LABORATORY MANUAL

ON

NETWORK SECURITY LAB

(For 6th Semester CSE/IT)

Prepared by:

Smt Reetanjali Panda
Lecturer(CSE&IT)
UCP Engineering School
Berhampur.

Miss Sasmita Panigrahi
PTGF(CSE&IT)
UCP Engineering School
Berhampur.

EXPERIMENT-1 Installation and comparison of various anti virus software

Antivirus software is one of the most important pieces of software that should be installed on every computer since it helps prevent viruses and malware from infecting it. Your computer will be slower than it was previously If your computer has been infected with a virus. On the Internet, there are thousands of spyware andviruses that can be more harmful to you in order to damage personal files or the computer's operating system. If you are running your computer system without installing an antivirus program, it is highly recommended you install an antivirus to keep running your computer in safe mode. To download and install software, including upgrading an antivirus application on your computer, follow the instructions below. It will keep your files safe from the most recent viruses. To help protect a computer from viruses, all new versions of Microsoft Windows contain a feature, Windows Defender, which serves as an antivirus program.

Install the antivirus program

- If you bought antivirus software on a CD or DVD from a store, you must first put the CD or DVD into your computer's disc drive. However, in any case, you can also get the program set up in your USB drive, like Pen drive. When you install the program, through the install process, a window will open that helps guide you, and the installation process should start automatically.
- If you did not buy a CD or DVD and instead downloaded an antivirus application from the Internet, you must now locate the downloaded file on your computer. If you downloaded the zip file for the program setup, you are required to unzip the file to access the installation files. Then, find the file that has a name like install.exe, setup.exe, or a similar name, and double-click on that file to start the installation process of the antivirus program. When you install the program, through the install process, a window will

open that helps guide you, and the installation process should start automatically.

Follow the steps for installing the antivirus program in the installation process window.

- The recommended options are provided by the install process, which helps the antivirus program to work properly. There is one exception that the install process recommends installing any helpful program for your computer or any toolbar for the Internet browser. Whenever you are installing an antivirus program and if prompted to install other software, in this condition, you need to decline the install of those other programs or uncheck all boxes. Also, the antivirus program does not require any additional software to install and run successfully on the computer.
- Close out the install window when you have completed the installation process of an antivirus.
- If you installed the software with a CD or DVD, remove it from the computer's disc drive.
- After following all the above steps, the antivirus program will be installed successfully and ready to use. Restart your computer system; however, it is not required. However, if you restart the computer, any changes to the operating system will be applied appropriately.

Once Installed, Scan for Viruses

You will need to scan your system for finding threats in your computer after you installed antivirus software. Mainly, three kinds of scan options are provided by most security suites, either manual or automatic. A different depth of inspection is offered bythree scan options.

Quick Scan: Usually, a quick scan only checks the common areas where are most chances to be infected, and it takes around 10 to 20 minutes. In this mode of the scan, the scanner passes around most of your network that reduces processing power but increases speed; therefore, you need to leave your computer alone at the time it is running. This option is often appropriate for highlighting any problems.

Full Scan: If you have quickly scanned your computer, you are still encountering the problem of viruses. Then, you must go for

a full scan. The full scan option examines all areas of your computer system to identify if there is no virus; however, it can take more time, even many hours, to complete. In a quick scan, the spyware or other complex malware threats may not be obvious. They need an in-depth check to uncover. Although a full scan option is a slow process, it provides surety your system has not any kind of threats.

A Scheduled Scan: The schedule scan option provides real-time security for your computer by scanning files for viruses as you use them.

Update the antivirus program after installation

- Antivirus applications that come out of the box don't have the latest spyware and virus definitions and are not up to date. The antivirus software will work improperly and not know about the recently created spyware and viruses, which makes your computer insecure and vulnerable to infection.
- It is advised that you update your antivirus application with the most recent virus and spyware definitions after it has been installed on your computer. Your antivirus application will safeguard your computer from all viruses and malware if you maintain it up to date.
- The antivirus program, in many cases, checks and installs the current updates automatically If you are offered to pick an antivirus update automatically, choose Yes to update your antivirus application. If it does not urge you to update automatically, you must do it right away.

Enable automatic updates for the antivirus program

- Generally, most antivirus applications have the automatic update function activated by default. It is strongly recommended, you must keep your antivirus program up-to-date at all times; therefore, automatic updates feature should be enabled in your antivirus program settings.
- The procedures outlined below will assist you in determining whether or not automatic updates are enabled in your antivirus application.
- First, you need to open the antivirus program.

- Locate the Settings or Advanced Settings button or link in the antivirus program's interface. If you are unable to see such an option, you can find Updates or something similar options.
- Now, in the Updates or Settings box, look for an option called Automatically download and apply updates. Also, instead of updates, it may refer to virus definitions.
- Next, check if the automatic updates option is checked or not; check it for automatic update the program if not already checked.
- Finally, click on the Apply or Save button to save the settings that you made changes to.

Various types of Anti viruses:

Norton 360 with LifeLock keeps improving on its history as a top antivirus option with its PC maintenance features, making it the best for Windows computers.

Pros

- PC protections including firewall and backup
- Excellent malware protection
- Password manager
- LifeLock identity theft protection

Cons

- Ransomware detection could be improved
- Slows the computer during full scans
- One of the more expensive offerings

Norton introduced its first antivirus software in 1991 under the Symantec umbrella.

McAfee Antivirus Plus is our top choice for multiple devices because its subscriptions offer protection for every device in the home for a reasonable cost.

Pros

- Offers protection for all devices, including Android and iOS
- Good malware detection
- Offers a number of deals for the product
- Good firewall

Cons

- No options for protecting one single device

McAfee Antivirus Plus is the one antivirus platform that recognizes the growing number of devices used in a single household, which could include four or more different operating systems.

The basic package supports up to 10 devices, support, secure web browsing, and antivirus. The MTP 10 Device plan is for one year for 10 devices, but also includes features such as full protection for the home network, password manager, encrypted storage, firewall booster, and identity theft protection.

Trend Micro Antivirus+ Security has an aggressive antivirus system at a reasonable price, making it our pick for best for premium options.

Pros

- Affordable pricing
- Easy-to-use dashboard
- Protects online financial transactions

Cons

- Resource intensive
- Most versions only work on Windows

Malwarebytes: Used for malware scanning, Malwarebytes, is the best at removing malware on demand among any providers.

Pros

- Removes malware
- Blocks ransomware
- Real-time detection

Cons

- Free version has a lot less protection and features

Webroot: SecureAnywhere for Mac offers excellent phishing detection and fast scanning ability specifically designed for Macs.

Pros

- Excellent phishing detection
- Fast virus scanning
- Labels malicious links during online searches

Cons

- Webroot is not as well known as other antivirus companies

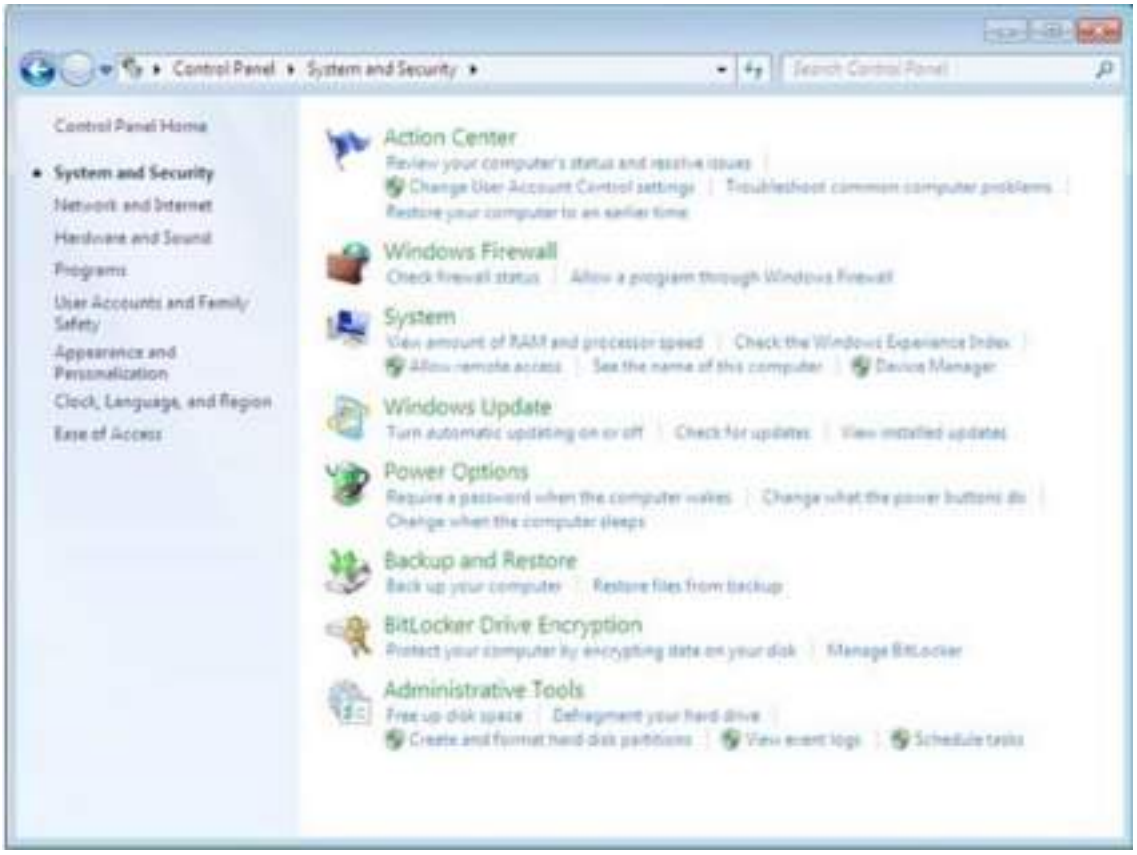
EXPERIMENT-2 : Installation and study of various parameters of firewall.

- A firewall policy defines how an organization's firewalls should handle inbound and outbound network traffic for specific IP addresses and address ranges, protocols, applications, and content types based on the organization's information security policies.

Setting Up a Firewall:

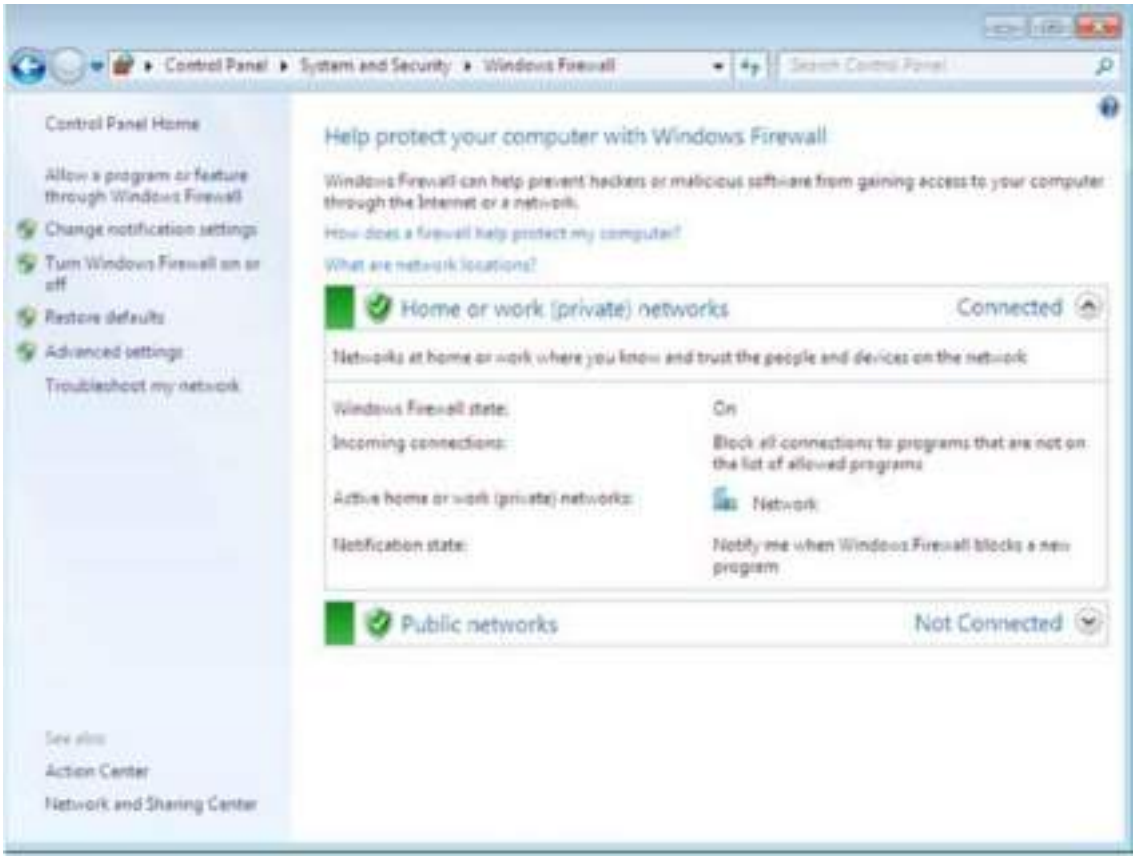
1. Set up System and Security Setting

- From the Start menu, click **Control Panel**, then click **System and Security**
- Under Windows Firewall, select either **Check firewall status** to determine whether the firewall is turned on or off, or **Allow a program through Windows Firewall** to allow a blocked program through the firewall



2. Select Program features

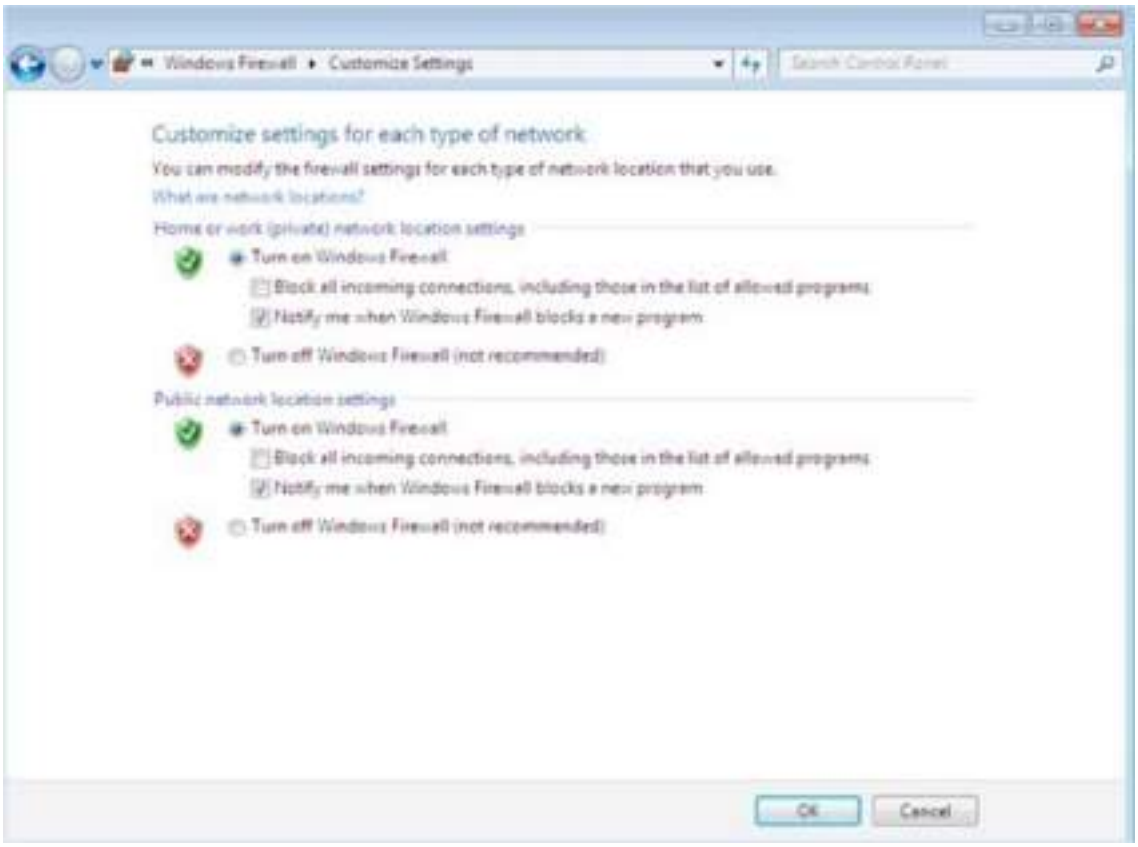
- Click **Turn Windows Firewall on or off** from the left side menu
- Configure the settings for your home/work (private) or public network
- Click **OK** to save your changes



3. Choose firewall settings for different network location types

Turn on Windows Firewall for each network location you use - **Home or work (private)** or **Public**

- Click **What are network locations?** for more information on network types
- Domain network locations are controlled by your network administratorand can't be selected or changed
- Select **Turn on Windows Firewall** under the applicable network location type (in image below, both locations are selected)
- Select **Notify me when Windows Firewall blocks a new program** for each network type, if the box is not already checked
- Click **OK** to save your changes



- A basic guide to configure a firewall in 5 steps: create zones, configure settings, and review firewall rules.
- As the first line of defense against online attackers, your firewall is a critical part of your network security. Configuring a firewall can be an intimidating project, but breaking it down into simpler tasks can make the work much more manageable. The following steps will help you understand the major steps involved in firewall configuration.
- There are many suitable firewall models that can be used to protect your network. You can consult a HIPAA security expert or PCI security expert to learn more about your options. The following steps are critical, regardless of the firewall model you choose. This guide assumes that you are using a business grade firewall that supports multiple internal networks (or zones) and performs stateful packet inspection.
- Due to the technical nature of firewalls, a detailed step-by-step guide is beyond the scope of this blog post. However, I will provide some direction to help illustrate the process so you can understand how to configure a firewall in 5 steps.
- Step 1: Secure your firewall
- If an attacker is able to gain administrative access to your firewall it is “game over” for your network security. Therefore, securing your firewallis the first and most important step of this process. Never put a firewall

into production that is not properly secured by at least the following configuration actions:

- Update your firewall to the latest firmware.
- Delete, disable, or rename any default user accounts and change all default passwords. Make sure to use only complex and secure passwords.
- If multiple administrators will manage the firewall, create additional administrator accounts with limited privileges based on responsibilities. Never use shared user accounts.
- Disable simple network management protocol (SNMP) or configure it to use a secure community string.
- Step 2: Architect your firewall zones and IP addresses
- In order to protect the valuable assets on your network, you should first identify what the assets are (for example, payment card data or patient data). Then plan out your network structure so that these assets can be grouped together and placed into networks (or zones) based on similar sensitivity level and function.
- For example, all of your servers that provide services over the internet (web servers, email servers, virtual private network (VPN) servers, etc.) should be placed into a dedicated zone that will allow limited inbound traffic from the internet (this zone is often called a demilitarized zone or DMZ). Servers that should not be accessed directly from the internet, such as database servers, must be placed in internal server zones instead. Likewise, workstations, point of sale devices, and voice over Internet protocol (VOIP) systems can usually be placed in internal network zones.
- Generally speaking, the more zones you create, the more secure your network. But keep in mind that managing more zones requires additional time and resources, so you need to be careful when deciding how many network zones you want to use.
- If you are using IP version 4, Internal IP addresses should be used forall of your internal networks. Network address translation (NAT) must be configured to allow internal devices to communicate on the Internet whennecessary.
- Once you have designed your network zone structure and established the corresponding IP address scheme, you are ready to create your firewall zones and assign them to your firewall interfaces or subinterfaces. As you build out your network infrastructure, switches that support virtual LANs (VLANs) should be used to maintain level-2 separation between the networks.
- Step 3: Configure access control lists
- Now that you have established your network zones and assigned them to interfaces, you should determine exactly which traffic needs to be able to flow into and out of each zone.
- This traffic will be permitted using firewall rules called access control lists (ACLs), which are applied to each interface or subinterface on the

firewall. Make your ACLs specific to the exact source and/or destination IP addresses and port numbers whenever possible. At the end of every access control list, make sure there is a “deny all” rule to filter out all unapproved traffic. Apply both inbound and outbound ACLs to each interface and subinterface on your firewall so that only approved traffic is allowed into and out of each zone.

- Whenever possible, it is generally advised to disable your firewall administration interfaces (including both secure shell (SSH) and web interfaces) from public access. This will help to protect your firewallconfiguration from outside threats. Make sure to disable all unencrypted protocols for firewall management, including Telnet and HTTP connections.
- Step 4: Configure your other firewall services and logging
- If your firewall is also capable of acting as a dynamic host configuration protocol (DHCP) server, network time protocol (NTP) server, intrusion prevention system (IPS), etc., then go ahead and configure the services you wish to use. Disable all the extra services that you don’t intend to use.
- To fulfill PCI DSS requirements, configure your firewall to report to your logging server, and make sure that enough detail is included to satisfy requirement 10.2 through 10.3 of the PCI DSS.
- SEE ALSO: Understanding the HIPAA Application of Firewalls
- Step 5: Test your firewall configuration
- In a test environment, verify that your firewall works as intended. Don’t forget to verify that your firewall is blocking traffic that should be blocked according to your ACL configurations. Testing your firewall should include both vulnerability scanning and penetration testing.
- Once you have finished testing your firewall, your firewall should be ready for production. Always remember to keep a backup of your firewall configuration saved in a secure place so that all of your hard work is not lost in the event of a hardware failure.
- Remember, this is just an overview to help you understand the major steps of firewall configuration. When using tutorials, or even if you decide to configure your own firewall, be sure to have a security expert review your configuration to make sure it is set up to keep your data as safe as possible.
- Firewall management
- With your firewall in production, you have finished your firewall configuration, but firewall management has just begun. Logs must be monitored, firmware must be updated, vulnerability scans must be performed, and firewall rules must be reviewed at least every six months. Last of all, be sure to document your process and be diligent about performing these ongoing tasks to ensure that your firewall continues to protect your network.
- Block by default

- Block all traffic by default and explicitly enable only specific traffic to known services. This strategy provides good control over the traffic and reduces the possibility of a breach because of service misconfiguration.
- You achieve this behavior by configuring the last rule in an accesscontrol list to deny all traffic. You can do this explicitly or implicitly, depending on the platform.
- Allow specific traffic
- The rules that you use to define network access should be as specific as possible. This strategy is the *principle of least privilege*, and it forces control over network traffic. Specify as many parameters as possible in the rules.
- A layer 4 firewall uses the following parameters for an access rule:
- Source IP address (or range of IP addresses)
- Destination IP address (or range of IP addresses)
- Destination port (or range of ports)
- Protocol of the traffic (TCP, ICMP, or UDP)
- Specify as many parameters as possible in the rule used to define network access. There are limited scenarios where any is used in any of these fields.
- Specify source IP addresses
- If the service should be accessible to everyone on the Internet,then *any* source IP address is the correct option. In all other cases, you should specify the source address.
- It's acceptable to enable all source addresses to access your HTTP server. It's not acceptable to enable all source addresses to access your server management ports or database ports. The following is a list of common server management ports and database ports:
- Server management ports:
- Linux®SSH : Port 22
- Windows® RDP: Port 3389
- Database ports:
- SQL® Server : Port 1433
- Oracle® : Port 1521
- MySQL® : Port 2206
- Be specific about who can reach these ports. When it is impractical to define source IP addresses for network management, you might consider another solution like a remote access VPN as a compensating control to allow the access required and protect your network.
- Specify the destination IP address
- The destination IP address is the IP address of the server that runs the service to which you want to enable access. Always specify which server or servers are accessible. Configuring a destination value of any could lead to a security breach or server compromise of an unused protocol that might be accessible by default. However, destination IPs with a destination value of any can be used if there is only one IP assigned to

the firewall. The value any can also be used if you want both public and servicenet access to your configuration.

- Specify the destination port
- The destination port corresponds to the accessible service. This value of this field should never be any. The service that runs on the server and needs to be accessed is defined, and only this port needs to be allowed. Allowing all ports affects the security of the server by allowing dictionary attacks as well as exploits of any port and protocol that is configured on the server.
- Avoid using too wide a range of ports. If dynamic ports are used, firewalls sometimes offer inspection policies to securely allow them through.
- Examples of dangerous configurations
- This section describes dangerous examples of firewall rules, but also shows some alternative good rules to follow when configuring firewall rules.
- permit ip any any - Allows all traffic from any source on any port to any destination. This is the worst type of access control rule. It contradicts both of the security concepts of denying traffic by default and the principal of least privilege. The destination port should be always specified, and the destination IP address should be specified when practical. The source IP address should be specified unless the app is built to receive clients from the Internet, such as a web server. A good rule would be permit tcp any WEB-SERVER1 http.
- permit ip any any WEB-SERVER1 - Allows all traffic from any source to a web server. Only specific ports should be allowed; in the case of a web server, ports 80 (HTTP) and 443 (HTTPS). Otherwise, the management of the server is vulnerable. A good rule would be permit ip any WEB- SERVER1 http.
- permit tcp any WEB-SERVER1 3389 - Allows RDP access from any source to the web server. It is a dangerous practice to allow everyone access to your management ports. Be specific about who can access the server management. A good rule would be permit tcp 12.34.56.78 3389 WEB-SERVER1 (where 12.34.56.78 is the IP address of the administrator's computer on the Internet).
- permit tcp any DB-SERVER1 3306 - Allows MySQL access from any source to the database. Database servers should never be exposed to the whole Internet. If you need database queries to run across the public Internet, specify the exact source IP address. A good rule would be permit tcp 23.45.67.89 DB-SERVER1 3306 (where 23.45.67.89 is the IP address of the host on the Internet that needs access to the database). A best practice would be to allow database traffic over a VPN and not in clear text across the public Internet.

EXPERIMENT-3 Writing program in C to Encrypt/Decryptusing XOR key.

- XOR Encryption is an encryption method used to encrypt data and ishard to crack by brute-force method, i.e generating random encryption keys to match with the correct one.

```
#include<bits/stdc++.h>

// The same function is used to encrypt and

// decrypt

void encryptDecrypt(char inpString[])

{

    // Define XOR key

    // Any character value will work

    char xorKey = 'P';

    // calculate length of input string

    int len = strlen(inpString);

    // perform XOR operation of key

    // with every character in string

    for (int i = 0; i < len; i++)

    {

        inpString[i] = inpString[i] ^ xorKey;

        printf("%c",inpString[i]);

    }

}

// Driver program to test above function
```

```
int main()
{
    char sampleString[] = "UCPES";


    // Encrypt the string
    printf("Encrypted String: ");
    encryptDecrypt(sampleString);
    printf("\n");
     // Decrypt the string
    printf("Decrypted String: ");
    encryptDecrypt(sampleString);
    return 0;
}
```

- The basic idea behind XOR – encryption is, if you don't know the XOR-encryption key before decrypting the encrypted data, it is impossible to decrypt the data. For example, if you XOR two unknown variables you cannot tell what the output of those variables is. Consider the operation A XOR B, and this returns true. Now if the value of one of the variable is known we can tellthe value of another variable. If A is True then B should be Falseor if A is False then B should be true according to the properties of the boolean XOR operation. Without knowing one of the value we can not decrypt the data and this idea is used in XOR – encryption.

EXPERIMENT-4 Study of VPN.

VPN stands for "Virtual Private Network" and describes the opportunity to establish a protected network connection when using public networks. VPNs encrypt your internet traffic and disguise your online identity. This makes it more difficult for third parties to track your activities online and steal data. The encryption takes place in real time.

How does a VPN work?

A VPN hides your IP address by letting the network redirect it through a specially configured remote server run by a VPN host.This means that if you surf online with a VPN, the VPN server becomes the source of your data. This means your Internet Service Provider (ISP) and other third parties cannot see which websites you visit or what data you send and receive online. A VPN works like a filter that turns all your data into "gibberish". Even if someone were to get their hands on your data, it would beuseless.

What are the benefits of a VPN connection?

A VPN connection disguises your data traffic online and protects it from external access. Unencrypted data can be viewed by anyone who has network access and wants to see it. With a VPN,hackers and cyber criminals can’t decipher this data.

Secure encryption: To read the data, you need an encryption key

. Without one, it would take millions of years for a computer to decipher the code in the event of a brute force attack . With the help of a VPN, your online activities are hidden even on public networks.

Disguising your whereabouts : VPN servers essentially act as your proxies on the internet. Because the demographic location data comes from a server in another country, your actual location cannot be determined. In addition, most VPN services do not store logs of your activities. Some providers, on the other hand,

record your behavior, but do not pass this information on to thirdparties. This means that any potential record of your user behaviorremains permanently hidden.

Access to regional content: Regional web content is not always accessible from everywhere. Services and websites often contain content that can only be accessed from certain parts of the world. Standard connections use local servers in the country to determine your location. This means that you cannot access content at home while traveling, and you cannot access international content from home. With VPN location spoofing , you can switch to a server to another country and effectively "change" your location.

Secure data transfer: If you work remotely, you may need to access important files on your company's network. For security reasons, this kind of information requires a secure connection. Togain access to the network, a VPN connection is often required. VPN services connect to private servers and use encryption methods to reduce the risk of data leakage.

Security is compulsory in today's generation because of emergingthreats initiated by hackers ready to compromise your network and resources. There are three states of data that we need to protect – data at rest, data in use, and data in transit. Data in transit is more vulnerable to attacks as the data will travel outside your protected network. The best and cheapest option to protect our data in transit is by using Virtual Private Network (VPN). Cisco VPN solutions are offered as well.

Why Do We Need VPN?

A Virtual Private Network (VPN) is an encrypted tunnel between two or more devices, usually a firewall, such as the Cisco Adaptive Security Appliance (Cisco ASA), over an unsecured network such as the internet. All the network traffic that is sent through the VPN tunnel will be encrypted and kept confidential from hackers on a network or the internet. VPN replaces the

dedicated point-to-point link with the emulated point-to-point link or secure connection that shares the common infrastructure. Using VPN will cost you nothing as it is completely free since most organizations have firewalls already installed with a built-in VPN feature. VPN also provides security for all the traffic that is sent outside your network through VPN tunnels. Lastly, VPN is scalable in that you can add unlimited tunnels and users.

Two Types of VPN

There are two types of VPN that we are commonly using, and both are secured but implemented and used in different ways.

1. Site-to-Site VPN

Organizations are continuously expanding into different branches, and to protect the data in transit between two branches, we need to implement a site-to-site VPN. Common VPN protocols used in site-to-site VPN are Internet Security Protocol (IPSec). In implementing this type of VPN, we need to set up the Phase 1 and Phase 2 VPN negotiations. IKE Phase 1 negotiation is where we create a secure encrypted channel or encrypted network connectivity for the two firewalls can start the Phase 2 negotiation.

In IKE Phase 2 negotiation, the two firewalls will agree on the configured parameters that define what traffic can go via the VPN tunnel and how to authenticate and encrypt the traffic. The agreement is called Security Association. Both Phase 1 and Phase2 should have the same parameters, such as pre-shared keys, authentication, encryption, and IKE version.

There are two ways to implement site-to-site VPN:

Intranet VPN – it provides secured site-to-site connectivity within the company or internally.

Extranet VPN – it provides secured site-to-site connectivity outside the company. For example, customers or partners can securely access the shared resources of the company.

The below image shows the Site-to-Site VPN implementation:

Site-to-Site VPN

2. Remote Access VPN

Commonly called a mobile VPN. Using this type of VPN connection permits the users to connect through the internet anywhere in the world to access the corporate network resourcessecurely. It can be used in a work-from-home setup where the employees can securely access the company's internal resources through a VPN. To implement this, the employee must install a VPN client, such as a Cisco anyconnect secure mobility client or Cisco anyconnect VPN client, to their device, and a virtual IP address will be assigned to the employee's device/PC that will beused to establish a secured tunnel.

Remote access VPN can use SSL, IKEv2, L2TP, and IPSec protocols. The most secure and easy to implement protocol is IKEv2. Some internet connections blocked the IKEv2 and L2TPprotocols. That is why some are using SSL VPN as it uses the typical HTTP/HTTPS traffic that is allowed on all internet connection types. IPSec for remote access VPN is not usually used, as there is already a known vulnerability on the protocol.

The system administrator can choose between two modes to implement the remote access VPN:

Full Tunnel – all the traffic that is coming out from the employee's device will go directly to the firewall, and the firewallwill forward it to the internet if necessary. This is a completely secured implementation as all the security services of the firewallwill be applied to all the traffic coming out from the employee's device.

Split Tunnel – the traffic that will go to the internet like HTTP/HTTPS traffic will go to the typical internet connection such as broadband/LTE, while the VPN traffic will be used to

access the internal resource of the company will use a VPNtunnel. The traffic will be split based on its purpose.

The below image shows the Remote Access VPN implementation:

Remote Access VPN

EXPERIMENT-5 Study of various hacking tools.

Ethical Hacking - Tools

1. NMAP

Nmap stands for Network Mapper. It is an open source tool that is used widely for network discovery and security auditing. Nmap was originally designed to scan large networks, but it can work equally well for single hosts. Network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.

Nmap uses raw IP packets to determine −what hosts

are available on the network, what services those

hosts are offering,

what operating systems they are running on,

what type of firewalls are in use, and other such characteristics.

Nmap runs on all major computer operating systems such asWindows, Mac OS X, and Linux.

2. Metasploit

Metasploit is one of the most powerful exploit tools. It's a productof Rapid7 and most of its resources can be found at:www.metasploit.com. It comes in two versions − commercial and free edition. Matasploit can be used with command prompt or with Web UI.

With Metasploit, you can perform the following operations −Conduct basic

penetration tests on small networks

Run spot checks on the exploitability of vulnerabilitiesDiscover the

network or import scan data

Browse exploit modules and run individual exploits on hosts

3. Burp Suit

Burp Suite is a popular platform that is widely used for performing security testing of web applications. It has various tools that work in collaboration to support the entire testing process, from initial mapping and analysis of an application's attack surface, through to finding and exploiting security vulnerabilities.

Burp is easy to use and provides the administrators full control tocombine advanced manual techniques with automation for efficient testing. Burp can be easily configured and it contains features to assist even the most experienced testers with their work.

4. Angry IP Scanner

Angry IP scanner is a lightweight, cross-platform IP address andport scanner. It can scan IP addresses in any range. It can be freelycopied and used anywhere. In order to increase the scanning

speed, it uses multithreaded approach, wherein a separate scanning thread is created for each scanned IP address.

Angry IP Scanner simply pings each IP address to check if it's alive, and then, it resolves its hostname, determines the MAC address, scans ports, etc. The amount of gathered data about eachhost can be saved to TXT, XML, CSV, or IP-Port list files. With help of plugins, Angry IP Scanner can gather any information about scanned IPs.

5. Cain & Abel

Cain & Abel is a password recovery tool for Microsoft OperatingSystems. It helps in easy recovery of various kinds of passwordsby employing any of the following methods −

sniffing the network,

cracking encrypted passwords using Dictionary, Brute-Force andCryptanalysis attacks,

recording VoIP conversations, decoding

scrambled passwords, recovering wireless

network keys,revealing password boxes,

uncovering cached passwords and analyzing routing protocols.

Cain & Abel is a useful tool for security consultants, professionalpenetration testers and everyone else who plans to use it for ethical reasons.

6. Ettercap

Ettercap stands for Ethernet Capture. It is a network security toolfor Man-in-the-Middle attacks. It features sniffing of live

connections, content filtering on the fly and many other interesting tricks. Ettercap has inbuilt features for network and host analysis. It supports active and passive dissection of many protocols.

You can run Ettercap on all the popular operating systems suchas Windows, Linux, and Mac OS X.

7. EtherPeek

EtherPeek is a wonderful tool that simplifies network analysis in a multiprotocol heterogeneous network environment. EtherPeek is a small tool (less than 2 MB) that can be easily installed in a matter of few minutes.

EtherPeek proactively sniffs traffic packets on a network. By default, EtherPeek supports protocols such as AppleTalk, IP, IP Address Resolution Protocol (ARP), NetWare, TCP, UDP, NetBEUI, and NBT packets.

8. SuperScan

SuperScan is a powerful tool for network administrators to scan TCP ports and resolve hostnames. It has a user friendly interfacethat you can use to −

Perform ping scans and port scans using any IP range. Scan any port range

from a built-in list or any given range.View responses from connected

hosts.

Modify the port list and port descriptions using the built in editor.Merge port lists to

build new ones.

Connect to any discovered open port.

Assign a custom helper application to any port.

9. QualysGuard

QualysGuard is an integrated suite of tools that can be utilized to simplify security operations and lower the cost of compliance. It delivers critical security intelligence on demand and automates the full spectrum of auditing, compliance and protection for IT systems and web applications.

QualysGuard includes a set of tools that can monitor, detect, andprotect your global network.

10. WebInspect

WebInspect is a web application security assessment tool that helps identify known and unknown vulnerabilities within the Web application layer.

It can also help check that a Web server is configured properly, and attempts common web attacks such as parameter injection, cross-site scripting, directory traversal, and more.

11. LC4

LC4 was formerly known as L0phtCrack. It is a password auditing and recovery application. It is used to test password strength and sometimes to recover lost Microsoft Windows passwords, by using dictionary, brute-force, and hybrid attacks.

LC4 recovers Windows user account passwords to streamline migration of users to another authentication system or to access accounts whose passwords are lost.

12. LANguard Network Security Scanner

LANguard Network Scanner monitors a network by scanning connected machines and providing information about each node. You can obtain information about each individual operating system.

It can also detect registry issues and have a report set up in HTML format. For each computer, you can list the netbios name table, current logged-on user, and Mac address.

13. Network Stumbler

Network stumbler is a WiFi scanner and monitoring tool for Windows. It allows network professionals to detect WLANs. It is widely used by networking enthusiasts and hackers because it helps you find non-broadcasting wireless networks.

Network Stumbler can be used to verify if a network is well configured, its signal strength or coverage, and detect interference between one or more wireless networks. It can also be used to non-authorized connections.

14. ToneLoc

ToneLoc stands for Tone Locator. It was a popular war dialling computer program written for MS-DOS in the early 90's. War dialling is a technique of using a modem to automatically scan a list of telephone numbers, usually dialling every number in a localarea code.

Malicious hackers use the resulting lists in breaching computer security - for guessing user accounts, or locating modems that might provide an entry-point into computer or other electronic systems.

It can be used by security personnel to detect unauthorized devices on a company's telephone network.

EXPERIMENT-6 Practical applications of digital signature

The success rate of various electronic mechanisms such as E- Governance, E-Learning, E-Shopping, E-Voting, etc. is absolutely dependent on the security, authenticity and the integrity of the information that is being transmitted between the users of sending end and the users of receiving end. To attain all these parameters, these sensitive information must be digitally signed by its original sender which should be verified categorically by its intended receiver. Since digital signature schemes are basically various complex cryptographic algorithmswhich are embedded with the plain text message, the performancelevel of these E-services vary based on certain attributes like key size, block size, computational complexities, security parameters, application specific customizations, etc. In this paper the author have made a thorough study of the industry standard digital signature schemes to obtain optimum security level for the electronic mechanisms and explored its probable applications in various domains.

Introduction to Digital Signature

A digital signature is an electronic signature form used for authentication of the identity of the communicator or an authority signing the document. It ensures authenticity and originality of the content of the communication or the document. Digital Signatures remain unchanged throughout the communication or documentation, they are easily transportable and it cannot be imitated by anyone else. It also makes sure that the sender cannot deny the content sent via that signed document.

Understanding Digital Signature Certificate

Digital signature certificate can be better understood as the electronic alternative to physical or paper certificates such as driving license, PAN Card, passport, etc. Digital Certificates are proof of the identity of a person having a specified purpose. For example, a passport identifies a citizen's identity with relation to a nationality and that citizen is eligible to legally travel to any country on a grant of permission. Under these identity

requirements, the digital certificate is used to electronically provea citizen's identity and helps access to information or services via the internet or other electronic mediums or to sign documents digitally.

Need for a Digital Signature Certificate?

A digital signature certificate is a convenient way to authenticate an identity electronically with a high level of security for online transactions while safeguarding one's privacy of information shared via Digital Signature Certificate. These certificates are used to encrypt data in a way that only the desired recipient can have access to it. The digitally signed information also ensures that it remains unchanged throughout the process of digital transfer as well as verifying the identity of the sender of the message.

Purchasing a Digital Signature Certificate

Legally validated Signature Certificates can only be issued by the Controller of Certifying Authority (CCA), Government of India licensed Certifying Authority (CA) as per the requirement of an individual as well as organizational needs.

Applications of Digital Signature

To send and receive encrypted emails, that are digitally signedand secured

To carry out secure online transactions

To identify participants of an online transaction

To apply for tenders, efiling with Registrar of Companies (MCA),efiling of income tax returns and other relevant applications

To sign and validate Word, Excel and PDF document formatsDigital Signature Web Application Process

A digital signature certificate links the identity of a person with apair of electronic keys, i.e. public and private keys, endorsed bya CA. The certificate consists of information related to the user's identity (Like: name, pin code, country, email address, certificateissue date, and the Certifying Authority Name).

The keys are complementary to each other and one cannot work without the presence of another. The browsers and servers to encrypt and decrypt the information of the certificate user duringthe complete process. The private key can be stored on the user'shard disk, computer or any external device. The user controls the access and it only works with the assigned password. In case of mismatch of the two, the authentication process fails. This ensures that only authorized personnel can use the Digital signatures whereas the unauthorized ones cannot access the data.

Digital Signature Web Application allows a faster, convenient and secure way to create your digital signatures that are authenticand can be used for almost every documentation process. Also, the digital signature web application is equally useful for personaland business use. It can be stored safely and can be used for applications of digital signatures to avail various services.

We at Sigplex are constantly building efficient and effective technological solutions for businesses. Our Digital Signature webapplication is made for safe, secure and convenient transactions. Feel free to write to us at contact@sigplex.com on how your personal and business transactions can be secured via digital signature.

Uses for digital certificates in Internet applications

Applications using public-key cryptography systems for key exchange or digital signatures need to use digital certificates to obtain the needed public keys. Internet applications of this kind are numerous. Following are brief descriptions of a few of the commonly used Internet applications that use public-key cryptography:

SSL

A protocol that provides privacy and integrity for communications. This protocol is used by

Web servers to provide security for connections between Web servers and Web browsers,LDAP to provide security for connections between LDAP clients and LDAP servers,Host-on- Demand V2 to provide security for connections between the client and the host system.

Additional applications based on this protocol are in development.

SSL uses digital certificates for key exchange, server authentication, and optionally, client authentication.

Client Authentication

Client authentication is an option in SSL that requires a server to authenticate a client's digital certificate before allowing the client to log on or access certain resources. The server requests and authenticates the client's digital certificate during the SSL handshake. At that time the server can also determine whether it trusts the CA that issued the digital certificate to the client.

Secure Electronic Mail

Many electronic mail systems, using standards such as Privacy Enhanced Mail (PEM) or Secure/Multipurpose Internet Mail Extensions (S/MIME) for secure electronic mail, use digital certificates for digital signatures and for the exchange of keys to encrypt and decrypt messages.

Virtual Private Networks (VPNs)

Virtual private networks, also called secure tunnels, can be set upbetween firewalls to enable protected connections between secure networks over insecure communication links. All traffic destinedto these networks is encrypted between the firewalls.

The protocols used in tunneling follow the IP Security (IPsec) standard. For the key exchange between partner firewalls, the Internet key exchange (IKE) standard, previously known as ISAKMP/Oakley, has been defined.

The standards also allow for a secure, encrypted connection between a remote client (for example, an employee working from home) and a secure host or network.

Secure Electronic Transaction (SET)

SET is a standard designed for secure credit card payments using insecure networks, for example, the Internet. Digital certificates are used for card holders (electronic credit cards) and merchants. The use of digital certificates in SET allows for secure, private connections between card holders, merchants, and banks. The transactions created are secure and indisputable, and they cannot be forged. The merchants receive no credit card information that can be misused or stolen.

a. output in the screen.