27/04/24

(3/8) - Connect and Protect Networks and Network Security

⇒ **MODULE 1 :** Network Architecture

↳ Network security

↳ Security threats and Vulnerabilities.

↳ Network Architecture

↳ Secure a Network

⇒ **MODULE 2 :** Network Operations

↳ Network Protocols

↳ Network Communications → Vulns

↳ Common security measures

⇒ **MODULE 3 :** Secure against network intrusions

↳ Types of network attacks & techniques

↳ Malicious actors exploit vulnerabilities

↳ Identify and close potential loopholes.

⇒ **MODULE 4 :** Security hardening

↳ Network hardening practices

↳ Defend against malicious actors and intrusion method

→ Security challenged posed by cloud infrastructure

"Make Connections withe more
PEOP[redacted]E"
PEOPLE

↦ MODULE 1:

→ Introduction to networks

⇒ Network:
A group of connected devices

⇒ Local Area Network: [LAN]
A network that spans a small area like an office building, a school, or a home.

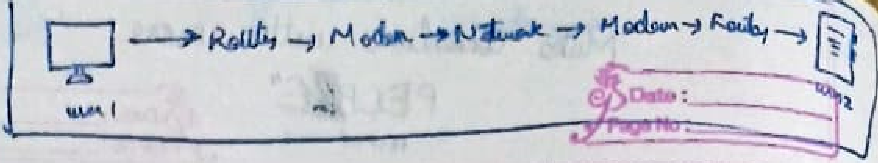
⇒ Wide Area Network: [WAN]
A network that spans a large geographic area like a city, state, or country.

⇒ Hub:
A network device that broadcasts information to every device on the network.

⇒ Switch:
A device that makes connections between specific devices on a network by sending and recieving data between them

⇒ Router:
A network device that connects multiple network together.

⇒ Modem:
A device that connects your routes to the internet and brings internet access to the LAN.



⇒ **Virtualization tools:-**

Pieces of software that performs network operations.

- Network devices send data packets.
  ↳ provide info about the source and destination of the data

- Each devices and desktop computers has a unique MAC and IP addresses

⇒ **Firewall:**

It is a ~~sec~~ network security device that monitors traffic to or from your network. It is like your firsttime line of defense.

⇒ **Servers:**

Servers provide information ↗from database and services for devices like computers, smart home devices, and smartphone on the network

- Ex: DNS server → looksup domain names

⇒ Network Diagrams

⇒ **Cloud Computing:**

The practice of using remote servers, applications, and network services that are hosted on the internet instead of on local physical devices.

⇒ Cloud Network:

A collection of servers or computers that stores resources and data in remote data centres that can be accessed through the internet

⇒ Cloud services provides :-

- On demand storage
- Processing Power
- Analytics

⇒ Cloud Service Provider's (CSP's) provide:

(1) Software as a service (SaaS)
(2) Infrastructure as a service (IaaS)
(3) Plaform as a service (PaaS)

⇒ Hybrid Cloud environments:

When organizations use a CSP's services in addition to their on-premise computer, networks and storage, it is referred to as a hybrid cloud envir.

⇒ Software Defined networks: [SDN]

These are made up of virtual network devices and services.

↦ Network Communication :-

⇒ Data Packet :

A basic unit of information that travels from one device to anothes within a network.

↓

Header	Body	Footes
↓ IP/MAC/ Protocol no.	↓ the message	↓ signals that the packet is finished

⇒ Bandwidth :

The amount of data a device recieves every second.

$$\boxed{\text{Bandwidth} = \frac{\text{Quantity of data}}{\text{Time(ins)}}}$$

⇒ Speed :

The rate at which data packets are recieved or downloded.

⇒ Packet Sniffing :

The practice of capturing and inspecting data packets across a network.

(TCP/ IP model)

⇒ Transmission Control Protocol: [TCP]

An internet communication protocol that allows two devices to form a connection and stream data.

⇒ Internet Protocol : [IP]

A set of standards used for routing and addressing data packets as they travel between devices on a network.

⇒ Port :-

A software-based location that organizes the sending and recieving of data between devices on a network.

⇒ TCP/IP model :

A framework used to visualize how data is organized and transmitted across the network.

- Layers of the TCP/IP model :
  (1) Network access layer
  (2) Internet layer
  (3) Transport layer
  (4) Application layer

Application layer → HTTP, TLS, DNS
Transport layer → TCP, UDP
Internet layer → IP (V4, V6)
Network access layer → LAN, Wireless LAN, Ethernet

⇒ The OSI model :-

It is a more abbreviated concept of TCP/IP model. Also it is a standardized concept that describes the seven layers computer use to communicate and send data over the network.

(1) Physical layer
(2) Data link layer
(3) Network layer
(4) Transport layer
(5) Session layer
(6) Presentation layer
(7) Application layer

⇒ IP address:

A unique string of characters that identifies the location of a device on the internet.

(1) IP version 4, IPV4
(2) IP version 6 IPV6

(1) IPV4 :→ ___

19.117.63.126

(2) IPV6 : (32 char)

684D:1111:222:3333:4444:5555:6:77

⇒ MAC address: [Media Access Control]

A unique alphanumerical identifier that is assigned to each physical device on a network.

↦ MODULE 2 :-

↦ Introduction to network protocols

⇒ Network Protocols:-
A set of rules used by two or more devices on a network to describe the order of delivery and structure of the data.

⇒ Address Resolution Protocol: [ARP]
A network protocol used to determine the MAC address of the next router or device on the path.

⇒ Hypertext Transfer Protocol Secure: [HTTPS]
A network protocol that provides a secure method of communication between clients and website servers.

⇒ Domain Name System: [DNS]
A network protocol that translates internet domain names into IP addresses

- when you visit any one website our device uses 4 different protocols
↓
TCP ⟶ ARP ⟶ HTTPS ⟶ DNS
(1) (2) (3) (4)

WPA2 , WPA3 } network security protocols

Date:
Page No:

⇒ **IEEE 802.11: (WIFI)**

A set of standards that define communication for wireless LAN's

⇒ **WiFi Protected Access: [WPA]**

A wireless security protocol for devices to connect to the internet.

↦ **System Identification :-**

⇒ **Firewall :-**

A network security device that monitors traffic to and from your network. (allows & blocks)

• **Port filtering :-**

A firewall function that blocks or allows certain port numbers to limit unwanted communic

(1) Hardware firewall
(2) Software firewall
(3) Cloudbased firewall

⇒ **Statefull:**

A class of firewall that keeps track of information passing through it and proactively filters out threats.

⇒ **Stateless:**

A class of firewall that operates base on predef rules and does not keep track of information from data pack

NGFW > Statefull > Stateless] secure order

⇒ **Next generation firewalls : [NGFW]**

- Deep packet inspection
- Intrusion protection
- Threat intelligence

⇒ **Virtual Private Networks : [VPN]**

A network security service that changes your public IP address and hides your location so that you can keep your data private when you are using a public network like the internet.

- **Encapsulation :**

A process performed by a VPN service that protects your data by wrapping sensitive data in other data packets

⇒ **Security Zone :**

A segment of a network that protects the internal network from the internet.

- **Network Segmentation :**

A security technique that divides the network into segments.

~~(1) [illegible]~~

(1) Uncontrolled zone

(2) Controlled zone

↳ DMZ - demilitarized zones

↳ Internal network

↳ Restricted zone

Proxy vs VPN

⇛ <u>Proxy server:</u>

A server that fulfills the requests of a client by forwarding them on to other servers.

(1) <u>Forward proxy servers:-</u>

It regulates and restricts a person's access to the internet.

person → proxy server (forward) → internet server

(2) <u>Reverse proxy servers:</u>

It regulates and restricts internet's access to an internal server.

internet server → proxy server (reverse) → internal server

→ MODULE 3 :

→ Introduction to network intrusion attacks

⇒ Common network intrusion attacks :-

- Malware
- Spoofing
- Packet Sniffing
- Packet flooding

⇒ Network Interception attacks :-

⇒ Backdoor attacks

⇒ Denial of Service attack : [DoS]

An attack that targets a network or server and floods it with network traffic.

⇒ Distributed Denial of Service attack :- [DDoS]

A type of denial of service attack that uses multiple devices or servers in different locations to flood the target network with unwanted traffic.

⇒ Network level DoS attack :-

1) SYN (synchronize) flood attack :

A type of DoS attack that simulates a TCP connection and floods a server with SYN packets.

- ICMP : [Internet Control Message Protocol]

An internet protocol used by devices to tell each other about data transmission errors across the network.

(2) ICMP flood attack:

A type of DoS attack performed by an attacker repeatedly sending ICMP packets to a network server.

(3) Ping of death:

A type of DoS attack caused when a hacker pings a system by sending it an oversized ICMP packet that is bigger than 64KB

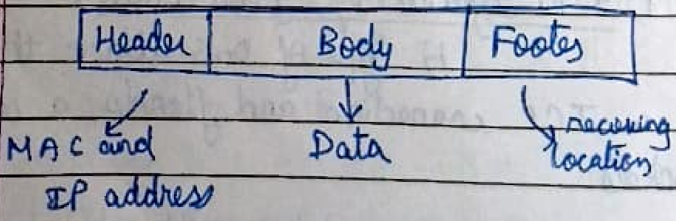
⇒ Network Protocol analyzer / Packet Sniffer:

A tool to capture and analyze data traffic within a network.

Ex: SolarWinds Netflow
tcpdump
Wireshark ✓

↦ Network attack tactics and defense:

⇒ What do packets contain?



Learn how to hack data packets in ~~pt pub~~ public places because those places does not have encrypted wifi

⇒ **Passive packet sniffing :-**

A type of attack where data packets are read in transit.

⇒ **Active Packet Sniffing :-**

A type of attack where data packets are manipulated in transit.

⇒ **How to prevent Packet Sniffing :**

- Use a VPN tunnel
- HTTPS → this encrypts data to and from

→ because hackers cannot be able to read the data packets because they are encrypted

⇒ **IP spoofing :-**

A network attack performed when an attacker changes the source IP of a data packet to impersonate an authorized system and gain access to a network.

(1) On-path attack
(2) Replay attack
(3) Smurf attack

(1) On-path attack :-

An attack where a malicious actor places themselves in the middle of an authorized connection and intercepts or alters the data in transit.

(2) Replay attack:
A network attack performed when a malicious actor intercepts a data packet in transit and delays it or a repeats it at another time.

(3) Smurf Attack: (Combination of DDoS and IP spoof)
A network attack performed when an attacker sniffs an authorized user's IP address and floods it with packets

⇒ Protect from IP spoofing:

- Encrypt data
- Use a firewall

⟼ Network hardening :-

- Port filtering
- Network access privileges
- Encryption

⇒ Tasksperformed:

- Firewall rules maintenance
- Network log analysis
- Patch updates
- Server backups

⇒ Network log analysis :
The process of examining network logs to identify events of interest.

➡ MODULE 4 :-

software update, ... etc

⇒ **Security hardering:**
The process of strengthening a system to reduce its vulnerability and attack surface.

- **Attack surface:**
All the potential vulnerabilities that a threat actor could exploit

* Security hardening is conducted on :-
(1) Hardware
(2) OS
(3) Applications
(4) Computer Networks
(5) Databases

⇒ **Penetration test :-**
A simulated attack that helps identify vulnerabilities in systems, networks, websites, applications, and processes.

➡ OS hardening :-

⇒ **Operating System :- [OS]**
The interface between computer hardware and the user.

⇒ **Patch update :**
A software and operating system update that addresses security vulnerabilities within a program or product

⇒ <u>Baseline configuration :(baseline image)</u>

A documented set of specifications within a system that is used as a basis for future builds, releases, and updates.

➡ <u>Network hardering:</u>

- Port filtering
- Network access privelages
- Encryption

⇒ <u>Task performed:</u>

- Firewall rules maintainedance
- Network log analysis
- Patch updates
- Server backups

⇒ <u>Network log analysis:</u>

The process of examining network logs to identify events of interests.

- SIEM tools are used to do it

⇒ <u>Port filtering:-</u>

A firewall function that blocks or allows certain port numbers to limit unwanted communication.

⇒ Intrusion Detection System :- [IDS]

An IDS is an application that monitors system activity and alerts on possible intrusions.

⇒ Intrusion Prevention System :-

An IPS is an application that monitor system activity for intrusive activity and takes action to stop the activity.

↦ Cloud hardening :

⇒ Cloud network :-

A collection of servers or computers that stores resources and data in remote data centres that can be accessed through the internet.

* learn more about it"!