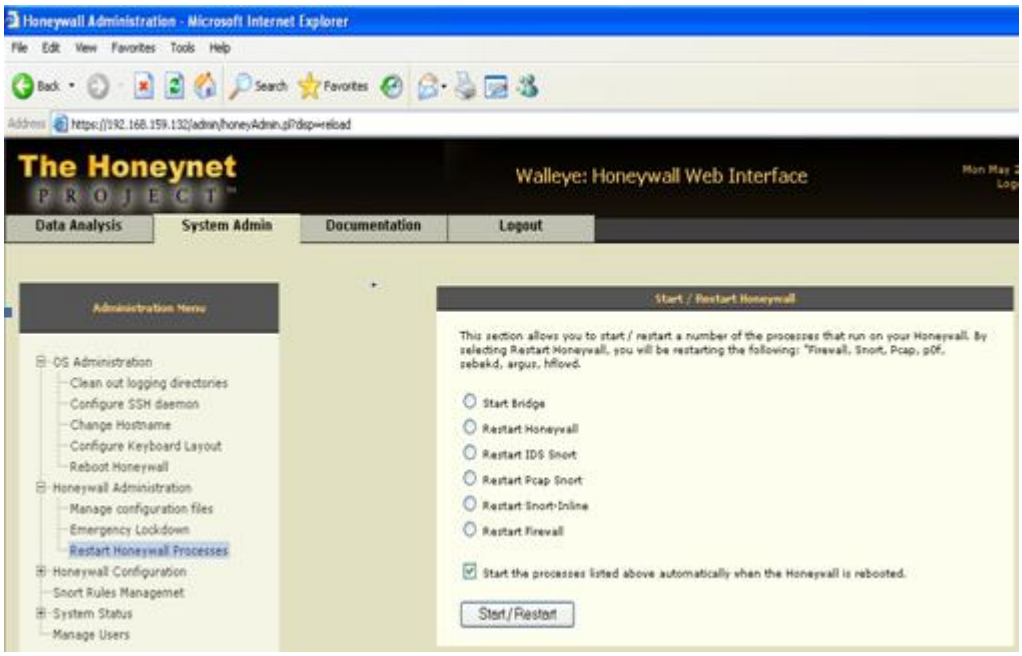


Figure 4.38 Restart the honeywall process remotely

5.1 Metasploit Attack

The Metasploit Project is an open source, computer security project which provides information about security vulnerabilities and aids in penetration testing and IDS signature development. Its most well known sub project is the Metasploit Framework, a tool for developing and executing exploit code against a remote target machine. Other important sub projects include the opcode database, shell code archive, and security research.

5.2 Case Study

This is MS08-067 Vulnerability in server service could allow remote code execution with the help of metasploit. Remote code execution vulnerability exists in the Server service on Windows systems. The vulnerability is due to the service not properly handling specially crafted RPC requests. By exploiting this vulnerability attacker got the shell of window xp honeypot and make use of this vulnerability with the help of metasploit and install as backdoor on windows xp sp2 systems. Attacker attack on honeypot by exploiting vnc server installed on honeypot using metasploit msfconsole as shown in Figure 5.1 [25],[31].

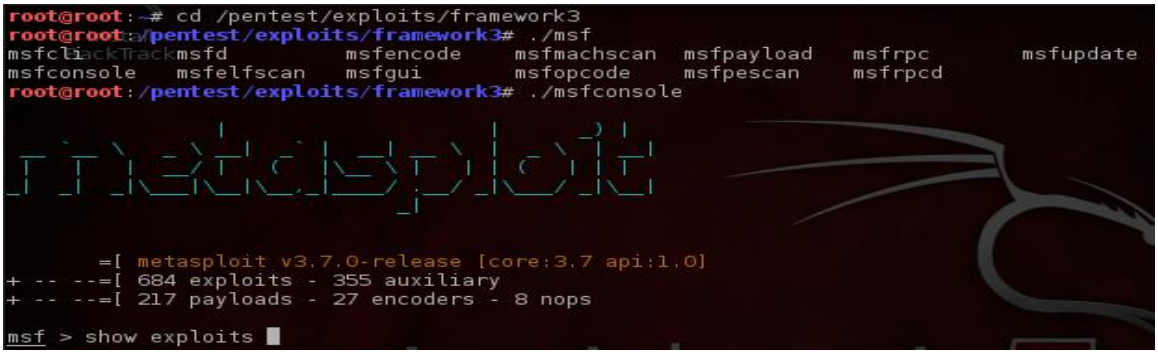


Figure 5.1 Metasploit framework using msfconsole

Attacker search in metasploit ms_08_067_netapi exploits, find its name and use command to exploit as shown in Figure 5.2 and set RHOST to honeypot ip address.

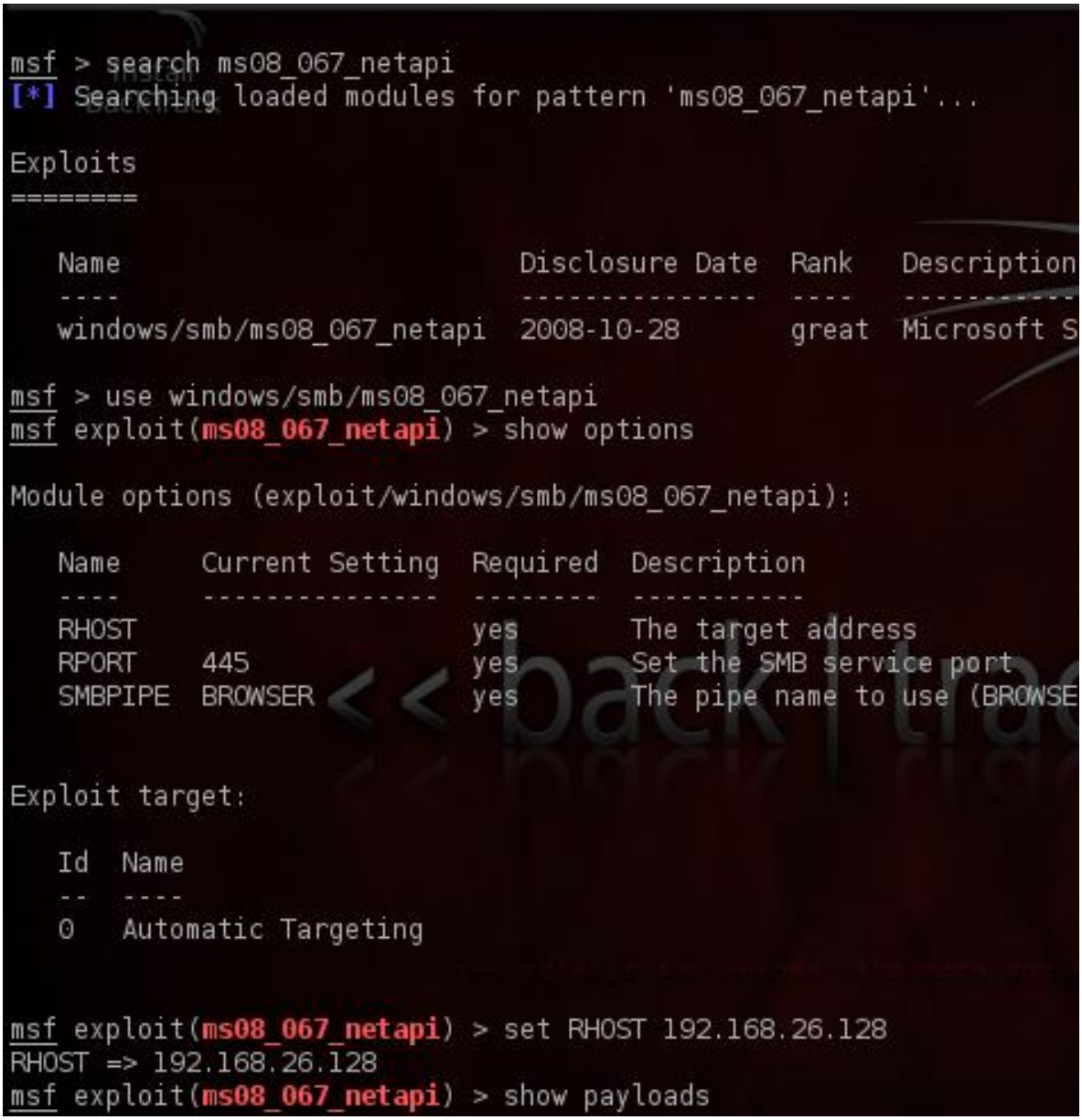


Figure 5.2 window vnc server exploits

Attacker use the command show payloads for search the exploit, use set PAYLOAD command with windows/shell/reverse_tcp payload and LHOST to attackers ip address as shown in Figure5.3 and 5.4.

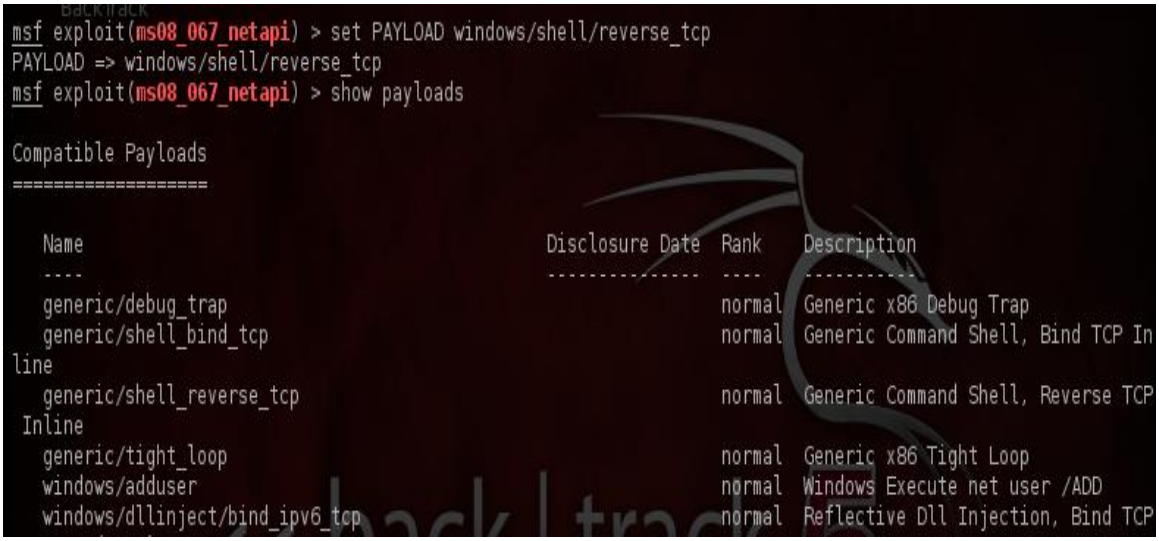


Figure 5.3 Payload set for vnc server

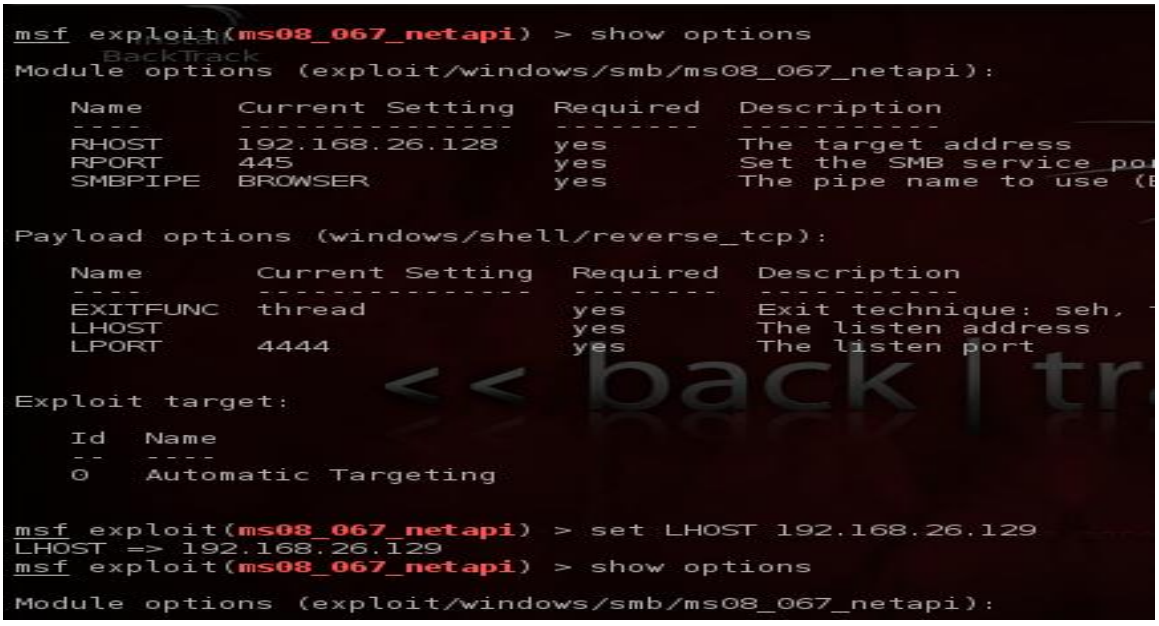


Figure 5.4 Set the local host ipaddress by LHOST command

Attacker write exploit command to get the window xp shell now work is done attacker got the shell as shown in Figure 5.5.

Figure 5.5 Attacker got the honeypot command shell

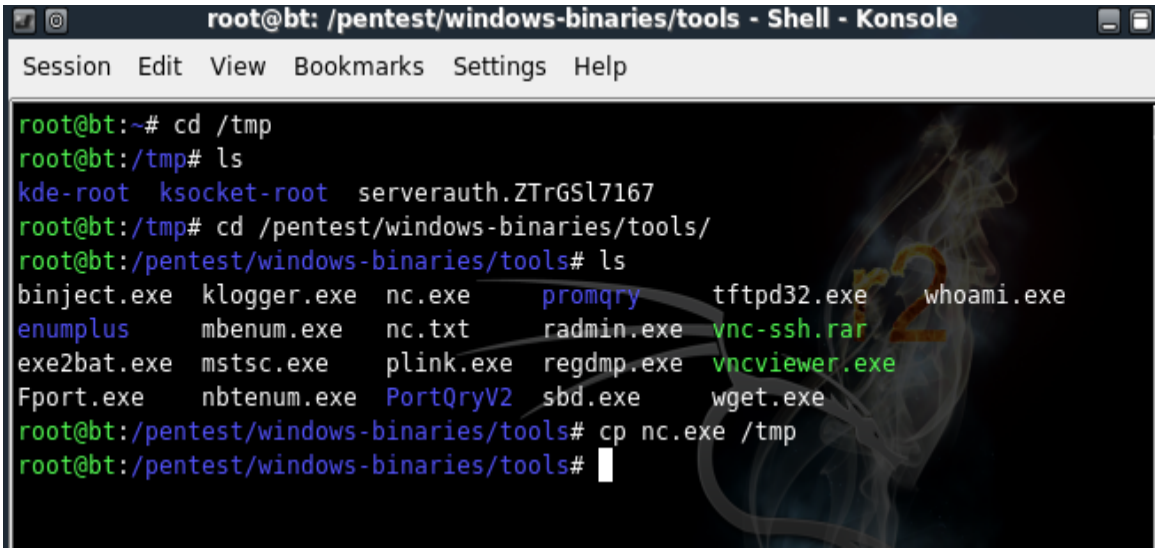


Figure 5.6 Attacker try to install backdoor on honeypots

After getting shell attacker try to maintain their access on the machine so that he had hold on the system after restart. Attacker use netcat as backdoor with tftp service.

Honeywall capture the technique use by attacker through pcap files, find the attack as shown in Figure 5.7 and capture the attacker backdoor technique using tftp as shown in Figure 5.8 in black color. Due to firewall rules and bound limit install backdoor doesn't succeed and give error illegal tftp operation. Administrator came to know the technique used by attacker.

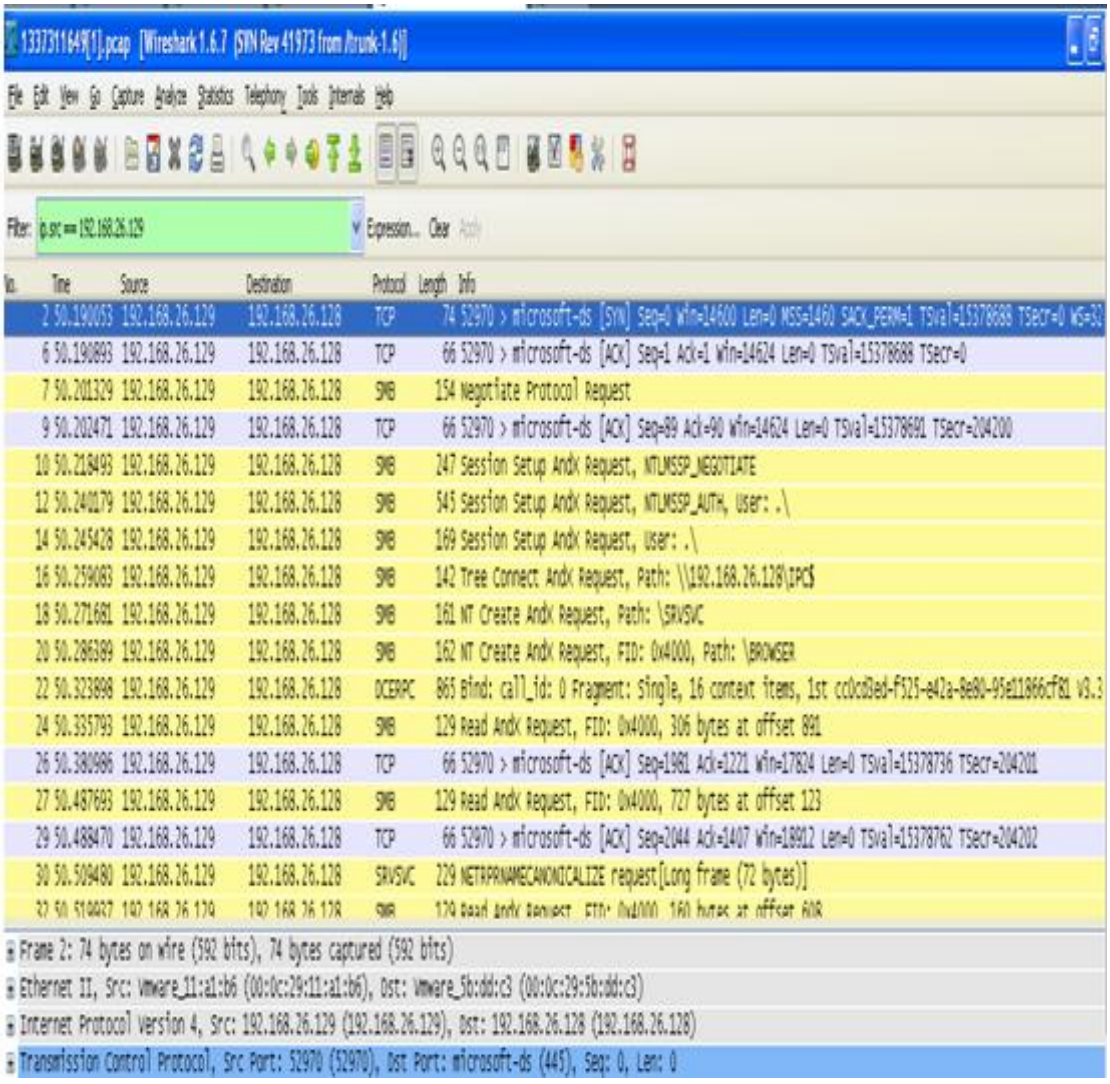


Figure 5.7 Honeywall detect the metasploit attack

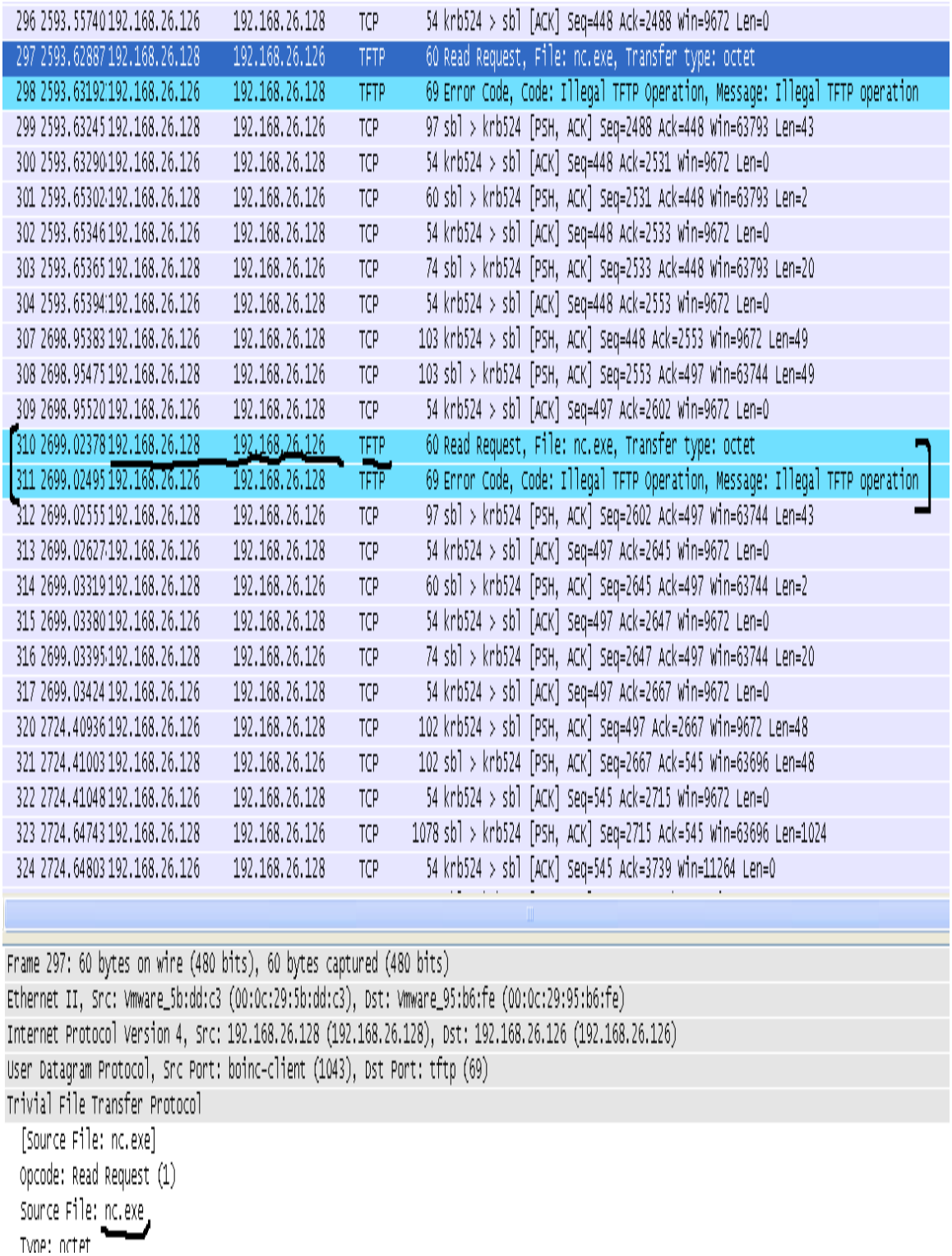


Figure 5.8 Detect the Attacker technique who is trying to install backdoor netcat using tftp

Suggestions for a user to secure the system

1) Do not use Administrator account login and use guest account .

2) Security patches of windows use windows operating system with MBSA Microsoft baseline security analyzer patch management tool to update your operating system.

3) Use of netstat utility to check which ports are open and what the connections are established as shown in Figure 5.9 [29].

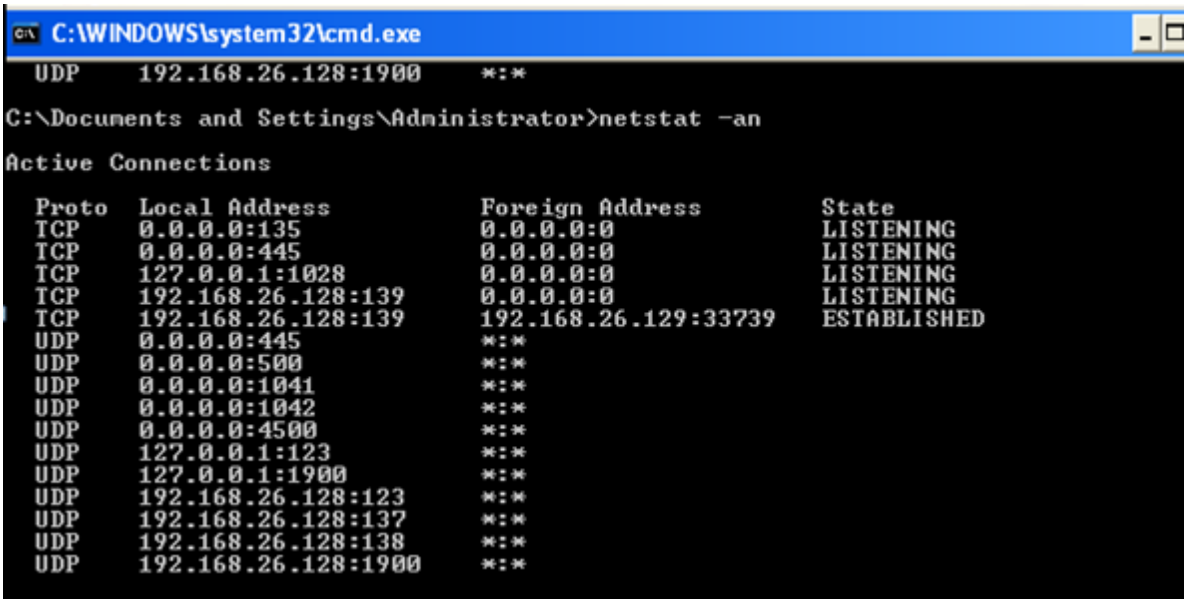


Figure 5.9 Netstat utility for knowing the active connections

Chapter 6

Conclusion and Future Scope

6.1 Conclusion

1) Self contained virtual high interaction honeynet is developed by using Honeywall CDROM Roo which is 3rd generation honeynet. Honeynet is configured and deployed in the vmware successfully to detect the various attacks.

2) This honeynet helps in finding the zero day attack in which attacker use zero day exploits (software which uses the security loop hole to carry out the attacks).

3) Honeynet collect small amount of information in MB's instead of GB's data. All the activity within honeynet is malicious, suspected and can be easily tracked by administrator.

4) Honeynet provides the capability to view the detailed logs and outputs remotely by using walleye so that administrator can monitor the status of honeynet from his location and need not to go the location of honeywall where the honeynet is deployed.

5) This honeynet helps the administrator to detect the attacker's technique such as banner grabbing, port scanning, operating system fingerprinting, ddos attack, remote code execution and installing backdoor to maintain access on the system. These are the some techniques used by the attackers for attacking the honeypots.

6.2 Future scope

1) Although honeynet detects the technique used by attacker. There is one technique which is called sebek in which attacker's keystroke are send to the honeywall administrator, can be configured with honeywall.

2) Honeynet can be used to detect the different botnet such as irc botnet, http botnet in their network and with the help of sebek to know about the keystrokes of command and control centre.

3) Honeynet can be used to prevent the attacks on the web server and know the attacker various technique such as sql injection and cross site scripting.

4) Distributed Honeynet can be used to detect the various attacks on different location and analyze the all attacker's techniques to exploit the system.

References

[1] Network Security [Online]. Available http://en.wikipedia.org/wiki/ Network_ security.

[2] Five Phases of Hacking, [Online].Available : http://iclass.eccouncil.org/index.php ? option=com_content&view=article&id=174&Itemid=197.

[3] Clifford Stoll, "The Coocoo's egg Pocket Books", 1990 [Online]. Available: http://mario.elinos.org.mx/docencia/herseg/cuckoo_egg.pdf.

[4] Diagram of different phases of hacking [Online].Available: http://technohackers bhutan.blogspot.in/2011/04/phases-of-malicious-hacking_9540.html.

[5] Internet Crime Report, [Online]. Available: http://www.ic3.gov/media/annual report/ 2011_IC3Report.pdf.

[6] The Honeynet Project (2005, May 12), "Know Your Enemy GenII Honeynets" [Online]. Available: http://old.honeynet.org/papers/gen2/index.html.

[7] Vmware, "Workstation User's Manual," [Online]. Available: www.vmware.com/ pdf/ws65_manual.pdf.

[8] The Honeynet Project (March, 2002 4), "Know Your Enemy: Passive Fingerprinting", [Online]. Available: http://old.honeynet.org/papers/finger/.

[9] The Honeynet Project (2007, May 25), "CDROM Roo manual" http:// old.honeynet.org /tools/cdrom/roo/manual/index.html.

[10] The Honeynet Project (2006, May 31), "Know Your Enemy: Honeynets," [Online]. Available: http://old.honeynet.org/papers/honeynet/.

[11] The Honeynet Project (2003, January 27), "Know Your Enemy: Defining Virtual Honeynets," [Online]. Available: http://old.honeynet.org/papers/virtual/.

[12] The Honeynet Project (2005, August 17), "Honeywall CDROM," [Online].

Available: http://www.honeynet.org/project/HoneywallCDROM.

[13] The Honeynet Project (2003, November 17), “Sebek”, [Online]. Available: http:// www.honeynet.org/tools/sebek.

[14] M. Zalewski (2006). “The new p0f,” [Online]. Available: http://lcamtuf.coredump .cx/p0f.shtml.

[15] The Honeynet Project, “Honeywall CDROM Roo”, [Online]. Available: http://old.honeynet.org/papers/cdrom/roo/index.html.

[16] Remote OS Detection [Online]. Available: http://nmap.org/book/osdetect.html.

[17] Fahim H. Abbasi and R. J. Harris,” Experiences with a Generation III Virtual Honeynet,”SEAT, Massey University, New Zealand.

[18] Brett Ussher, “Honeywall as a Viable Production-Level Solution” Southern Illinois University, Illinois USA, 2010.

[19] Lance Spitzner, “Honeypots: Tracking Hackers,” Addison Wesley.

[20] Pakistan Honeynet Project (2004), “Honeynet,” [Online]. Available: http:// www. honeynet.pk/honeynet/.

[21] SAUDI HONEYNET PROJECT, “KFUPM USER MANUAL,” [Online]. Available:www1.kfupm.edu.sa/honeynet/PDF/SaudiHoneynet-UserManual.pdf.

[22] F. A. Shuja, (2005), “Virtual Honeynet: Deploying Honeywall using VMware,” [Online]. Available: http://www.honeynet.pk/honeywall/roo/index.htm.

[23] Honeywall Community, “Honeywall Mail Archive," [Online]. Available: http:// www.mail-archive.com/honeywall@public.honeynet.org/.

[24] The Honeynet Project, “Know Your Enemy Learning about Security Threats,” Addison Wesley, Boston, USA, July 2004, 2nd Ed.

[25] MITRE Common Weakness Enumeration [Online]. Available: http://cwe.mitre.org/.

[26] Kurt Seifried, “Honeypotting with Vmware basics,” [Online]. Available: http://seifried.org/security/ids/20020107-honeypot-vmware-basics.html.

[27] The Honeynet Project: Know Your Enemy: Learning about Security Threats (2nd Edition) Addison-Wesley 2004.

[28] Christian Doring, “Improving network security with Honeypots,” Master's thesis by University of Applied Sciences Darmstadt, 2005.

[29] Microsoft TechNet netstat. [Online]. Available: http://technet.microsoft.com/en-us/library/bb490947.aspx.

[30] D.Watson (2007), “Honeynets: a tool for counterintelligence in Online security,” [Online]. Available: http://linkinghub.elsevier.com/retrieve/pii/S1353485807700041.

[31] MS08-067, “Vulnerability in Server service could allow remote code execution” [Online]. Available: http://technet.microsoft.com/en-us/security/bulletin/ms08-067.

[32] Zero day attack [Online]. Available: http://en.wikipedia.org/wiki/Zero-day_attack.

[33] The Honeynet Project (April, 2004 26),”Know Your Enemy: Honeynets in Universities”, [Online]. Available: http://old.honeynet.org/papers/edu/.

[34] E. Alata, V. Nicomette, M. Kaaniche, M. Dacier, M. Herrb, “Lessons Learned from the Deployment of a High-Interaction Honeypot”, 6th European Dependable Computing Conference (EDCC-6), (Coimbra, Portugal), 2006, pp. 39-44.

[35] Snort (2010) [Online]. Available: http://www.snort.org/snort/faq/.

Publications

Kapil Madan, Dr. Maninder Singh, Mr. Sumit Miglani "Design and Implementation of High Interaction Honeypot for Campus Network using Honeywall CDROM Roo", International Journal of Computer Applications ISSN:1741-5047 (Communicated)