CO2:- Demonstrate the applicable footprinting techniques and Scanning methods.

Syllabus:- Footprinting, Types, Using ping and ns lookup commands in windows command line, Scanning, Basics of scanning, Basic Techniques of Scanning, Enumerating DNS using dns enum, Performing flag scan using hping3.

→ Footprinting:- It is first phase in hacking. In this collection of information took place. Information which is generally available may contain sensitive information. using footprinting attacker can collect information like emails, contacts, domain name information and using social engineering even more sensitive data.

It is necessary step, to gather the information this step is used further to exploit or hack the target. In this module various aspects of footprinting would be covered.

→ Types :- 1) Internal Footprinting.
2) External Foot printing.

1) Internal Footprinting:-

Footprinting performed inside the network is known as internal footprinting. In this, attack may access internal network or is directly or indirectly connected to the internal network.

In the Internal Footprinting the following attacks can be used :-

a) Dumpster Diving :- Looking for sensitive information in garbage or dumps is known as dumpster diving. Sometimes, attacker may find a piece of paper of some important documents from which sensitive information can be retrieved. when penetration testing or hacking is performed each and every possible aspect of gathering information is taken into consideration

b) Shoulder Surfing :- Looking at shoulder or guessing the password by viewing a person typing or indirectly seeking into his hand movement to get password. Sometimes it provides quite sensitive information

c) Private Websites :- If attacker found any private websites of the target, it becames treasure for him as he can gain bunch of sensitive information like employee and client details etc.

2) External Foot printing :-

when attacker is not connected to the target network, in order to gather information, external foot printing is used. Generally external foot printing provides huge number of information about the data.

There are lots of ways and possibilities to gather the information from out side of network.

In the external footprinting the following attacks can be used:-

1) Website :- Website of the target may contain some sensitive information or may be a vulnerable. from the website, attacker can easily get the contact details like e-mails and phone numbers, attacker can simply call and perform social engineering in order to gain sensitive information Besides, attacker can also perform social engineering over e-mails.

2) Google :- It is one of the biggest search engine and helping hand for a hacker. sometimes simply googling about target can give much sensitive information like admin contents or about target profiles over social media.

3) Whois :- It is a tool which is used to gather information about target domain like name server, domain records, admin contacts and other relative information. Whois is one of the major information provider and this information is used in writing penetration testing reports. It also contains almost every domain.

www.whois.sc is one of the popular website to check whois information.

* Using whois.sc
  - → Navigate to www.whois.sc
  - → It provide's domain name
  - → Crawl and look for required information (Information will be look like screen shot.)

4) Domain Name Server (DNS) :- DNS footprinting provide information same as of whois, sometimes attacker get sensitive information which lead to compromise of Domain of target.

5) Social Networking :- Public profiles on social network contain contact information and activity details.

Target may be social engineered easily over social networking which lead to disclosure of sensitive information.

6) Social Engineering :- It is art of human exploitation. It is one of the major attack which leads to vast compromises. social engineering may be tool based or human based.

In tool based, tools like phishing, tabnapping and Social Engineering toolkits are used.

In human based, manupating the target is used to gain sensitive information like client details and passwords ... etc.

7) Archive websites:- There are some websites over internet which keeps archives of almost every websites. looking in Archives can provide sensitive information about the target. way back Machine is one of the website which contains archives of websites.

* using way Back machine:-

→ navigate to www.archives.org.
→ Input target domain
→ check the archives, highlighted dates are the dates when website is updated

→ Footprinting tools:-

Footprinting can be used using the following tools:-

1) Ping:- It is a command line tool used to check the target is live or not. only if target is live, further exploitation can be done.

Using Ping in windows command line:-

a) Open Command Prompt (CMD) in windows (press windows + R and type cmd)

b) Type "ping target" (replace target with IP or website of target)

Ex: Ping www.xyz.abc or ping 127.0.0.1

c) packet will be transferred between attacker and target. 0% loss indicates ping command completed and packets are successfully transferred.

d) TTL stands for Time to live and generally 4 packets are transferred between attacker and target but it can be increased.

e) To understand more about ping command, type ping -h or ping /? In terminal. It will open help for ping command. It can be used in linux as well.

2) nsLookup :- It is a command line tool used to gather information about name server of target.

Using nsLookup in windows command line :-

a) Open Command Prompt (CMD) in windows (press windows + R and type cmd).

b) Type "nslookup target" (replace target with IP or website of target).
Ex:- nslookup www.xyz.abc or nslookup 127.0.0.1

c) To access interactive mode type nslookup and hit enter.

d) you can gather following information

e) To understand more about ping command, type nslookup -h or nslookup /? in terminal. It will open help for nslookup command. It can be used in linux as well.

f) you can change for looking up mail server, SOA (Service oriented Architecture) and different services.

→ Scanning :- It is a phase of information gathering in which attacker gather more advanced information about the target like open ports and services running, ~~operating~~ operating system of the target etc.

Generally this phase gives us vulnerable point about the target. Information gathered by scanning is very important in performing actual Hack. It is an important phase which help in gaining access into the system. In scanning, port scanning, os finger printing, DNS enumerating etc. will be covered.

Attacker → OSI Layer (3&4) → Target Network.

Between attacker and target the core OSI module layers, layer 3 which is IPv4 and IPv6 and icmp and layer 4 which is TCP and UDP is present. Transmission over a network is done through these layers. It is compulsory to understand the working of layer 3 and layer 4 of OSI module if attacker wish to penetrate over network layer.

There are two ways of scanning :-

* Active scanning (Port scanning)
* Passive scanning (connectivity of host)

* Active Scanning :- It is a type of network scanning technique that is used to gather information about a target system or network. It actively interacts with the target system to gather information.

It involves sending requests or packets to a target system and analyzing the responses to gather information about the target.

It can be performed using a variety of tools and techniques, including portscanning, Vulnerability Scanning and penetration testing.

* Passive Scanning :- It is a type of network scanning technique that is used to gather information about a target system or network without actively interacting with the target.

It only gathers the information that is readily available, such as information transmitted over the network or stored in system logs.

It is used to gather information about a target system or network for a variety of purposes, including network mapping, vulnerability assessment, and compliance testing.

→ Basic techniques of scanning:-

1) Ping Sweep:- Ping Sweep is scanning a range of ip address one by one to check whether the target ip is alive or not. In this technique a range of ip address is defined in the same ping command just like: ping 123.43.23.45/24, the whole range of ip address is scanned until or unless live target is found.

2) Transmission control protocol (TCP): It contains flag, sniffing into tcp flags can provide information to a gather extent. There are following flags present in tcp.

A) SYN: synchronize, initiates the connection between two systems.

B) FIN: Finish, Indicates that transmission is Finished

c) ACK: Acknowledgement, It establish the connection.

D) RST: Reset, used for resetting the connection established.

E) URG: Urgent, gives packet a priority to process immediately.

F) PSH: PUSH, instructs the target to respond with buffer data immediately

3. 3-way Handshake Mechanism :- It is used for successful transmission of information or successful connection establishment.

* Process :- → The system will initiate a connection request to the server via a packet with only SYN FLAG.

→ Server will reply back with packet having both SYN & ACK flag set.

→ Now the client responds back to the server with a single ACK packet.

→ If the above steps are completed without any problem or complication, Then a TCP connection will be established b/w the client and server.

4) Full scan :- In this, Full TCP connection is established between attacker and target. If the port is open then only connection will be established.

5) IDLE Scan :- In this the attacker performs scanning without sending a single packet from own IP address to the target. Zombies are used in IDLE scan. Attacker spoofs the IPID of the zombie system (spoofed system which is under control of attacker). and SYN/ACK packets by the target are received by that zombie system.

6) Half open Scan :- In this Full TCP connection is not completed. Attacker send SYN packet to initiate the connection, if target responds back with ACK packet then attacker consider that target is listening and if target replies back with RST packet then target is not open.

7) XMAS Scan :- It don't work against any versions of windows, if tested on windows machine it lists all the ports as closed. It works only if the standard of tcp/ip implementation is used which is based on RFC 793.

8) ICMP-ECHO Scan :- It is used to check whether all the hosts in the target network are live or not by pinging them all.

9) UDP Scan :- It doesn't contains any flag. Though it don't contain any packet, UDP is simple but at the same difficult to perform scan.

-> Scanning using tools :-

-> Nmap

-> DNS enum

-> Hping3

* Nmap :- It is a powerful network mapping tool. It is mainly used to perform port scanning and fingerprinting. open kali Linux terminal and type nmap -h. It will show the help window of Nmap.

1) Port Scanning Using Nmap :-

a) Open terminal in kali linux, type "ifconfig". It will show internet address and mac address, to specifically check for Ethernet interface type "ifconfig eth0".

b) Open new terminal, type "nmap -h". It will open nmap help screen

c) Name command structure is: nmap [scan type] [target] [target specification]

d) To check how nmap works, Etherape and wireshark are used.

e) To install the etherape, open new terminal and type "apt-get install etherape". Input Y for the additional space.

f) Open a terminal and type "wireshark". wireshark windows will opens, now select the layers on which analysis has to take place. click on start capturing.

g) Open a terminal and type "Etherape". once the packets starts exchanging, the network traffic will be illustrated in etherape.

h) Nmap will list all the ports open and this information is used to exploit the vulnerable ports.

g) OS Fingerprinting using Nmap :-

a) Open terminal in kali linux, type "ifconfig". It will show your internet address and mac address, to specifically check for Ethernet interface type "ifconfig eth0".

b) Open new terminal, type "nmap -h". It will open nmap help screen.

c) Name command structure is : nmap [scan type] [target] [target specification]

d) For OS Fingerprinting : nmap -O [target.]

e) Nmap will list all the open ports along with the operating system running on target machine. It may be range or operating system like XP sp1 - sp3 or specified OS.

→ Dnsenum :

Dnsenum is one of the powerful dns enumeration tool, pre-installed in kali linux.

Enumerating DNS using dns enum :-

a) Open terminal in kali linux and type "dnsenum -h". Help screen will be shown up.

b) Command for performing enumeration is "dnsenum [target]"

c) For ex: dnsenum www.xyz.abc

d) Details of dns will be enumerated as shown in screenshot.

f) There are many information gathering tools which are pre-installed in kalilinux.

Note:- to check working of any tool, just type "[tool name] -h" or "[tool name] /?"

→ Hping3: It is a powerful tool which is pre-installed in kali linux. Hping is used for advanced pinging, packet crafting, flooding the target by dos and many other uses.

To take the overview of hping tool, open terminal in kali linux and type "hping3 -h", it will open help screen of hping tool. there are many options for performing various attacks.

* performing flag scan using hping3:-

a) Open terminal in kali linux and type "wireshark". will be opened and choose interface on which packet sniffing is to be performed.

b) Open new terminal and type "hping -S [target]".

c) Once the command is completed, maximize the wireshark window and analyse the packets, all the captured packets will be SYN Packet.

d) Practise for various attack vectors of hping3. It is one of the important tools which is also useful in later stages.