
Technical report, IDE1014, May 2010

Develop a Secure Network – A Case Study

Master's Thesis in Computer Network Engineering

Habeeb Rayapati



School of Information Science, Computer and Electrical Engineering
Halmstad University

Develop a Secure Network – A Case Study

Master Thesis in Computer Network Engineering

School of Information Science, Computer and Electrical Engineering
Halmstad University
Box 823, S-301 18 Halmstad, Sweden

May 2010

Preface

First and foremost, I would like to express my gratitude and heartiest thanks to my supervisors Olga Torstensson and Yan Wang for their suggestions, guidance and constant support even in the toughest moments of my master thesis.

I would like to dedicate this thesis work to my parents and siblings in hometown who always motivate and inspire in my hardest times being away from home. I am also thankful to Sweden which gave me an opportunity to make my dream come true. Finally I would like to say thanks to all my friends for their support and belief in my ability to do the work and write this thesis.

Habeeb Rayapati

Halmstad University, April 2010

Abstract

In recent years, so many networks are being built and some of the organizations are able to provide security to their networks. The performance of a network depends on the amount of security implemented on the network without compromising the network capabilities. For building a secure network, administrators should know all the possible attacks and their mitigation techniques and should perform risk analysis to find the risks involved in designing the network. And they must also know how to design security policies for implement the network and to educate the employees, to protect the organization's information. The goal behind this case-study is to build a campus network which can sustain from reconnaissance attacks.

This thesis describes all the network attacks and explores their mitigation techniques. This will help an administrator to be prepared for the coming attacks. This thesis explains how to perform risk analysis and the two different ways to perform risk analysis. It also describes the importance of security policies and how security policies are designed in real world.

Contents

Preface	1
Abstract	2
1 Introduction	5
1.1 Goal	5
1.2 Methodology	5
1.3 Back ground	6
1.4 Structure of the thesis	6
2 Attacks and Attacks Mitigation.....	7
2.1 Reconnaissance attacks	7
2.1.1 Packet Sniffers	8
2.1.2 Port Scans and Ping Sweeps	9
2.1.3 Internet Information Queries.....	10
2.2 Access Attacks	11
2.2.1 Password attacks	11
2.2.2 Trust Exploitation	12
2.2.3 Port redirection	12
2.2.4 Man-in-the-middle attacks	12
2.2.5 Buffer overflow.....	13
2.3 DoS and Distributed DoS Attacks.....	13
2.4 Viruses, Worms and Trojan horse Attacks.....	14
2.5 Application Layer Attacks.....	15
2.6 Threats to management protocols.....	16
2.6.1 SNMP Protocol.....	16
2.6.2 SysLog Protocol.....	17
2.6.3 TFTP Protocol.....	17
2.6.4 NTP protocol.....	17
3 Risk Analysis.....	19
3.1 Identification of assets.....	19
3.2 Identification of threats	20
3.3 Identification of vulnerability.....	20
3.4 Identification of existing controls.....	22
3.5 Types of risk analysis	22

3.5.1 Qualitative risk analysis	22
3.5.2 Quantitative risk analysis	23
4 Security policy	24
4.1 Importance of a security policy	24
4.2 Roles of a security policy	25
4.3 Security services and mechanisms	26
4.3.1 Security services	27
4.3.2 Security mechanisms	28
4.4 Examples of security policies	29
4.4.1 Network access policy	30
4.4.2 Password policy	30
5 Implementation and Results	32
5.1 Implementation overview	32
5.2 Network design	32
5.3 Design description	33
5.4 Mitigation of Packet Sniffing	34
5.4.1 Results	34
5.5 Mitigation of Ping Sweeps	36
5.5.1 Results	37
5.6 Mitigation of Port Scans	38
5.6.1 Results	38
5.7 Mitigation of Internet Information Queries	39
5.7.1 Result	39
6 Conclusion	41
7 References	43
8 Appendix	45

1 Introduction

For any organization, having a secure network is the primary thing to reach their business requirements. A network is said to be secure when it can sustain from attacks, which may damage the whole network. Over the last few decades, internetworking has grown tremendously and lot of importance is given to secure the network. To develop a secure network, network administrators must have a good understanding of all attacks that are caused by an intruder and their mitigation techniques. Choosing a particular mitigation technique for an attack has an impact on the overall performance of the network, because each attack has different ways for mitigation. By performing risk analysis, network administrators will identify the assets that need to be protected, threats and vulnerabilities that the network may posse. With the help of risk analysis administrators will have sufficient information about all risks which helps to build a network with high security. After risk analysis, designing a set of security policies is very important to provide high level of security. Security policies provide information for network users for using and auditing the network.

1.1 Goal

Goal of this thesis is to evaluate the network attacks and build a secure network which can protract against reconnaissance attacks. To performing risk analysis to identify assets, threats, vulnerabilities and existing controls. Another goal is to know the importance of security policies and to know how security policies are designed based upon security services and security mechanisms.

1.2 Methodology

For building a secure network, every organization should follow a method which includes finding all the network attacks, performing risk analysis, designing security policies. Then the network is build based upon the policies and it is monitored on a regular intervals. This thesis follows the same method for building and securing a campus network. Network attacks are of different types and are executed at different stages. All the attacks are executed with the help of reconnaissance attacks, so it is the first and the most important thing to mitigate. This case study focuses on the importance of risk analysis, how risk analysis is performed and the different ways to perform risk analysis. It also focuses on importance of security policies, roles of security policies and how security policies are designed with the help of security services and security mechanisms. A campus network is built and scanned for reconnaissance attacks without proving security. The same network is scanned after implementing security. Results from both the scans are analyzed and compared to show the mitigation of reconnaissance.

1.3 Back ground

According to our knowledge, there are many projects on network attacks, risk analysis and security policies individually. This thesis gives an overall idea on these topics to build a secure network. Network attacks are defined as operations to destroy or disrupt information and assets of computer networks. All the attacks can be mitigated, but cannot be eliminate completely. It is not possible to eliminate all the attacks completely without compromising network features. This thesis provides a way to mitigate reconnaissance attacks. A campus network is designed by using Cisco switches and routers. Cisco Security Device Manager (SDM) is used to configure IPSec VPN and Firewalls. SDM is one of the applications used in this thesis. SDM is web-based device-management tool which is used for Cisco routers to improve productivity of the network and helps to troubleshoot complex network issues [1]. Wireshark is used to capture the packets. Wireshark is a windows scanning tool for capturing the packets. Another application used in this thesis is Nmap. Nmap is an open source utility for network exploration or security auditing [2]. Nmap is a network scanning tool which is used to monitor the network for finding the security breaches.

1.4 Structure of the thesis

Chapter 2 explains all the attacks briefly which are good to know for building a secure network. Reconnaissance attacks and their mitigation techniques are explained in detailed by describing the operation of the attack. Reconnaissance attacks are information gathering attacks which are performed by every intruder for successfully execute an attack in the network.

Chapter 3 describes about risk analysis, which is useful to estimate the amount of risk involved in the network. This chapter explains how a risk analysis is performed and also explains the two different ways to perform risk analysis.

Chapter 4 describes about security policies, which are very basic to build a network. Security policies are designed with the help of security services and security mechanisms. This chapter explains all the security services and security mechanisms.

Chapter 5 presents the implementation part and discusses the results of different scans that are performed on the network before and after giving the security.

2 Attacks and Attacks Mitigation

Now-a-days there are so many attacks which cause serious problems to an enterprise network. To protect the network from attacks, network administrator must detect all the vulnerabilities present in the network and must know how to defend and mitigate all attacks. An attack occurs in several stages for successfully executing against an enterprise network. Initially an attacker may have limited information about the target network, so one of the primary objectives of an attacker is to gather intelligence or information about the target vulnerabilities. After gathering information about the target network, a range of attacks can be launched against the organization. For gathering information, attackers typically do not require in-depth knowledge about the target network. For example they can just use WHOIS to find the domain name and IP address of the target network which is not a crime. This information can be used later to perform an attack. All the network attacks can be divided into two parts [1]

1. Attacks that require less intelligence about the target network
2. Attacks that require more intelligence about the target network

Attacks that require less intelligence about the target network are divided into [3]

- Reconnaissance attacks
- Access attacks
- DoS and Distributed DoS attacks

Attacks that require more intelligence about the target network are divided into

- Worms, Viruses and Trojan horses
- Application layer attacks
- Threats to management protocols

This paper describes all attacks and their mitigation techniques very briefly and gives more emphasis on reconnaissance attacks and their mitigation techniques.

2.1 Reconnaissance attacks

Reconnaissance attack is defined as the unauthorized discovery and mapping of systems, services, or vulnerabilities of the target network. If an attacker or intruder wants to attack a network, he needs some information about target network like which IP (Internet Protocol) addresses are alive, which ports and services are active on those IP addresses and what operating system is running. With reconnaissance attacks, an attacker can gather such information and can execute an actual attack on the target network. For a considerable time reconnaissance attacks are not detected because they have no impact on the network. [3] [4]

Operation of reconnaissance attacks

Reconnaissance attack is an initial step for an intruder to attack a network. To gather information about the target network, first, an intruder performs a ping sweep of the target network to get IP addresses that are alive. Then, the intruder performs port scans to determine which ports or services are active on the IP addresses which are alive. After determining live ports, the intruder starts querying the ports to find what operating system is running, the type and version of the applications, software running and the configuration that has been applied on the target host. Reconnaissance attack can be used as an administrative tool or as an attacking tool.

Reconnaissance attacks consist of

- Packet sniffers
- Port scans
- Ping sweeps
- Internet information queries

2.1.1 Packet Sniffers

Packet sniffing is a method of capturing each packet that flows across the network. Packet sniffer is an application program which uses Network Adapter Card (NAC) to capture packets that travel across a network layer of the Transmission Control Protocol/Internet Protocol (TCP/IP) layer. NAC should in promiscuous mode for capturing packets. Promiscuous mode is mode in which NAC reports every packet that is received on the physical layer to an application for processing. [3] [5]

Packet sniffing can be developed very easily when a network application sends packets in plaintext. Plaintext is nothing but information without encryption. When packets are sent in plaintext it is easy to capture and understand the packets. Packet sniffing can be used as an administrative tool for monitoring and validating network traffic or as an attacking tool.

Packet sniffer mitigation

Packet sniffing can be mitigated by using tools like

- Authentication
- Switched infrastructure
- Antisniffer tools
- Cryptography

Authentication

Authentication is the process of identifying the users who have access to the network. Having strong authentication is the primary option for defending against packet sniffer. One Time Password (OTP) is a common example for strong authentication. OTP is a password which is valid only for single login session or transaction. OTP is a two-factor authentication, which involves combination of new password with known password. Once the new password is used and the hacker learns that password by packet sniffing, it is useless because the password is already expired. This mitigation technique is useful when packet sniffers are intended for

Network Attacks

capturing passwords, but packet sniffers which are intended for sensitive data (like e-mail) will still have the effect.

Switched infrastructure

It is a very common technique used in networks to defend against packet sniffers. In switched infrastructure every device is given its own switch port. Once the network deploys switched environment hackers cannot capture all packets passing through the network. Hackers can gain access only to a specific port where they are connected. Because of this switched infrastructure cannot eliminate the threat of packet sniffers completely, but can reduce the effect of impact greatly.

Antisniffer tools

Antisniffer tools are used to detect sniffers that are present in the network. Antisniffer tools can be designed by using software or hardware. Antisniffer tools can not eliminate the threat completely but they are the part of overall mitigation system. Antisniffer tools detect the change in the response time of the host. Time taken for processing the traffic that is coming from server or next host is called response time. If this time is more it is said that the host is processing more traffic than the actual traffic. By observing the response time, antisniffer tools will detect the sniffers. There are many antisniffer tools available in the market. One such software tool for network security is AntiSniff.

Cryptography

Cryptography is the more effective method for detecting or preventing packet sniffers. Cryptography is the process of encrypting the data. When packet sniffers capture the encrypted data, they see only a cipher text (random string of bits), which is very hard to understand. Encrypting packets is the best solution to prevent sniffers. Packet encryption is made by Data Encryption Standard (DES), 3DES and Advanced Encryption Standard (AES) algorithms. Terminal access is made by cryptographic protocols like Secure Shell (SSH) and Sockets Layer (SSL).

2.1.2 Port Scans and Ping Sweeps

Both Port scans and Ping sweeps are called scanning tools. They are the most common type of reconnaissance attacks. They can be used as administrative tools or as hacking tools. Network administrator will use this tool for finding vulnerable services in the network. Hacker will use to find services in an illegitimate way. [6]

Ping Sweep

With the help of ping sweep, an intruder will get the IP addresses of target network which are alive. It can be done by sending an Internet Control Message Protocol (ICMP) ping to every IP address of the target network or by sending network ping. ICMP ping will send echo requests to multiple hosts. If a host sends an ICMP echo replay, that host is alive. Ping sweeps are the slower and older techniques used to scan a network.

Port Scans

With the help of port scan, an intruder can find open ports and services that are active on the live IP addresses. Port scan is performed by sending a series of messages to a target hosts. Depending upon the kind of response received, the intruder will find which ports are open, which ports are closed and what services are associated to that port. Well-known port numbers are assigned to every service. For example Simple Mail Transfer Protocol (SMTP) has a port number of 25. If port scan finds port number 25, then the intruder will know that the host is using SMTP. Most commonly used port scanning tools are SAINT, Nmap and Nessus.

Port Scans and Ping Sweeps Mitigation

Port scans and ping sweeps cannot be prevented completely. Without compromise the network capabilities it is hard to prevent port scans and ping sweeps completely, because they are not a crime. When a computer is connected to the Internet, it opens a port. Once a port is open, port scan will find that port. By using some mitigation techniques damage to the system can be prevented.

Using filtering devices is the most common method for stopping port scans and ping sweeps. Filtering device can be a Firewall or a Cisco router with access control list. To stop ping sweeps, ICMP echo and echo-reply should be turned off on edge routers. By doing so, organization will lose network diagnostic data. Port scans are able to find IP addresses, but will take long time when compared with ping sweeps. Port scans can be mitigated by using Intrusion Prevention Systems (IPS) at network and host levels. IPS will give an alert message when a reconnaissance attack is under way. With that alert message network administrator can prepare for the coming attack.

2.1.3 Internet Information Queries

Querying the internet for getting information about a website or an organization is called internet information queries. Domain Name System (DNS) queries can give information about particular domains like who owns the domain and what address is assigned to that domain. DNS are the largest and active distributed databases on the planet. The function of DNS is to translate the human-readable domain name into the machine-readable IP addresses.

Intruders can use internet tool like “WHOIS” for getting information from internet. There is no way to mitigate these queries. While giving information to DNS, organizations have to make sure that only certain information which does not cause harm has to be given. [3]

2.2 Access Attacks

Access attacks can be said as accessing network traffic in an illegal way. With the help of access attacks intruders can retrieve data, gain access and can escalate their access privileges across the networks or systems. They are used to gain access to confidential databases, web accounts and other sensitive information. Access attack can occur in different ways. [3] [4]

Access attacks consist of

- Password attacks
- Trust exploitation
- Port redirection
- Man-in-the-middle attacks
- Buffer overflow

2.2.1 Password attacks

Passwords are used to authenticate users. Passwords are very sensitive data and are easily captured by hackers because they are human understandable. Password attacks are used to guess system passwords. It is done by a series of attempts to the system by an attacker. A dictionary attack is the common example for password attack. Dictionary attack will try all possible passwords until it finds the correct password.

Password attacks can be implemented by

- Brute-force attacks
- Trojan horse programs
- IP spoofing
- Packet sniffers

Password Attack Mitigation

Users must understand how important to secure their passwords. Some of the techniques for mitigating password attacks are

- Do not share passwords with others
- Do not use same password on multiple systems, use different passwords for each system
- Change passwords every 6 to 12 months
- After a certain number of unsuccessful login attempts, disable the account
- Do not use plaintext passwords.
- Use strong passwords, using upper and lowercase letters, special characters, and numbers

2.2.2 Trust Exploitation

Devices operating in a shared environment should trust the information coming from other devices. Hackers will try to exploit this trust by gaining access to one of the compromised device in the network. With trust exploitation hacker can listen or send or modify data as a trusted user. For example, if Demilitarized Zone (DMZ) host is compromised then attacker can exploit the inside host connected to the inside firewall interface, because inside host trusts the DMZ host.

Trust Exploitation Mitigation

Having tight constraints on trust levels within a network can mitigate trust exploitation. Systems inside the firewall should never completely trust systems on the outside the firewall. Trust should be limited to specific protocols. In the above example, when the DMZ host is controlled by an attacker, his next goal is to compromise the inside systems connected to the trusted interface of the firewall. It can be done by finding the permitted protocols from the DMZ host to the inside interface and then searching the vulnerabilities on the inside host. This attack can be stopped if the firewall has minimum or no connectivity from the DMZ host to inside hosts.

2.2.3 Port redirection

Port redirection attack is a type of trust exploitation attack. With the help of compromised host, port redirection attack will redirect all the raw packets to a secondary destination by installing port redirection software like HTTPtunnel or NetCat. Port redirection attack will not violate any rule and it makes the administrator to feel that communication is taking place between two genuine hosts. With the help of port redirection hacker can know the communications, user id/password and protocols used in the network.

Port Redirection Mitigation

To mitigate port redirection, organizations should use good trust models that are network-specific. Trust models are implemented by proper access restrictions between hosts. As long as hosts are trusting based upon IP addresses, port redirection cannot be mitigated. HIPS (Host-based Intrusion Prevention System) helps to detect an intruder by assuming a system is under attack and can prevent installations of port redirection software.

2.2.4 Man-in-the-middle attacks

Man-in-the-Middle (MitM) attacks are one of the most popular and challenging attacks in securing a networks. MitM attack can be defined as attack where an intruder will read and write the data that is being communicated between two hosts without knowing the hosts. For executing this attack an intruder must have access to network packets that are passing across the network. MitM attacks are also referred as session hijacking attacks. MitM attack is implemented by using network packet sniffers and routing and transport protocols.

The main purposes of MitM attacks are:

- To compromise confidentiality, integrity and availability
- To capture the information
- To corrupt the transmitted data
- To introduce new information into network sessions

Man-in-the-middle attacks Mitigation (MitM)

When two hosts are communicating with each other there is a chance for MitM attack and it is very hard to mitigate. By using cryptographic encryption, MitM attacks can be mitigated very effectively. When the data is encrypted, the attacker will see only the cipher text with the help of MitM attack which is useless.

2.2.5 Buffer overflow

Buffer overflow attack is the most common attack that can compromise the security of a computer system in a network environment. Buffer overflow is a process of overflowing or overloading the space in a buffer. This is done by writing a program which stores data beyond the allocated end of a buffer in memory. Buffer overflows usually occur as a consequence of a bug and the improper use of languages such as C or C++ that are not memory-safe. Buffer overflow attacks help all most all existing malicious worms to propagate themselves from one machine to another machine. With buffer overflow attack, an attacker can insert his own code into a victim's machine so that he can control or compromise the services of the host.

Buffer Overflow Mitigation

Having an up-to-date bug reports for the network and application server products will help to detect the buffer overflows and apply the latest patches to these products. The most common way to mitigate buffer overflow attacks is to check buffers at constant times. [7] If a buffer contains more data, it is clear that the buffer is overflowed and that buffer can be restricted.

2.3 DoS and Distributed DoS Attacks

DoS (Denial of Service) Attacks

After reconnaissance attacks, DoS attacks are the most common form of security attacks. DoS attacks are the most difficult attacks to eliminate completely because they are not targeted to gain access to the network or the information on the network. Attackers use DoS attack to prevent legitimate users from accessing information or services in the network. DoS attacks can also target an entire network, to prevent outgoing traffic or to prevent incoming traffic to certain network services. DoS attacks make services useless to the legitimate user. DoS attack can be executed by Flood Attack, Ping of Death Attack and SYN Attack. Most common type of DoS attack is distributed DoS attack. [3] [4]

Distributed DoS Attacks

A distributed DoS attack uses a DoS attack on a server and sends an extremely large number of requests to a network. To process all requests, the server takes long time and dramatically becomes slow and becomes unavailable for the legitimate access and use. For executing distributed DoS attacks, attackers require very little effort because they take advantage of weaknesses of protocols. These attacks are very difficult to eliminate because they attack on the traffic that is normally allowed into the network.

DoS and Distributed DoS Attacks mitigation

It is very difficult to completely eliminate DoS and Distributed DoS attacks, but their damage can be minimized by using some mitigation methods like

- Anti-spoof feature
- Anti-DoS feature
- Traffic rate limiting

Anti-spoof features

Configuration anti-spoof features on the routers and firewalls will reduce the risk. Anti-spoof features include filtering of packets with access lists, disabling of source route options, and others.

Anti-DoS features

Configuration of anti-DoS features on routers and firewalls can mitigate the effectiveness of an attack. These features include the limits on the amount of half-open TCP connections that a system allows at any time. This method is called as SYN-flooding prevention.

Traffic rate limiting

An organization can limit the traffic that is coming from its ISP. This is one of the ways of filtering the traffic. This filtering will limit the nonessential traffic that is crossing the network segments at a certain rate. ICMP-based distributed DoS attacks are very common. ICMP traffic can be limited, because it is used only for diagnostic purposes.

2.4 Viruses, Worms and Trojan horse Attacks

Virus

Viruses are malicious software programs attached to a program or file capable of executing a particular unwanted function on a computer. A virus can propagate from one program to another program so that it can infect entire system. Virus can do serious damages like erasing files or erasing entire disk. Some viruses are very simple and do not cause any harm. Viruses cannot spread from one system to another system without human interaction. Viruses can spread by sharing infected file or opening an infected file or opening an e-mail attachment which has virus. [4]

Worm

A worm is a sub-class of virus which can affect the system in a same way as virus. Worm installs copies of itself in the memory of infected computer and executes arbitrary code. Worms can spread from one system to another system without user interaction. Worms have the capability of infecting entire network. Worms take advantage of automatic file sending and receiving features for spreading. [3]

Trojan horse

Trojan horse is a name given to software which looks useful but will do damage once installed or run on the system. Trojan horse can cause serious damage like deleting files and destroying information on your system. Some Trojans are simple and does not cause any harm. Trojans cannot reproduce nor replicate. But they can make a system to vulnerable for many attacks. [1]

Viruses, Worms and Trojan horses Mitigation

Viruses and Trojan horse attacks can be mitigated by using effective use of antivirus software. Antivirus software can detect most viruses and many Trojan horse attacks and can prevent them from spreading in the network. Keeping up-to-date with the latest developments of these attacks can help to handle these attacks effective. Everyday new virus or Trojan horse applications are releasing, so keeping up-to-date with the latest antivirus software will help to protect a system. By using host-based intrusion prevention systems, such as the Cisco Security Agent (CSA), can effectively defend viruses and Trojan horse attacks against the hosts. Worms can be mitigated by following some steps like Containment, Inoculation, Quarantine and Treat.

2.5 Application Layer Attacks

Application layer attacks are implemented in different ways. One of the most common methods is to exploit the well-known weaknesses of an application or system such as sendmail, HTTP, and FTP. They display a screen, banner, or prompt, with the help of Trojan horse programs, to the user to enter the login details. Once the user enters the details, that program sends login details to the attacker. This type of attack is the oldest form of application layer attacks. Newest forms of application layer attacks exploit the ports that are allowed through a firewall. These attacks include java applets and ActiveX controls and pass harmful programs through open ports and load them in the user browser. Application layer attacks can never be eliminated completely, because new vulnerabilities are being discovered daily. [3]

Application Layer Attacks mitigation

By taking some measures, the risks of application layer attacks can be reduced. They include

- Reading operating system and network log files will review all logs and can take appropriate action accordingly
- Subscribing to mailing lists that publicize vulnerabilities
- Keeping the operating system updated with latest patches
- Using IDS, IPS, or both that scan for known attacks, monitor and log attacks, so that the network administrator can prevent the attacks

2.6 Threats to management protocols

For extending the scope of computing environment beyond a single LAN or few PCs, a set of automated network management tools are required. To deal with the multi-vendor environment, a network management system is needed that is based on standardized network management protocols and applications. Most commonly used management protocols are Simple Network Management Protocol (SNMP), SysLog, Trivial File Transfer Protocol (TFTP) and Network Time Protocol (NTP) and if proper security measurements are not taken, these protocols can be compromised

2.6.1 SNMP Protocol

SNMP is used to retrieve information from a network device or to remotely configure parameters on the device. SNMP version 1 and 2 uses passwords within each message as a simple form of security. These SNMP versions send the passwords in plaintext along with the message. So these versions can be intercepted by anyone with a packet sniffer located along the data path between the device and the management server. SNMP version 3 overcomes these shortcomings by providing authentication and encryption to the message exchange.

Recommendations for the correct use of SNMP protocol [3]

- Configure SNMP with read-only community strings.
- Set up access control on the device that is managed via SNMP to allow access by only the appropriate management hosts.
- Use SNMP version 3 which provides combination of authentication and encryption to packets over the network.

2.6.2 SysLog Protocol

SysLog protocol is designed to carry messages from a device that is configured for logging to a syslog server that collects the information. Messages are sent as plaintext between the managed device and the management host. Syslog do not have packet-level integrity checking to ensure that the packet contents have not been interrupted and altered in the transit. So an attacker may alter syslog data in order to confuse a network administrator during an attack.

Recommendations for using SysLog protocol

- Encrypt syslog traffic with an IPSec tunnel.
- Implement access control filtering at the perimeter router when allowing syslog from devices on the outside of a firewall.
- Implement ACLs on the firewall for allowing syslog data from only the managed devices themselves to reach the management hosts.

2.6.3 TFTP Protocol

TFTP is used for transferring system files or configurations across the network. System files and configurations are very important to protect because they can reveal the entire information of the network which may cause lot of damage once the attacker captures the data. TFTP uses UDP for transferring data between the requesting host and the TFTP server. TFTP also sends data in plaintext which is vulnerable and can be interrupted by an intruder in the transit.

Recommendations for using TFTP protocol

- Encrypt TFTP traffic within an IPSec tunnel in order to reduce the chance of interception.
- Restrict the TFTP server for accessing from unauthorized clients.
- TFTP should be configured correctly.

2.6.4 NTP protocol

NTP is used to synchronize the clocks of various devices across a network. Synchronization of the clocks within a network is essential for digital certificates and for correct interpretation of events within syslog data. An intruder could attempt a DoS attack on a network by sending bogus NTP data across the internet in an attempt to change the clocks on the network devices in such a manner that digital certificates are considered invalid. An intruder can also attempt to confuse a network administrator during an attack by disrupting the clocks on the network attacks. These attacks make it difficult for the network administrator to determine the order of syslog events in multiple devices.

Recommendations for using NTP protocol

- Implement your own master clock for private network synchronization.
- Use NTP version 3 or above to support a cryptographic authentication mechanism between hosts.
- Use ACLs that specify which devices in the network are allowed to synchronize with other network devices.

3 Risk Analysis

Risk analysis is defined as the process of identifying the risks to a network or system and determining the probability of occurrence of that risk, their impact and the methods or procedures that would mitigate that impact. Risk analysis is the very fundamental process that should be performed for any organization or network to provide security. Risk analysis plays a major role in designing a network. Previously network managers used to give a little importance to risk analysis and they build the network. When the network is completely built, they face a lot of problems, which cause huge losses to the organizations because of lack of estimation of risk. With the help of risk analysis, managers, designers, administrators will have handful of information about all risks and they can build a network with high security. Risk analysis is a continuous process throughout the implementation of network. Every time the risk analysis is performed, organizations will find new risks which may cause damage to the network. By having new methods for the mitigation of the new risks, organization can improve overall security of the network.

Risk cannot be managed unless it is identified. Risk can be defined as the probability of exploitation of a particular threat to a particular vulnerability. With the help of risk identification organizations will determine what could happen to cause a loss and get more information about how, where and why that loss happened. With the help of risk identification organizations will try to identify all knowable risks. Risk analysis can be done in different ways. Whatever risk analysis process is used, the method of risk analysis remains same. The standard methodology of risk analysis is [8]

- Identification of assets
- Identification of threats
- Identification of vulnerabilities and
- Identification of existing controls

3.1 Identification of assets

In an organization, asset is nothing but a thing which requires protection. Identifying assets is very important because the remaining part of risk analysis is made on these assets. Normally assets can be more than hardware and software. In a network the hardware assets are processors, boards, monitors, keyboards, terminals, drives, cables, connections, controllers, communications media, switches, routers, hubs, modems, printers, fax machines. Each device is very important and must be protected. Some of the software assets are source programs, executable programs, systems programs, purchased programs, diagnostic programs, and operating systems. Software assets are more likely to be attacked because they are available to everyone, including hackers in different versions. Data is another important asset. The entire security of a network can be judged on how the data is being protected. As an asset data can be said as data used during execution, stored data on various devices, and data in the routing process. Employees are big assets to an organization. Identifying employee and what services he or she can access will help to improve the security of an organization. Network assets are front-end processors,

workstations, communication lines, data encryption tools, satellite connections, remote access security.

3.2 Identification of threats

After identifying assets that need to be protected, organizations must identify the threats that are associated with assets. Threat is a potential cause of an unwanted event that may harm assets. A threat may harm one or more assets. In a network threats can be accidentally triggered or intentionally exploited. Threats occur naturally or with human origin. Both accidental and intentional threats sources must be identified to protect the network.

Threat-source identification

A threat-source is defined as any event or location with the potential to cause harm to the network. Common threat-sources which cause serious damage to the network are natural, human, or environmental. Organizations must consider all the threats of each threat-source before building the network. Necessary precautionary steps must be listed for each threat. Natural threats can be floods, earthquakes, tornadoes, landslides, avalanches, electrical storms. Human threats are events that are either enabled by or caused by human beings, unintentional acts or deliberate actions. Environmental threats can be long-term power failure, pollution, chemicals, and liquid leakage. Threats that are natural and environmental can be found easily, but human threats are very difficult to find. Human threat sources are of different types. Table 2.1 shows the different human threat sources their motivation and threat actions.

3.3 Identification of vulnerability

Vulnerability is defined as “a flaw or weakness in system security procedures, design, implementation, or internal controls that could be accidentally triggered or intentionally exploited and result in a security breach or a violation of the systems security policy” [9]. The presence of vulnerability does not cause harm unless there is a threat to exploit it. A vulnerability that has no threat to execute may not require implementation of a control but it has to be identified and monitored for changes. Assets of a network are the main source for vulnerabilities when they are used with an intention to cause harm. Some of the sources of vulnerabilities are

- Organization
- Processes and procedures
- Management routines
- Personnel
- Physical environment
- Information system configuration
- Hardware, software or communications equipment
- Dependence on external parties

Threat-source	Motivation	Threat actions
Hacker, cracker	Challenge Ego Rebellion	<ul style="list-style-type: none"> • Hacking • Social engineering • System intrusion, break-ins • Unauthorized system access
Computer criminal	Destruction of information Illegal information disclosure Monetary gain Unauthorized data alteration	<ul style="list-style-type: none"> • Computer crime • Fraudulent act • Information bribery • Spoofing • System intrusion
Terrorist	Blackmail Destruction Exploitation Revenge	<ul style="list-style-type: none"> • Bomb/Terrorism • Information warfare • System attack • System penetration • System tampering
Industrial espionage	Competitive advantage Economic espionage	<ul style="list-style-type: none"> • Economic exploitation • Information theft • Intrusion on personal privacy • System penetration • Unauthorized system access
Insiders	Curiosity Ego Intelligence Monetary gain Revenge Unintentional errors and omissions	<ul style="list-style-type: none"> • Assault an employee • Blackmail • Computer abuse • Fraud and theft • Information bribery • Interception • Malicious code • System intrusion • Unauthorized system access

Table 2.1 Human threat sources, their motivation and threat actions

3.4 Identification of existing controls

Controls are defined as mechanisms or procedures that are used in the mitigation of vulnerabilities. Controls are used to detect and prevent the vulnerabilities. Identification of existing controls is very important to avoid unnecessary work or cost. Existing controls can be identified with the help of documentation of controls and plans of risk treatment implementation. When identifying the controls, a check list is made to ensure that the existing controls are working properly. If a control is not working correctly it may cause vulnerabilities. When a control fails to operate correctly, complementary controls are addressed to mitigate the risk. The effect of a control is measured by how it reduces the likelihood of threat and ease of exploiting the vulnerability, or impact of the incident. [9]

Existing or planned controls can be identified by

- Reviewing documents containing information about the controls
- Checking with the people responsible for information security and the users as to which controls are really implemented
- Conducting an on-site review of the physical controls
- Reviewing results of internal audits

3.5 Types of risk analysis

Risk analysis is performed in different ways, depending upon the organization. The approaches of processing risk analysis fall into two categories [8]

- Qualitative risk analysis
- Quantitative risk analysis

3.5.1 Qualitative risk analysis

Qualitative risk analysis is used to determine the amount of protection required for systems, applications and assets of an organization. [10] It provides a systematic examination of assets, threats, and vulnerabilities that establish the threats, the cost of losses if those threats occur and value of controls or safeguards designed to reduce the vulnerabilities and threats to an acceptable level. Qualitative risk analysis uses a scale of attributes that are qualified to describe the level of potential consequences and the likelihood that those consequences will occur. Qualitative risk analysis attempts to prioritize the risk elements that are present in the subjective scope and identifies areas that have to be improved to address the vulnerabilities. It is often used first to get the general indication of level of risk because of the advantage of its ease of understanding by all relevant members. Choosing the scale to analysis the risk is a concerning factor in qualitative estimation. To perform qualitative risk analysis, having good data is prerequisite and if organizations lack good data qualitative risk analysis is not performed. Qualitative analysis may be used

- As an initial screening activity to identify risks that require more detailed analysis
- Where this kind of analysis is appropriate for decisions
- Where the numerical data or resources are inadequate for a quantitative estimation

3.5.2 Quantitative risk analysis

Quantitative risk analysis used to find the probability of occurrence of vulnerabilities, threats and likelihood of losses that they cause. Quantitative risk analysis assigns numerical values to a scale for both consequences and likelihood with the help of data from variety of sources. With the help of these numerical the overall risk of an asset can be identified. If there is not good data for analysing risk, quantitative risk analysis is used. With the help of data provided from quantitative analysis, qualitative analysis is performed to estimate the overall risk of an asset. The basic elements of a quantitative risk analysis are [8]

- The financial value of the asset
- The cost to build the asset
- The cost to protect the asset
- The value of the asset to the competition
- The cost to recover the asset

One way to identifies the value of an asset by quantitative risk analysis is

- Assign a monetary value to each asset class
- Input the asset value for each risk
- Produce the single loss expectancy value (SLE)
- Determine the annual rate of occurrence (ARO)
- Determine the annual loss expectancy (ALE)

With the help of SLE, the expected impact of a specific threat can be identified. It is calculated by multiplying the exposure factor of the threat with financial value of the asset, where exposure factor is the percentage of asset loss. ARO is the probability of occurrence of a threat in one-year time frame. ALE is obtained by multiplying SLE with ARO. To estimate the cost-benefit of an asset, it is necessary to apply these formulas. The main disadvantage of quantitative risk analysis is assigning numerical to the assets and calculations can be complex.

This analysis may cause problems when auditable data is not available and data is not factual.

4 Security policy

Security policy is defined as “a formal statement of the rules by which people who are given access to an organization’s technology and information assets must abide” [11]. To design a secured computer network, it is very important to have a set of security policies. The main purpose of a security policy is to inform the users, staff and managers about the protection of technology and information assets. A security policy provides road map in the design and operation of the security within the network. A network security policy sets the rules and access limitations for accessing various assets that are present in the network. Network users and administrators will use the security policy as the source of information for using and auditing the network.

4.1 Importance of a security policy

Security policies are very important to organizations for a number of reasons including the following

- Create a baseline of organizations current security posture
- Set the framework for security implementation
- Define allowed and disallowed behaviour
- Help determine necessary tools and procedures
- Define how to handle security incidents

Understanding the present security position is very important for any organization to achieve their goals. It will help to provide more security if the current security measurements are not reaching the organizations requirements. Security measurement is nothing but the amount of security provided to protect the organization’s assets. Security measurements can be implemented in different ways, but choosing a particular implementation will have an impact on the organization. Security implementation is a systematic approach to reach the desired security. Security policies help to choose a particular implementation with a framework to achieve the organization goals.

Security policies define the roles and responsibilities of the organization’s personnel. For example in a university campus network, students have different roles and lectures have different roles. Students are not allowed to download and install software for internet where as lectures have access to install the software. These types of allowed and disallowed behaviour are defined by security policies. There are different tools to protect the data, but choosing the best tool according to organizations goals is important. With the help of security policies organizations can find the tools that are necessary to protect the data.

A security policy defines a way to take care of the security incidents. For example consider an employee who is using a laptop for storing all the information. If that laptop is lost or crashed, lot of information which is stored on the laptop will be loosed which causes huge loss to the organization. In this case a security policy can be defined for the employees who are using

Security Policy

laptops to give data backup at the end of the day. Security policies also provide measures that are to be taken against the personnel in the case of violations of policy.

4.2 Roles of a security policy

A security policy should attempt to play the following three roles [12]

- Clarify what is being protected and why it is being protected.
- States who is responsible for providing protection.
- Provide grounds on which to interpret and resolve any later conflicts that might arise.

Before designing the security policies, the developers must find what is important in the organization and what things need to be protected. The important things that need to be protected are

- Information assets
- Information infrastructure
- Information availability
- People

Information assets

Information is the most important asset in every organization. It needs to be protected for instance, accessing should be restricted to those people who have a need to know. If any change is made to the information it should be informed. When information is transformed from one system to another system in the network, actions should be taken to ensure that no intruders can read and intercept the information.

Information infrastructure

If information assets are important so is the information infrastructure. Information infrastructure is nothing but computer systems, operating system, databases, application software and networks. The overall security of the information depends on the integrity of the infrastructure that contains information.

Information availability

Information must be made available to authorized people when they want it without any alternations. When information is passing in the network steps must be taken to ensure that intruders and others are not able to alter the information or information infrastructure to make information unavailable to those who need it.

People

People are very important asset to any organization to run for a long time. People must be educated about the security concerns of the organization. People must know the information to manage the organizations assets and to operate the systems and networks.

Security Policy

In any organization a single person cannot provide and maintain the entire security, because security is achieved at different levels like managerial level, design level, implementation level. A security policy will classify the people into different levels to get the security and people who write the security policies will clarify who is responsible for providing security to the organization. Normally a business security or information security group will write the security policies. People responsible for providing the security requirements can be one or more of the following

- The network's users
- The network's administrators and managers
- The auditors who audit the network's usage
- The managers who have overall ownership of the network and its associated resources

Issues that are not covered in the security policy are important and should not leave them. One of the main roles of security policy is to explain what to do with this type of issues. For example consider a security policy which states that, all the resigned employees should not access the organization assets. If this policy is failed, it causes serious issues like revealing the information to unauthorized persons. In this situation, some action should be taken to protect the information. So the security policy will address that action to specific individuals to interpret and resolve them.

4.3 Security services and mechanisms

For making good decisions about security, the organization should determine their security goals and what services they need in the network. Security service is a service provided by a system to give a specific kind of protection to system resources. Security mechanism is defined as a process that is used to implement a security service. Depending upon the services required a set of security policies are made.

Security services are divided into five categories [13]

- Authentication
- Access control
- Confidentiality
- Integrity
- Non-repudiation

Security mechanisms are divided into five categories

- Encryption
- Digital signature
- Access control
- Data integrity
- Authentication

4.3.1 Security services

Authentication

“Authentication is a mechanism to establish proof of identities” [13] Authentication guaranties the source of information is genuine. Authentication is the assurance that a message is coming from a valid source. Without authentication an organization cannot achieve its goals. With a valid user name and password users are authenticated. Protecting the password from hackers is very important and is done by encryption. Authentication is a feature of encryption. Authentication service is of two types

- Peer entity authentication
- Data origin authentication

Access control

Access is defined as the ability and the means necessary to make use of resources of a system. To make a network to be secured, it is important to allow only authorized users to access the resources of the system. Controlling access is nothing but giving access to only authorized users. In a network giving access to resources is limited to individual depending on their roles and responsibilities. Access control service gives protection against the unauthorized use of resources by verifying or identifying the eligibility of individual to access specific categories of information. Access control service is achieved with the mechanism of access control.

Confidentiality

Confidentiality is the assurance that information is not made available or disclosed to unauthorized individuals. Sensitive data should not be disclosed to unauthorized users because it can result in loss or damage to organization, such as identity theft. When sensitive data is passing across the networks, an attacker can gain access to the information if it is not protected. Confidentiality service is used to provide protection for sensitive data. Confidentiality service uses encryption mechanism. By encrypting the data with cipher text, the unauthorized users cannot see the original data only authorized users with encryption key can see the original data. Confidentiality service is of four types

- Connection confidentiality
- Connectionless confidentiality
- Selective field confidentiality
- Traffic-flow confidentiality

Integrity

Integrity is the assurance that data is not modified or altered by an unauthorized user when is transported from one system to another system. A network must maintain the integrity of information when they are processed, stored and transferred across a network. Integrity service will help to know that data which is sent from a system is unaltered and is ready to use. Integrity service makes use of encryption, digital signature and data integrity mechanisms.

Non-repudiation

Repudiation is the act of denial of participation by one of the entities involved in the communication. This is a serious issue because data is seen by unauthorized users which cause harm or less to the network. Non-repudiation is the assurance that an individual is not denying his participation in the communication. Non-repudiation service uses digital signature and data integrity mechanisms. When an individual sends a message with digital signature, he cannot deny the authenticity of that signature. Non-repudiation service is of two forms

- Non-repudiation with proof of origin
- Non-repudiation with proof of delivery

4.3.2 Security mechanisms

Encryption

Encryption is the main source for cryptography. Encryption is defined as the process of transformation of plaintext into an unreadable form (cipher text) so that the original plaintext cannot be obtained without using the inverse decryption process [13]. Decryption returns the information to readable form with the help of a key provided by the encryption process. Encryption mechanism is a very important mechanism in protecting the information from attackers. When an attacker captures the encrypted information, he can see only the cipher text which is hard to understand and unable to read. Encryption is of two types [14]

- Symmetric-key encryption
- Public-key encryption

Digital signature

Digital signature is an electronic signature which is used to authenticate the identity of the sender and to ensure that the original message that has been sent is unchanged. Digital signature is a message integrity code, which is generated by a signing algorithm (hash function). Sender sends the message along with his public key and code. When receiver what to generate that code he must know a private key. If he gets the same code, it is assumed that the signature of the sender is valid.

Data integrity

Data integrity is the mechanisms for eliminating data corruption which may happen in the process of data reading and writing. Data integrity is a process where data in any information system is accurate, timely, accurate and integrated. Data integrity ensures that the received data is accurate and is not modified in its transformation.

Security services are obtained from security mechanisms. Table 4.1 shows the relationship between security services and mechanisms. Each security service uses one or more security mechanisms to form a security policy. For example to achieve the availability service to organization's information, authentication mechanism is mandatory. Authentication allows only authorized users to read, write or modify the information. When unauthorized users do not have access to the information, information availability is automatically achieved.

Mechanisms	Encryption	Digital Signature	Access Control	Data Integrity	Authentication
Services					
Peer Entity Auth.	Y	Y			Y
Data Origin Auth.	Y	Y			
Access Control			Y		
Confidentiality	Y				
Traffic-flow Confidentiality	Y				
Data Integrity	Y	Y		Y	
Non-repudiation		Y		Y	
Availability				Y	Y

Table 4.1 Relationship between security services and mechanisms

4.4 Examples of security policies

All the security policies that are required for an organization are developed based on the security services and security mechanisms discussed above. Some of the common security policies which are being developed and used by many organizations are discussed here. Security policies must be precise and easy to understand. Every policy contains the following steps to help better understand them.

- Purpose
- Persons affected
- Policy
- Enforcement
- Responsibilities

4.4.1 Network access policy

Purpose

Accessing to the network must be controlled because of the danger of an unauthorised person accessing to the organization's network. This policy must be enforced thoroughly.

Persons affected

IT, all employees of the university

Policy

Authorized users are issued with user accounts. All employees are issued accounts and must use their accounts to perform their daily activities. No one should revile the user account to unauthorized persons. Some employees are given different privileges to access the network when compared with other employees, it depends upon their roles.

Enforcement

When any employee found to have violated this policy may be subject to disciplinary action. When an employee leaves the organization, his/her user account is cancelled on the same day he/she leave the organization.

Responsibilities

Each user is responsible for protecting their information from disclosure. The IT department which is responsible for creating user accounts will establish user roles by having discussion with senior executives and management.

4.4.2 Password policy

Purpose

The purpose of this policy is to generate a standard for creating strong passwords, protection of those passwords, and the frequency of changing.

Persons affected

All the employees who have access to computers

Policy

A strong password has the following characteristics and all employees must follow them

- Contain both upper- and lowercase characters (az, AZ)
- Have digits and punctuation characters as well as letters, including 09,!@#\$\$%^&*()_+|~-=\`{ }[]: ";'<>?.,/
- Are at least eight alphanumeric characters long
- Are not a word in any language, slang, dialect, or jargon
- Are not based on personal information or names of family members
- Are never be written down or stored online

After creating a strong password it should be protected from intruders. For doing so, employees are strongly recommended not to use the same password for various access needs. For protecting the passwords employees must follow the following

- Don't reveal a password over the phone to anyone.
- Don't reveal a password in an e-mail message.
- Don't reveal a password to your boss.
- Don't talk about a password in front of others.
- Don't hint at the format of a password (for example, "my family name").
- Don't reveal a password on questionnaires or security forms.
- Don't share a password with family members.
- Don't reveal a password to coworkers while on vacation.

Employees are recommended to change their password for every four months.

Enforcement

Any employee found to have violated this policy can be subject to disciplinary action and may cause the termination of employment.

Responsibilities

Every employee is responsible for creating a strong password, for protecting the password and it change the password for every four months. IT department is responsible for taking care of the passwords.

5 Implementation and Results

5.1 Implementation overview

This section describes how to implement configurations in a campus network and how to mitigate the reconnaissance attacks that the network may contain, with the help of security implementation like IPSec VPN firewalls. The network is scanned with Wireshark and Nmap to find the attacks, before implementing security. The same scanning is made after implementing security. Both the results from the scanning are compared to show whether the reconnaissance attacks are mitigated or not.

5.2 Network design

The campus network design is shown in figure 5.1. The design shows all the connections from ISP router to Host routers.

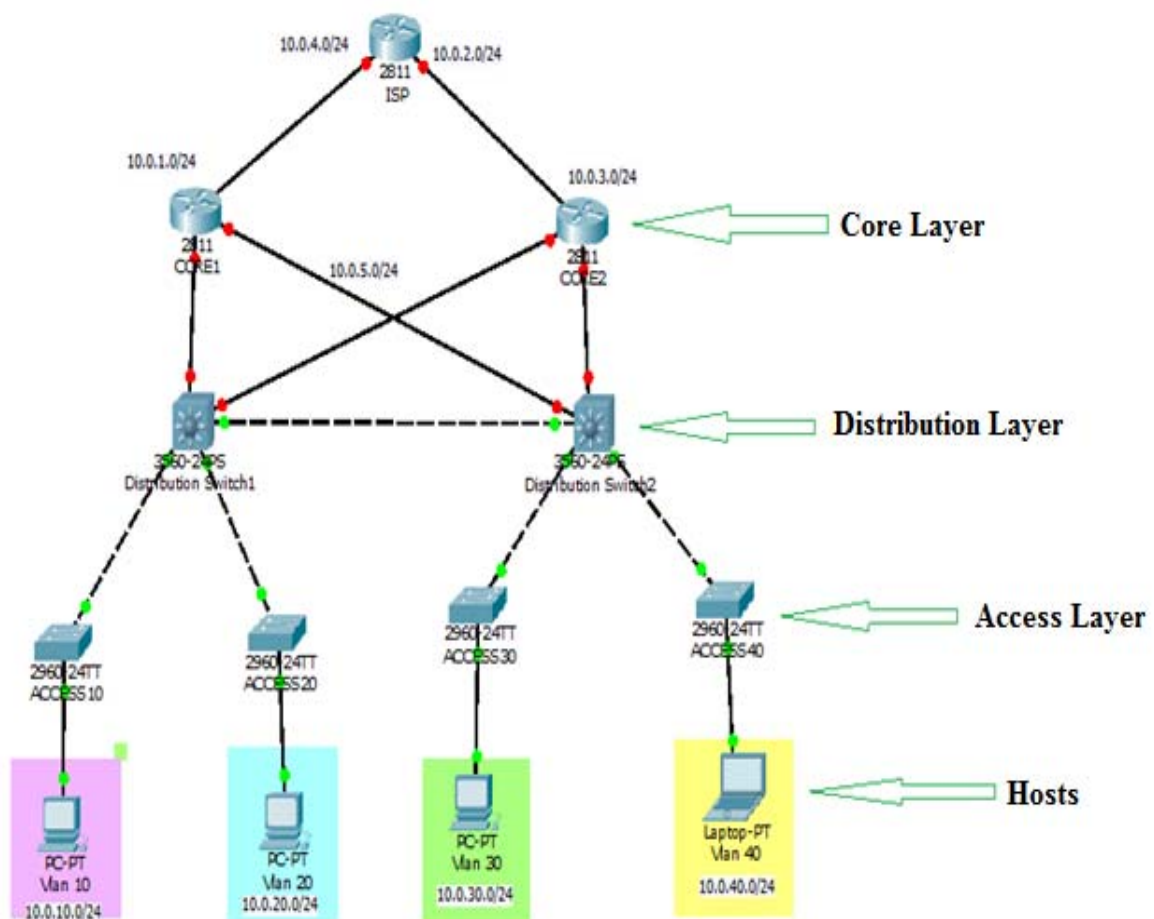


Figure 5.1: Campus Network design

5.3 Design description

The above campus network is configured in a lab environment. In the core layer, Cisco 2811 router is used to distribute the packets from ISP to the network. Another Cisco 2811 router is used as a backup router. In the distribution layer, Cisco Catalyst 3560 multilayer switches are used and in access layer Cisco Layer 2 2960 switches are used. Table 5.1 shows the equipment used in the implementation and Table 5.2 shows the software used for the test.

Device	Description	Quantity
Cisco 2811	Router	3
Cisco catalyst 3560	Multilayer switch	2
Cisco layer 2 2960	Layer 2 switch	2
Laptop/Computers	Acts as host	4

Table 5.1: Equipment used to built network

Software	Description
Cisco SDM	For configuring security
Wireshark	Windows Network Scanning tool
Nmap	Network scanning tool
WHOIS	Internet tool

Table 5.2: Applications used in the network

All the physical interfaces are configured as shown in the topology and hosts are placed in different VLANs and table 5.3 shows IP addressing of the hosts. All hosts are named with respective VLAN numbers. See Appendix B for configurations.

	VLAN 10	VLAN 20	VLAN 30	VLAN 40
VLAN	10	20	30	40
IP address	10.0.20.10	10.0.20.20	10.0.30.30	10.0.40.40
Subnet mask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
Default gateway	10.0.10.1	10.0.20.1	10.0.30.1	10.0.40.1

Table 5.3: Network configuration of hosts

Implementation and Results

EIGRP routing protocol is used to route the packets from ISP to inside network. (Appendix A) HSRP is used to provide redundant, fault tolerant routing to the internal network. HSRP provides a transparent failover mechanism to the end hosts on the network. Router CORE1 is set as primary router. If CORE1 fails, secondary router CORE2 takes the role of CORE1, which is a backup to primary router. This provides users with uninterrupted service to the network in the event of a router failure. See Appendix C for HSRP configuration.

5.4 Mitigation of Packet Sniffing

As we know packet sniffing is a process of capturing information which is in plain text. In this step the main task is to secure the data passing from router CORE1 to router CORE2. This data should be secured because there are possible chances for this communication to be sniffed by intruders. For securing the communication, Virtual Private Network (VPN) is built. VPN provides a private network tunnel over a public network. One of the ways for utilizing the VPN technology is using IPsec VPN. It also provides security for the entire conversation.

The above topology is setup in the lab environment and packets passing through router CORE2 are sniffed with help of Wireshark, a windows packet sniffing tool. After configuring VPN, the network is sniffed again. The results are analyzed before and after building the VPN. Before setting the VPN, it is important to know how IPsec works. IPsec is a framework of open standards which provides authentication, integrity, confidentiality and access control for IP traffic as it traverses through the network, so that the traffic remains secure in the transmission. When two sites want to communicate with each other, they have to authenticate themselves. IPsec uses pre-shared or digital certificates for providing the authentication between the two sites. When the authentication is completed, the sender site encrypts data using DES, 3DES or AES encryption algorithm to provide confidentiality. The sender also hashes the data using MD5 or SHA1 algorithm to protect it from tempering. In this way IPsec provides encryption to the original payload, port information and source and destination address and new header is placed in front of encrypted data.

To demonstrate how to mitigate packet sniffing, we will telnet to router CORE2 from router CORE1. Telnet sends the data in plain text, so an intruder can sniff the data easily. We will show what an intruder has sniffed before encryption. For protecting the data, IPsec is configured between router CORE1 and router CORE2. Now we again sniff packets to analyze what an intruder has captured. See Appendix D for configurations.

5.4.1 Results

The following figure shows the data that was captured. It is clear that the plain text of data is captured by an intruder.

Implementation and Results

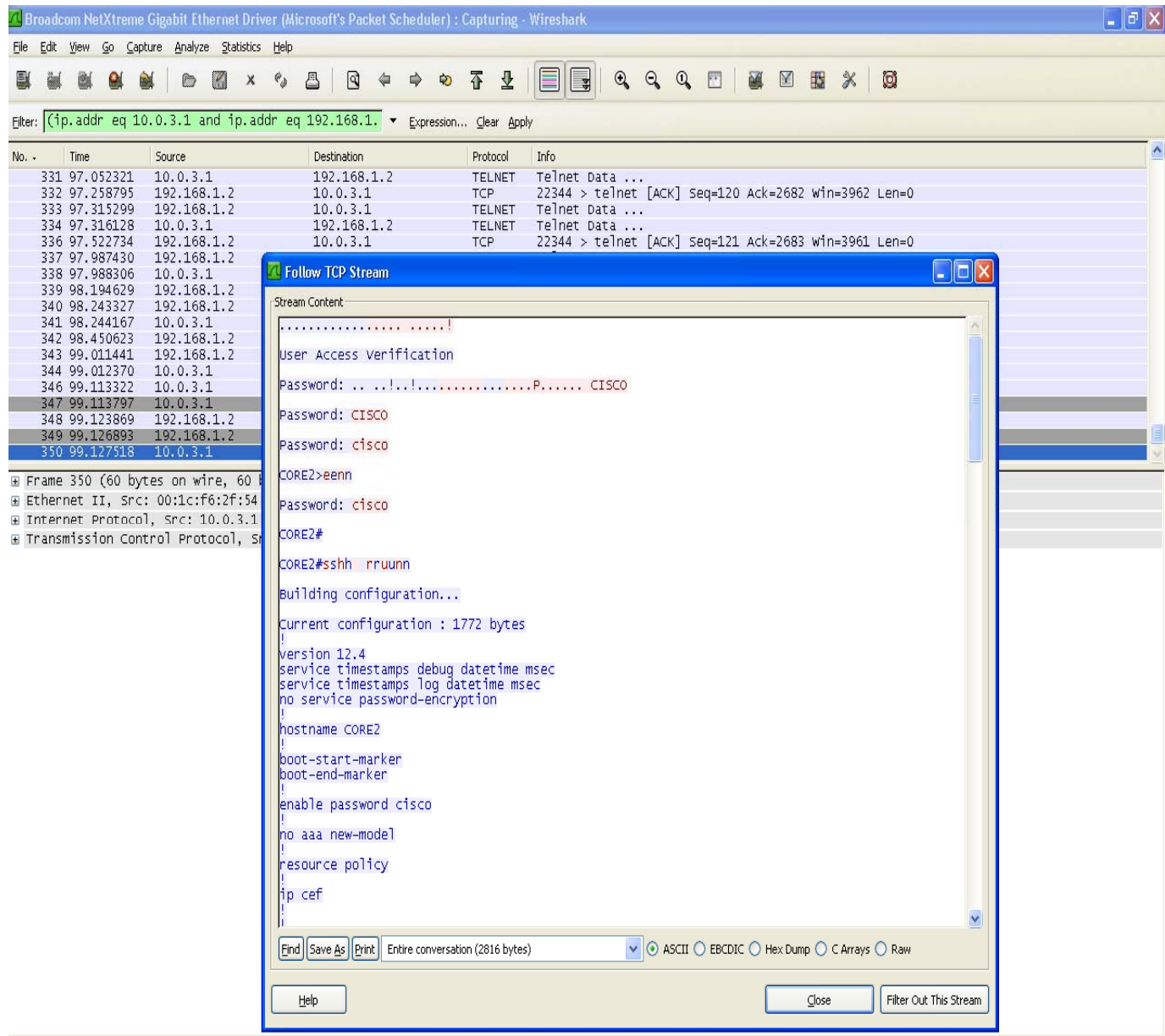
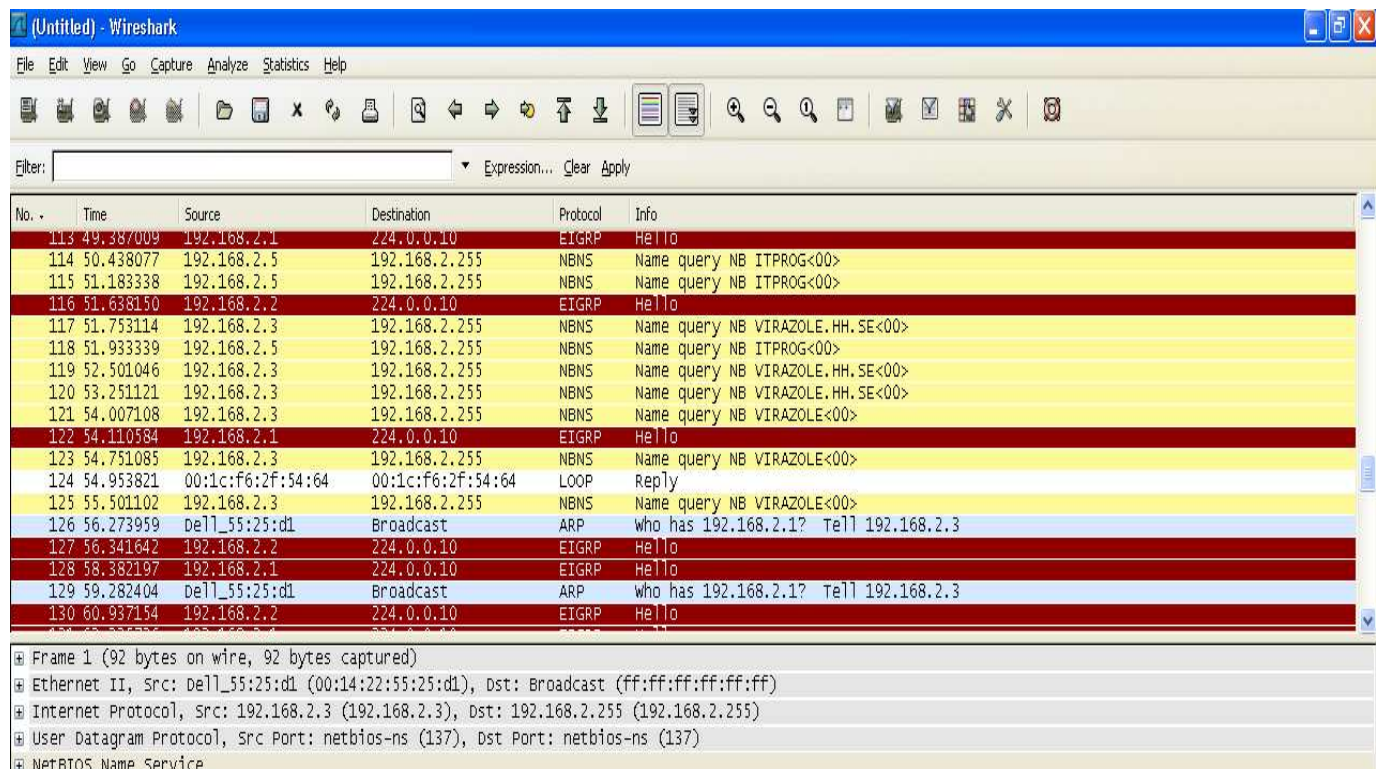


Figure 5.1 Sniffing data across the network using Wireshark without security

Now the packets are encrypted, so the packet sniffer was unable to capture the original data. Captures information was in unreadable form so an intruder has no idea about the data that is passing across the network.

Implementation and Results



The image shows a Wireshark network traffic capture. The main pane displays a list of captured packets with columns for No., Time, Source, Destination, Protocol, and Info. The packets include EIGRP Hello messages, NBNS Name queries, and ARP requests. The packet list is as follows:

No.	Time	Source	Destination	Protocol	Info
113	49.387009	192.168.2.1	224.0.0.10	EIGRP	Hello
114	50.438077	192.168.2.5	192.168.2.255	NBNS	Name query NB ITPROG<00>
115	51.183338	192.168.2.5	192.168.2.255	NBNS	Name query NB ITPROG<00>
116	51.638150	192.168.2.2	224.0.0.10	EIGRP	Hello
117	51.753114	192.168.2.3	192.168.2.255	NBNS	Name query NB VIRAZOLE.HH.SE<00>
118	51.933339	192.168.2.5	192.168.2.255	NBNS	Name query NB ITPROG<00>
119	52.501046	192.168.2.3	192.168.2.255	NBNS	Name query NB VIRAZOLE.HH.SE<00>
120	53.251121	192.168.2.3	192.168.2.255	NBNS	Name query NB VIRAZOLE.HH.SE<00>
121	54.007108	192.168.2.3	192.168.2.255	NBNS	Name query NB VIRAZOLE<00>
122	54.110584	192.168.2.1	224.0.0.10	EIGRP	Hello
123	54.751085	192.168.2.3	192.168.2.255	NBNS	Name query NB VIRAZOLE<00>
124	54.953821	00:1c:f6:2f:54:64	00:1c:f6:2f:54:64	LOOP	Reply
125	55.501102	192.168.2.3	192.168.2.255	NBNS	Name query NB VIRAZOLE<00>
126	56.273959	Dell_55:25:d1	Broadcast	ARP	who has 192.168.2.1? Tell 192.168.2.3
127	56.341642	192.168.2.2	224.0.0.10	EIGRP	Hello
128	58.382197	192.168.2.1	224.0.0.10	EIGRP	Hello
129	59.282404	Dell_55:25:d1	Broadcast	ARP	who has 192.168.2.1? Tell 192.168.2.3
130	60.937154	192.168.2.2	224.0.0.10	EIGRP	Hello

The packet details pane for Frame 1 (92 bytes on wire, 92 bytes captured) shows the following layers:

- Ethernet II, Src: Dell_55:25:d1 (00:14:22:55:25:d1), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
- Internet Protocol, Src: 192.168.2.3 (192.168.2.3), Dst: 192.168.2.255 (192.168.2.255)
- User Datagram Protocol, Src Port: netbios-ns (137), Dst Port: netbios-ns (137)
- NetBIOS Name Service

Figure 5.2 Sniffing data across the network using Wireshark with security

5.5 Mitigation of Ping Sweeps

With ping sweep scanning tool, an intruder will get the IP addresses that are alive in the network. It is done by sending an ICMP ping to a range of IP addresses and if any host sends an ICMP echo replay, it is considered that the IP address is active. Ping sweeps can be mitigated by turning off the ICMP and ICMP echo replay which will lead to compromise the network capabilities.

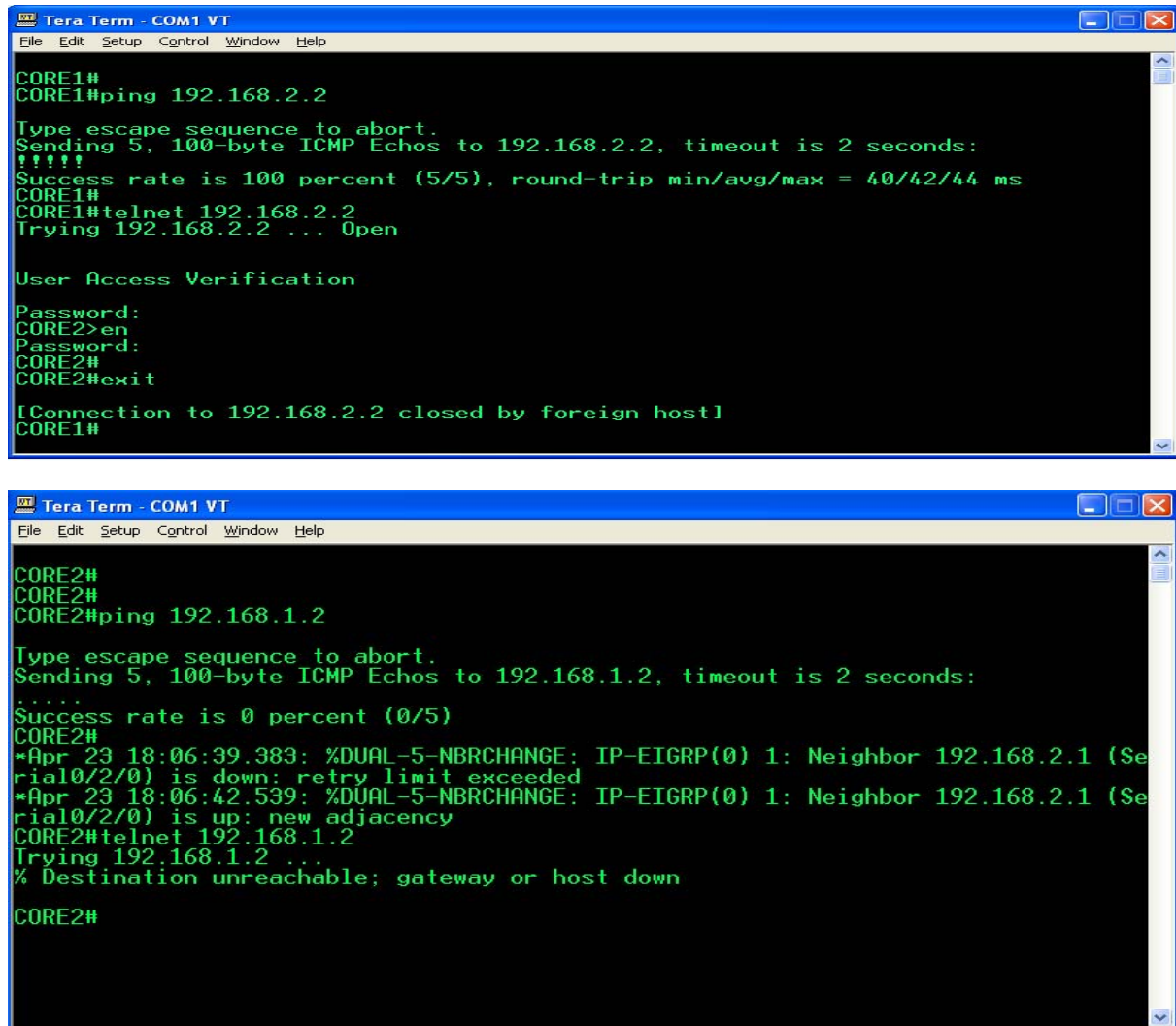
This step shows how to mitigate ping sweep with help of CBACS (Content Based Access Control Lists)/Classical firewall without turning off ICMP echo replay. CBACS is a stateful packet inspection system which specifies what traffic needs to be let in and what traffic needs to be let out by using access lists. What CBACS if configured in a router, it inspects the data, that is initiated from inside to reach outside network. The inspection rule will block any uninvited data what data is returning from outside to inside.

In this demonstration we will show that users from CORE1 can ping the CORE2 router, but users from CORE2 cannot ping CORE1 even there is a direct connection between them. Intruders between these two routers cannot find the IP address of the CORE1 because CBACS does not allow the data that is other than the data of CORE1. See Appendix E for configurations.

Implementation and Results

5.5.1 Results

The following results are obtained after configuring the CBACS between the routers



The figure consists of two screenshots of a Tera Term window, which is a terminal emulator. The top screenshot shows the command prompt for CORE1. The user enters 'ping 192.168.2.2', and the output shows a successful ping with a 100 percent success rate and round-trip times of 40/42/44 ms. Then, the user enters 'telnet 192.168.2.2', and the output shows a successful connection to CORE2. The bottom screenshot shows the command prompt for CORE2. The user enters 'ping 192.168.1.2', and the output shows a failed ping with a 0 percent success rate. Then, the user enters 'telnet 192.168.1.2', and the output shows a failed connection with the message '% Destination unreachable; gateway or host down'.

```
Tera Term - COM1 VT
File Edit Setup Control Window Help

CORE1#
CORE1#ping 192.168.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/42/44 ms
CORE1#
CORE1#telnet 192.168.2.2
Trying 192.168.2.2 ... Open

User Access Verification
Password:
CORE2>en
Password:
CORE2#
CORE2#exit

[Connection to 192.168.2.2 closed by foreign host]
CORE1#

Tera Term - COM1 VT
File Edit Setup Control Window Help

CORE2#
CORE2#
CORE2#ping 192.168.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
CORE2#
*Apr 23 18:06:39.383: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 192.168.2.1 (Se
rial0/2/0) is down: retry limit exceeded
*Apr 23 18:06:42.539: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 192.168.2.1 (Se
rial0/2/0) is up: new adjacency
CORE2#telnet 192.168.1.2
Trying 192.168.1.2 ...
% Destination unreachable; gateway or host down

CORE2#
```

Figure 5.3 Results of CBAC configuration

Looking at the above figures, it is clear that CORE1 can ping and telnet the CORE2 Whereas CORE2 tried to ping the CORE1 but it was unsuccessful.

5.6 Mitigation of Port Scans

Port scans allow an intruder to find open ports and services that are active on the live IP address. An intruder will use the information from port scanning for executing an actual attack on the target network. So it is important to mitigate this attack. By using Cisco IOS Firewall, we can mitigate the port scanning.

Primary goal of this step is to protect router CORE1 so that an intruder cannot execute the port scanning attack and find the details of the network. The router CORE1 is configured with Cisco IOS Firewall and Access list using Cisco Security Device Manager (SDM). Firewall helps to ensure the network availability and the security of the router against network attacks. Access list specified in the configuration is used as a packet filtering.

In this demonstration data passing through CORE1 router is scanned with the help of Nmap, an open source utility for security auditing or network exploration, for finding open ports. We will again scan the network after configuring firewalls. Both the results are analyzed to show the mitigation of port scan attack. See Appendix F for configurations of Firewall and ACL.

5.6.1 Results

The following figure shows the scanning result of the CORE1 router without security.

Port		State	Service	Reason	Product
23	tcp	open	telnet	syn-ack	Cisco router
80	tcp	open	http	syn-ack	Cisco IOS administrative httpd
67	udp	open filtered		no-response	
68	udp	open filtered		no-response	
1701	udp	open filtered		no-response	

Figure 5.4 Result of Nmap scanning

Form the above figure we can observe the ports that are open and the services which are using by theses open ports. It also shows the reason why these ports are open and the product of the device.

After configuring Firewall, the scan result does not show any information regarding the ports, whether the ports are open or closed which mean that the ports are protected by the Firewall.

5.7 Mitigation of Internet Information Queries

Internet Information Queries are used to get information about a website or an organization. DNS are the main source to get information like who owns the domain and what address is assigned to that domain. After getting the domain name and IP address, the intruder can execute an actual attack later. For demonstrating this attack WHOIS, an internet tool, is used to query the university website 'hh.se' and results are observed.

5.7.1 Result

The following table shows the result of WHOIS for hh.se

Canonical name	hh.se
Address	194.47.12.29
State	Active
Domain	hh.se
Created	1990-09-05
Modified	2009-12-31
Expires	2010-12-31
Nserver	Lundns.lu.se
Status	Ok
Register	SE Direkt

Table 5.1 Domain WHOIS record for hh.se

From the above table we can see the domain name, IP address, date of creation and so on for the website hh.se. This information can be used to perform an attack. There are no mitigation techniques to mitigate these queries. When giving information to DNS only limited or certain information which does not cause harm has to be given.

Implementation and Results

6 Conclusion

This thesis presented a way to build a secured network. All the attacks that are present in the network are studied and different mitigation techniques are discussed to mitigate the attacks. A research is made on how to perform risk analysis and the two different ways are discussed to perform the risk analysis. This thesis also explained how to design security policies to achieve organizations goals with the help of security services and security mechanisms.

The goal of the thesis is achieved where a network is practically built for the mitigation of reconnaissance attacks. The results of the thesis clearly show that a network cannot be protected completely without compromising the network features but the attacks are mitigated. This work can be further carried to build a secure network that can have all the features without compromising network capabilities.

Conclusion

7 References

- [1] Duane De Capite, “Self-Defending Networks: The Next Generation of Network Security”, Cisco Systems, Inc., September 2006.
- [2] Angela Orebaugh and Becky Pinkard, “Nmap in the Enterprise: Your Guide to Network Scanning” Syngress Publishing, Inc, January 2008.
- [3] Cisco Systems, “Implementing Secure Converged Wide Area Networks (ISCW)” Volume 2. Cisco Press, August 2006.
- [4] Richard A. Dea, “Cisco Router Firewall Security” Cisco Press, August 2004.
- [5] Sabeel Ansari, Rajeev S.G and Chandrashekar H.S., “Packet Sniffing: A Brief Introduction” IEEE Xplore, December 2002/January 2003.
- [6] Jayant Gadge and Anish Anand Patil, “Port Scan Detection”, IEEE Xplore, November 2008.
- [7] Fu-Hau Hsu, Fanglu and Tzi-Chiueh, “Scalable Network-based Buffer Overflow Attack Detection, IEEE Xplore, May 2008.
- [8] International std BS ISO/IEC 27005-2008, “Information technology- Security techniques- Information security risk management” First edition, June 2008.
- [9] Gary Stonebumer, Alice Goguen, and Alexis Feringa, “Risk Management Guide for Information Technology Systems”, Recommendations of the National Institute of Standards and Technology, July 2002.
- [10] Thomas R. Peltier, “Information Security Risk Analysis”, Auerbach Publications, ISBN 0-8493-0880-1, 2005.
- [11] Network Working Group, “Site Security Handbook”, RFC-2196, September 1997
- [12] Saadat Malik, “Network Security Principles and Practices”, Cisco Press, ISBN 1-58705-025-0, November 2002.
- [13] Manuel Mogollon, “Cryptography and Security Services: Mechanisms and applications”, Cybertech Publishing, New York, 2007
- [14] Douglas W. Frye, “Network Security Policies and Procedures” Springer, 2007

References

8 Appendix

Appendix A: EIGRP

EIGRP is configured on all routers.

```
router eigrp 1
 network 10.0.0.0 0.0.255.255
 network 192.168.1.0
 no auto-summary
```

Appendix B: VLAN

Configurations for all VLANS

```
interface Vlan10
 ip address 10.0.10.2 255.255.255.0
 no ip redirects
 !
interface Vlan20
 ip address 10.0.20.2 255.255.255.0
 no ip redirects
 !
interface Vlan30
 ip address 10.0.30.2 255.255.255.0
 no ip redirects
 !
interface Vlan40
 ip address 10.0.40.2 255.255.255.0
 no ip redirects
```

Appendix C: HSRP

Configuration of HSRP

```
standby 1 ip 10.0.10.1
standby 1 priority 150
standby 1 preempt
!
standby 1 ip 10.0.20.1
standby 1 priority 150
standby 1 preempt
```


Appendix

!

```
standby 1 ip 10.0.30.1
standby 1 priority 150
standby 1 preempt
```

!

```
standby 1 ip 10.0.40.1
standby 1 priority 150
standby 1 preempt
```

Appendix D: IPSec VPN

This configuration should be configured on both routers. It should be exactly the same, otherwise connection will not form.

```
crypto isakmp policy 10
authentication pre-share
enc aes
hash sha
group 5
crypto isakmp key 0 sharedsecret address <it should be IP of other side>
crypto ipsec transform-set mytrans esp-aes esp-sha-hmac
crypto map mymap 10 ipsec-isakmp
set peer <address of other side>
match address 101
set transform-set mytrans
interface fastethernet 0/1
ip address 192.168.2.1 255.255.255.0
crypto map mymap
access-list 101 permit ip <source network> <source network-mask> <destination network>
<destination network-mask>
```

Appendix E: CBACS

Check where to apply rules. Inside network will be allowed to reach outside network but outside network will not be allowed to get inside the network.

First inspection rule is needed.

```
ip inspect name CBAC telnet
ip inspect name CBAC tcp
ip inspect name CBAC udp
ip inspect name CBAC icmp
interface fastethernet 0/0
ip inspect CBAC in
```

Appendix

Next step is apply tough access list on outside interface.

```
access-list 101 deny ip any any
```

```
interface fastethernet 0/1
```

```
ip access-group 101 in
```

Appendix F: Firewall and ACL

Configuration for Firewall and ACL

```
!
```

```
ip domain name THESIS
```

```
ip name-server 200.200.20.2
```

```
ip ssh time-out 60
```

```
ip inspect log drop-pkt
```

```
ip inspect name SDM_HIGH appfw SDM_HIGH
```

```
ip inspect name SDM_HIGH http
```

```
ip inspect name SDM_HIGH icmp
```

```
ip inspect name SDM_HIGH dns
```

```
ip inspect name SDM_HIGH esmtp
```

```
ip inspect name SDM_HIGH https
```

```
ip inspect name SDM_HIGH imap reset
```

```
ip inspect name SDM_HIGH pop3 reset
```

```
ip inspect name SDM_HIGH tcp
```

```
ip inspect name SDM_HIGH udp
```

```
!
```

```
!
```

```
access-list 100 remark auto generated by SDM firewall configuration
```

```
access-list 100 remark SDM_ACL Category=1
```

```
access-list 100 deny ip 10.0.1.0 0.0.0.255 any
```

```
access-list 100 deny ip 192.168.1.0 0.0.0.255 any
```

```
access-list 100 deny ip host 255.255.255.255 any
```

```
access-list 100 deny ip 127.0.0.0 0.255.255.255 any
```

```
access-list 100 permit ip any any
```

```
access-list 101 remark auto generated by SDM firewall configuration
```

```
access-list 101 remark SDM_ACL Category=1
```

```
access-list 101 deny ip 192.168.1.0 0.0.0.255 any
```

```
access-list 101 deny ip 10.0.4.0 0.0.0.255 any
```

```
access-list 101 deny ip host 255.255.255.255 any
```

```
access-list 101 deny ip 127.0.0.0 0.255.255.255 any
```

```
access-list 101 permit ip any any
```

Appendix

```
access-list 102 remark auto generated by SDM firewall configuration
access-list 102 remark SDM_ACL Category=1
access-list 102 deny ip 10.0.1.0 0.0.0.255 any
access-list 102 deny ip 10.0.4.0 0.0.0.255 any
access-list 102 permit icmp any host 192.168.1.2 echo-reply
access-list 102 permit icmp any host 192.168.1.2 time-exceeded
access-list 102 permit icmp any host 192.168.1.2 unreachable
access-list 102 deny ip 10.0.0.0 0.255.255.255 any
access-list 102 deny ip 172.16.0.0 0.15.255.255 any
access-list 102 deny ip 192.168.0.0 0.0.255.255 any
access-list 102 deny ip 127.0.0.0 0.255.255.255 any
access-list 102 deny ip host 255.255.255.255 any
access-list 102 deny ip host 0.0.0.0 any
access-list 102 deny ip any any log
!
```