UNIT 15: NETWORK SECURITY

UNIT STRUCTURE

15.1 Learning Objectives

15.2 Introduction

15.3 Computer Security

15.4 Network Security

15.5 Network Security Threats

15.6 Threat Prevention Techniques/ Solutions

- 15.6.1 Working of Network Security
- 15.6.2 Types of Network Security

15.7 Packet Sniffer

15.8 DoS Attack

15.9 Firewall

- 15.9.1 Types of Firewall
- 15.9.2 IPTABLES

15.10 Virtual Private Network

15.11 Let Us Sum Up

15.12 Further Readings

15.13 Answers To Check Your Progress

15.14 Model Questions

15.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- understand the Issues related to network security
- learn different threats in network security
- learn how to prevent threats to network
- understand packet sniffer
- describe the concept of firewall and virtual private network

15.2 INTRODUCTION

In the previous unit, we have learnt how to configure the NFS, NIS,

DNS, FTP, squid proxy, and DHCP server. In this unit, we will discuss about network security issues and threat prevention techniques and solutions.

15.3 COMPUTER SECURITY

Computer Security refers to the process of detecting and preventing unauthorized access of computer. Security involves the process of protecting the data and information of the devices from intruders.

Types of Computer Security

- Information security: Information security refers to securing information from unauthorized access, modification & deletion.
- Application Security: Application security refers to securing different application in the system by taking appropriate measures at the time of designing the software.
- Network Security: Network security refers to securing the devices from different network attacks and keeps safe both software and hardware in the devices from intruders.
- Cyber Security: Cyber security refers to protecting of computer systems, which communicate over the computer networks.

15.4 NETWORK SECURITY

Network Security refers to the measures taken by an organization to secure their computer network and data by using both hardware and software systems. It aims to secure the confidentiality and accessibility of data and network. Every organization that handles large amount of data, has adopted different mechanism to prevent their network from many cyber threats.

The most basic example of Network Security is password protection which is set by the user itself. The network security solutions protect various vulnerabilities of the computer systems such as:

- data loss (deletion of data or encryption of data)
- security breaches
- malicious attacks, such as hacking and viruses

15.5 NETWORK SECURITY THREATS

Network security threats are the possible ways by which it can possibly hamper the normal functioning of your computer. Currently, network security threats are constantly increasing as the whole world is moving for digitization. New threats are arising day by day and attackers use new methods every day to break the securities. The most harmful types of computer security are:

Virus: A computer virus is a malicious program which is inserted into the computer without the knowledge of the user. These are pieces of software designed to spread from one computer device to another. It also replicates itself and infects the files and programs on the computer. Typically, they are automatically downloaded when users browse on the internet downloaded as an attachment with some other downloads or sent as e-mail attachments with the intent of infecting the host computer as well as other computers via network or by data transfer devices such as pen drive, CD etc. Virus can deactivate the security settings, send spam, steal and corrupt data in the computer. Further, it can delete every single thing on the hard drive. The ultimate goal of a virus is to ensure that the victim computer will never be able to operate properly.

Worm: A computer worm is a software program just like virus which can copy itself from one computer to another, without user interaction. The potential risk with the worm is that it will occupy the computer hard disk space because it can replicate in great volume and great speed.

Phishing: This is one type of online fraud, which is designed to steal sensitive information of users, such as bank account detail like credit card numbers, debit card numbers, ATM pins and passwords, OTPs, personal contacts etc. from users. In phishing, the phishers conceal as a trustworthy person or business or reputable banking institutions, websites etc. and attempt to steal sensitive financial or personal information through fraudulent email or instant messages. Phishing is unfortunately very easy to execute. Users may think it's the legitimate mail and enter the personal information, financial details and phishers use those information for fraud.

Sometimes phishers send fraud links on phone messages or WhatsApp or as popup messages in some websites by showing some greedy approach to the users. By clicking those URL or reply to the messages, users are prompted to enter financial details or user credentials, which then sends the data to the malicious source. Phishing attacks are the practice of sending fraudulent communications that appear to come from a reputable source.

Botnet: A botnet is a group of computers connected via internet, that have been compromised to the hacker. Botnet attacks typically involve sending spam, data theft, exploiting sensitive information, or launching vicious DDoS attacks. As different types of devices are in the botnet and grow on increasing, it is very difficult to monitor, detect, and stop botnet attacks.

Botnet attacks typically start when intruders gain access to devices by injecting Trojan viruses or utilizing basic social engineering tactics. Once hackers successfully gain access to these devices, they are brought under control with software that allows them to carry out attacks.

Malware/Ransomware/ Spyware: Malware is malicious software mostly used by hackers to hold control over the system, steal confidential data, or install malicious programs in the device without user knowledge. It spreads spyware, Trojans, and worms through pop-up ads, infected files, bogus websites, or e-mail messages.

On the other hand, ransomware is a type of malware where the attacker locks the victim's device through a virus or phishing e-mails, then asks for ransom to unlock the device. It can hinder the users from running applications, encrypting files, and even completely block the device.

Spyware describes software with malicious behaviour that aims to gather information about a person or organization and sends such information to cyber criminals. Cyber criminals use those information's and hack user's computer or use those information's for financial fraud.

Denial-Of-Service Attack: A denial-of-service attempts to hinder legitimate users from accessing services or information from website. It happens when botnet or malicious software attacks a website with heavy

traffic. It is carried out by one computer and its internet connection, which may enable the intruder to access user's credentials. A distributed denial-of-service is similar to the denial-of-service but is harder to overcome. This is because it is launched from different computers that are distributed all over the globe. The Distributed DoS attack will send multiple requests to the attacked web resource, with the aim of exceeding the website's capacity to handle multiple requests and prevent the website from functioning correctly.

Rogue Security Software: This type of malicious software cheats users by making them to believe that their security measures are not up-to-the-minute or their computer has a virus. They do help by installing software or by updating user's security settings by asking users to pay for the tool or download their program to keep away with the alleged viruses. This can lead to the installation of actual malware in the device.

15.6 THREAT PREVENTION TECHNIQUES/ SOLUTIONS

Typical preventive measures that can be adopted by any enterprise or individual to avoid network security threats include:

- Secure the computer physically by installing reliable, reputable security and anti-virus software and activating your firewall.
- Stay up-to-date on the latest software and news surrounding your devices and perform software updates as soon as they become available.
- Avoid clicking on email attachments unless the source is genuine and known.
- Change passwords on regular basis, using a unique combination of numbers, letters and upper case letters.
- Use the internet with caution and ignore pop-ups, drive-by downloads while surfing.
- Taking the time to research the basic aspects of computer security and educate yourself on evolving cyber-threats.
- Perform full system scans daily and create a periodic system backup

schedule to ensure that your data is retrievable.

- Set the security settings as per latest norms in the router or the system.
- Regular updating of firmware and software.
- Use data encryption technique to store sensitive data.
- Regular backup of data in secondary storage devices not attached to the computer.
- Restricting access of network infrastructure to authorised personnel only.
- Train staff to safe and secure use of the equipment.

As well as training staff, we should also implement policies and rules for computer use in the workplace.

15.6.1 Working of Network Security

The basic principle of network security is to protect data in the computer as well as in the cloud and networks communicating information or data as per the rules and regulations that have to be acknowledged before performing any activity on the data. There are basically three types of network security-

Physical Network Security: Physical network security is the most basic level security that includes protecting the data and network from any unauthorized access to break the confidentiality of the network communication. Physical network security incudes securing of external peripherals, routers and other devices connected in the network communication.

Technical Network Security: This network security is basically to protect the data stored in the network or data involved in transitions through the network. Technical network security serves two purposes: protects from unauthorized access and protects from malicious activities.

Administrative Network Security: Administrative network security deals with the permission and authorization given to the users and guests. This also ensures the level of sophistication the

network might need for protecting it from the attacks. This level also suggests necessary amendments that have to be done to the infrastructure.

15.6.2 Types of Network Security

Few network securities are discussed in the following:

Access Control: All the users in the system or in the network should not have the complete accessibility to the network or its data. This is done through Network Access Control which ensures that only a handful of authorized personnel must be able to work with the allowed number of resources. Not all the users have same authorization.

Antivirus and Anti-malware Software: Antivirus software also known as anti-malware is a computer program used to prevent, detect, and remove malware. Antivirus software was originally developed to detect and remove computer viruses. This type of network security ensures that no malicious software enters to the network and expose the security of the data. The malicious software like Viruses, Trojans, and Worms is handled by the Anti-virus software's.

Cloud Security: Now a days, a lot many organizations are joining hands with cloud technology where a large amount of important data is stored over the internet. Cloud is very vulnerable to the hackers. These data must be protected and it should be ensured that this protection is not compromised at any cost.

Computer Firewall: A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted network and an untrusted network over the Internet.

15.7 PACKET SNIFFER

For monitoring traffic in the network, packet sniffer is used. Packet sniffer can be a software application or hardware tool. The data packets transferred from one computer to another computer in a network is examined by sniffer. Packet sniffer is also known as a packet analyser, protocol analyser or network analyser. Sniffers work by examining streams of data packets that flow between computers on a network as well as between networked computers and the larger Internet. Each of the network packets are intended to a target machine. It contains the address of the target machine. A packet sniffer is in "promiscuous mode" and allows IT professionals, end users or malicious intruders to examine any packet in the network, regardless of destination. Packet sniffers are configured in two ways, "unfiltered," and "filtered". In unfiltered mode the sniffer captures all the possible packets and write them to the local hard drive for examination at a later state. In "filtered" mode sniffers will capture packets that contain some specific data elements as set in the filter.

Packet sniffing is the practice of gathering, collecting, and logging some or all packets that pass in a computer network, regardless of how the packet is addressed. In this way, every packet, or a defined subset of packets, may be gathered for further analysis. A network administrator can use the collected data for a wide variety of purposes like monitoring bandwidth and traffic. Packet sniffers work on both wired and wireless networks, the efficacy of packet sniffers depends on how much they are able to "see" as a result of network security protocols. On a wired network, sniffers might have access to the packets of every connected machine or may be limited by the switches or routers. On a wireless network, most sniffers can only scan one channel at a time. If we use multiple wireless interfaces, it can expand the capability.

POPULAR PACKET SNIFFING TOOLS IN LINUX

- **tcpdump:** It is a popular free and open-source packet analyser. tcpdump uses libpcap library to capture packets on OSI layer 2 and above. It supports regular expressions for packet filtering, and allows one to export

and import packet dumps to and from a file. Using command line interface, tcpdump provides us the packet contents in desired format.

- **Wireshark:** Wireshark is an open-source packet analyser with graphical front end. It captures network traffic from local area networks like Ethernet, Bluetooth, Token Ring, IEEE 802.11 and can store and analyse the data in offline. Wireshark is quite similar to tcpdump though it is more flexible than tcpdump. Wireshark is available on multiple platforms like Linux, BSD, and Mac OS and MS Windows.
- **dhcpdump:** Snoops on DHCP request/response traffic is captured by libpcap library, and displays the DHCP packets in human readable formats. dhcpdump is useful for DHCP debugging and troubleshooting.
- **mysql-sniffer:** An open source MySQL sniffer tool captures live packets sent to a MySQL server, and dumps MySQL queries in a human readable format.

15.8 DoS ATTACK

A denial-of-service (DoS) attack is a cyber-attack on devices, information systems, or other network resources. It prevents authentic users from accessing expected services and resources. A DoS attack is accomplished by flooding the targeted host or network with traffic until the target stops responding or crashes. DoS attacks can launch anywhere from a few hours to many months and can cost institutions or businesses time and money by making their resources and services unavailable.

Working of Denial-of-Service Attacks

The primary focus of a DoS attack is to oversaturate the capacity of a targeted machine, resulting in denial-of-service to additional requests. DoS attack can be categorized mainly into two forms.

- **Buffer overflow attacks -** This is the most common DoS attack. The buffer overflow attack sends more and more packets to a network address so that system cannot able to handle those requests. As a result of this attack, memory buffer overflows and causes the machine to consume all available hard disk space, memory, or CPU time. This

form of exploit often results in sluggish behaviour, system crashes, or other deleterious server behaviours, resulting in denial-of-service.

- **Flood attacks -** By saturating a targeted server with an overwhelming number of packets, a malicious actor is able to oversaturate server capacity, resulting in denial-of-service. In order to a DoS flood attacks to be successful, the malicious machine must have more bandwidth than the target machine. Flood attack can be of one of two types-

ICMP flood - effects misconfigured network devices by sending spoofed packets that ping every computer on the targeted network, instead of just one specific machine. The network is then triggered to amplify the traffic.

SYN flood - sends a request to connect to a server, but never completes the handshake. Continues until all open ports are saturated with requests and none are available for legitimate users to connect to.

DoS attacks are on the rise as businesses and consumers use more digital platforms to communicate and transact with each other. In a DoS attack, the cyber-attacks typically use one Internet connection and one device to send rapid and continuous requests to a target server to overload the server's bandwidth. DoS attackers exploit a software vulnerability in the system and proceed to exhaust the RAM or CPU of the server.

Distributed Denial-of-Service (DDoS) Attack

A common type of DoS attack is the distributed denial-of-service (DDoS) attack. The attacker floods its target with numerous amounts of internet traffic so that normal traffic does not able to reach the intended destination. This attack is launched from many compromised connected devices (e.g., smartphones, PCs, network servers, and Internet of Things devices) from around the world go after a targeted website, network, web application, application programming interface, or data centre infrastructure simultaneously to block traffic.

In most of the time, sources of attack are operated form of a botnet. A botnet is a network of personal devices that have been compromised to cybercriminals without the knowledge of the owners. For creating botnet,

the hackers infect the devices with malicious software and gain control of the system to send spam and fake requests to other devices and servers. A target server that attacks by DDoS attack will experience an overload due to hundreds or thousands of network packets come to it. Since in DDoS attack, the victim is attacked from multiple sources, detecting it becomes very difficult. Separating legitimate traffic from fake traffic also becomes impossible, hence it is harder for the victim server to withstand to a DDoS attack.

15.9 FIREWALL

A firewall is a network security device that monitors incoming and outgoing network traffic and permits or blocks data packets based on a set of security rules. The basic purpose of firewall is to establish a barrier between host computer on the network and the network traffic from external sources in order to block malicious traffic like viruses, trojan, worm etc.

A Linux firewall is a solution or service that regulates, protects, and blocks network traffic as it passes to and from a Linux-based environment. Most of the Linux distributions came with In-built firewall services of their own. There are two types of Linux firewall:

- **A command line or GUI utility:** Linux firewall utilities sit on top of pre-built firewall services such as Netfilter, UFW, FirewallD, iptables, etc. We can configure these manually or install an additional utility that reveals the service's full functionalities, simplified configurations and enables point-and-click setup. The pre-built firewall imposes some default firewall zones, like a trusted zone, a demilitarized zone, or a block zone. The utility lets us configure these zones further, set up custom zones, and enforce more granular policies as per our needs.
- **A standalone Linux firewall solution:** It is a comprehensive firewall solution that exists independent of Netfilter, iptables, etc. This comes within a secure, hardened OS that we can install in a shell of our choice - a public cloud environment, or a private virtualized shell. These solutions usually include network management capabilities like traffic

routing or monitoring reports to enable a 360-degree network management landscape.

Both types of Linux firewall solutions can coexist in the same organization. A rule of thumb is to use the first one for solo deployments, while the latter is more suited to enterprise.

Firewalls are one of the core components of a network security implementation. Several vendors in market sells firewall solutions catering to all levels of the marketplace: from home users to data centre solutions. Firewalls can also be a stand-alone hardware solution, such firewall appliances are manufactured by Cisco, Nokia, and Sonicwall. Vendors such as Checkpoint, McAfee, and Symantec have developed proprietary software firewall solutions for home and business markets.

15.9.1 Types of Firewall

- **Packet Filtering Firewall:** One of the most fundamental types of firewalls is packet filtering firewall. The main function of this firewall is to monitor traffic and filter of packets based on security rules configured earlier. If any certain IP address or port number violates the security rules, it immediately blocks it. The main advantages of packet filtering firewall include its inexpensiveness, fastness and efficient.
- **Circuit Level Gateways:** This firewall performs at session layer of OSI model. It does not verify the actual content like packet filtering firewall. It only focuses on TCP connections and sessions. If certain packet follows the valid TCP connection, then it can pass through the gateway irrespective of its content.
- **Application Level Gateways (Proxy Firewall):** Application level gateways or proxy firewall performs at application layer of OSI model. It acts as an intermediary filter between two end systems. Proxy firewall protects the internal network by not letting it direct connect with the outside internet. It verifies validity of a packet based on particular standard protocol (e.g. FTP, HTTP) through

which the packet is sent. If it does not match, it drops the packet.

15.9.2 IPTABLES

Iptables is a firewall, installed by default on all official Ubuntu distributions. After fresh installation of ubuntu iptables allows all traffic by default. Ubuntu comes with ufw - a program for managing the iptables firewall easily. Following command lists the current rules in iptables. After fresh installation of server iptables -L shows nothing.

sudo iptables -L

Basic Iptables Options

Some of the Iptables options are:

- -A - Append this rule to a rule chain. Valid chains for what we're doing are INPUT, FORWARD and OUTPUT, but we mostly deal with INPUT in this tutorial, which affects only incoming traffic.
- -L - List the current filter rules.
- -m conntrack - Allow filter rules to match based on connection state. Permits the use of the --ctstate option.
- --ctstate - Define the list of states for the rule to match on. Valid states are:
- NEW - The connection has not yet been seen.
- RELATED - The connection is new, but is related to another connection already permitted.
- ESTABLISHED - The connection is already established.
- INVALID - The traffic couldn't be identified for some reason.
- -m limit - Require the rule to match only a limited number of times. Allows the use of the --limit option. Useful for limiting logging rules.
- --limit - The maximum matching rate, given as a number followed by "/second", "/minute", "/hour", or "/day" depending on how often you want the rule to match. If this option is not used and -m limit is used, the default is "3/hour".
- -p - The connection protocol used.

- --dport - The destination port(s) required for this rule. A single port may be given, or a range may be given as start:end, which will match all ports from start to end, inclusive.
- -j - Jump to the specified target. By default, iptables allows four targets:
- ACCEPT - Accept the packet and stop processing rules in this chain.
- REJECT - Reject the packet and notify the sender that we did so, and stop processing rules in this chain.
- DROP - Silently ignore the packet, and stop processing rules in this chain.
- LOG - Log the packet, and continue processing more rules in this chain. Allows the use of the --log-prefix and --log-level options.
- --log-prefix - When logging, put this text before the log message. Use double quotes around the text to use.
- --log-level - Log using the specified syslog level. 7 is a good choice unless you specifically need something else.
- -i - Only match if the packet is coming in on the specified interface.
- -I - Inserts a rule. Takes two options, the chain to insert the rule into, and the rule number it should be.
- -I INPUT 5 would insert the rule into the INPUT chain and make it the 5th rule in the list.
- -v - Display more information in the output. Useful for if you have rules that look similar without using -v.
- -s --source - address[/mask] source specification
- -d --destination - address[/mask] destination specification
- -o --out-interface - output name[+] network interface name ([+] for wildcard)

Allowing Established Sessions: We can allow established sessions to receive traffic by following command

sudo iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT

The above rule has no spaces either side of the comma in ESTABLISHED,RELATED

Allowing Incoming Traffic on Specific Ports: We can start blocking traffic as we wish, but if we are working over SSH, we need to allow SSH before blocking everything else.

To allow incoming traffic on the default SSH port (22), we can tell iptables to allow all TCP traffic on that port to come in.

sudo iptables -A INPUT -p tcp --dport ssh -j ACCEPT

To block an IP address (say xxx.xxx.xxx.xxx) in Iptables firewall:

iptables -A INPUT -p tcp -s xxx.xxx.xxx.xxx -j DROP

To save changes in iptables:

iptables-save

To view all options available or for help:

iptables -h

15.10 VIRTUAL PRIVATE NETWORK

Virtual Private Network (VPN) allows users to connect computers to a private network, creating an encrypted connection that masks the computers connecting to the network securely share data and surf on the web, protecting the identity of the user.

A virtual private network, or VPN, is an encrypted connection over the Internet from a device to a network. The encrypted connection helps to ensure that sensitive data is safely transmitted. It prevents unauthorized people from eavesdropping on the traffic and allows the user to conduct work remotely. VPN technology is widely used in corporate environments. Virtual private network is mainly of two types:

Remote Access VPN: Through remote access VPN, users can connect to private network and able to access all resources and services remotely. It is used by both individual users and business organisation. For

example, during work from home service by an employee for an organisation, the employee can take the help of VPN to access the private network of his company securely to access all the resources of the company and perform his work.

Router-to-Router VPN: Router-to-router VPN is also known as site-to-site VPN which is commonly used in large organisations. An organisation or multiple organisations, which have many branches at different locations of a state or country is connected over their own private network using site-to-site VPN. It can be of two types:

- **Intranet based VPN:** A site-to-site Virtual Private Network through which many branches of the same organization are connected, is known as Intranet based VPN.
- **Extranet based VPN:** A site-to-site Virtual Private Network through which a branch of an organization is connected to branch or office of another organization, then it is known as extranet-based VPN.



CHECK YOUR PROGRESS

Q 1: In computing _____ is a network security system that monitors and controls network traffic. (spyware / Cookie / Spam / Firewall)

Q 2: A computer virus is a _____ . (Program/ Hardware / freeware)

Q 3: DDoS stands for _____.

Q 4: Iptables use _____ . (for IP address tracking / to find a IP Address / as firewall)

Q 5: _____ is a popular packet sniffing toll. (Wireshark/ IP capture / Iptables)



15.11 LET US SUM UP

- Computer Security refers to the process of detecting and preventing unauthorized access of computer. Security involves the process of safeguarding the devices data and information from intruders.

- Network Security refers to the measures taken by an organization to secure their computer network and data using both hardware and software systems. Network security aims to secure the confidentiality and accessibility of data and network.
- Basic network security threats are virus, worm, phishing, botnet, malware, DoS attack
- The few types of network securities that one can adopt are Access Control, Antivirus, Cloud Security, Computer Firewall.
- Packet sniffing is the practice of gathering, collecting, and logging some or all packets that pass in a computer network, regardless of how the packet is addressed.
- Popular packet sniffing tools are tcpdump, Wireshark, dhcpdump, mysql-sniffer
- A denial-of-service (DoS) attack is a cyberattack on devices, information systems, or other network resources that prevents authentic users from accessing expected services and resources.
- DoS attack can be categorized mainly two ways, Buffer overflow attacks and Flooding attacks.
- A firewall is a network security device that monitors incoming and outgoing network traffic and permits or blocks data packets based on a set of security rules.
- Iptables is a firewall, installed by default on all official Ubuntu distributions.
- Virtual Private Network (VPN) allows users to connect computers to a private network, creating an encrypted connection that masks the computers connecting to the network securely share data and surf on the web, protecting the identity of the user.



15.12 FURTHER READINGS

1) Linux System Administration by Tom Adelstein, Bill Lubanovic
2) Linux Network Administrators Guide by Olaf Kirch
3) Linux security cookbook by Daniel J. Barrett

15.13 ANSWERS TO CHECK YOUR PROGRESS

Ans to Q No 1: Firewall

Ans to Q No 2: Program

Ans to Q No 3: Distributed Denial of Service

Ans to Q No 4: as firewall

Ans to Q No 5: Wireshark

15.14 MODEL QUESTIONS

Q 1: What is network security? What are the threats in network security?

Q 2: Explain the different types of network security.

Q 3: What is firewall? Explain its working.

Q 4: What is virtual private network? Explain briefly.

Q 5: What is DoS attack? How DoS attacks are performed? Explain in detail.

Q 6: What is packet sniffing? Explain the different packet sniffing tools.

*** ***** ***