Design and Develop a Campus Honeypot to Detect Intrusions

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

Master of Engineering
in
Software Engineering

by:
Kiran Deep Singh
(80731010)

Under the supervision of:
Dr. Maninder Singh
Associate Professor (CSED)

COMPUTER SCIENCE AND ENGINEERING DEPARTMENT
THAPAR UNIVERSITY
PATIALA – 147004

JULY 2009

Certificate

I hereby certify that the work which is being presented in the thesis entitled, **"Design and Develop a Campus Honeypot to Detect Intrusions"**, in partial fulfilment 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 *Dr. Maninder Singh* and refers other researcher's works which are duly listed in the reference section.

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

(Kiran Deep Singh)

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

(Maninder Singh)
Computer Science and Engineering Department,
Thapar University,
Patiala.

Countersigned by

14/07/09.

(RAJESH KUMAR BHATIA)
Assistant Professor & Head
Computer Science & Engineering Department
Thapar University
Patiala.

(R.K.SHARMA) 15/7/09
Dean (Academic Affairs)
Thapar University,
Patiala.

Acknowledgement

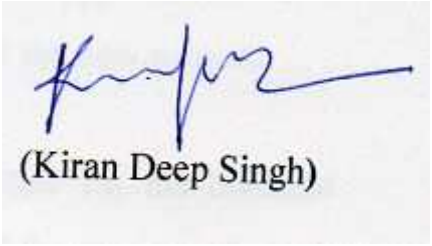
First and foremost, I would like to express my sincere gratitude to my guide **Dr. Maninder Singh,** Associate Professor, Computer Science and Engineering Department for immense help, guidance, stimulating suggestions, and encouragement all the time with this thesis work. This work would have not been possible without his encouragement. He always provided a motivating and enthusiastic atmosphere to work with, it was a great pleasure to do this thesis under his supervision.

I am equally grateful to **Dr Rajesh Kumar Bhatia,** Assistant Professor and Head, Computer Science and Engineering Department for their appreciation and satisfactorily healing me off my inexperienced inquisitions about the new subject.

I am greatful to **Dr. R.K. Sharma**, Dean of Academic Affair for his constant encouragement that was of great importance in the completion of the thesis.

I would also like to thank Mr. Balwinder Singh, SMC In-charge for providing me with the material support. I am deeply indebted to my parents and friends for their inspiration and ever encouraging moral support, which enabled me to pursue my studies.

I cannot skip mentioning the help which my colleague Ms. Sheenam Goyal, has provided throughout my work. I am also very thankful to the entire faculty and staff members of Computer Science and Engineering Department for their direct-indirect help, cooperation, love and affection which made my stay at Thapar University memorable.


(Kiran Deep Singh)

Abstract

Computer networks, both public and private are essential in today's life. Security is the key issue in almost all companies and organizations. Security leads to "Defence in Depth" which can be achieved by using security solutions like antivirus softwares, firewalls, and Intrusion Detection Systems. Most of organizations have security solutions such as firewalls, Intrusion Detection Systems etc. to prevent from the outside world but there is still threat from the intruders residing inside. To overcome the shortcomings of traditional intrusion detection systems in organizations, honeypot is used, based on proactive approach to detect intrusions. Honeypots are deployed in the organization to prevent internal attacks and keep track on hackers' activities. There are two types of honeypots, production and research honeypots. Production honeypots are used to prevent attacks where research honeypots are used in depth analysis of intrudes' activities.

The need of honeypots in organisations is not only to prevent the internal attacks but also to keep track on malicious activities and intruders. The design of campus honeypot is proposed which run as a daemon and create virtual honeypots with production systems of organization deployed in DMZ zone. In order to keep track on intruder's activities Snort and Sebek are integrated with the campus honetpot. Snort is used to capture all the activities performing on the network and Sebek save the every key log of the intruder. Logs are maintained for the further prevention and the research work.

The focus of this thesis is to design a campus honeypot used to prevent the network from malicious activities and the log generated by campus honeypot is helpful for the organization in the research work of organization.

Table of Contents

List of Figures

Chapter 1

Introduction

Now a day's Internet has become the largest public data network, enabling and facilitating both personal and business communications worldwide. The volume of traffic moving over the Internet, as well as corporate networks, is expanding exponentially every day, so network and computer systems connected to it are still too vulnerable and attacks are becoming ever more frequent and computer security is severely threatened by software vulnerabilities. To identify and extract their fundamental characteristics, in-depth analysis of vulnerabilities is required. Computer networks are vulnerable to a variety of exploits that can compromise their intended operations.

1.1 Network Security

Network security is an ongoing process that helps to keep unauthorized parties from gaining access on the network. The goal of network security is to support the network and computer business requirements, using methods that reduce risk. Network security is a prominent feature of the network ensuring accountability, confidentiality, integrity, and above all protection against many external and internal threats such as email based network security problems, denial of service network security attacks, worms and Trojans, and wireless network security attacks Network security is vital to keeping hackers from viewing sensitive information. Implementation of effective network security provides both physical and information security to paths, links, and databases. Security policies describe what must be secured to support the business or mission. As technology, computer security emerged with the development of timesharing and multi-user systems. Security technology research remains an active academic field, attracting much interest from government, military, and commercial sectors [1].

1.2 Security Actions

With the growth of Internets, Extranet and e-Commerce, network security has become a major concern. Now a day most damaging attacks on computer systems involve the exploitation of network infrastructure. To improve network security, organizations have solutions such as firewalls, Virtual Private Networks (VPNs), and intruder detection variants. A firewall filters the traffic flowing between an internal private network and an external public network in order to protect the internal network. Same intrusion detection systems (IDSs) are used to monitor computers or networks for unauthorized entrance or activities, thereby detecting if a system is being targeted by an attack. An intrusion detection system (IDS) monitors network traffic and monitors for suspicious activity and alerts the system or network administrator Preventing, detecting, and reacting to intrusions without disturbing the operations of existing systems represent a big challenge for networks that provide round the clock services such as web servers [2]. The only way to stay ahead of new vulnerabilities and attacks is through detection and response.

Internal network security is very often underestimated by the administrators. In fact, in certain environments such security does not even exist, allowing one user to easily access another user's computer using well-known exploits, trust relationships and default settings. An insider intrusion' is any compromise of a network, system or database that is committed by someone who legitimate access to the network, system or data. Such insiders can include current and former employees, part-time employees, business partners, consultants and contractors.

1.3 Honeypot Technology

The honeypot technology is an attempt to overcome the shortcomings of traditional intrusion detection systems. It can be used to gather information that identifies the collaborator and to answer questions such as how to defend against and defeat the intruder when his identity is not known and no a priori knowledge is available about how he operates and his motives Honeypots provide mechanisms for answering these questions by luring hackers to a controlled environment and then analyzing their activities. Honeypot is a new network security solution based on proactive approach

which is deployed to being attacked, probed, exploited and compromised. As it has no production value so every communication with it is created as malicious. The honeypot generates the log of only those activities which are malicious so, it helps the administrator to analysis the attack and the behaviour of intruders.

In any organisation attacks are suspected from both external and internal environment. Organisations find it convenient to single out employees as the main threat to internal network security so they can put a face on the problem. But unwanted intruders, not employees, pose the greatest risk to organizations [3]. An intruder can be a malicious hacker, former employee or one of the thousands of third-party connections organizations have opened to help further business goals.

Various network security solutions prevent the attacks from the external environment. To detect the intrusions from the internal network honeypot plays an important role. Deploying honeypot inside the organisation helps the administrator to identify the person who is doing malicious work in the organisation. When a honeypot is attacked or compromised it collects the data about the attacks and the system. Production honeypots are easy to use, capture only limited information, and are used primarily by companies or corporations used for production purposes. Research Honeypots are honeypots designed to gain information on the blackhat community [4]. Honeypot has no production activity, no authorized, legitimate interactions will take place on it.

As the network in organisation should be prevented from intruders residing outside, inside the network and depth analysis of every activity performing on the network to analysis of various types of attacks and intrusions. A security system such as honeypot should be designed in such a way that it may prevent from the intruders inside the network and used for the research work. So a honeypot having features of both production and research should be deployed in the campus to solve both purposes as discussed above. The frame work for campus honeypot is proposed and designed in the thesis work in which honeyed is deployed along with partially implementing snort and sebek to make useful for an organisation.

Chapter 2

Literature Survey

2.1 Importance of Networks in Today' life

In today's technological society, protecting the security of information stored on computers and network systems has become a very important issue.

Security

Security is the reduction of risk. One can never eliminate risk, but security helps reduce risk to an organization and its information related resources. Bruce Schneier breaks security down into the three categories as follows.

Prevention: To stop the bad guys. To secure a house, prevention would be similar to placing dead bolt locks on the doors, locking window, and perhaps installing a chain link fence around your yard.

Detection: To detect the bad guys when they get through. Sooner or later, prevention will fail. Sure to detect when such failures happen. Once again using the house analogy, this would be similar to putting a burglar alarm and motion sensors in the house. These alarms go off when someone breaks in.

Reaction: To react to the bad guys once after detecting. Detecting the failure has little value when there is no response. What good does it to be alerted to a burglar if nothing is done? If someone breaks into the house and triggers the burglar alarm, one hopes that the local police force can quickly respond. The same holds true for information security. After detecting a failure, an effective response must execute to the incident [5].

2.2 Goals of Network Security

A successful security management solution begins as an integral part of an organization's overall business strategy. Once security management is accepted as a core business operation, it necessitates the development of guidelines that create the security practices necessary to support the business strategy. The framework is monitored for vulnerability, attack and misuse. The increment in the dependence of societies on information systems, the overall security of t systems should be measured and improved [6].

Confidentiality:

Information in system or transmitted over network, only be accessible to authorized users. Encryption/decryption is used to protect even the existence of data and unauthorized users should not even know about the existence of a message or its properties.

Authentication:

Authentication should be able to verify that a user is indeed who it claims to be here user may be a human being, a program accessing a service and two communicating parties.

Integrity

Integrity means messages are received as sent, with no modification, duplication, insertion, reordering, replays.

Non-repudiation:

Non-repudiation means that sender or receiver cannot deny their role in a communication.

Access Control:

Access Control limits and control access to system services and Applications.

Availability:

Availability means Services must be available to authorized users.

2.3 Network Security Life Cycle

Security needs to be addressed as a continued lifecycle to be effective. There are new attack signatures being developed, viruses and worms being written, natural disasters occurring, changes in the organization workplace taking place and new technologies evolving, these all affect the security posture in the organization. Any one piece of the lifecycle cannot be effective without the other. Identifying risks and correcting them are essential.

2.3.1 Elements of the Lifecycle

- Perimeter Protection.
- Risk and Vulnerability Assessment.
- Information Systems Security Policies.
- Penetration Testing.
- Intrusion Detection.

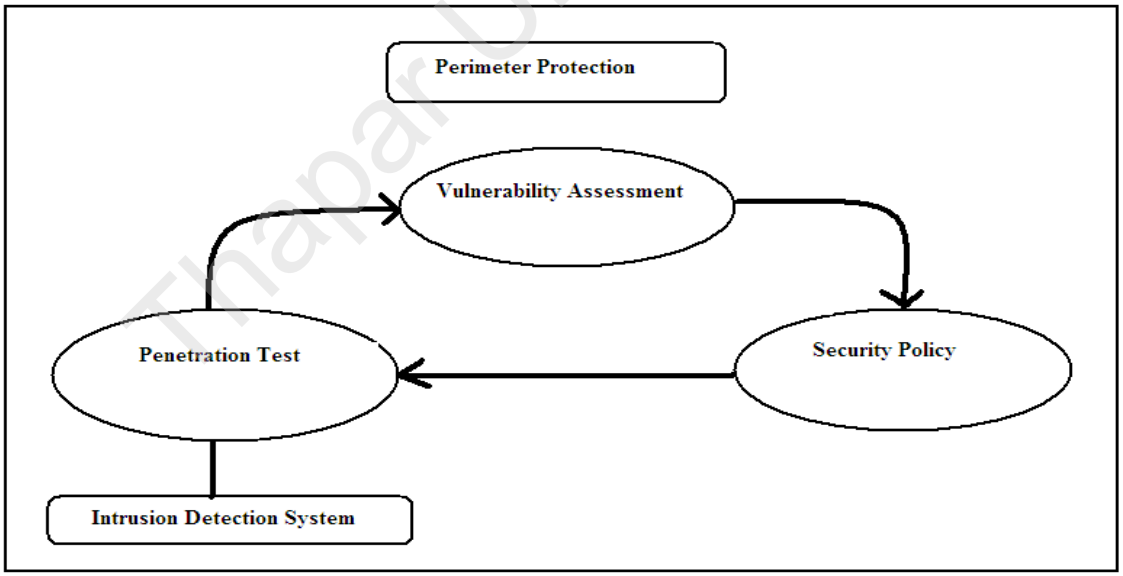


Figure: 2.1 Security Life Cycle

The lifecycle needs to be a continued effort for any organization to keep abreast of changes in technology and weaknesses in security that are created as a result of these changes [7].

2.4 Threats to Network Security

Viruses: Computer programs written by devious programmers and designed to replicate themselves and infect computers when triggered by a specific event.

Trojan horse programs: Delivery vehicles for destructive code, which appear to be harmless or useful software program.

Attacks: Including reconnaissance attacks (information-gathering activities to collect data that is later used to compromise networks); access attacks (which exploit network vulnerabilities in order to gain entry to e-mail, databases, or the corporate network); and denial-of-service attacks (which prevent access to part or all of a computer system).

Data interception: Involves eavesdropping on communications or altering data packets being transmitted.

Social engineering: This is an approach to gain access to information, primarily through misrepresentation, and often relies on the trusting nature of most individuals. [8]. Obtaining confidential network security information through non technical means, such as posing as a technical support person and asking for people's passwords.

2.5 Network Security Tools

Antivirus software packages: These packages counter most virus threats if regularly updated and correctly maintained.

Secure network infrastructure: Switches and routers have hardware and software features that support secure connectivity, perimeter security, intrusion protection, identity services, and security management. Dedicated network security hardware and software-tools such as firewalls and intrusion detection systems provide protection for all areas of the network and enable secure connections.

Virtual private networks: These networks provide access control and data encryption between two different computers on a network. This allows remote workers to connect to the network without the risk of a hacker or thief intercepting data.

Identity services: These services help to identify users and control their activities and transactions on the network. Services include passwords, digital certificates, and digital authentication keys.

Encryption: Encryption ensures that messages cannot be intercepted or read by anyone other than the authorized recipient. Encryption is another method by which network security is heightened. An encrypted document cannot be read by anyone who does not possess the key or the formula that's used to translate the original text into cipher text. Two methods of encryption, Cryptext and Kerberos, are tools that can be used to increase network security by encrypting documents on the network [9].

Security management: This is the glue that holds together the other building blocks of a strong security solution.

2.6 Approaches to Network Security

With the number of security threats on the rise, network security has become an essential part of maintaining the privacy and integrity of an enterprise. Most security professionals are aware of the two basic approaches used to deal with security vulnerabilities: proactive and reactive. Proactive approaches include all measures that are taken with the goal of preventing host-based or network-based attacks from successfully compromising systems. Reactive approaches are those procedures that organizations use once they discover that some of their systems have been compromised by an intruder or attack program.

2.6.1 Proactive Approaches

Every modern organization realizes the value of dedicating some resources to the prevention of expensive damages that will likely occur if such preventive measures are not taken. Intrusion Detection and Response Systems to try to detect computer intrusions and then activate defensive measures when an attack is detected Proactive network security is the act of managing the network security to get the most performance system with a vulnerability management system [10].

2.6.2 Reactive Approaches

Reactive methods include Disaster Recovery Plans, use of private investigation services and loss recovery specialists, reinstallation of operating systems and applications on compromised systems, or switching to alternate systems in other locations. Having an appropriate set of reactive responses prepared and ready to implement is just as important as having proactive measures in place.

Using the components of our layered network security model, Network Security Provider design a high-performance security solution customized to fit the specific business strategy. Network Security Provider has the technology helps to defend the network against attacks by implementing preventative security solutions.

2.7 Protection against External Threats

Intrusion Prevention: Safeguard the network inside and out from lethal worm invasions and other malicious attacks.

Firewall & VPN: Secure the Internet access points and guard your network's privacy with complete Firewall/VPN protection.

Antivirus Protection: Protect the PC by automatically by eliminating viruses, worms and Trojan horses.

Vulnerability Scanning: Scan the network to identify and dramatically reduce the number of vulnerabilities within the network.

Protection against Internal Threats

Web & Email Filtering: Eliminate productivity, network and legal threats by implementing web and email filtering systems.

Event Management: By monitoring the security event logs of all Windows NT/2000/XP servers and workstations administrator can be alerted to internal intrusions/attacks in real time.

2.8 Network Security Solutions

2.8.1 Firewall

A firewall is hardware or software solution to enforce security policies or another way to look at it is in a physical security analogy. A firewall permits only authorized users such as those with a key or access card to enter. A firewall blocks unauthorized and potentially dangerous material from entering the system. Depending on its placement within a network, a firewall or IDS may not protect a network from internal attacks [11]. Yet, the largest shortcoming inherent to both firewalls and Intrusion Detection Systems is their reliance on signatures of known attacks. The rules used by both firewall and intrusion detection systems are based on information gathered from previous attacks.

Firewall Characteristics

1. All traffic from inside to outside, and vice versa, must pass through the firewall. This is achieved by physically blocking all access to the local network except via the firewall.
2. Only authorized traffic, as defined by the local security policy, will be allowed to pass. Various firewalls are used, which implement various types of security policies.
3. The firewall itself is immune to penetration. This implies that use of a trusted system with a secure operating system.

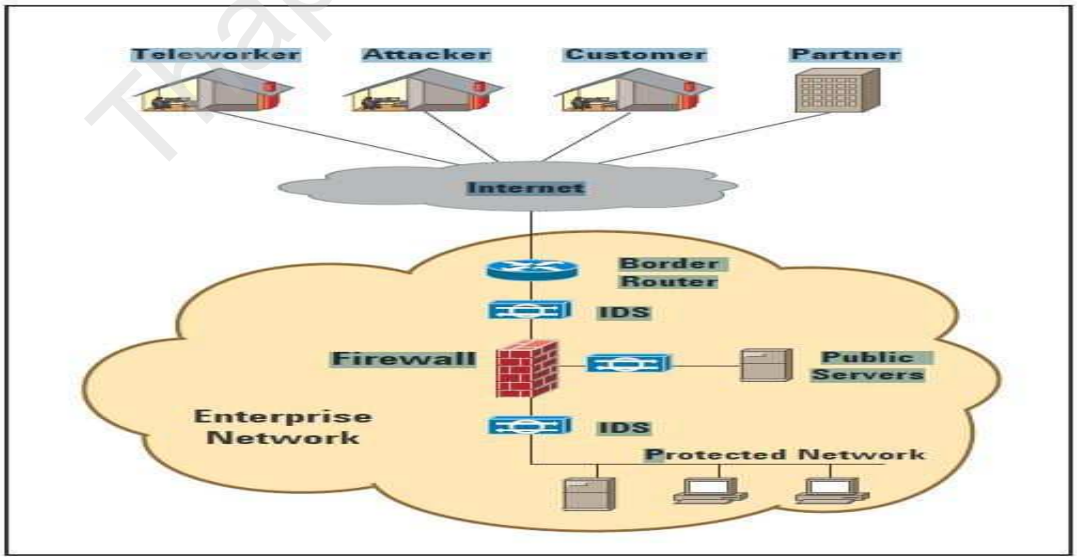


Figure2.2 Firewall

Firewalls fall into four broad categories: packet filters, circuit level gateways, application level gateways and stateful multilayer inspection firewalls.

2.8.2 Intrusion Detection Systems

An IDS system is used to make security professional aware of packets entering and leaving the monitored network. IDS are often used to sniff out network packets giving a good understanding of what is really happening on the network [12].Intrusion Detection is the art of detecting inappropriate, incorrect, or anomalous activity. Among other tools, an Intrusion Detection System (IDS) can be used to determine if a computer network or server has experienced an unauthorized intrusion.

Captured packets are analyzed in a number of different ways. Some NID devices will simply compare the packet to a signature database consisting of known attacks and malicious packet "fingerprints", while others will look for anomalous packet activity that might indicate malicious behavior. In either case, network intrusion detection should be regarded primarily as a perimeter defense. Intrusion detection has historically been incapable of operating in the like environments switched networks, encrypted networks and high-speed networks.

IDS Techniques

There are four basic techniques used to detect intruders: anomaly detection, misuse detection (signature detection), target monitoring, and stealth probes [13].

Anomaly Detection

Designed to uncover abnormal patterns of behavior, the IDS establishes a baseline of normal usage patterns and anything that widely deviates from it gets flagged as a possible intrusion.

Misuse Detection or Signature Detection

Commonly called signature detection, this method uses specifically known patterns of unauthorized behaviour to predict and detect subsequent similar attempts. These specific patterns are called signatures. For host-based intrusion detection, one example of a signature is "three failed logins." For network intrusion detection, a signature can be as simple as a specific pattern that matches a portion of a network packet.

Target Monitoring

These systems do not actively search for anomalies or misuse, but instead look for the modification of specified files. This is more of a corrective control, designed to uncover an unauthorized action after it occurs in order to reverse it. One way to check for the covert editing of files is by computing a cryptographic hash beforehand and comparing this to new hashes of the file at regular intervals

Stealth Probes

This technique attempts to detect any attackers that choose to carry out their mission over prolonged periods of time. Attackers will check for system vulnerabilities and open ports over a two-month period, and wait another two months to actually launch the attacks. Stealth probes collect a wide-variety of data throughout the system, checking for any methodical attacks over a long period of time.

An Intrusion Detection System provides much the same purpose as a burglar alarm system installed in a house. In case of an intrusion, the IDS system will issue some type of warning or alert. An operator will then tag events of interest for further investigation by the Incident Handling team. After the initial response the events need to be handled, looking at issues such as investigation, Computer Forensics and prosecution. There are two general types of Intrusion Detection Systems:

2.8.2.1 Host Based Intrusion Detection Systems (HIDS)

IDS systems that operate on a host to detect malicious activity on that host. Host-based intrusion detection is best suited to combat internal threats because of its ability to monitor and respond to specific user actions and file accesses on the host .Host intrusion detection systems are installed locally on host machines making it a very versatile system compared to NIDS. HIDS can be installed on many different types of machines namely servers, workstations and notebook computers. Traffic transmitted to the host is analyzed and passed onto the host if there are not potentially malicious packets within the data transmission. HIDS are more focused on the local machines changing aspect compared to the NIDS [14].

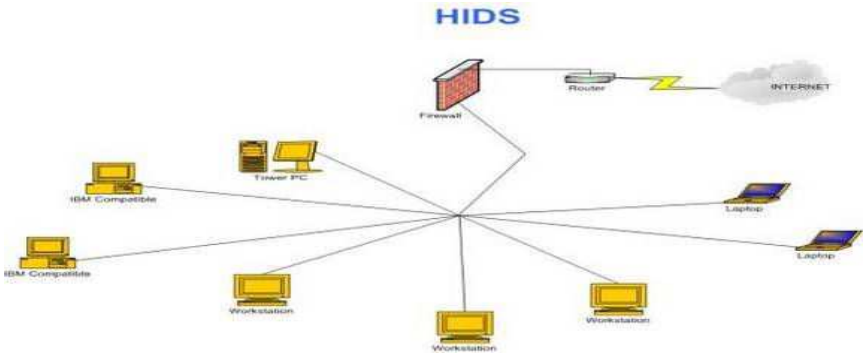


Figure: 2.3 Host Based Intrusion Detection System

HIDS is also more platforms specific and caters strongly in the windows market of the computing world however there are products available that function in the UNIX and other OS topology environments. Host based IDS are a more comprehensive solution and displays great strengths in all network environments

2.8.2.2 Network Based Intrusion Detection Systems (NIDS)

IDS systems that operate on network data flows. Network-based intrusion detection analyzes data packets that travel over the actual network. These packets are examined and sometimes compared with empirical data to verify their nature: malicious or benign. Because they are responsible for monitoring a network, rather than a single host, Network-based intrusion detection systems (NIDS) tend to be more distributed than host-based IDS.

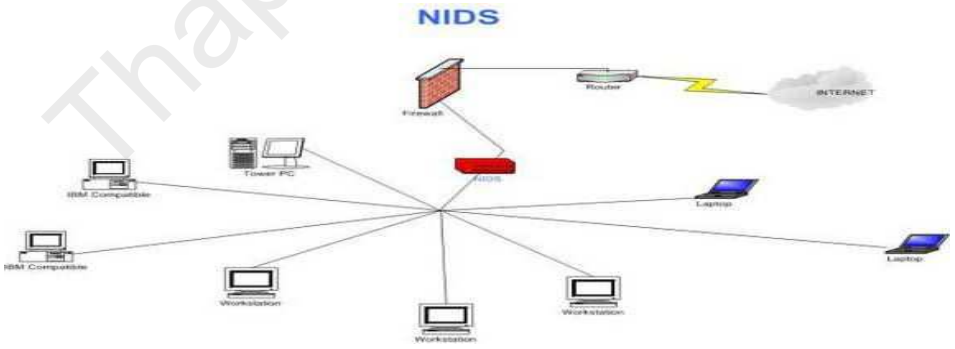


Figure: 2.4 Network Based Intrusion Detection System

The diagram above represents the typical NIDS scenario where an attempt has been made to funnel the traffic through the NIDS device on the network [15]. Network-

based IDS uses techniques like "packet-sniffing" to pull data from TCP/IP or other protocol packets travelling along the network. This surveillance of the connections between computers makes network-based IDS great at detecting access attempts from outside the trusted network. In general, network-based systems are best at detecting the following activities:

Unauthorized outsider access: When an unauthorized user logs in successfully, or attempts to log in, they are best tracked with host-based IDS. However, detecting the unauthorized user before their log on attempt is best accomplished with network-based IDS.

Bandwidth theft/denial of service: These attacks from outside the network single out network resources for abuse or overload. The packets that initiate/carry these attacks can best be noticed with use of network-based IDS.

Some possible downsides to network-based IDS include encrypted packet payloads and high-speed networks, both of which inhibit the effectiveness of packet interception and deter packet interpretation.

Snort as IDS

Snort is a libpcap-based packet sniffer/logger based on Network Intrusion Detection System that can be used as a lightweight network intrusion detection system. It is an open source Network Intrusion Detection System (NIDS) which is available free of cost and used for scanning data flowing on the network [16]. It has three primary uses. It can be used as a straight packet sniffer like tcpdump, a packet logger and a full blown network intrusion detection system.

Snort may help you to detect certain types of attacks that can take place at the security perimeter of the network.

2.8.3 Intrusion Prevention System

A new type of Intrusion Detection system is becoming more and more popular: the Intrusion Prevention System, or IPS. This is a system that actively monitors a network or host for attacks and prevents those attacks from occurring. These systems are proactive defence mechanisms designed to detect malicious packets within normal network traffic (something that the current breed of firewalls do not actually do, for

example) and stop intrusions dead, blocking the offending traffic automatically before it does any damage rather than simply raising an alert as, or after, the malicious payload has been delivered.

2.8.3.1 Host-based intrusion-prevention

A host-based IPS (HIPS) is where the intrusion-prevention application is resident on that specific IP address, usually on a single computer. HIPS complements traditional finger-print-based and heuristic antivirus detection methods, since it does not need continuous updates to stay ahead of new malware. As ill-intended code needs to modify the system or other software residing on the machine to achieve its evil aims, a truly comprehensive HIPS system will notice some of the resulting changes and prevent the action by default or notify the user for permission

2.8.3.2 Network based intrusion-prevention

A network-based IPS is one where the IPS application/hardware and any actions taken to prevent an intrusion on a specific network host(s) is done from a host with another IP address on the network (This could be on a front-end firewall appliance.)
Network intrusion prevention systems (NIPS) are purpose-built hardware/software platforms that are designed to analyze, detect, and report on security related events. NIPS are designed to inspect traffic and based on their configuration or security policy, they can drop malicious traffic.

Unfortunately for the System Administrator, there are numerous and ever more ingenious techniques for circumventing firewalls [17]. For instance, firewalls do not protect against the transfer of an email carrying a virus infected attachment, or they might be fooled by packets that have been intentionally fragmented, in ways designed to bypass firewalls. Some networks (i.e. those at large public universities) cannot have extremely protective firewalls because of their need to maintain academic openness. Networks with extremely large amounts of traffic, such as those at major corporations and universities, may be impractical to firewall due to the sheer volume of traffic.

While this warning system is useful and an extremely powerful defensive tool, especially combined with a firewall, it too has shortcomings. Neither a firewall or an

IDS can defend against an attack that bypasses the defense, such as unauthorized modems or even encrypted tunnels passing through them. Any attack from those the rules are based on will likely bypass both a firewall and IDS without raising an alarm[18].

The majority of computer threats come from within organizations, from many different sources; disgruntled employees and corporate spies are just two examples. In fact, intrusion detection expert Richard Power states, "each year, we've asked the respondents to rate the likely sources of network or a attack [19].

2.8.4 Honeypot IDS

Honeypots are systems used to lure hackers by exposing known vulnerabilities deliberately.Once a hacker finds a honeypot,it is more likely that the hacker will stick around for some time.Duding this time the activities of hackers can be logged to find out hackers' actions and techniques.Honeypots can emulate numerious operating systems dedicated services like ftp,http etc. and track the finger print of an inruder.

2.9 Honeypot

A honeypot is used in the area of computer and Internet security. It is a resource which is intended to be attacked and compromised to gain more information about the attacker and the tools used by attackers. It can also be deployed to attract and divert an attacker from their real targets.

L. Spitzner1 defines the term honeypot as follows:" A honeypot is a resource whose value is being in attacked or compromised. This means, that a honeypot is expected to get probed, attacked and potentially exploited. Honeypots do not fix anything. They provide us with additional, valuable information".

Honeypots do not help directly in increasing a computer network's security. On the contrary, they do attract intruders and can therefore attract some interest from the Blackhat community on the network where the honeypot is located. So the above definition can be modified as "A honeypot is a resource which pretends to be a real target. A honeypot is expected to be attacked or compromised. The main goals are the

distraction of an attacker and the gain of information about an attack and the attacker."There is a general definition which covers all the different manifestations of honeypots.A honeypot is an information system resource whose value lies in unauthorized or illicit use of that resource [20].

This means that the honeypot is designed according to expectation and goal to have the system probed, attacked, and potentially exploited. Compared to an intrusion detection system, honeypots have the big advantage that they do not generate false alerts as each observed traffic is suspicious, because no productive components are running on the system.

Theoretically, a honeypot should see no traffic because it has no legitimate activity. This means any interaction with a honeypot is most likely unauthorized or malicious activity. Any connection attempts to a honeypot are most likely a probe, attack, or compromise. The beauty of a honeypot's lies in its simplicity. It is a device intended to be compromised, not to provide production services. This means there is little or no production traffic going to or from the device. Any time a connection is sent to the honeypot, this is most likely a probe, scan, or even attack. Any time a connection is initiated from the honeypot, this most likely means the honeypot was compromised. There are tremendous advantages and disadvantages of honeypots.

Advantages: Honeypot is a concept, which gives them some very powerful strength.

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.

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

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

Encryption or IPv6*:* Unlike most security technologies (such as IDS systems) honeypots work fine in encrypted or IPv6 environments. It does not matter what the bad guys throw at a honeypot, the honeypot will detect and capture it.

Information*:* Honeypots can collect in-depth information that few, if any other technologies can match.

Simplicity: Finally, 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.

Disadvantages: Like any technology, honeypots also have their weaknesses. It is because of this they do not replace any current technology, but work with existing technologies.

Limited view*:* Honeypots can only track and capture activity that directly interacts with them. Honeypots will not capture attacks against other systems, unless the attacker or threat interacts with the honeypots also.

Risk*:* All security technologies have risk. Firewalls have risk of being penetrated, encryption has the risk of being broken, and IDS sensors have the risk of failing to detect attacks. Honeypots are no different, they have risk also. Specifically, honeypots have the risk of being taken over by the bad guy and being used to harm other systems. This risks various for different honeypots. Depending on the type of honeypot, it can have no more risk than an IDS sensor, while some honeypots have a great deal of risk [21].

2.9.1 Attackers

The main value of honeypot lies on being attacked so that the administrator can study their attackers and kinds of attacks. The main objective of the honeypot is to lure the bad guys or attackers. There are mainly two types of attackers:

Script Kiddies

Script kiddies are attackers who use malicious programs written by other, more sophisticated attackers. Script kiddies normally do not understand the fundamentals of the attack, and simply use these programs to gain access to your computer. For some, the main goal is to hack computer with less effort using already existing scripts or with minor changes to scripts [22].

Black Hat

These are more knowledgeable and more experienced with the internal working of various communication systems, the Internet and focus on system of high value. Black hat attackers are mostly financially driven and affect the corporate and national level and are more dangerous because of skills level. Black hat attackers try to get information like personal data, credit card information and in higher level for any business their data and system resources.

Personal Enemies

Personal enemies are those people who are most likely known. Perhaps it's an ex-boyfriend or ex-girlfriend, a co-worker, or maybe even family member. The skill level of the attacker can vary, as does the motivation of the attack. A personal enemy could want to read the email, or damage the data. An attack from a personal enemy is always targeted.

2.9.2 Values of Honeypots

There are two categories of honeypots – production honeypots and research honeypots. A production honeypot is used to help migrate risk in an organization while the second category, research, is meant to gather as much information as possible.

Production honeypots: Production honeypots are easy to use, capture only limited information, and are used primarily by companies or corporations.When used for production purposes, honeypots are protecting an organization. This would include

preventing, detecting, or helping organizations respond to an attack.production honeypots apply to the three areas of security, Prevention, Detection, and Reaction.

Research honeypots Research Honeypots, are honeypots designed to gain information on the blackhat community. These honeypots do not add direct value to a specific organization. Instead they are used to research the threats organizations face, and how to better protect against those threats. are complex to deploy and maintain, capture extensive information, and are used primarily by research, military, or government organizations.When used for research purposes, honeypots are being used to collect information. This information has different value to different organizations [23].

Honeypots can add value in research by giving us a platform to study the threat. What better way to learn about the bad guys then to watch them in action, to record step-by-step as they attack and compromise a system. Research honeypots are excellent tools for capturing automated attacks. Since these attacks target entire network blocks, research honeypots can quickly capture these attacks for analysis.

2.9.3 Honeypots as a Detection Solution

Honeypots are a relatively new security technology whose real value lies in being probed, attacked, or compromised so that the actions of the intruders can be observed, analyzed and understood.

Honeypot has no production activity , no authorized, legitimate interactions will take place on it. Anytime anything or anyone is interacting with the honeypot, it is most likely indicative of unauthorized or malicious activity. Honeypots are in many ways the very opposite of NIDS and other traditional detection technologies. Where NIDS fail honeypots can excel. The disadvantages of NIDS are solved by the honeypots.in following ways. Combined, what this means is that honeypots can make extremely simple, cost-effective detection. By simple, the concept of honeypots is very easy to understand and implement. Honeypots have no rules to update or modify, and no advanced algorithms are required to analyze network traffic. Simplicity has its own inherent advantages.

Honeypots dramatically reduce the amount of information to be collected, correlate, and archive. This reduction in man-hours allows security personnel to focus on other critical activities, such as patching. Honeypots also address some of the inherent failings of NIDS, such as detecting new attacks, or working in environments with encryption or IPv6 protocols [24].

Most production honeypots used for detection capture no more information then traditional security technologies, such as firewalls, routers, or NIDS.

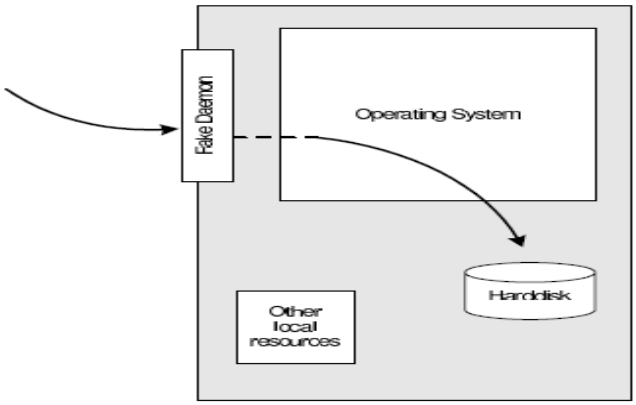
2.9.4 Level of Involvement

The level of involvement does measure the degree an attacker can interact with the operating system.

2.9.4.1 Low-Involvement Honeypot

A low-involvement honeypot typically only provides certain fake services. In a basic form, these services could be implemented by having a listener on a specific port. For example a simple **netcat -l -p 80 > /log/honeypot/port 80.log** could be used to listen on port 80 (HTTP) and log all incoming traffic to a log file. In such a way, all incoming traffic can easily be recognized and stored. With such a simple solution it is not possible to catch communication of complex protocols.

On a low-involvement honeypot there is no real operating system that an attacker can operate on. This will minimize the risk significantly because the complexity of an operating system is eliminated. On the other hand, this is also a disadvantage. It is not possible to watch an attacker interacting with the operating system, which could be really interesting. A low-involvement honeypot is like a one-way connection, can only listen, but not ask questions. The role of this approach is very passive. A low-involvement honeypot can be compared to an ID, as both are passive systems and do not alter any traffic or interact with the attacker or the traffic flow



.

Figure 2.5 Low-Involvement Honeypot

2.9.4.2 Mid Interaction Honeypot

A mid-involvement honeypot provides more to interact with, but still does not provide a real underlying operating system. A mid involvement honeypot does interact with the attacker in a minimal way Developing a mid-involvement honeypot is complex and time consuming. Special care has to be taken for security checks as all developed fake daemons need to be as secure as possible.

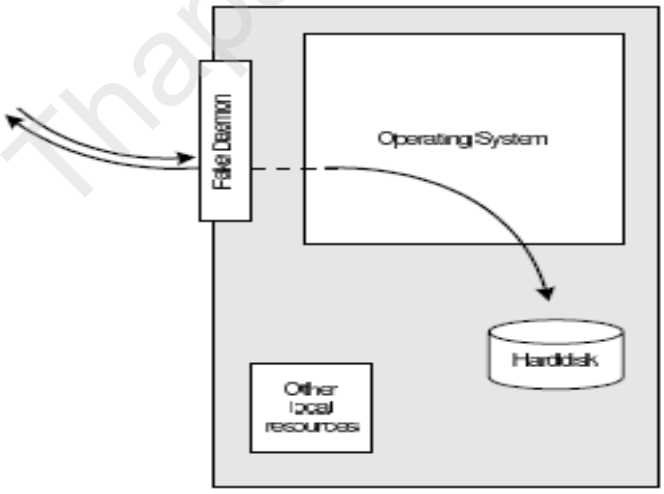


Figure: 2.6 Mid-Involvement Honeypot

2.9.4.3 High Interaction Honeypot

A high-involvement honeypot has a real underlying operating system. This leads to a much higher risk as the complexity increases rapidly. Unfortunately the attacker has to compromise the system to get this level of freedom. Attackers will have root rights on the system and can do everything at any moment on the compromised system. This system is no longer secure. Even the whole machine cannot be considered as secure [25].

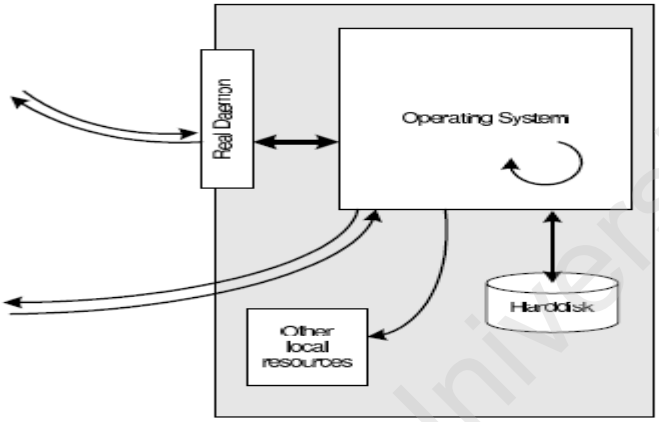


Figure: 2.7 High-Involvement Honeypot

A high involvement honeypot has great risk as the attacker can compromise the system and use all its resources. By providing a full operating system to the attacker, he has the possibilities to upload and install new files. This is where a high-involvement honeypot can show its strength, as all actions can be recorded and analyzed. Gathering new information about the blackhat community is one main goal of a high-involvement honeypot and legitimates the higher risk.

A honeypot will attract and generate a lot of unwished traffic like port scans or attack patterns. By placing a honeypot outside the firewall, such events do not get logged by the firewall and an internal IDS system will not generate alerts. Otherwise, a lot of alerts would be generated on the firewall or IDS.

2.9.5 Honeypot Topologies

Honeypot Location

Honeypot can be used on the Internet as well as the intranet, based on the needed service. Placing a honeypot on the intranet can be useful if detecting some bad guys inside a private network is wished. It is especially important to set the internal thrust for a honeypot as low as possible as this system could be compromised, probably without immediate knowledge. If the main concern is the Internet, a honeypot can be placed at two locations:

1. In front of the firewall (Internet)
2. Demilitarized Zone, (a network segment that is only partly accessible from the Internet.)
3. Behind the firewall (intranet)

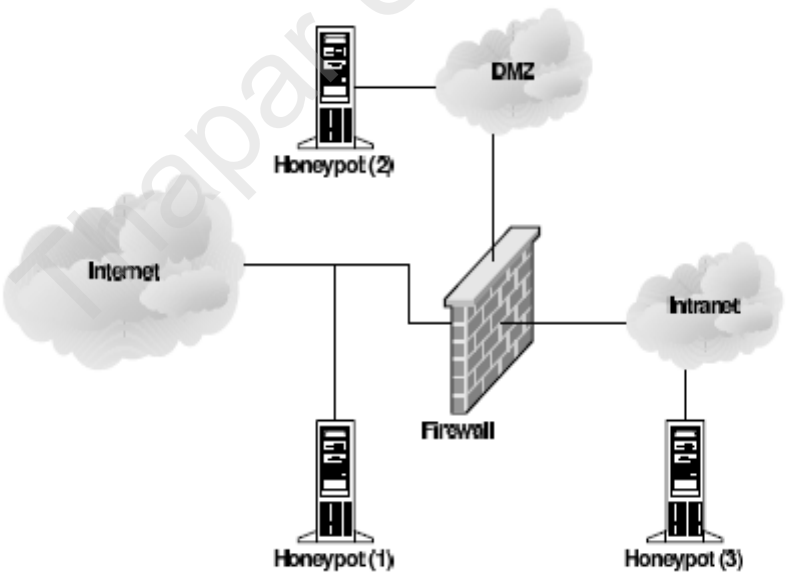


Figure: 2.8 Location of honeypot

2.9.5.1 In Front of the Firewall

By placing the honeypot in front of a firewall the risk for the internal network doesn't increase. The danger of having a compromised system behind the firewall is eliminated. This could be a special problem as soon as no additional firewalls are used to shield some resources or if the IP is used for authentication.

A honeypot will attract and generate a lot of unwished traffic like portscans or attack patterns. By placing a honeypot outside the firewall, such events don't get logged by the firewall and an internal IDS system won't generate alerts. Otherwise, a lot of alerts would be generated on the firewall or IDS.

Probably the biggest advantage of the firewall or IDS, as well as any other resources, is that they haven't to be adjusted because the honeypot is outside the firewall and viewed as any other machine on the external network. Running a honeypot does therefore not increase the risk of the internal network nor does it introduce new risks [26].

The disadvantage of placing a honeypot in front of the firewall is that internal attackers can't be located or trapped that easy, especially if the firewall limits outbound traffic and therefore limits the traffic to the honeypot.

2.9.5.2. In DMZ

Placing a honeypot inside a DMZ seems a good solution as long as the other systems inside the DMZ can be secured against the honeypot. Most DMZs are not fully accessible as only needed services are allowed to pass the firewall. In such a case, placing the honeypot in front of the firewall should be favoured as opening all corresponding ports on the firewall is too time consuming and risky.
Using an own DMZ for the honeypot is a good approach and should be considered. The preliminary firewall can be connected to the Internet or intranet, depending on the main goal of the honeypot mission. The attempt of using a DMZ for the honeypot itself enables tight control as well as a flexible environment with maximum security.

The only disadvantage is the increased demand for hardware as well as some administration effort for the additional firewall [27].

Based on the reviewed advantages and disadvantages, placing a honeypot behind the firewall is only important if spotting internal attackers is a main concern or placing in front of the firewall isn't possible. If possible in any way, using an separate DMZ for the honeypot should be chosen. The advantages are significantly, especially the gained security.

2.9.5.3 Behind the Firewall

A honeypot behind a firewall can introduce new security risks to the internal network, especially if the internal network is not secured against the honeypot through additional firewalls.

A honeypot often provides a lot of services. Probably most of them aren't used as exported services to the Internet and are therefore blocked by the firewall. By placing the honeypot behind this firewall, it is inevitable to adjust the firewall rules and probably also the IDS signatures as it could be wished not to generate an alert every time the honeypot is attacked or scanned.

The biggest problem arises as soon as the internal honeypot is compromised by an external attacker. He then has the possibility to access the internal network through the honeypot. This traffic will be unstopped by the firewall as it is regarded as traffic to the honeypot only, which in turn is granted. Securing an internal honeypot is therefore mandatory, especially if it is a high-involvement honeypot.

The main reason for placing a honeypot behind a firewall could be to detect internal attackers. With an internal honeypot it is also possible to detect a mis-configured firewall. Sometimes, placing a honeypot in front of a firewall is not possible since no external IP's are available nor access to the network in front of the firewall is possible.

2.9.6 Honeypot Solutions

2.9.6.1 KFSensor

KFSensor serves both as the honeypot and an intrusion detection system. It is windows based software with a graphical user interface monitoring system. The KFSensor is a low interaction honeypot, which emulates preconfigured services and also programmable services. The software keeps track of all the communication between the server and the outside party.

KFSensor has two main important components:

KFSensor Server:
It runs at the background as one of the windows services. It is the major core of the software as it interacts with outsider and records the events. It listens on both TCP and UDP port.

KFSensor Monitor:

It is the front end of the program and user can use its user friendly GUI to configure the services, scenario and monitor the events generated by the server [28].The main component of the KFSensor is the KFSensor server, which listen to all the configured service on both the TCP and UDP ports.
Some of the other features are:

The GUI and easy wizard makes it simple and its really flexible which can be handled to:

- customize multiple scenarios based on our test.
- both TCP and UDP port
- to program server.
- HTTP and SMTP.

2.9.6.2 Honeyd

Honeyd is low interaction; freely available, open source pre-packaged virtual honeypot solution. The software was developed by Niels Provos of the University of Michigan. Since it is an Open source, the program is constantly developing and evolving with new features and functionalities from contributors from all around. The low interaction classification of honeyd will only allow emulating the services and doesn't allow attacker to interact with the operating system of the honeypot. Similar to KFSensor the services can be ran into any TCP port.

As shown in figure Honeyd is a daemon application which enables the setup of multiple virtual honeypots on a single machine. The main important difference with the KFSensor is that, personality feature. This feature or configuration will allow configuring the each production honeypot with a personality of OS IP stack and it binds a script to the emulated port to visualize the service.

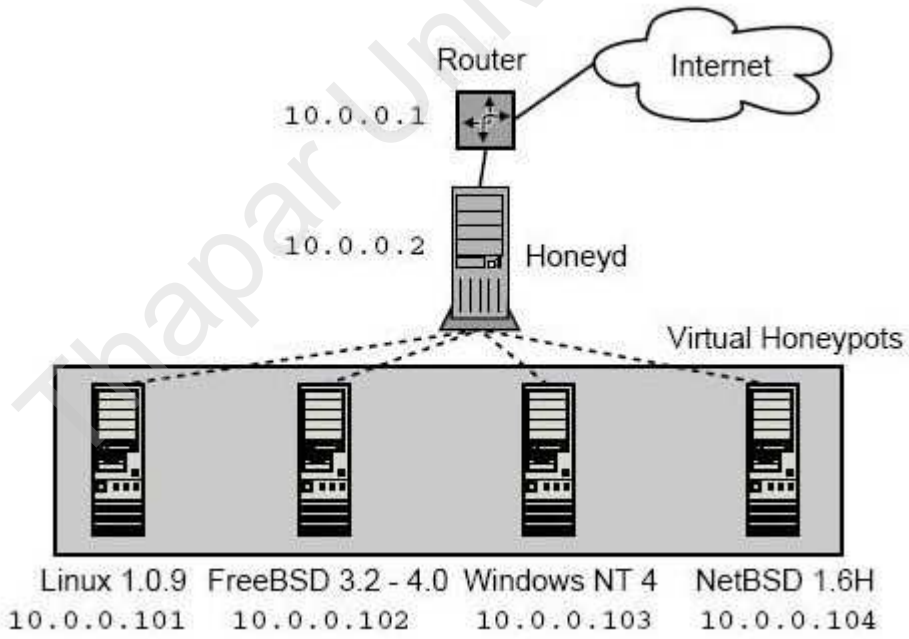


Figure 2.9 : Honeyd is a daemon application

Honeyd is primarily used for detecting attacks. It works by monitoring IP addresses that are unused, that have no system assigned to them. Whenever an attacker attempts to probe or attack an non-existent system, Honeyd assumes the IP address of the

victim and then interacts with the attacker through emulated services. Honeypots are limited to detecting attacks only on the ports that have emulated services listening on. it detects and logs connections made to any port, regardless if there is a service listening [29].

2.9.6.3 Honeynet Sebek

This is High-interaction honeypot designed to capture in-depth information which has different value to different organizations. As shown in Figure 2.10 architecture is populated with live systems. A highly controlled network where every packet entering or leaving is monitored, captured, and analyzed.

Sebek is a data capture tool that capture data and recreate the events on a honeypot. In order to determine information such as when an intruder broke in, how they did it, and what they did after gaining access it is used. This information is used to answer about who the intruder is, what their motivations are, and who they may be working with,an intruder did after gaining access, data that provides the intruder's keystrokes and the impact of the attack.

Earlier the sebek were designed to collect keystroke data from directly within the kernel. These are equivalent to a Rootkit that used a trojaned sys_read call to capture keystrokes. This system logged keystrokes to a hidden file and exported them over the network in a manner to make them look like other UDP traffic.The current iteration of Sebek not only record keystrokes but also read all sys_read data [30].

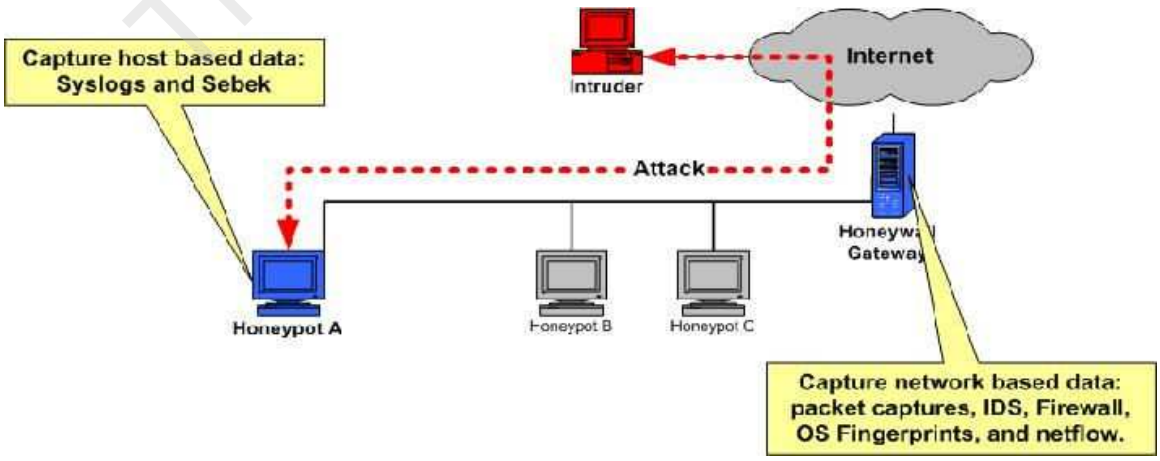


Figure: 2.10 Sebek-Honeynet Architecture.

Data Control:

- Mitigate risk of honeynet being used to harm production system
- Count outbound connections.
- IPS (Snort-Inline).
- Bandwidth throttling.

Data Capture:

- Capture activities at various levels.
- Application
- Network
- OS level.

Data Analysis:

- Manage and analysis captured data from honeypots
- Investigate malware.
- Forensic purpose.

2.9.7 Honeynets

A honeypot is physically a single machine, probably running multiple virtual operating systems. Controlling outbound traffic is not possible, as the traffic goes directly onto the network. The only possibility to limit outbound traffic is to use a preliminary firewall. Such a more complex environment is often referenced as honeynet. A typical honeynet consists of multiple honeypots and a firewall (or firewalled-bridge) to limit and log network traffic. An IDS is often used to watch for potential attacks and decode and store network traffic on the preliminary system [31].

2.9.8 Need of Honeynets in Organization

Honeynets have demonstrated their value as a research tool in the area of Information Assurance (IA). Many researchers and organizations in the security community, both public and private, are currently employing honeynets to continue to gather knowledge concerning the tactics, techniques and procedures of the hacker community**.**

The Georgia Institute of Technology (Georgia Tech), successfully deployed a honeynet on the internal network to collect information on hackers and to help secure their campus enterprise network. [32]. Georgia Tech have established a network of honeypots known as a honeynet with in the Gerogia Tech IP (Internet Protocol) address range. This honeynet is accessible from both the Internet and within the campus network and is subject to frequent intrusions and attacks.

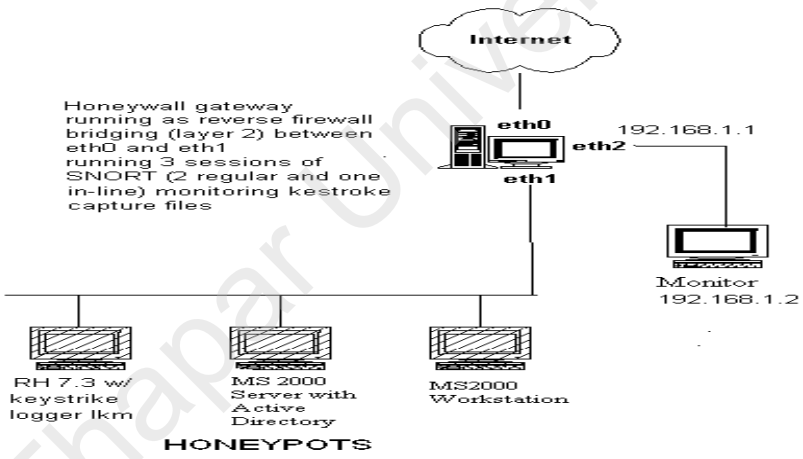


Figure 2.11: Network of honeypots established at Georgia Tech.

The Honeynet has been established with monitoring capabilities to observe and record this intrusion and attack activity. The main objective of the Georgia Tech Honeynet is to increase the overall security of the Georgia Tech campus network by observing the actions of would-be attackers of Georgia Tech systems [33].

As shown in Figure 2.11 Georgia Tech employs a mixture of Linux and Microsoft systems on their Honeynet. These are actual live systems and not emulated software systems.

Chapter 3

Problem Statement

As reviewed in the literature honeypot is essential in every organisation for the both purposes preventing from intruders and keeping track on the activities. So the problem is to make a honeypot with features of both production and research honeypot and should be deployed in mix environment of low and high interaction. There are some other but important issues also that must be solved with the implementation of compus honeypot.

Difficulty in examination of log files: Existing systems like firewalls, intrusion detection systems generate logs, which contains all information processed on the network which makes logs are very big and redundant. It is very difficult for administrator to understand and identify the intruders.

Signature of predefined attacks: Existing systems only finds the exploits which are existing once, means these vulnerabilities on the networks has been already discovered. These systems find only signatures of predefined attacks. These systems provide no signatures of new attacks, which can be one of the most dangerous vulnerability of the network in the future.

Reactive approach: Existing systems detect the problem when the problem had been occurred means these are reactive. The consequences of the problem one has to face cannot cure the system.

Identification of internal threats: These systems help to find the external threats of the organisations. This system restricts the access of the outsiders, but these systems cannot do anything if any insider who has the authority can steal the information and cause some problem.

Depth analysis of intruders' activity: Existing security techniques only identify the information of intruder's current malicious activities; they do not provide any clue of intruder's future's malicious activity.

Visibility of production System: If an organisation wants to hide the identifications of its productive system. If it is live means existing on the network, then cannot hide the visibility of the system. So, it is very big problem to hide the identity of the system and for intruder it is very easy to do bad with system using various attacks.

Objectives

The main aim behind this thesis work is to make a honeypot having features of both production and research honeypot which fulfil the following objectives.

1. Prevent production systems deployed in campus from the internal intruders and keep intruders busy with fake operating systems.
2. Keep track on intruders' activities and analyze their actions to take decisions accordingly.

Chapter 4

Problem Solution

The solution of the problems discussed in the previous section is to design and develop a campus honeypot. The campus honeypot is specifically designed to luring in the potential hackers and the intruders in order to monitor their malicious activities and observe how they break into a computer. The production systems residing in the campus is integrated with the campus honeypot with fake operating systems and fake services running on it to engage the intruder with virtual operating systems and services.Data gathered by a honeypot is also valuable and can help the administrator.

4.1 Proposed Design

The campus honeypot for the Thapar University is proposed as a Mid Interaction Honeypot which is integrated with Snort and Sebek. The campus honeypot is installed on a separate system and attached with the production systems.

Virtual router and operating systems with dedicated fake services is being configured in campus honeypot which will prevent the production systems from the hackers and keep them busy with other fake services.
In order to keep track on the activities of intruders and do analysis, Snort and Sebek are being installed with campus honeypot. As snort is a powerful Intrusion Detection System it helps the organisation in research work while doing in depth analysis. Snort logs every activity performing on the network space associated with the campus honeypot and alert alarms according to the rules specified. On the other hand sebek keeps track on every key log of the intruder.

The proposed design for the campus honeypot which enrich it with the features of production as well as research honeypots is shown in Figure 4.1.

The Design of campus honeypot is shown in Figure 4.1. Campus honeypot is integrated with snort and sebek deployed in DMZ zone with production systems.

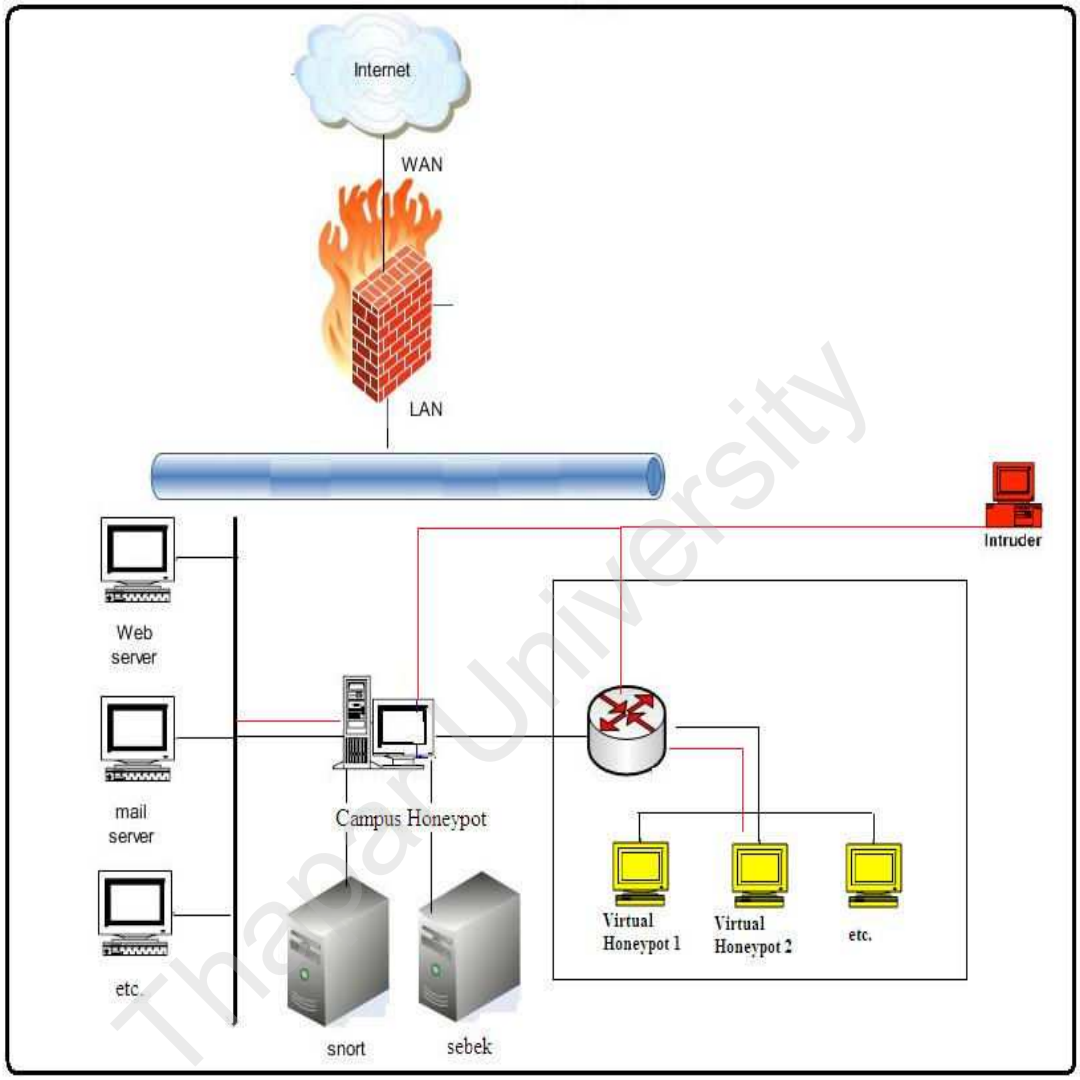


Figure 4.1: Proposed Design for Campus Honeypot.

A small daemon that creates virtual hosts on a network is configured to make a virtual router and some virtual operating systems. The campus honeypot is configured to run arbitrary services also. It can also emulate any TCP or UDP port number with open, closed, or blocked states with simple port listeners. Port applications can be mimicked by installing service scripts and proxies.anyone can ping and/or traceroute the virtual machines simulated with any type of service.

4.2 The Virtualization software

VMware Server Console is used as a Virtualization software.Virtualization is a proven software technology that is rapidly transforming the IT landscape and fundamentally changing the way that people compute. Today's powerful x86 computer hardware was designed to run a single operating system and a single application. This leaves most machines vastly underutilized. Virtualization runs multiple virtual machines on a single physical machine, sharing the resources of that single computer across multiple environments. Different virtual machines can run different operating systems and multiple applications on the same physical computer [34]. The exact specifications are as follows:

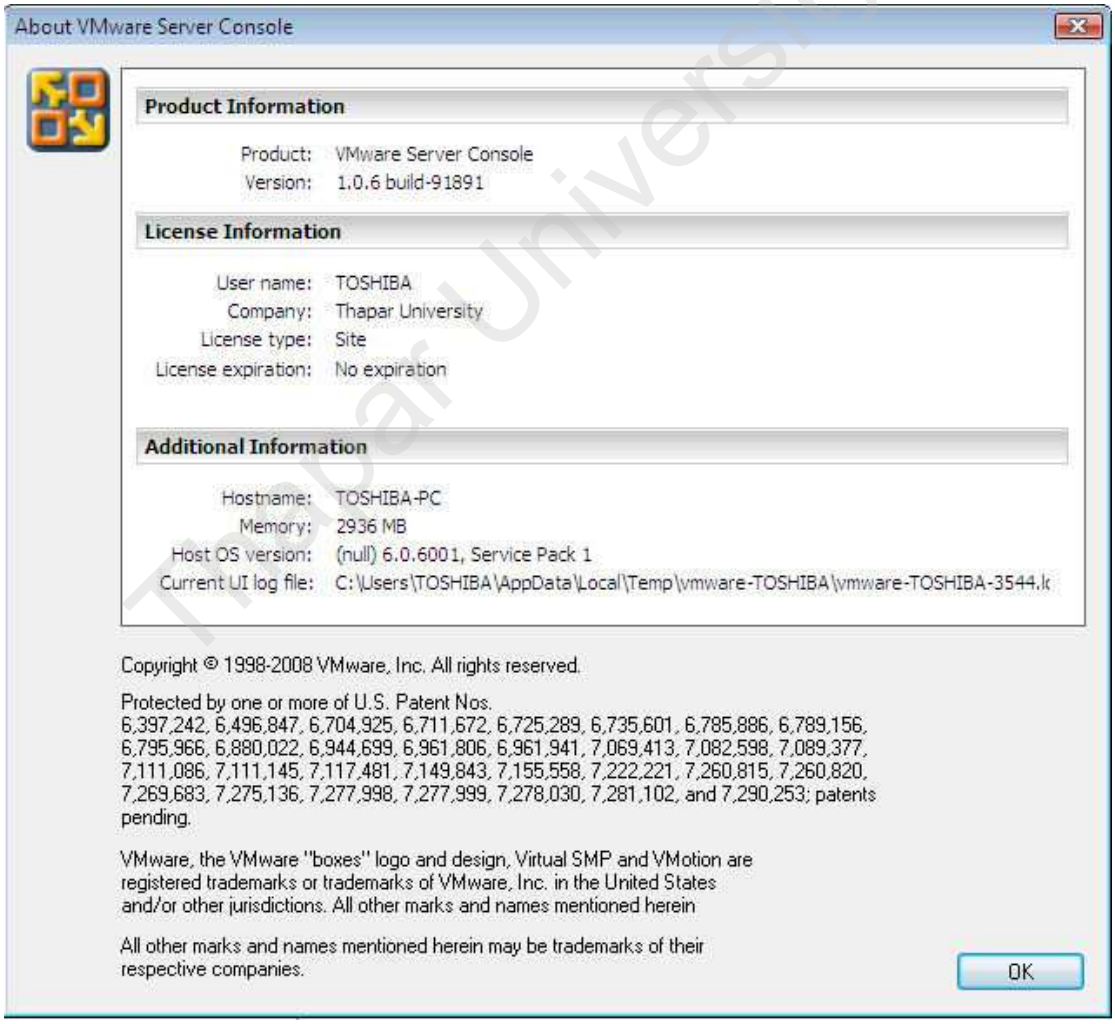


Figure 4.2 The Virtualization Software

4.3 Procedure

1. Arpd deamon uses the free address space and allocate the Mac address of the machine with each IP address.
2. Templates of different types of Operating Systems are created emulating many fake services and opening ports which make honeypot more vulnerable.
3. Bind each template with each IP address which shows the identity of every operating system assigned to different IP address.
4. Run campus honeypot alongwith snort and sebek. Rules are specified in the snort according to the administrator and log is maintained in doing depth analysis.

4.4 Implementation and Results

Tha campus honeypot is installed along with arpd-0.2, libdnet-1.11-1.2, libevent-1.4.5 and libpcap-0.9.8. A "thapar.conf" file is configured is shown in the Appendix-A which contains virtual operating systems, cisco routers etc with emulated services.

Each system is designed with the following commands.
Create command create a new system.
Add command used to add services, therefore binding scripts to a certain port.
Set command assigns personality to a created system.

Running Arpd

The fake IP addresses are created with the help of arpd demon, which further bind these IP addresses with different templates specified in "thapar.conf" configuration file. In this file The templates are created which are nothing but completely fake script modules for the different operating systems [35].

Some fake instances of different operating systems are created with fake IP addresses and then bind the templates accordingly. This assigning and binding is done as follows and shown in Figure 4.3.

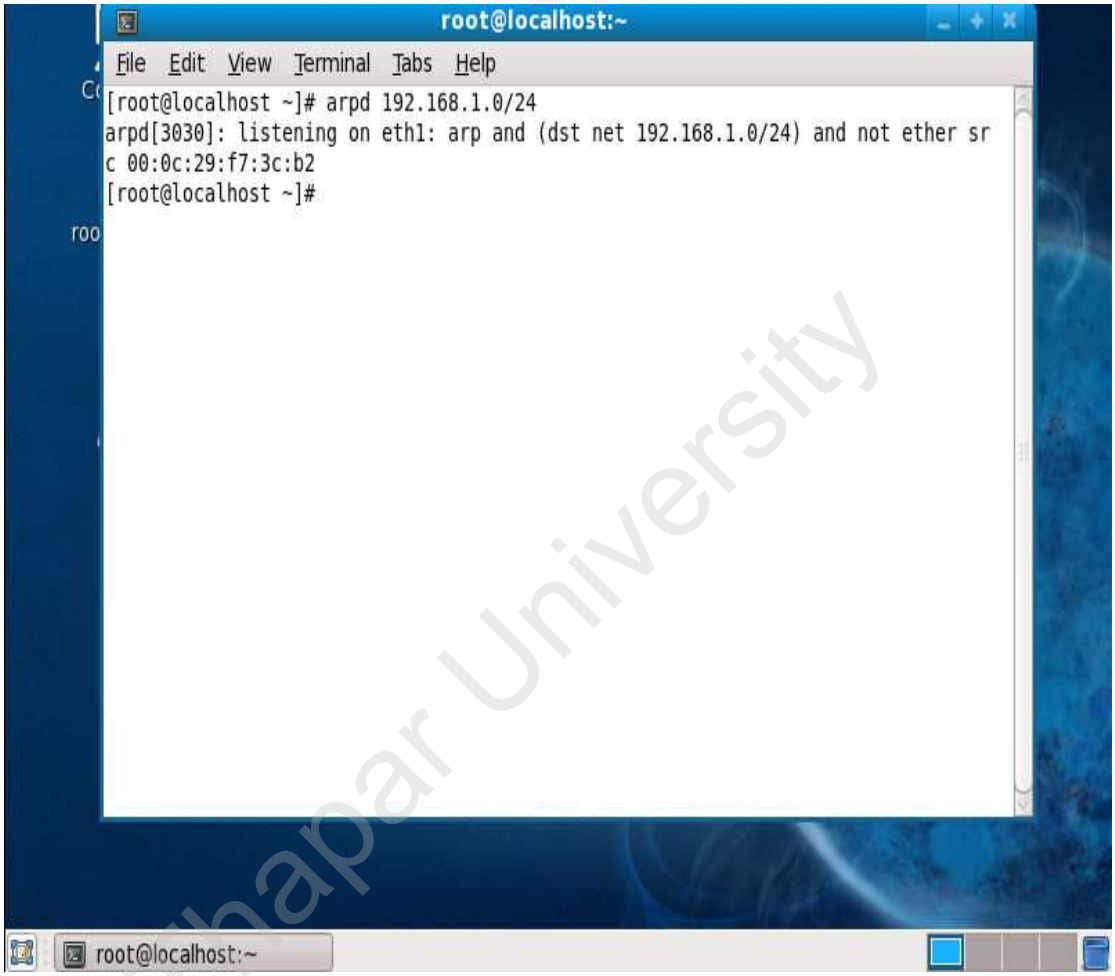


Figure 4.3 Binding IP addresses with Arpd.

This command binds the 192.168.1.0/24 IP addresses (subnet) with the MAC address of machine's network card.

Now run the campus honeypot demon with the following command:

honeyd –f thapar.config -p nmap.prints –x xprobe2.conf –a nmap.assoc -0 pf.os – l /var/log/honeyd 192.168.1.100-192.168.1.253.

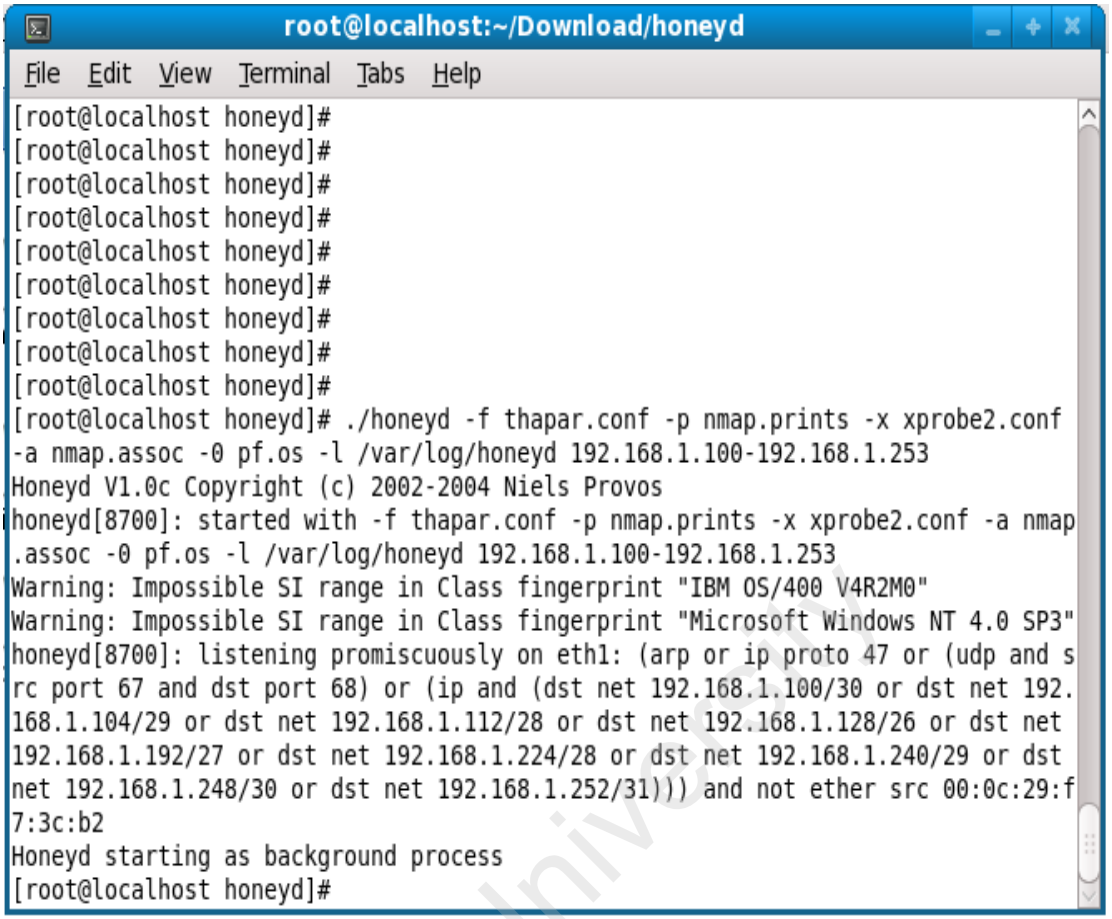


Figure 4.4 Starting Campus Honeypot with honeyd.

Running Snort

Snort

Snort is a libpcap-based packet sniffer/logger which can be used as a lightweight network intrusion detection system. Snort has three primary uses: It can be used as a straight packet sniffer like tcpdump, a packet logger or as a full blown network intrusion prevention system [36].

The initialization of snort is shown in the Figure 4.5.

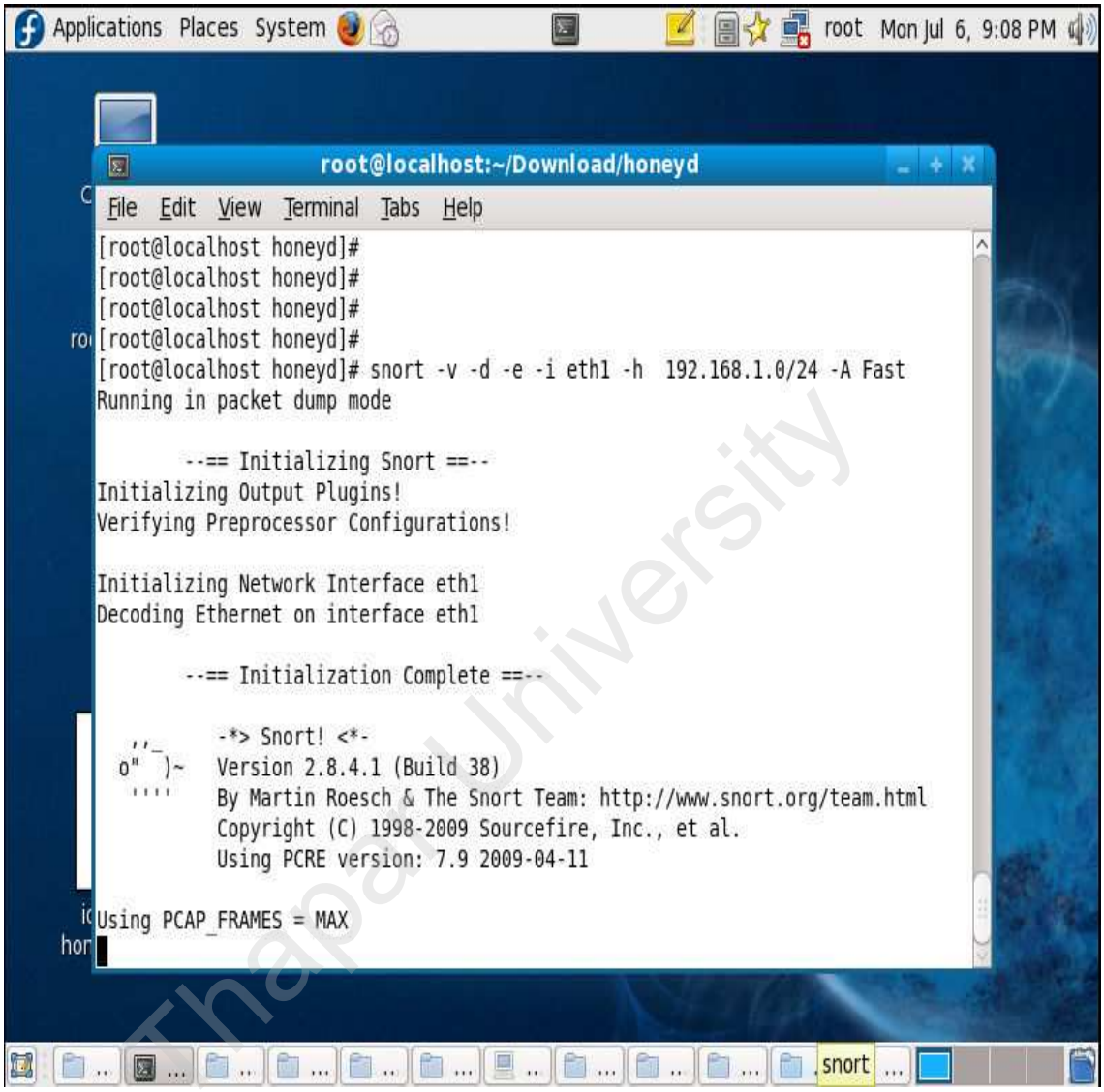


Figure 4.5 Initialization of snort.

Snort is run in Fast mode and eth1 interface is used to capture the network traffic.It capture the network traffic which is coming on the campus honeypot. Since campus honeypot is not a production so each interaction with it is considered as malicious.

The traffic captured with snort is shown in the Figure 4.6. machine 192.168.1.102 is interacting with the campus honeypot.

The log of snort is shown in Appendix B which are taken during testing attacks on the virtual honeypots. In order to test that campus honeypot is working and doing it's job, Nmap and Xprobe2 are used.

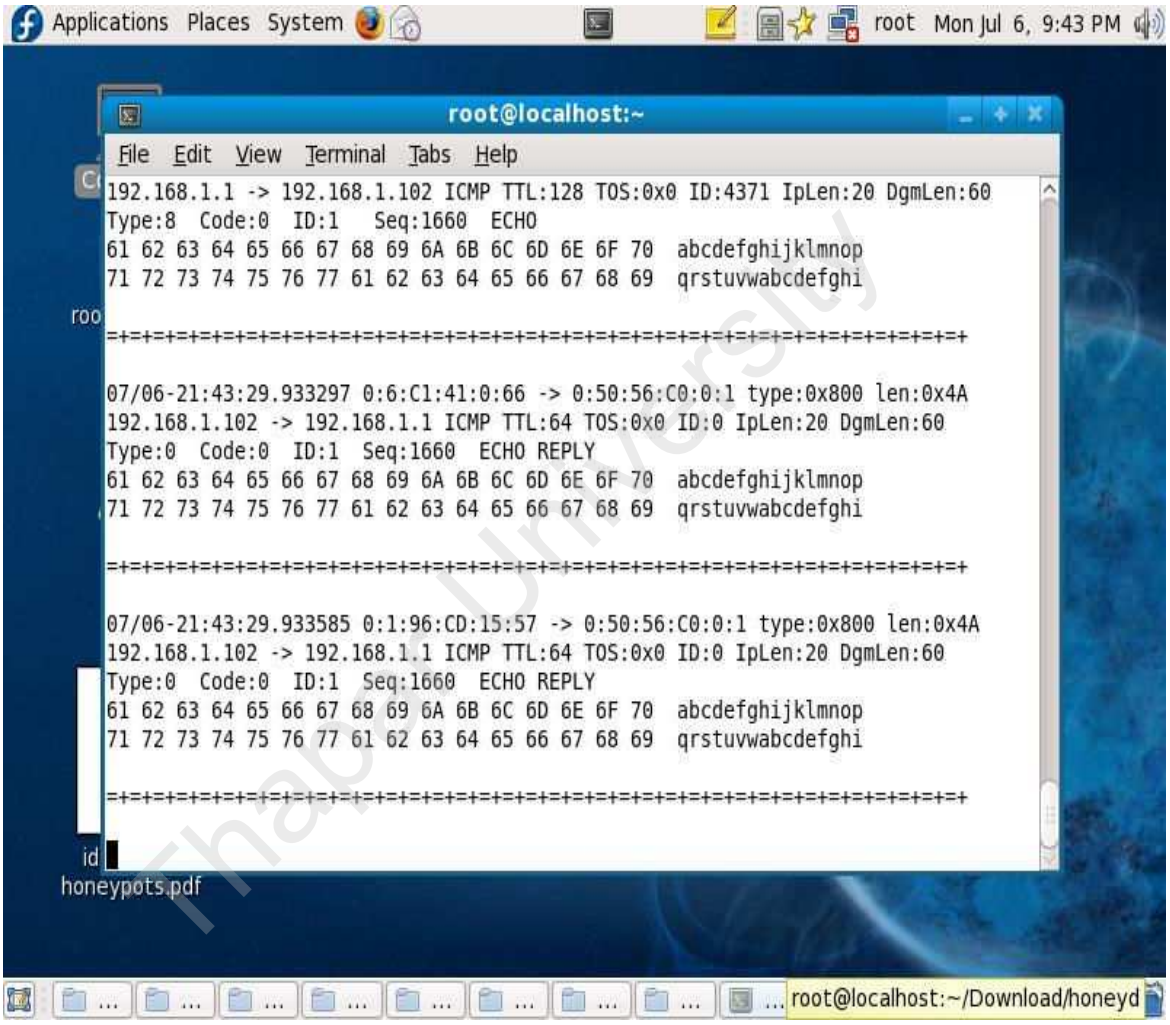


Figure 4.6 Packets captured by snort.

For the test purpose the campus honeypot is being attacked with nmap, xprobe2 and ping attack.Snort captured the test data when this machine is communicated with different tools. The Appendix-B contains the different format of traffic when communicated.

Nmap

Nmap is a network mapper tool that can be used to scan the IP addresses and for open ports. It scans for open TCP/UDP type ports. Nmap can be used to detect which operating system is on the other end by using what is called active stack fingerprinting. It also keeps a database that helps in enumerating what the OS of a remote host is. Nmap always displays this server's name, port number, state and protocol. It has three states: open, filtered and unfiltered. Open means that target machine will accept your connecting request at this port; filtered means that there has firewall, filtering advice or other network obstacles that obstruct Nmap from finding out whether port is opened or not; unfiltered only appear when most scanning port are at the state of filtered [37].

Using the following Command line: nmap -O [remote host] nmap performs the following as shown in result.

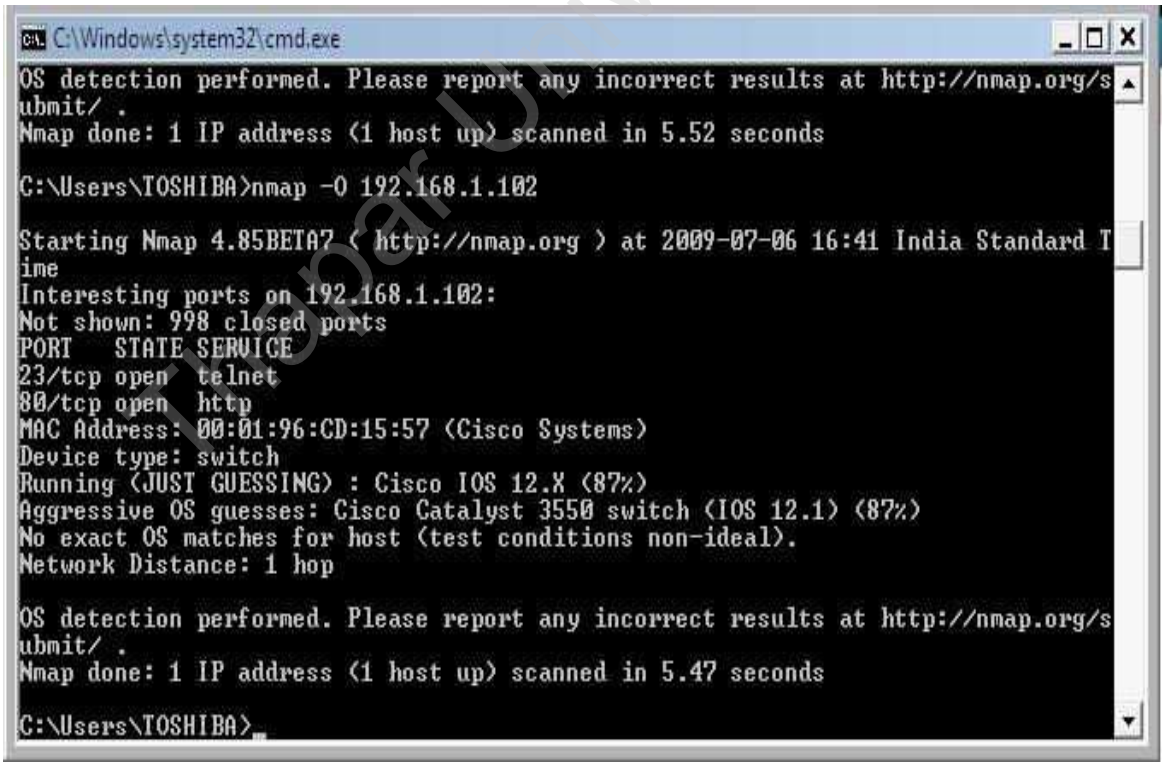


Figure 4.7 nmap attack on machine 192.168.1.102.

The following Figure 4.8 shows that the telnet is emulated on the IP address 192.168.1.102 which is binded with the template of cisco system.

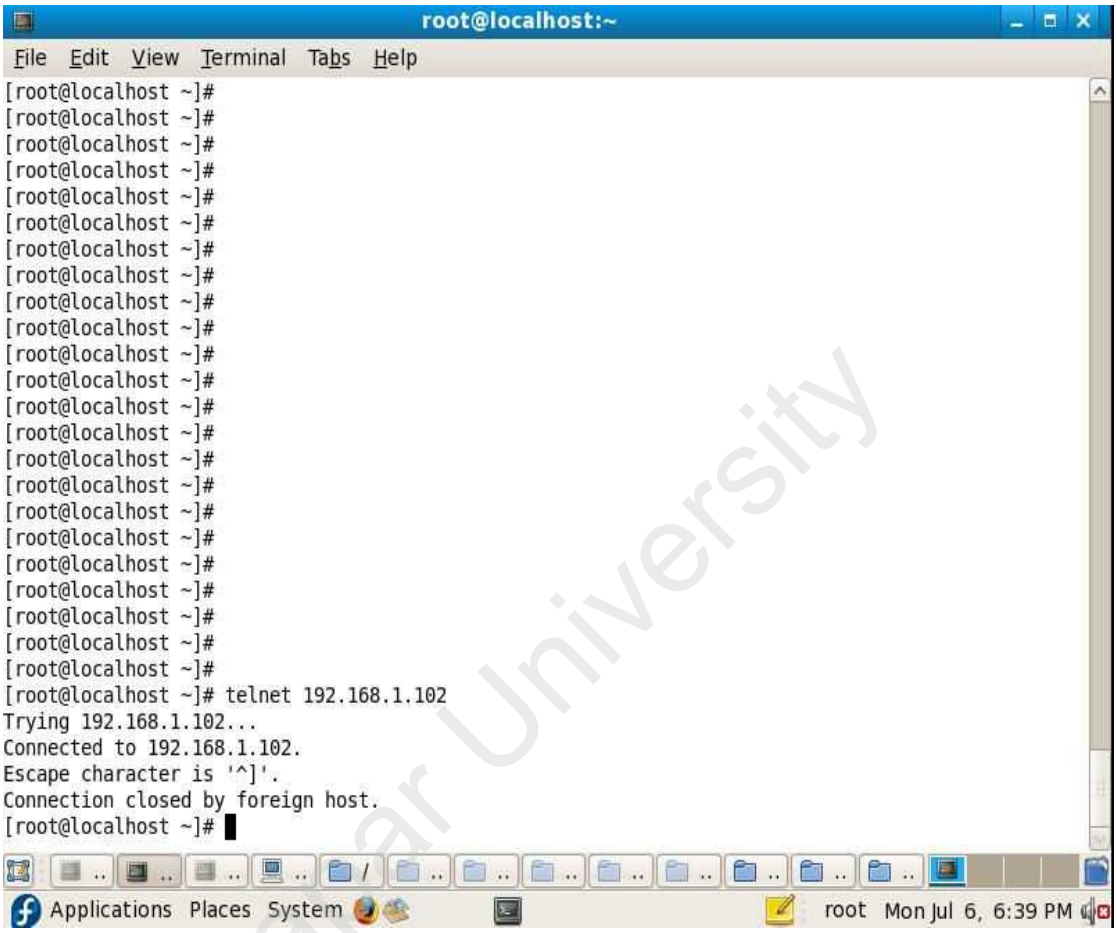


Figure 4.8 Telnet is emulated on machine 192.168.1.102.

Xprobe

Xprobe2 is an active operating system fingerprinting tool with a different approach to operating system fingerprinting. Xprobe2 rely on fuzzy signature matching, probabilistic guesses, multiple matches simultaneously, and a signature database.Xprobe2 is a remote active OS fingerprinting tool. It is designed with a different approach to OS fingerprinting. The Xprobe2 OS detection method identifies the type of the remote OS with a matrix based fingerprinting approach. This approach is also known as ‘’fuzzy’’ matching.

Unlike the other tools, Xprobe2 doesn't run a port scan against the target machine. Xprobe2 needs at least one closed UDP port to work. Xprobe2 is modular in design so it has the capability to accept new modules, or other fingerprinting tests [38]. Another idea to note is that Xprobe2 comes with an API so that users can write their own modules.

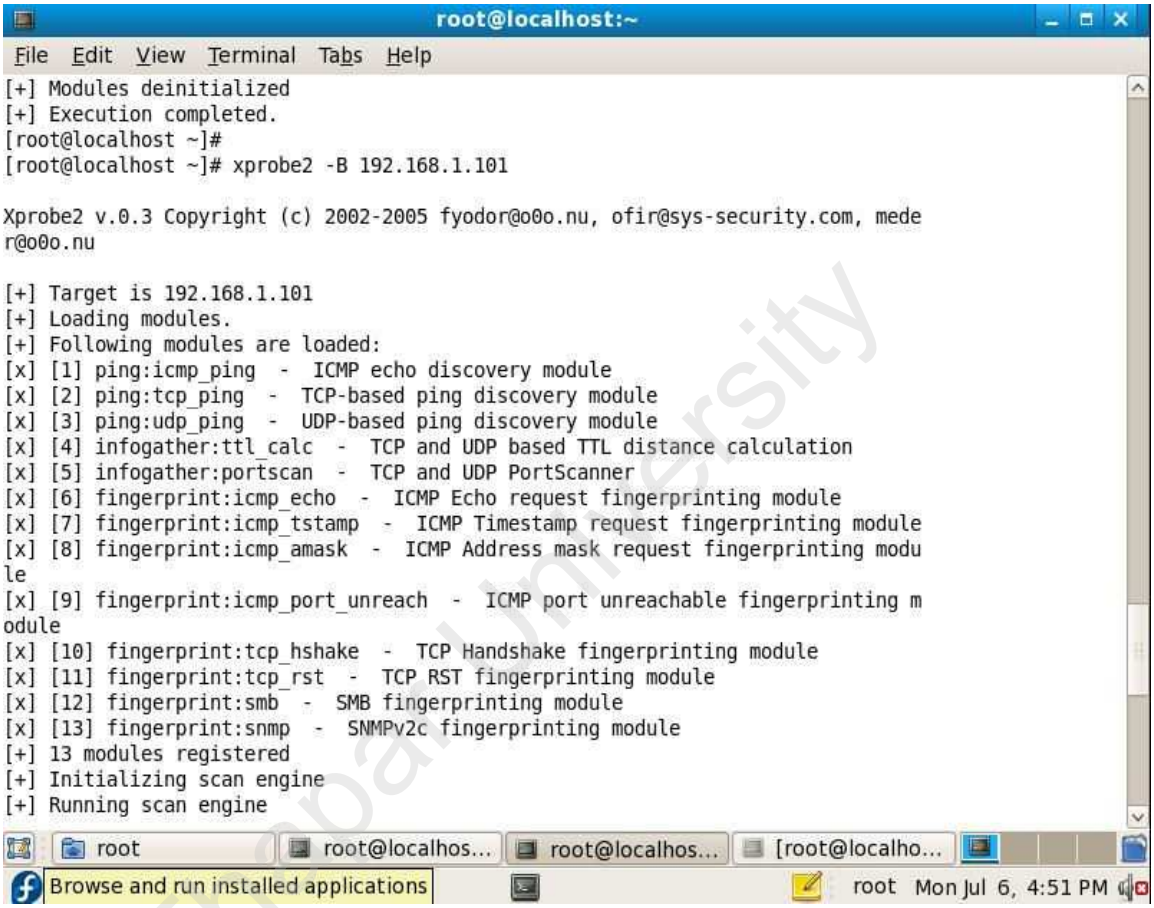


Figure 4.9 xprobe2 attack on machine 192.168.1.101.

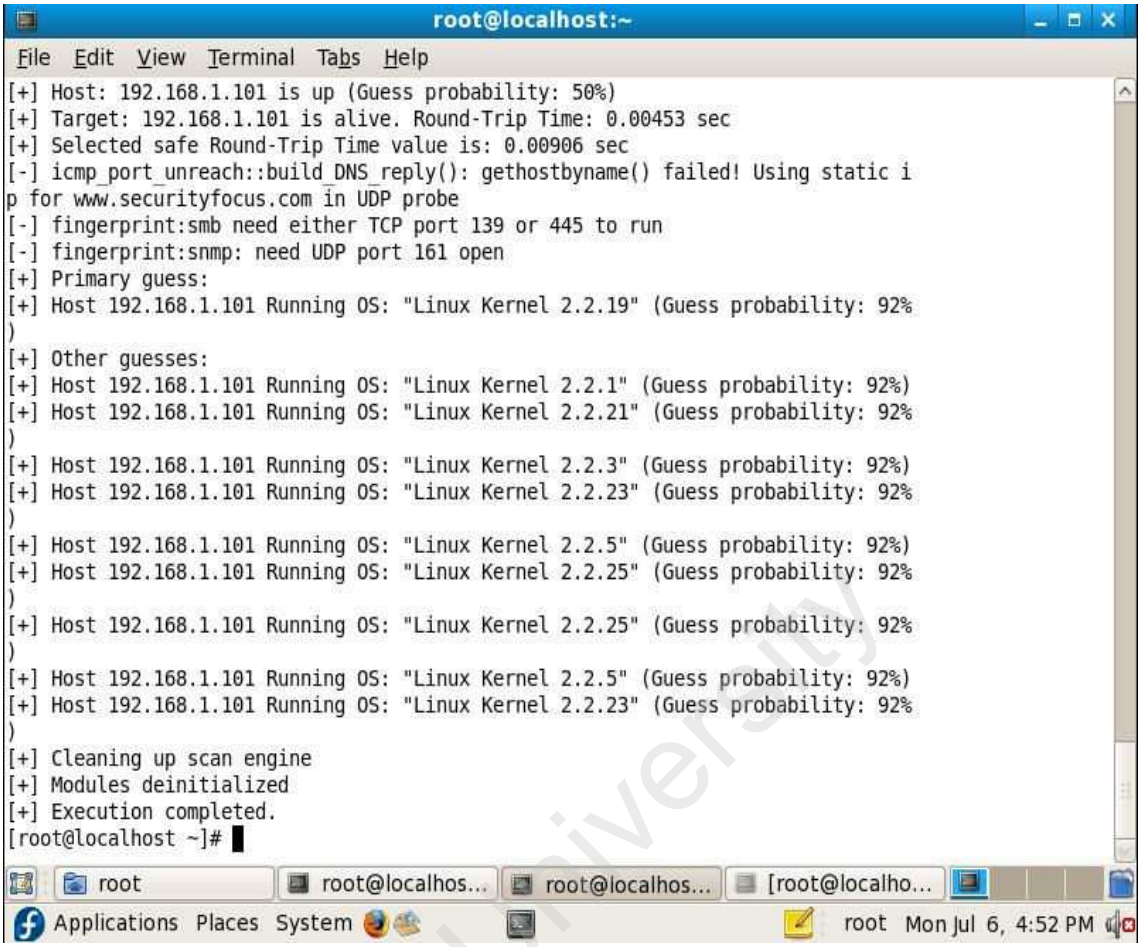


Figure 4.10 Result of Xprobe2 showing running virtual operating system.

The result shows that the nmap and xprobe2 identify the operating systems which are virtually created by the campus honeypot.

The above result shows that campus honeypot has created virtual honeypots successfully with emulated services such as telnet. These fake operating systems are also communicated with intruder who attacked on the same with different tools.

Chapter 5

Conclusions and Future Scope

Honeypots can be valuable resources, especially in the fight against intruders and the tools they are using to break into your computer. Honeypots are rapidly gaining a place in defense strategies, while they maintain an important status in the security research community. This helps companies and organizations learn how hackers get into their systems so they can prevent such occurrences in the future.

A honeypots are just a tool. There are a variety of honeypot options, each having different value to organizations. Production honeypots help reduce risk in an organization. While they do little for prevention, they can greatly contribute to detection or reaction. Research honeypots are different in that they are not used to protect a specific organization. Instead they are used as a research tool to study and identify the threats in the Internet community. Level of interaction should be kept in the mind to learn more from it. The Mid Interation honeypot deployed with snort and sebek shows the result of both Production and Research honeypot which helps to prevent the organisation from the intruders and have a track on the every malicious activity performing on the honeypot host. The best relationship of risk to capabilities that exist can be determined.

Monitoring the honeypot not only includes proactive monitoring, such as checking all log files, checking active connections, and looking at active processes for things out of the ordinary, but it also involves reactive measures. These must be outside of the attackers' visibility to ensure that they work. Giving notice to the administrator in a timely fashion is imperative because actions must be taken quickly in the case of an incident.

Honeypots are an extremely powerful tool that allows learning about the black-hat community. Honeypot also provide an inside window on how the black-hat community works. There are a variety of different approaches to building and implementing a honeypot by comparing different layers of information, it is easy to gain a better understanding of what the black-hat are doing.

The proposed design of campus honeypot is mid interaction honetpot which can be upgraded into high interaction honeypot. This honeypot will have more interaction with intruders to deep analysis of attacks and will help Unified Threat Management.

References

[1] Gassman, B.,"Internet security, and firewalls protection on the internet",Somerset, NJ, USA, ELECTRO '96. Professional Program Proceedings, 30 April-2 May 1996.

[2] Sarah Diesburg, "Monitoring Network Sludge: Using Intrusion Detection to Monitor Network Traffic", University of Northern Iowa, November 2004.

[3] Jonathan Bingham,"Intruders the biggest threat to network security", Network World , February 2005.

[4] Lindsey Manes, Abby Pais-Bernath, Jennifer Fisher,Michele Hoyt, Daniel Dugan, "ANALYSIS OF HONEYPOT TECHNOLOGIES" ,April 14, 2006.

[5] Lance Spitzner, "Definitions and Value of Honeypots ", http://www.enteract.com/~lspitz, Last Modified: 17 May, 2002.

[6] Marcel Frigault,Lingyu Wang, "Measuring Network Security Using Bayesian Network-Based Attack Graphs", IEEE Computer Socity 2008.

[7] Mark King, "Security Lifecycle - Managing the Threat", http://www.securitydocs.com, March 2004.

[8] Whitepaper, "Social Engineering – Are You at Risk?",DAS Information Security Office, May 2008.

[9] Whitepaper, "Internet Technical Solution, Network Security",Cisco Systems, 2001.

[10] Gary Miliefsky, "A guide to proactive network security",ZDNet News,November 2004.

[11] S. M. Shahriar Nirjon, "The Emerging System and Network Security",, Bangladesh University of Engineering and Technology May 2009.

[12] Whitepaper, "Host-Based IDS vs Network-Based IDS", http://www.windowsecurity.com/articles/Hids_vs_Nids_Part1.html,July 10, 2003.

[13] Paul Innella,Oba McMillan,"An Introduction to Intrusion Detection Systems",Tetrad Digital Integrity December 2001.

[14] Ricky M. Magalhaes,"Host-Based IDS vs Network-Based IDS (Part 2 – Comparative Analysis)",Jul 2004.

[15] Ricky M. Magalhaes, "Host-Based IDS vs Network-Based IDS (Part 1)",August 2006.

[16] Rafeeq Ur Rehman,"Intrusion Detection Systems with Snort", New Jersey,2003.

[17] Whitepaper, "Host and Network Intrusion Prevention",McAfee Network Protection Solutions, February 2005.

[18] Timothy R. Jackson, John G. Levine, Julian B. Grizzard, Henry L. Owen, "An Investigation of a Compromised Host on a Honeynet Being Used to Increase the Security of a Large Enterprise Network", Proceedings of the 2004 IEEE Workshop on Information Assurance and Security T1B2 1555 United States Military Academy, West Point, NY, 10-11 June 2004.

[19] Paul Innella and Oba McMillan" An Introduction to Intrusion Detection Systems", Tetrad Digital Integrity, LLClast updated December 6, 2001.

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

[21] Lance Spitzner "'Know Your Enemy': Everything you need to know about honeypots" September 27, 2004.

[22] Whitepaper, "Types of attackers", http://www.mattgiannetto.com/drexel/web2/final/attackers.html.

[23] Mark King,"Security Lifecycle – Managing the Threat", GSEC Practical v1.3,January 14, 2002.

[24] Lance Spitzner, "Honeypots: Catching the Insider Threat",19th Annual Computer Security Applications Conference (ACSAC '03), 2003.

[25] Lance Spitzner,Marty Roesch ,"The Value of Honeypots, Part Two: Honeypot Solutions and Legal Issues ", October 23, 2001.

[26] Reto Baumann"Honeypots",Christian Plattner, http://www.christianplattner.net,March 2002.

[27] Nathalie Weiler, "Honeypots for Distributed Denial of Service Attacks,",Eleventh IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE'02), 2002.

[28] Dr. A.K. Aggarwal,Sunil Gurung, "KFSensor Vs Honeyd Honeypot System",Thursday, November 25, 2004.

[29] Nirbhay Gupta, "Is Honeyd Effective or Not?",Edith Cowan University, Western Australia, November 2003.

[30] Lang Navorigin, “Know Your Enemy: Intrusion Detection Honeypots,Sebek”, The Honeynet Project, 12/10/2004.

[31] Fabien Pouget, Marc Dacier,"Honeypot, Honeynet: A comparative survey",Institut Eurécom Corporate Communications ,France,September 14, 2003.

[32] Gordon W. Romney, Jeremiah K. Jones, Brandon L. Rogers and Philip MacCabe, "IT Security Education is Enhanced by Analyzing Honeynet Data", ITHET 6th Annual International Conference, July 2005.

[33] Whitepaper, “The Use of Honeynets to Detect Exploited Systems Across Large Enterprise Networks”, June, 2003.

[34] Christian Plattner, ” Honeypots Reto Baumann, http://www.rbaumann.net” Whitepaper, http://www.christianplattner.net March 2002.

[35] Laurent Oudot, Thorsten Holz, "Defeating Honeypots : Network issues, Part 1",September 2004.

[36] Trevor Warren ,"Intrusion Detection System Part 3: Snort", http://www.freeos.com/articles/3496/ ,2001.

[37] Fyodor, "Nmap: Scanning the Internet", Black Hat Briefings USA August 6, 2008.

[38] Ofir Arkin,Fyodor Yarochkin,"The Present and Future of Xprobe2 The Next Generation of Active Operating System Fingerprinting",Meder, July 2003.

Appendix A

thapar.conf

```
#########################################################################
########This template is binded with 192.168.1.101 ######################
#########################################################################
create linux
set linux personality "Linux 2.4.16 - 2.4.18"
set linux default tcp action reset
set linux default udp action reset
add linux tcp port 110 "sh scripts/pop/emulate-pop3.sh"
#set linux subsystem "/usr/sbin/httpd"
add linux tcp port 21 "sh scripts/ftp.sh"
set linux uptime 3285460
bind 192.168.1.101 linux
#########################################################################
```

```
#############################################################################
#########This template is binded with 192.168.1.101 ########################

#############################################################################

create router

set router personality "Cisco IOS 11.3 - 12.0(11)"

set router default tcp action reset

set router default udp action reset

add router tcp port 23 "/usr/bin/perl scripts/router-telnet.pl"

set router uid 32767 gid 32767

set router uptime 1327450

bind 192.168.1.102 router

#############################################################################
```

Appendix B

Traffic captured by the campus honeypot while attacked with nmap.

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
07/06-21:16:40.470506 0:50:56:C0:0:1 -> 0:6:C1:41:0:66 type:0x800 len:0x3C
192.168.1.1:38679 -> 192.168.1.102:25 TCP TTL:51 TOS:0x0 ID:51853 IpLen:20 DgmLen:44
******S* Seq: 0xAF443C39  Ack: 0x0  Win: 0x1000  TcpLen: 24
TCP Options (1) => MSS: 1460
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
07/06-21:16:40.470520 0:50:56:C0:0:1 -> 0:6:C1:41:0:66 type:0x800 len:0x3C
192.168.1.1:38679 -> 192.168.1.102:587 TCP TTL:37 TOS:0x0 ID:49483 IpLen:20 DgmLen:44
******S* Seq: 0xAF443C39  Ack: 0x0  Win: 0x800  TcpLen: 24
TCP Options (1) => MSS: 1460
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
07/06-21:16:40.470533 0:50:56:C0:0:1 -> 0:6:C1:41:0:66 type:0x800 len:0x3C
192.168.1.1:38679 -> 192.168.1.102:3389 TCP TTL:48 TOS:0x0 ID:46105 IpLen:20 DgmLen:44
******S* Seq: 0xAF443C39  Ack: 0x0  Win: 0x400  TcpLen: 24
TCP Options (1) => MSS: 1460
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
07/06-21:16:40.470548 0:50:56:C0:0:1 -> 0:6:C1:41:0:66 type:0x800 len:0x3C
192.168.1.1:38679 -> 192.168.1.102:1723 TCP TTL:53 TOS:0x0 ID:29457 IpLen:20 DgmLen:44
******S* Seq: 0xAF443C39  Ack: 0x0  Win: 0x800  TcpLen: 24
TCP Options (1) => MSS: 1460
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
07/06-21:16:40.473676 0:6:C1:41:0:66 -> 0:50:56:C0:0:1 type:0x800 len:0x3A
192.168.1.102:80 -> 192.168.1.1:38679 TCP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:44
***A**S* Seq: 0x47D0878  Ack: 0xAF443C3A  Win: 0x1020  TcpLen: 24
TCP Options (1) => MSS: 1460
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
07/06-21:16:40.473885 0:50:56:C0:0:1 -> 0:1:96:CD:15:57 type:0x800 len:0x3C
92.168.1.1:38679 -> 192.168.1.102:80 TCP TTL:128 TOS:0x0 ID:4156 IpLen:20 DgmLen:40 DF
*****R** Seq: 0xAF443C3A  Ack: 0xAF443C3A  Win: 0x0  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
07/06-21:16:40.474053 0:6:C1:41:0:66 -> 0:50:56:C0:0:1 type:0x800 len:0x36
192.168.1.102:25 -> 192.168.1.1:38679 TCP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:40
***A*R** Seq: 0x3D4808C4  Ack: 0xAF443C3A  Win: 0x0  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
07/06-21:16:40.474384 0:6:C1:41:0:66 -> 0:50:56:C0:0:1 type:0x800 len:0x36
192.168.1.102:587 -> 192.168.1.1:38679 TCP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:40
***A*R** Seq: 0xC7D5DB07  Ack: 0xAF443C3A  Win: 0x0  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
07/06-21:16:40.474668 0:6:C1:41:0:66 -> 0:50:56:C0:0:1 type:0x800 len:0x36
192.168.1.102:3389 -> 192.168.1.1:38679 TCP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:40
***A*R** Seq: 0xA1210540  Ack: 0xAF443C3A  Win: 0x0  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
```

Traffic captured by the campus honeypot while attacked with ping flood.

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
07/06-21:15:22.967399 0:1:96:CD:15:57 -> 0:C:29:58:D2:6E type:0x800 len:0x62
```

```
92.168.1.102 -> 192.168.1.5 ICMP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:84
Type:0  Code:0  ID:23823  Seq:1  ECHO REPLY
FC FA 51 4A 16 BE 09 00 08 09 0A 0B 0C 0D 0E 0F  ..QJ............
10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F  ................
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F   !"#$%&'()*+,-./
30 31 32 33 34 35 36 37                          01234567
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
07/06-21:15:22.968058 0:6:C1:41:0:66 -> 0:C:29:58:D2:6E type:0x800 len:0x62
192.168.1.102 -> 192.168.1.5 ICMP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:84
Type:0  Code:0  ID:23823  Seq:1  ECHO REPLY
FC FA 51 4A 16 BE 09 00 08 09 0A 0B 0C 0D 0E 0F  ..QJ............
10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F  ................
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F   !"#$%&'()*+,-./
30 31 32 33 34 35 36 37                          01234567
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
07/06-21:15:23.966744 0:C:29:58:D2:6E -> 0:6:C1:41:0:66 type:0x800 len:0x62
192.168.1.5 -> 192.168.1.102 ICMP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:84 DF
Type:8  Code:0  ID:23823   Seq:2  ECHO
FD FA 51 4A BB BE 09 00 08 09 0A 0B 0C 0D 0E 0F  ..QJ............
10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F  ................
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F   !"#$%&'()*+,-./
30 31 32 33 34 35 36 37                          01234567
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
07/06-21:15:23.967170 0:1:96:CD:15:57 -> 0:C:29:58:D2:6E type:0x800 len:0x62
192.168.1.102 -> 192.168.1.5 ICMP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:84
Type:0  Code:0  ID:23823  Seq:2  ECHO REPLY
FD FA 51 4A BB BE 09 00 08 09 0A 0B 0C 0D 0E 0F  ..QJ............
10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F  ................
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F   !"#$%&'()*+,-./
30 31 32 33 34 35 36 37                          01234567
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
07/06-21:15:23.967527 0:6:C1:41:0:66 -> 0:C:29:58:D2:6E type:0x800 len:0x62
192.168.1.102 -> 192.168.1.5 ICMP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:84
Type:0  Code:0  ID:23823  Seq:2  ECHO REPLY
FD FA 51 4A BB BE 09 00 08 09 0A 0B 0C 0D 0E 0F  ..QJ............
10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F  ................
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F   !"#$%&'()*+,-./
30 31 32 33 34 35 36 37                          01234567
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
07/06-21:15:24.966756 0:C:29:58:D2:6E -> 0:6:C1:41:0:66 type:0x800 len:0x62
192.168.1.5 -> 192.168.1.102 ICMP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:84 DF
Type:8  Code:0  ID:23823   Seq:3  ECHO
FE FA 51 4A 75 BE 09 00 08 09 0A 0B 0C 0D 0E 0F  ..QJu...........
10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F  ................
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F   !"#$%&'()*+,-./
30 31 32 33 34 35 36 37                          01234567
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
```

Traffic captured by the campus honeypot while attacked with xprobe2.

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
07/06-21:17:14.687571 0:6:C1:41:0:66 -> 0:C:29:58:D2:6E type:0x800 len:0x62
192.168.1.102 -> 192.168.1.5 ICMP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:84
Type:0  Code:0  ID:2651  Seq:0  ECHO REPLY
4A 51 FB 6C 00 05 27 C3 08 09 0A 0B 0C 0D 0E 0F  JQ.l..'.........
10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F  ................
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F   !"#$%&'()*+,-./
```

```
30 31 32 33 34 35 36 37                     01234567
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
07/06-21:17:14.688139 0:1:96:CD:15:57 -> 0:C:29:58:D2:6E type:0x800 len:0x62
192.168.1.102 -> 192.168.1.5 ICMP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:84
Type:0  Code:0  ID:2651  Seq:0  ECHO REPLY
4A 51 FB 6C 00 05 27 C3 08 09 0A 0B 0C 0D 0E 0F  JQ.l..'.........
10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F  ................
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F   !"#$%&'()*+,-./
30 31 32 33 34 35 36 37                     01234567
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
07/06-21:17:14.701742 0:C:29:58:D2:6E -> 0:6:C1:41:0:66 type:0x800 len:0x62
192.168.1.5 -> 192.168.1.102 ICMP TTL:64 TOS:0x6 ID:239 IpLen:20 DgmLen:84 DF
Type:8  Code:123  ID:2651   Seq:1  ECHO
4A 51 FB 6C 00 05 64 76 08 09 0A 0B 0C 0D 0E 0F  JQ.l..dv........
10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F  ................
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F   !"#$%&'()*+,-./
30 31 32 33 34 35 36 37                     01234567
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
07/06-21:17:14.702131 0:6:C1:41:0:66 -> 0:C:29:58:D2:6E type:0x800 len:0x62
192.168.1.102 -> 192.168.1.5 ICMP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:84
Type:0  Code:0  ID:2651  Seq:1  ECHO REPLY
4A 51 FB 6C 00 05 64 76 08 09 0A 0B 0C 0D 0E 0F  JQ.l..dv........
10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F  ................
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F   !"#$%&'()*+,-./
30 31 32 33 34 35 36 37                     01234567
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
07/06-21:17:14.702484 0:1:96:CD:15:57 -> 0:C:29:58:D2:6E type:0x800 len:0x62
192.168.1.102 -> 192.168.1.5 ICMP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:84
Type:0  Code:0  ID:2651  Seq:1  ECHO REPLY
4A 51 FB 6C 00 05 64 76 08 09 0A 0B 0C 0D 0E 0F  JQ.l..dv........
10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F  ................
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F   !"#$%&'()*+,-./
30 31 32 33 34 35 36 37                     01234567
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
07/06-21:17:14.742169 0:C:29:58:D2:6E -> 0:6:C1:41:0:66 type:0x800 len:0x3C
192.168.1.5 -> 192.168.1.102 ICMP TTL:64 TOS:0x0 ID:2651 IpLen:20 DgmLen:40
Type:13  Code:0  ID: 2651  Seq: 0  TIMESTAMP REQUEST
0A 5B 00 00 00 05 FF ED 00 00 00 00 00 00 00 00  .[..............
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
07/06-21:17:15.354935 0:C:29:58:D2:6E -> 0:6:C1:41:0:66 type:0x800 len:0x3C
192.168.1.5 -> 192.168.1.102 ICMP TTL:64 TOS:0x0 ID:27746 IpLen:20 DgmLen:32
Type:17  Code:0  ID: 27746  Seq: 0  ADDRESS REQUEST
6C 62 00 00 00 00 00 00                     lb......
+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
07/06-21:17:16.354350 0:C:29:58:D2:6E -> 0:6:C1:41:0:66 type:0x800 len:0x76
192.168.1.5:53 -> 192.168.1.102:65534 UDP TTL:255 TOS:0x0 ID:1 IpLen:20 DgmLen:104 DF
Len: 76
```

Papers Communicated

Kiran Deep Singh, Dr. Maninder Singh, "Design and Develop a Campus Honeypot to Detect Intrusions" communicated in 3rd IEEE International Symposium on Advanced Networks and Telecommunication Systems, IEEE ANTS 2009 in India, New Delhi from 14-16 December 2009(**Communicated**).