UNIT-2

1.What is Footprinting and types of Footprinting?

Footprinting is the technique to collect as much information as possible about the targeted network/victim/system. It helps hackers in various ways to intrude on an organization's system. This technique also determines the security postures of the target. Footprinting can be active as well as passive.

Passive footprinting/pseudonymous footprinting involves collecting data without the owner, knowing that hackers gather his/her data.

In contrast, active footprints are created when personal data gets released consciously and intentionally or by the owner's direct contact.

2.Explain Footprinting through Social Networking Sites using sherlock.

Footprinting through Search Engines

This is a passive information gathering process where we gather information about the target from social media, search engines, various websites etc. Information gathered includes name, personal details, geographical location detrails, login pages, intranet portals etc. Even some target specific information like Operating system details, IP details, Netblock information, technologies behind web application etc can be gathered by searching through search engines

Eg: collecting information from Google, Bingo etc

Email Footprinting

email header reveals information about the mail server, original sender's email id, internal IP addressing scheme, as well as the possible architecture of the target network

Google Hacking/Google Dorks

This is a process of creating search queries to extract hidden information by using Google operators to search specific strings of text inside the search results.

Some google operators, site, allinurl, inurl, allintitle

DNS Footprinting

DNS is a naming system for computers that converts human-readable domain names into computer readable IP-addresses and vice versa. DNS uses UDP port 53 to serve its requests. A zone subsequently stores all information, or resource records, associated with a particular domain into a zone file; Resource records responded by the name servers should have the following fields:

- **Domain Name** — Identifying the domain name or owner of the records
- **Record Types** — Specifying the type of data in the resource record
- **Record Class** — Identifying a class of network or protocol family in use
- **Time to Live (TTL)** — Specifying the amount of time a record can be stored in cache before discarded.
- **Record Data** — Providing the type and class dependent data to describe the resources.

Footprinting through Social Engineering:

- Social media like twitter, Facebook are searched to collect information like personal details, user credentials, other sensitive information using various social engineering techniques. Some of the techniques include
- **Eavesdropping:** It is the process of intercepting unauthorized communication to gather information
- **Shoulder surfing:** Secretly observing the target to gather sensitive information like passwords, personal identification information, account information etc

3.What is network scanning and explain different types of Scanning

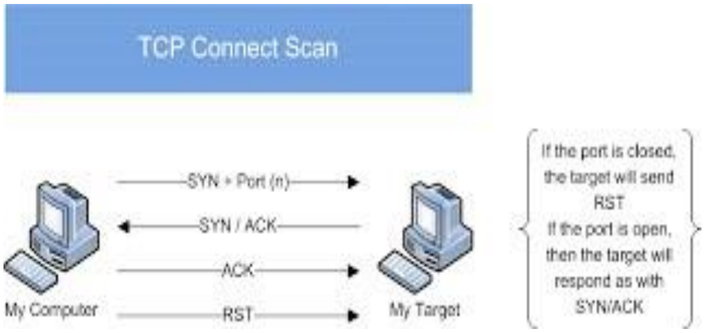
Network scanning is one of the components of intelligence gathering and information retrieving mechanism an attacker used to create an overview scenario of the target organization

<u>Types of Scanning</u>

1. Connect scan
2. Half-Open-Scan / Stealth scan
3. XMAS scan
4. FIN scan
5. ACK scan
6. Null scan
7. Idle scan
8. Port Scanning
9. Network Scanning
10. Vulnerability Scanning

XMAS scan: This is a l so called as inverse TCP scanning. This works by sending packets set with PSH,URG,FIN flags. The targets do not respond if the ports are open and send are set response if ports are closed.

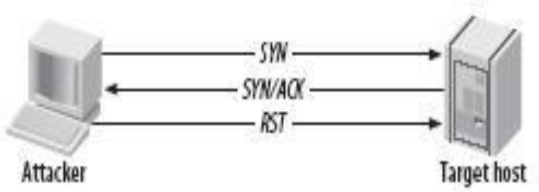
Connect scan: Identifies open ports by establishing a TCP handshake with the target.



If the port is closed, the target will send RST
If the port is open, then the target will respond as with SYN/ACK

Nmapcommand:nmap-sT -v-p-<TargetIP>

Half-open scan otherwise known as **Stealth scan** used to scan the target in a stealthy way by not completing the TCP handshake by abruptly resetting the communication.



Nmapcommand:nmap-sS -v<TargetIp>

FIN scan: F in flag is set in the TCP packets sent to the target. Open ports do not respond while closed ports send are set response.

ACK scan: Here the attacker sets the ACK flag in the TCP header and the target's port status is gathered based on window size and TTL value of RESET packets received from the target.

Null Scan: Works by sending TCP packets with no flags set to the target. Open ports do not respond while closed ports respond with a RESET packet.

Idle Scan: Here the attacker tries to mask his identity uses an idle machine on the network to probe the status detail softer get ports.

Port Scanning: In this process the hacker identifies available and open ports and understands what services are running. You must understand the ports and port numbers. The ports number scan be in these three ranges:

1. Well known Ports from 0 to 1023
2. Registered ports from 1024 to 49151
3. Dynamic Ports from 49152 to 65535

Banner Grabbing: Is a process of collecting information like operating system details, the name of the service running with its version number etc.

Network Scanning: This means to look for active machines or targets on the network. This can be done using tools or scripts that ping to all IP addresses on the networks and get a list of the alive nodes and their IP addresses.

Vulnerability Scanning: This is the mechanism where the target is scanned or looked for any vulnerability. In this scan the Operating system is found out with installed patches etc. and then based on the information vulnerabilities are found in that particular version of Operating System.

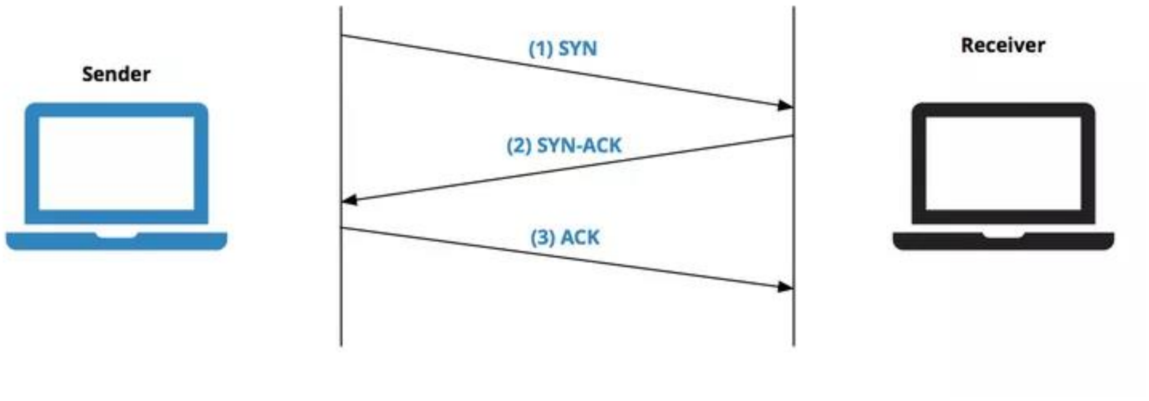
4.Explain TCP Communication Flags.

TCP flags are used within TCP packet transfers to indicate a particular connection state or provide additional information. Therefore, they can be used for troubleshooting purposes or to control how a particular connection is handled. There are a few TCP flags that are much more commonly used than others as such SYN, ACK, and FIN. However, in this post, we're going to go through the full list of TCP flags and outline what each one is used for.

List of TCP flags

Each TCP flag corresponds to 1 bit in size. The list below describes each flag in greater detail. Additionally, check out the corresponding RFC section attributed to certain flags for a more comprehensive explanation.

- SYN - The synchronization flag is used as a first step in establishing a three-way handshake between two hosts. Only the first packet from both the sender and receiver should have this flag set. The following diagram illustrates a three-way handshake process.



- ACK - The acknowledgment flag is used to acknowledge the successful receipt of a packet. As we can see from the diagram above, the receiver sends an ACK as well as a SYN in the second step of the three-way handshake process to tell the sender that it received its initial packet.
- FIN - The finished flag means there is no more data from the sender. Therefore, it is used in the last packet sent from the sender.
- URG - The urgent flag is used to notify the receiver to process the urgent packets before processing all other packets. The receiver will be notified when all known urgent data has been received.
- PSH - The push flag is somewhat similar to the URG flag and tells the receiver to process these packets as they are received instead of buffering them.
- RST - The reset flag gets sent from the receiver to the sender when a packet is sent to a particular host that was not expecting it.
- ECE - This flag is responsible for indicating if the TCP peer is ECN capable.
- CWR - The congestion window reduced flag is used by the sending host to indicate it received a packet with the ECE flag set. NS (experimental) - The nonce sum flag is still an experimental flag used to help protect against accidental malicious concealment of packets from the sender.

5.Explain about DNS and SMB enumeration countermeasures

SNMP:

- Remove the SNMP agent or turn off the SNMP service
- If shutting off SNMP is not an option, then change the default community string name
- Upgrade to SNMP3, which encrypts passwords and messages
- Implement the Group Policy security option called "Additional restrictions for anonymous connections"
- Ensure that the access to null session pipes, null session shares, and IPSec filtering is restricted.

DNS:

- Disable the DNS zone transfers to the untrusted hosts
- Make sure that the private hosts and their IP addresses are not published into DNS zone files of public DNS server
- Use premium DNS registration services that hide sensitive information such as HINFO from public
- Use standard network admin contacts for DNS registrations in order to avoid social engineering attacks

6.Explain about Horizontal and Vertical Privilege Escalation.

- **Vertical Privilege Escalation**

Vertical privilege escalation occurs when an attacker gains access directly to an account with the intent to perform actions as that person. This type of attack is easier to pull off since there is no desire to elevate permissions. The goal here is to access an account to further spread an attack or access data the user has permissions to.

Day in and day out I analyze numerous phishing emails that attempt to perform this attack. Whether it's a "bank", "Amazon", or any other countless number of ecommerce sites, the attack is the same. "*Your account will be deactivated due to inactivity. Please click this link and login to keep your account active."* This is, however, one example of many cookie-cutter phishing templates seen in "the wild".

- **Horizontal Privilege Escalation**

Horizontal privilege escalation is a bit tricky to pull off as it requires the attacker to gain access to the account credentials as well as elevating the permissions. This type of attack tends to require a deep understanding of the vulnerabilities that affect certain operating systems or the use of hacking tools.

Phishing campaigns have been used to perform the first part of the attack to gain access to the account. When it comes to elevating permissions, the attacker has a few options to choose from. One option is to exploit vulnerabilities in the operating system to gain system or root-level access. The next option would be to use hacking tools, like Metasploit, to make the job a bit easier.

7.How to Defend against privilege Escalation?

1. **Fully manage the identity lifecycle**, including provisioning and de-provisioning of identities and accounts to ensure there are no orphaned accounts that could be hijacked.

2. **Use a password management solution** to consistently apply strong credential management practices (discovery, vaulting, central management, check-in, check-out) for both human and machines. This also entails eliminating default and hardcoded credential.
3. **Enforce least privilege**: Remove admin rights from users and reduce application and machine privileges to the minimum required. Just-in-time access should also be implemented to reduce persistent or standing privileges.
4. **Apply advanced application control and protection** to enforce granular control over all application access, communications, and privilege elevation attempts.
5. **Monitor and manage all privileged sessions** to detect and quickly address any suspicious activity that might indicate a hijacked account or an illicit attempt at privilege escalation or lateral movement.
6. **Harden systems and applications**: This complements the principle of least privilege and can involve configuration changes, removing unnecessary rights and access, closing ports, and more. This improves system and application security and helps prevent and mitigate the potential for bugs that leave vulnerability to injection of malicious code (i.e. SQL injections), buffer overflows, etc. or other backdoors that could allow privilege escalation.
7. **Vulnerability management**: Continuously identify and address vulnerabilities, such as with patching, fixing misconfigurations, eliminating default and/or embedded credentials, etc.
8. **Secure remote access** should always be monitored and managed for any form of privileged access since attacks can occur horizontally and vertically to exploit privileges.

8.Explain about different techniques followed by an attacker to cover his/her tracks on the target system.

Clearing Tracks

- Covering tracks refers to the activities carried out by an attacker to hide malicious acts
- The attacker’s intentions include: continuing access to the victim’s system, remaining unnoticed and uncaught, deleting evidence that might lead to his prosecution
- The attacker overwrites the server, system, and application logs to avoid suspicious