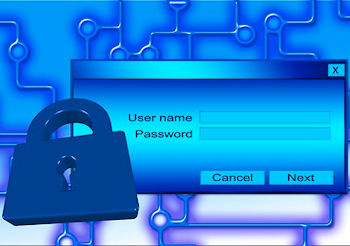
**VU1F14150\_\_**

**Expt no-**

**Aim:** To study network security software.

**Theory:**

Network security consists of the policies and practices adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs; conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises, and other types of institutions. It does as its title explains: It secures the network, as well as protecting and overseeing operations being done. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password.



**Overview of Network Security**



## ***Network Security concept***

Network security starts with authenticating, commonly with a username and a password. Since this requires just one detail authenticating the user name—i.e., the password—this is sometimes termed one-factor authentication. With two-factor authentication, something the user 'has' is also used (e.g., a security token or 'dongle', an ATM card, or a mobile phone); and with three-factor authentication, something the user 'is' is also used (e.g., a fingerprint or retinal scan).

Once authenticated, a firewall enforces access policies such as what services are allowed to be accessed by the network users. Through effective to prevent unauthorized access, this component may fail to check potentially harmful content such as computer worms or Trojans being transmitted over the network. Anti-virus software or an intrusion prevention system (IPS)help detect and inhibit the action of such malware. An anomaly-based intrusion detection system may also monitor the network like wireshark traffic and may be logged for audit purposes and for later high-level analysis. Newer systems combining unsupervised machine learning with full network traffic analysis can detect active network attackers from malicious insiders or targeted external attackers that have compromised a user machine or account.

Communication between two hosts using a network may be encrypted to maintain privacy.

Honeypots, essentially decoy network-accessible resources, may be deployed in a network as surveillance and early-warning tools, as the honeypots are not normally accessed for legitimate purposes. Techniques used by the attackers that attempt to compromise these decoy resources are studied during and after an attack to keep an eye on new exploitation techniques. Such analysis may be used to further tighten security of the actual network being protected by the honeypot. A honeypot can also direct an attacker's attention away from legitimate servers. A honeypot encourages attackers to spend their time and energy on the decoy server while distracting their attention from the data on the real server. Similar to a honeypot, a honeynet is a network set up with intentional vulnerabilities. Its purpose is also to invite attacks so that the attacker's methods can be studied and that information can be used to increase network security. A honeynet typically contains one or more honeypots.

## **Types of Network Security Devices**

## **Active Devices**

These security devices block the surplus traffic. Firewalls, antivirus scanning devices, and content filtering devices are the examples of such devices.

### **Passive Devices**

These devices identify and report on unwanted traffic, for example, intrusion detection appliances.

### **Preventative Devices**

These devices scan the networks and identify potential security problems. For example, penetration testing devices and vulnerability assessment appliances.

### **Unified Threat Management (UTM)**

These devices serve as all-in-one security devices. Examples include firewalls, content filtering, web caching, etc.

## **Wi‑Fi Protected Access (WPA)**

### WPA encrypts information, and checks to make sure that the network security key has not been modified. WPA also authenticates users to help ensure that only authorized people can access the network.There are two types of WPA authentication: **WPA** and **WPA2**.

## **WPA** is designed to work with all wireless network adapters, but it might not work with older routers or access points.

## **WPA2** is more secure than WPA, but it will not work with some older network adapters. WPA is designed to be used with an 802.1X authentication server, which distributes different keys to each user. This is referred to as WPA-Enterprise or WPA2-Enterprise. It can also be used in a pre-shared key (**PSK**) mode, where every user is given the same password. This is referred to as **WPA-Personal** or **WPA2-Personal**.

### **Wired Equivalent Privacy (WEP)**

## **WEP** is an older network security method that is still available to support older devices, but it is no longer recommended. When you enable **WEP**, you set up a network security key. This key encrypts the information that one computer sends to another computer across your network. However, WEP security is relatively easy to crack.

### **802.1X authentication**

### 802.1X authentication can help enhance security for 802.11 wireless networks and wired Ethernet networks. **802.1X** uses an authentication server to validate users and provide network access. On wireless networks, **802.1X** can work with WEP or WPA keys. This type of authentication is typically used when connecting to a workplace network.

## **MAC Address** A Media Access Control address is a unique identifier assigned to network interfaces for communications on the physical network segment. Can be described as Ethernet hardware address (EHA), hardware address or physical address. It is assigned by the manufacturer of a network interface card (NIC) and are stored in its hardware, the card's read-only memory, or some other firmware mechanism. The advantage to MAC filtering is that there is no attachment cost to devices that connect to the network. The policy is set on a router or switch, and the equipment attached either is permitted or it is not. The person attaching the equipment has nothing to do. The disadvantage to MAC filtering is that it is easy to spoof due to the broadcast nature of LAN and WLAN, an advisory can sit on the wire and just listen to traffic to and from permitted MAC addresses. Then, the advisory can change his MAC address to a permitted one, and in most cases obtain access to the network.

## **Authentication**

## **One-factor authentication –** this is “something a user knows.” The most recognized type of one-factor authentication method is the password.

## **Two-factor authentication –** in addition to the first factor, the second factor is “something a user has.” Examples of something a user has are a device that generates a predetermined code, a signed digital certificate or even a biometric such as a fingerprint.

## **Three-factor authentication –** in addition to the previous two factors, the third factor is “something a user is.” Examples of a third factor are all bio-metric such as the user’s voice, hand configuration, a fingerprint, a retinal scan or similar.

## The advantage of using a 3 factor authentication is that it's made reassuringly sure that the person who is authenticating is the person who is authenticating through multiple layers of security.

## The disadvantage is that there is a possibility that the person trying to authenticate loses first or the second authentication, the process can also take time.

## **Firewalls**

A firewall is a network security system that manages and regulates the network traffic based on some protocols. A firewall establishes a barrier between a trusted internal network and the internet.

Firewalls exist both as software that run on a hardware and as hardware appliances. Firewalls that are hardware-based also provide other functions like acting as a DHCP server for that network.

Most personal computers use software-based firewalls to secure data from threats from the internet. Many routers that pass data between networks contain firewall components and conversely, many firewalls can perform basic routing functions.

Firewalls are commonly used in private networks or *intranets* to prevent unauthorized access from the internet. Every message entering or leaving the intranet goes through the firewall to be examined for security measures.

An ideal firewall configuration consists of both hardware and software based devices. A firewall also helps in providing remote access to a private network through secure authentication certificates and logins.

### **Hardware and Software Firewalls**

Hardware firewalls are standalone products. These are also found in broadband routers. Most hardware firewalls provide a minimum of four network ports to connect other computers. For larger networks − e.g., for business purpose − business networking firewall solutions are available.

Software firewalls are installed on your computers. A software firewall protects your computer from internet threats.

## **Antivirus**

An antivirus is a tool that is used to detect and remove malicious software. It was originally designed to detect and remove viruses from computers.

Modern antivirus software provide protection not only from virus, but also from worms, Trojan-horses, adwares, spywares, keyloggers, etc. Some products also provide protection from malicious URLs, spam, phishing attacks, botnets, DDoS attacks, etc.

**Content Filtering**

Content filtering devices screen unpleasant and offensive emails or webpages. These are used as a part of firewalls in corporations as well as in personal computers. These devices generate the message "Access Denied" when someone tries to access any unauthorized web page or email.

Content is usually screened for pornographic content and also for violence- or hate-oriented content. Organizations also exclude shopping and job related contents.

Content filtering can be divided into the following categories −

* Web filtering
* Screening of Web sites or pages
* E-mail filtering
* Screening of e-mail for spam
* Other objectionable content

## **Intrusion Detection Systems**

Intrusion Detection Systems, also known as Intrusion Detection and Prevention Systems, are the appliances that monitor malicious activities in a network, log information about such activities, take steps to stop them, and finally report them.

Intrusion detection systems help in sending an alarm against any malicious activity in the network, drop the packets, and reset the connection to save the IP address from any blockage. Intrusion detection systems can also perform the following actions −

* Correct Cyclic Redundancy Check (CRC) errors
* Prevent TCP sequencing issues
* Clean up unwanted transport and network layer options

## **How Network Security is Implemented**

### **Hardware Appliance**

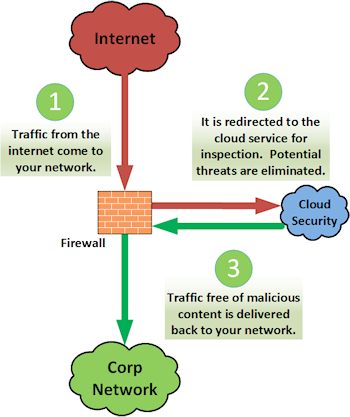
**Hardware appliances** are special servers or network equipment that perform a specific network security function. They are installed on the network either out of the direct path of network traffic (out-of-line), but most commonly in the direct line of network traffic (in-line). When appliances are in-line, they are able to stop security threats, instead of just monitoring and alerting you about them.

**2. Software**

Special network security software can be installed on servers or PC's to enable network protection functions.

### **As a Service (Cloud-based)**

Some network security functions can be outsourced to a third-party provider. This type of network security is provided to your company as a service and is often called a **cloud service**. While the concept of a cloud service may be abstract to some, the basic idea is described in the diagram here.



## ***Security managements***

## Security management for networks is different for all kinds of situations. A home or small office may only require basic security while large businesses may require high-maintenance and advanced software and hardware to prevent malicious attacks from hacking and spamming.

### ***Types of Attacks***

Networks are subject to attacks from malicious sources. Attacks can be from two categories: "Passive" when a network intruder intercepts data traveling through the network, and "Active" in which an intruder initiates commands to disrupt the network's normal operation or to conduct reconnaissance and lateral movement to find and gain access to assets available via the network.

Types of attacks include:

* **Passive**
  + Network
    - Wiretapping
    - Port scanner
    - Idle scan
* **Active**
  + Denial-of-service attack
  + DNS spoofing
  + Man in the middle
  + ARP poisoning
  + VLAN hopping
  + Smurf attack
  + Buffer overflow
  + Heap overflow
  + Format string attack
  + SQL injection
  + Phishing
  + Cross-site scripting
  + CSRF
  + Cyber-attack

There are four steps to protect your network from attacks and they are:

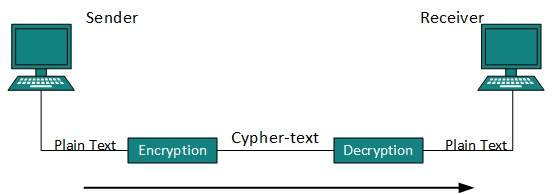
1. Implement
2. Analyze
3. Test
4. Modify

Implement: The first step is to create and implement a network security system that provides protection and has sufficient authorization policies.

Analyze: Once the network security system is created and implemented, the system needs to be analyzed to determine if the current security system is appropriate for the network it is protecting.

Test: When an appropriate network security system is in place, it is time to conduct tests to make sure all of the securities are working and will completely protect your network against any threats.

Modify: After conducting the tests, collect the data and enhance your protections. The results will reveal where your security system is effective and where it can be improved. Hackers are always improving their attacking procedures, so it is essential to test your system frequently to remain protected and stay one step ahead of them. No technique in the present world can provide 100% security. But steps can be taken to secure data while it travels in unsecured network or internet. The most widely used technique is Cryptography.



Cryptography is a technique to encrypt the plaintext data which makes it difficult to understand and interpret. There are several cryptographic algorithms available present day as described below:

* Secret Key
* Public Key
* Message Digest

## **Secret Key *Encryption***

Both sender and receiver have one secret key. This secret key is used to encrypt the data at sender’s end. After the data is encrypted, it is sent on the public domain to the receiver. Because the receiver knows and has the Secret Key, the encrypted data packets can easily be decrypted.

Example of secret key encryption is Data Encryption Standard (DES). In Secret Key encryption, it is required to have a separate key for each host on the network making it difficult to manage.

## ***Public Key Encryption***

In this encryption system, every user has its own Secret Key and it is not in the shared domain. The secret key is never revealed on public domain. Along with secret key, every user has its own but public key. Public key is always made public and is used by Senders to encrypt the data. When the user receives the encrypted data, he can easily decrypt it by using its own Secret Key.

Example of public key encryption is Rivest-Shamir-Adleman (RSA).

*Advantages of Network Security*

**Protect data**

As discussed, network security keeps a check on unauthorized access. A network contains a lot of confidential data like the personal client data. Anybody who breaks into the network may hamper these sensitive data. So, network security should be there in place to protect them.

**Prevents cyber attack**

Most of the attack on the network comes from internet. There are hackers who are experts in this and then there are virus attacks. If careless, they can play with a lot of information available in the network. The network security can prevent these attacks from harming the computers.

**Levels of access**

The security software gives different levels of access to different users. The authentication of the user is followed by the authorization technique where it is checked whether the user is authorized to access certain resource. You may have seen certain shared documents password protected for security. The software clearly knows which resources are accessible by whom.

**Centrally controlled**

Unlike the desktop security software, the network security software is controlled by a central user called network administrator. While the former is prone to worms and virus attacks, the latter can prevent the hackers before they damage anything. This is because the software is installed in a machine having no internet.

**Centralized updates**

It is very important that the anti-virus software is timely updated. An old version may not offer you enough security against attackers. But it is not guaranteed that every user of the network follows it religiously. A network security system which is centralized offers this advantage of timely updates without even the knowledge of the individuals.

***Disadvantages of Network Security***

Network security is a real boon to the users to ensure the security of their data. While it has many advantages, it has lesser disadvantages. Let us discuss some of them.

**Costly set up**

The setup of a network security system can be a bit expensive. Purchasing the software, installing it etc can become costly especially for smaller networks. Here we are not talking about a single computer, but a network of computers storing massive data. So, the security being of prime importance will definitely cost more. It cannot be ignored at any cost!

**Time consuming**

The software installed on some networks is difficult to work with. It needs authentication using two passwords to ensure double security which has to be entered every time you edit a document. It also requires the passwords to be unique with numbers, special characters and alphabets. The user may have to type a number of sample passwords before one is finalized which takes a lot of time.

**Requires skilled staff**

To manage large networks is not an easy task. It requires highly skilled technicians who can handle any security issue that arises. A network administrator needs to be employed to ensure smooth working of the network. He must be trained adequately to meet the requirement.

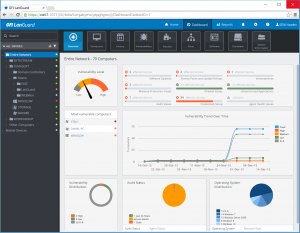
**Careless admin**

When the best software is installed and everything required is done, it is natural for the admin to be careless at times. It is his job to check the logs regularly to keep a check on the malicious users. But sometimes, he just trusts the system and that is when the attack happens. So, it is very important that the admin remains vigilant always.

NETWORK SECURITY SOFTWARE

**1.** [**GFI LanGuard**](http://www.gfi.com/products-and-solutions/network-security-solutions/gfi-languard?adv=13558&loc=131&utm_medium=social&utm_campaign=top20networkmonitoringblogpost&utm_source=gfi_blog&utm_content=title) **(our award-winning paid solution)**

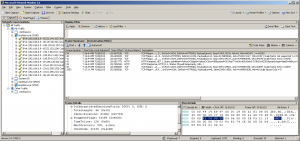
People say it’s good to be modest and not to brag, but we’re so proud of our network management tool that we had to start the list with GFI LanGuard. You can use it to scan both small and large networks, in search of software vulnerabilities and unpatched or unlicensed applications. Information coming from up to 60,000 devices, running on Windows, Mac OS or Linux, will be shown in a centralized web console, so you’ll be ablea to see the state of your whole network at any moment and from any location.



With centralized patch management and network auditing, GFI LanGuard prevents potential compliance issues, but if you’re a sysadmin the fact that all machines are patched and secured will surely seem like a more important advantage. But, don’t take our word for it.

## **2.****[Microsoft Network Monitor](http://www.microsoft.com/en-us/download/details.aspx?id=4865)**

Microsoft Network Monitor is a packet analyzer that allows you to capture, view and analyze network traffic. This tool is handy for troubleshooting network problems and applications on the network. Main features include support for over 300 public and Microsoft proprietary protocols, simultaneous capture sessions, a Wireless Monitor Mode and sniffing of promiscuous mode traffic, amongst others.



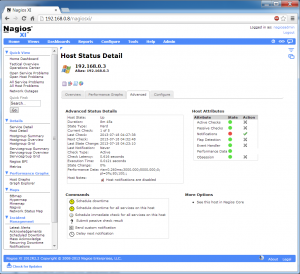
When you launch Microsoft Network Monitor, choose which adapter to bind to from the main window and then click “New Capture” to initiate a new capture tab. Within the Capture tab, click “Capture Settings” to change filter options, adapter options, or global settings accordingly and then hit “Start” to initiate the packet capture process. Although very useful, this tool has been archived, and now Microsoft recommends using Message Analyzer for the same purpose.

## **3.****[Nagios](https://www.nagios.com/products/)**

Nagios is a powerful network monitoring tool that helps you to ensure that your critical systems, applications and services are always up and running. It provides features such as alerting, event handling and reporting. The Nagios Core is the heart of the application that contains the core monitoring engine and a basic web UI. On top of the Nagios Core, you are able to implement plugins that will allow you to monitor services, applications, and metrics, a chosen frontend as well as add-ons for data visualisation, graphs, load distribution, and MySQL database support, amongst others.

**Tip:** If you want to try out Nagios without needing to install and configure it from scratch, download Nagios XI and enable the free version. Nagios XI is the pre-configured enterprise class version built upon Nagios Core and is backed by a commercial company that offers support and additional features such as more plugins and advanced reporting.

**Note:** The free version of Nagios XI is ideal for smaller environments and will monitor up to seven nodes.



Once you’ve installed and configured Nagios, launch the Web UI and begin to configure host groups and service groups. Once Nagios has had some time to monitor the status of the specified hosts and services, it can start to paint a picture of what the health of your systems look like.

**Conclusion**: Thus , case study for network security has been successfully implemented and studied.