—: CYBERSECURITY & ETHICAL HACKING :—

Day-01. Date.....

Computer Network →

Group of interconnected nodes or computing devices that exchange data & resources with each other.

- These networked devices use a system of rules, called communication protocols to transmit info over physical or wireless tech

Types of Network →

- PAN (Personal Area Network)
- LAN (local (like Building company) → like router wifi (Home & office) limited range small area) Ethernet Cable
- MAN (Metropolitan - -),
- WAN (wide - -) → through Satellite (Internet)
- CAN (Campus Area Network) like University Yaplar campus
- WLAN (Wireless Local Area Network)

* IP Address →

Internet Protocol, It's a set of rules governing the format of data sent via the internet or local network.

In essence, IP addresses are the identifiers that allows information to be sent b/w devices on a network: they contain location info & make devices accessible for communication.

Identifies होता है
वो info sent करता है
device & Network के बीच

17.172.224.47
8 bit 8 bit 8 bit 8 bit
1 byte each
32 bits = 4 bytes

0 - 255 8 bit का होता है

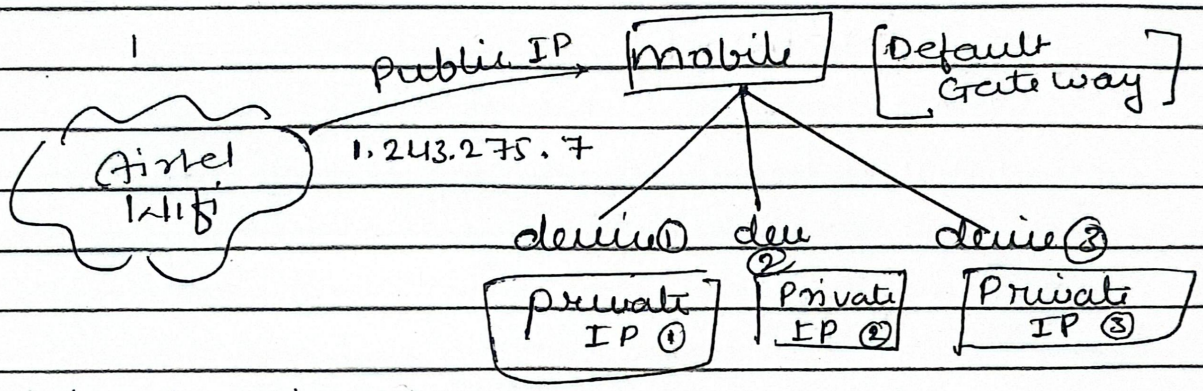
Spiral $2^0 - 2^7 - \sum(2, 4, 8, 16, 32, 64, 128) = 255$

First IP – 0.0.0.0
Last – 255.255.255.255

Date.....

- Public IP address →
  - https://whatismyipaddress.com/
- Private IP address → Windows / Mac / Linux
  - Windows key + R → cmd → ipconfig / ifconfig

like if we use a Router & share the data from hotspot for others → 80



* Network important part →
  Subnet mask – important about 30% IP → through this VLAN for segregation.

VERSIONS of IP Address →
→ Two types → IP Version 4 (IPV4)
IP Version 6 (IPV6)

- IP versions are made up of binary values & drives the routing of all data over the internet
- IPv4 are 32 bits long – 4.3 Billion IP possible
- IPv6 are 128 bits long – 340 Undecillion possible Address

Communication Requirement for device -

Date.....

IP Address (Mall address)
Port Number (Shop No.)
Protocol · (chay Cshop Name))

Source IP Address (Khud का)
Destination IP Add. (पता device से communicate)
Source Port No. (अपने System के Port No)
Destination Port No. (पता device से communicate).

PORT NO:-

Unique numerical Identifies to which an internet or other network message is to be forwarded when it arrives at a serv

total Port No: 0 - 65535

eg. netstat -a (Give all port of Ur PC)

Network Ports -

- Well known Ports 0-1023
- Registered Ports 1024 - 49151
- Dynamic Ports 49151 - 65535

M

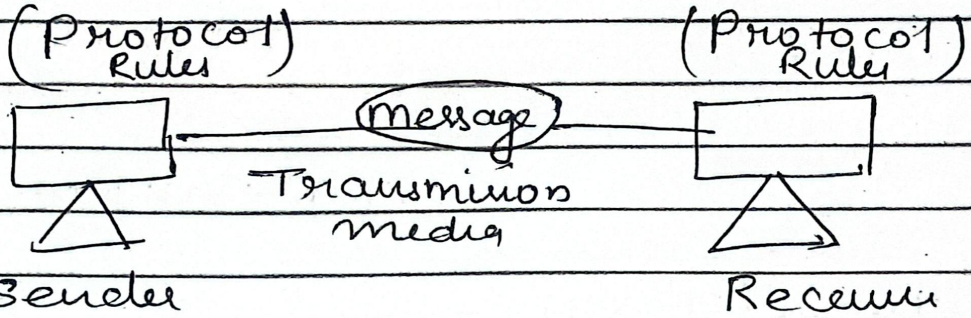
Date.....

PROTOCOL :-

It is a set of rules that Govern how data is transmitted ~~/exch~~ and received b/w devices on a network, ensuring they can communicate effectively.

Protocols serve as a common language for devices to enable communication irrespective of differences in ~~communication~~ software, hardware or internal Process.

eg: https, http, ftp, ssh, telnet etc--



OSI MODEL :-

Open System Interconnection (OSI) model describes seven layers that communicate computer systems used to communicate

(Host A) over a Network		(Host B)
1. Application layer	App. layer Protocol	App. layer
2. Presentation layer	Present. layer Protocol	Present. layer
3. Session layer	Session layer Protocol	Session layer
4. Transport layer	Tran. -P.	Transport layer
5. Network layer	N. L. P	Network layer
6. Data-link layer	D. L. P	Data link layer
7. Physical layer	P. L. P	Physical layer

TCP Layer - 3-layer Work -

1. Application layer - Data initiate होता है (First step) like Searching Google Engine.

2. Presentation layer पे - Data Compress होता है like पहले whatsapp से image send करने पे image की quality degrade हो जाती थी

3. Session layer मे Session को mentain करना & destroy करना iska काम होता है. like instagram से login करते हैं तो wo session mentain किए रखता है तब logout करते है wo session destroy करके logout करता है o ye token save कर लेता है aur dubara login करने मे help करता है without needing passcodes.

4. Transport layer - Data को fragment करके sent करना mtlb small part मे send करना like downloading movie/application & speed is 3Mb/s. (Data all small part मे break करना

5. Network layer - Data के small segment को एक IP address ~~maintain~~ ~~कर~~ provide करना

6. Data-link layer - mac address provide करता है Ethernet के through

7. Physical layer - data like send कर देना (Hub होता है वैसे)

All are Vice Versa or we can say for Host & it check all data from 7 to 1

OSI Model

Date.....

First developed in 1978 by French Software Engineer & pioneer Hubert Zimmermann.

NETWORK DEVICES

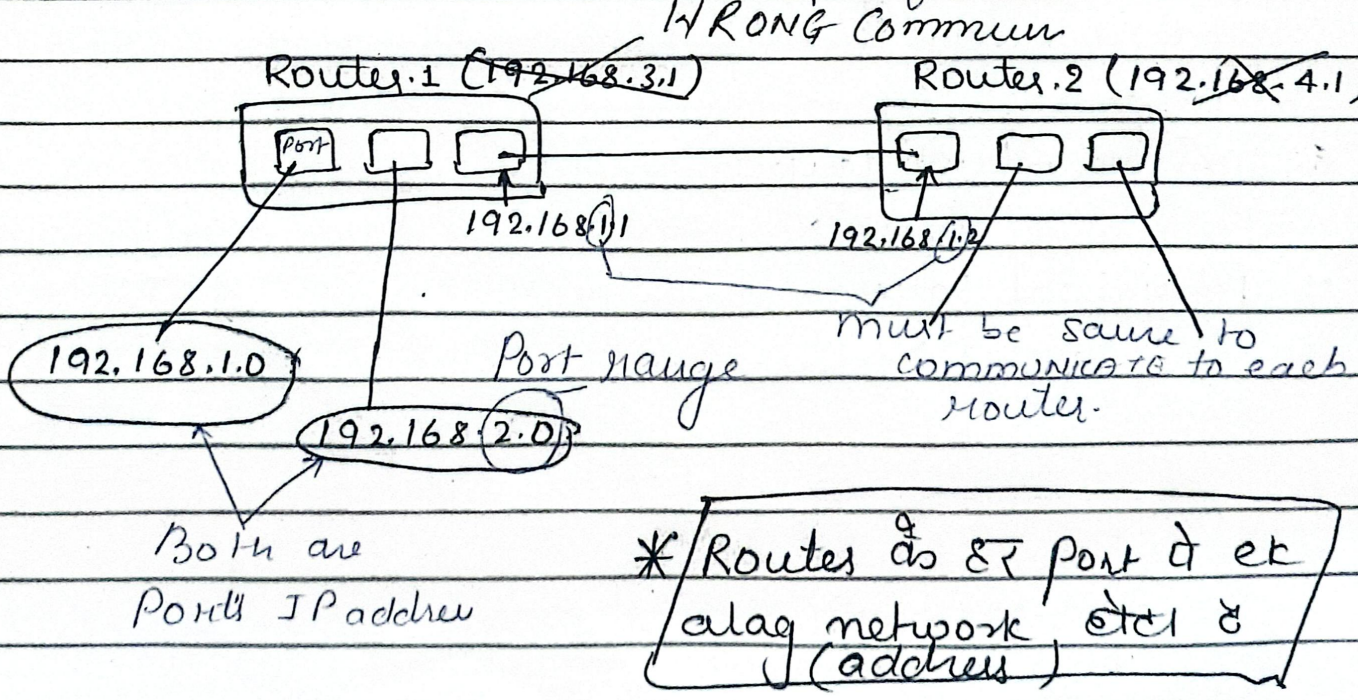
Router :-

- A routes is a devie that Connects two or more packet-switched networks or Subnetworks.
- It serves two primary functions:
  1. managing traffic b/w these networks by forwarding data packets to their intended IP addeses
  2. Allowsing multiple devie to use the same internet Connection.

0 - defiu all network

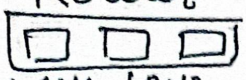
like 192.138.1.0 - defiu all network in 1-255

192.138.2.1 - Specifiu one network.



Router also called firewall or DHCP (Dynamic Host Configuration

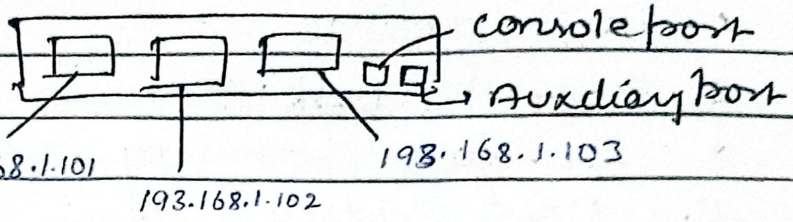
Router



(Port)

→ All are in same Network/Gate.....

SWITCH :



Router - feature -

1. Work as firewall (monitor & control traffic)
2. DHCP (Dynamic Host Configuration Protocol)
   - Give automatic IP address.
3. Wireless network (WiFi) & (MHB wifi)
4. Join more than 1 network

Switch :

It is a device in a computer network that connects other devices together.

Multiple data cables are plugged into a switch to enable communication b/w different networked devices.

CLIENT / SERVER Model

Client - Request Servic

Server - Provide Servic to client.

IP CONFIGURATION

Date.....

1. IP Address :
2. Subnet Mask.
3. Default Gateway
4. DNS Address
5. MAC Address

1. IP Address -

Unique numerical label assigned to each device connected to a computer network.

It enables identification and communication between devices on the network.

2. Subnet Mask -

Used to divide an IP address into network and host portions, determining which part of the address refers to the network and which to the device.

3. Default Gateway -

The device (usually a router) that serves as the forwarding host to other networks or the internet when a device tries to communicate outside its local network.

4. DNS Address :

The address of the domain Name System server, which translates domain names like (www.example.com) into IP addresses that computers use to identify each other

Date.....

5. MAC Address:

Media Access Control address, a unique identifier assigned to network interfaces for communications on the physical network segment, often used for security or identification within local networks

Commands -

Ping:

- Checks if another computer/server can be reached over the network.
- ~~Check~~ Sends small packet, wait for reply. is the target online? What is the response time?

tracert:

- Shows the path your data takes through different routers (hops) to the destination.
- Helpful for seeing where network slowdowns or failure happens.

netstate:

- lists all current network connections and ports on your network.
- Shows which applications are using the network and whether connections are established or just listning.

Orange - Connecting
Green - OK
Red - Not Connected.

802.3 fast Ethernet port
802.1 wifi port

CYBERSECURITY Foundation

KALI LINUX :- Lab setup -

- An OS used to create interface b/w User & Hardware.
- Kali linux came after BackTrack (banned in 2014)

Why:

- Information Gathering : Collect data of Network & str
- Vulnerabilities Analysis - check Weakness
- Web Application Analysis - check & fix.
- Database Assessment.
- Password Attacks.
- Wireless Attack - Wifi
- Reverse Engineering
- Exploitation Tools
- Sniffing & Spoofing
- Post exploitation
- Forensics
- Reporting Tools
- System Services
- Social Engineering tools

CIA — make Trusted OS
Confidentially Integrity & Availability

spiral

+ useradd Arbaaz create user

Gshell :
Bshell:

passwd Arbaaz give password
userdel Arbaaz delete user
kill -9 forcefully kill service

Commands for Kali Linux :

* cd - change directory
* pwd - path
* sudo - give root permission # (~)

- apt-get update :- update system at root user
- sudo apt update → for Normal user
- Figlet Arbaaz - AR
- apt-get install figlet* (for Install)
- apt-get autoremove figlet
  remove

make directory (Folder) - mkdir
create file → cat >Filetest
Empty File → touch File1 File2 --- File n

* ls -l → show details of files & folders
* rmdir → remove directory.
* rm filename → remove file
* rm -rf → forcefully delete any dir or file
* mv file1 dir1
  (source) (designation)
* mv file1 file6 (if not present than it rename automatically)
* gedit file1 (Open file1 & Edit)
* apt-get install leafpad* (for install)
* leafpad file2 (also for edit & write like gedit)
* vim file2 (Edit & Write & Save
  step1 → press i
  write

Date.....

Mutiple directories -

mkdir {1...10} it can create 10 directories

rm -rf * it can remove all

mkdir {a....g} it can create direct from a to g

ls -a show all hiddden files & Folders details

ls -all show permision included all hidden file & dir

ls / show file system hireracky.

umask show file permision

Permissions :-

r	read	4
w	write	2
x	Execute	1

NOTE - By using umask we give permision to any files or folders.

for example:

उगर हमे किसी फाइल को read write को permision देना है then we use umask 011 and after that create that file/folder mkdir test

How it Works:

```
7 7 7     4+2=6 //
0 1 1     r+w
-------
7 6 6
u g o
```

u = user
g = group
o = other

So in this case, I give all permision to User but for group & other, I give only read & write permision.

umask 022 for default permision

chmod 777 dir1 (Give permision to dir 1)
Permision Name

chmod 777 * (Give to all directories & files)
Permision

Spiral

Date.....

Usermod ~~-aG~~ kali ~~root~~

~~chmod~~ ~~777~~ ~~root~~ ~~give permission to root~~

add in Group ↙ group ↙ User

Usermod -aG root kali

~~chmod~~ ~~777~~ ~~root~~

Chown kali /root/Desktop (Change Ownership

~~su~~ ~~kali~~ Su kali - switch user to kali

- Firefox open firefox
- Ctrl + C Exit firefox

top show all running applications

press q for quit

Kill PID No. it can kill the service proces of apps.

Jobs - it can show running proces but in sleep. (in background)

gedit - it is running right now.

eg.

gedit & → & means this service also open but we can do another work at same time

fg → background proces will foreground

Ctrl + C → close service

bg → show background proces or service

Spiral

Date.....

ps - show process

Package Management :-

apt-get install tigervnc*

* Search kali linux repository on Google.
* /etc/apt/source.list:

apt-get install libreoffice* install msoffice

For HYDRA ATTACK

Download Apache Server

apt-get install apache2* downloading/browser/plugin details

Systemctl ~~status apache2~~ show all the Services (Online + Offline)

- Systemctl status apache2 show status of apache
- systemctl start apache2 start/Run apache Serv
- systemctl enable apache2 automatially Run everytim

FTP service

* place → Computer → Trash → Var → WWW → html (delete all)

* Open fb website → Right click → source code → copy.
* Open terminal linux → create a file (fb.html) → Open that fb.html (Vim Fib.html) → Paste all code. Now Sav

ifconfig → Copy ipaddress Now paste ON web.

Date.....

apt-get install Vsftpd*

System ctl status Vsftpd.service – show status
System ctl start Vsftpd.service → start

~~ufw~~ ~~sfo~~

F search → Indian password wordlist
Save dictionary

* Hydra → after do all.
* nmtui ⇒ ?

• apt-get install torbrowser-launcher

Chapter - 02.

Malware and Social Engineering Attack-

Date.....

Malware is a software that enter a computer system as an intruder.

- It is a harmful software
- Widely it is used to damage the program.

Malware Capabilities (uses)-

It is intentionally designed to harm, disrupt or gain unauthorized access to a computer system or network.

It includes various types of malicious software - such as viruses, trojans, worms, Ransomware and spyware, among others.

Malware circulation:

Refers to the distribution and propagation of malware. Malware can circulate through various means, including email attachments, malicious downloads, infected website etc.

Malware injection:

Process of inserting malicious code into a legitimate software program or system to carry out a range of harmful activities, such as stealing info, taking control of the system.

Concealment (Hide) in Malware:

Refers to the techniques used to techniques used by malware creators to hide the presence of their malicious software from detection & analysis

Date.....

Malware payload Capabilities :

Refers to specific actions or activities depending what a malware program is designed to carry out on an infected system. The payload can include a wide range of malicious activities, depending on the goals of malware creator.

ARMORED VIRUS INFECTION TECHNIQUE -

methods used by malware creators to evade detection and analysis by security tools.

1. **Polymorphism :**
   method to change the code of the virus with each infection, making it more difficult to detect.
2. **Encryption :**
   The virus code is encrypted to make it difficult for security tools to analyze it.
3. **Code obfuscation :**
   The technique involves modifying the virus code to make it more difficult for security tools to recognize & analyze it.
4. **Anti-debugging :**
   The virus includes code that detects when it is being analyzed or debugged and takes steps to evade detection.
5. **Rootkit installation :**
   The virus installs a rootkit to hide its presence and evade detection by security tools.

Spiral

CHAPTER : 05

VIRUS & WORMS

Date.....

- VIRUS :→ Communicable (Infected → Original).
  Insert malicious code into a program or data file.
- WORM :→ Use network to travel from 1 to another PC.
  Exploits a vulnerability in an apps or OS.

TROJAN :

Also known as Trojan horse or simply Trojan, is a type of malicious software that is designed to look like a legitimate program, but actually carries out harmful activities on a computer or network.

Keypoints →

- It tricking users into downloading & executing it.
- Once it is executed on victim's device, it can perform a variety of malicious activities such as stealing sensitive data, deleting or modifying files, or giving an attacker remote access to the device.
- It spreads through email attachments, malicious website or free downloads of Soft.
- It can be difficult to detect and remove, as they often operate in stealth mode & hide their presence from user and Anti-malware Software.
- To protect against trojan, it is important to practice safe browsing habits, keep software up to date & OS also. Don't download unknown application. Don't open unwanted application.

RANSOMWARE: Date.....

Ransomware is a type of "malicious software" (malware) that **encrypts a victim's files** and "demands payment" in exchange for the decryption key.

- It make victim's data encypted & after payment the hacker make your data decrypted by usually it happens in Companies

* It can spread through phishing emails, malicious websites or through vulnerabilities in software or OS.

CRYPTOMALWARE —

It is also known as crypto-ransonware, is atype of malicious software that encrypts a victim's files and demands payment in exchange for decryption key, Similar to regular ransomware

ROOTKITS —

It is a type of malicious software that allows an attacker to gain persistent (forcefully) access to victim's computer or network while remaining undetected.

It typically work by modifying the core component of kernel or driver or OS in order to hide their presence.

Shiva!

Date.....

SPYWARE —

It is designed to monitor the victim's activities on their computer or mobile device, often without their knowledge or consent

Used for stealing sensitive info, login credentials, financial data, recording audio and videos, display unwanted advertisement

KEYLOGGER — hardware & Software both type

It is a type of malicious software that is designed to capture and record the keystrokes entered by a victim on their computer or mobile device.

- Capture and record the password, username, credit number etc--

ADWARE —

designed to display advertisement on user's computer or mobile device. While adware can be a legitimate way for developer to monetize their software, it can also [illegible]

Date.....

SOCIAL ENGINEERING ATTACK –

It is a type of attack that exploits human psychology and behavior to trick people into divulging (to find) confidential details performing an actions or compromising a system.

It is a non-technical type of attack that focuses on manipulating human weakness to Gain access to sensitive info.

Various forms → phishing, pretexting, Baiting, Tailgating, Quid pro quo etc.