**Methods of Information Gathering-**

There are the following three methods of information gathering:

* Footprinting
* Scanning
* Enumeration

**Footprinting-**

In this technique, the information of a target network or system or victim is collected as much as possible. Footprinting provides various ways to intrude on the system of an organization. The security posture of the target is also determined by this technique. It can be active as well as passive. In Passive footprinting, the information of any user is collected without knowing him. If the user's sensitive information gets released intentionally and consciously or by the direct contact of the owner, active footprinting will be created.

Footprinting techniques are three types. These are as follows:

* Open source footprinting
* Network-based footprinting
* DNS interrogation

**Open source footprinting**

Open source footprinting is the safest footprinting. The limitation of footprinting is illegal. It is illegal; that's why hackers can do open source footprinting without fear.

Examples of open source footprinting include DOB, phone number, search for the age, finding someone's email address, using an automation tool scans the IP, etc. Most companies provide information on their official websites related to their company. Hackers will use the information provided by the company and take benefit from them.

**Network-based Footprinting**

Network-based footprinting is used to retrieve information like network service, information name within a group, user name, shared data among individuals, etc.

**DNS interrogation**

After gathering all the required information on various areas using different techniques, the hacker uses the pre-existing tools to query the DNS. DNS interrogation is performed by many freeware online tools.

**Scanning-**

Another essential step of footprinting is scanning, which contains the package of techniques and procedures. In the network, hosts, ports and various services are identified by it. It is one of the components of information gathering mechanism and intelligence gathering, which is used by an attacker to create an overview scenario of the target. To find out the possibility of network security attacks, pen-testers use vulnerability scanning. Due to this technique, hackers can find vulnerabilities like weak authentication, unnecessary services, missing patches, and weak encryption algorithms. So an ethical hacker and pen-tester provide the list of all vulnerabilities they found in an organization's network.

There are three types of scanning-

* Port scanning
* Network scanning
* Vulnerability scanning

**Port scanning**

Hackers and penetration testers use this conventional technique to search for open doors so that the hackers can access the system of any organization. Hackers need to identify the live hosts, topology of the target organization, firewall installed, different devices that are attached to the system, operating system used, etc., during this scan. Once the hacker fetches the IP address of the victim organization by scanning ports of UDP (user datagram protocol) and TCP (transmission control protocol), they map the organization's network under his grab. Port scanning is performed by the Amap tool.

**Network scanning**

You should understand the process of 3-way TCP/IP handshaking before learning the vulnerability scanning techniques. Handshaking is the automated process in which communication between two entities is set using some protocols. To provide handshaking between the server and client, two protocols, TCP and IP, are used. A synchronized packet sends by the client to establish a connection. The server listens to the packet and responds to the client with a syn/ack packet. The client again responds by sending the ack packet to the server. The initialized connection between server and client in packets is denoted by SYN (synchronization). The establishment of a connection between hosts is denoted by ACK.

There are various scans used by **Network scanning techniques**, which are as follows:

* SYNScan: The three-way handshaking technique of TCP is not completed by an SYN scan or stealth. An SYN packet is sent by the hacker to the target, and if the hacker receives back the SYN/ACK frame, the connection would be completed by the target, and the port is able to listen anything. If the target retrieves the RST, it will assume that the ports are not activated or closed. Some IDS system logs this as connection attempts or an attack that why SYN stealth scan is advantageous.
* XMASScan: This scan is used to send the packet containing PSH, FIN, and URG flags. The target will not provide any response if the port is open. But an RST/ACK packet is responded by the target if the port is closed.
* FINScan: XMAS scan and FIN scan is almost the same except that it does not send a packet with PSH and URG flags; it only sends packets with a FIN flag. The response and the limitations of the FIN scan are the same as the XMAS scan.
* IDLEScan: This scan determines the sequence number of IP header and port scan response and sends the SYN packet to the target using the spoofed/hoax IP. The port is open or not depends upon the response of the scan.
* Inverse TCP Flag scan: In this scan, the TCP probe packet with no flags or TCP flags send by the attacker. If the target does not provide any response, it means the port is open. If the RST packet is responded by the target, it means the port is closed.
* ACK Flag Probe Scan: In this scan, TCP probe packets are sent by the attacker where the ACK flag is set to a remote device, analyzing the header information. The port is open or not signified by the RST packet. This scan also checks the filtering system of the victim or target.

**Vulnerability scanning**

Vulnerability scanning is a proactive identification of Vulnerabilities on the target network. Using some automatic scanning tools and some manual support, vulnerabilities, and threats can be identified. To provide vulnerability scanning, the computer should have an internet connection.

The ports and network can be scanned by the following tools:

* Nmap: It is used to extract information like operating system, packet filters or firewall type, live host on network, version of the operating system.
* Angry IP scanner: It is used to scan for systems availability within the given range of input.
* Hping2/Hping3: They are network scanning tools and command-line packet crafting. TCP/IP protocols use them.
* Superscan: Macfee, which is a TCP port scanner, develops this powerful tool. A super scan is used for pinging.
* ZenMap: ZenMap is a very powerful GUI tool. It is used to detect the port scanning, ping sweep, OS type, version of OS, etc.
* Net scan Tool: It contains different types of tools. It is used to perform the web rippers, flooding, mass emailers, port scan. This tool is available as a trial version, but it is also has a paid version.

**Enumeration-**

Enumeration is the process in which information is extracted from the system like machine names, user names, network resources, shares and services. In enumeration, an active connection is established with the system by the hacker. Hackers use this connection and gain more target information by performing direct queries. If the attacker wants to directly exploit the system, the outcome of the enumeration phase is very useful for them. That's why, in penetration testing, the enumeration phase is considered risky.

There are various types of enumeration. These are as follows:

* **NetBIOS Enumeration**: NetBIOS means Network Basic Input Output System. It is developed by IBM. If you want to enumerate NetBIOS on Windows OS, printer and file server should be enabled. Using NetBIOS, an attacker can perform a DOS attack on a remote machine.
* **SNMP Enumeration**: SNMP means Simple Network Management Protocol. If the network device is run on Internet Protocol (IP) like a router, SNMP will be used for managing the device. It is based on the client-server architecture. Every network device has the SNMP client or agent, and using the request and response; it communicates with the SNMP managing station. Agent software can access the SNMP request and response, which are the configurable variable. Using the SNMP enumeration, an attacker can get information on network resources like devices, shares, routers, etc. An attacker can get device-specific information, traffic statistics, and ARP and Routing table by enumerating the SNMP on the remote device.
* **LDAP Enumeration**: LDAP means Light Weight Directory Access Protocol. It is based on the client-server architecture. The distributed directory services can be accessed by LDAP. Directory service is used for storing user's records, and it is a logical and hierarchical structure. Using the BER (Basic Encoding Rules), the information transmits between server and client. The LDAP transmits over TCP (Transmission control protocol). If the server has an anonymous remote query, LDAP supports it. Using the query, the sensitive information of users like contact details, address, user name, department details, etc., can be accessed.
* **NTP Enumeration**: NTP means Network time protocol. Clocks of network computers are synchronized by the NTP. If NTP is in ideal condition, it can achieve 200 milliseconds accuracy in the local area network. It is based on agent-server architecture. It works on port 123 and UDP (user datagram protocol). The NTP server is queried by the NTP agent. If the attacker queries the NTP server, they can enumerate the host's list, which is connected to the server of NTP. They can also enumerate the operating system, hostname and IP address of the internal clients.
* **SMTP Enumeration**: SMTP means Simple Mail Transfer protocol. It is used to transmit electronic mail. It is based on the client-server architecture. It works on port number 25 and TCP (Transmission control protocol). To send the mail through DNS, it will use the MX server (Mail exchange server).

The following built-in commands are given by SMTP:

VERY: In the SMTP server, this command validates the users.

EXPN: It is used to identify the list of mails and deliver the address of aliases.

RECT TO: It is used to define the message's recipients.

The response of the SMTP server towards the above command is different. Because of the varied response of SMTP, SMTP enumeration is possible. Using the same technique, an attacker can find a valid user on the server of SMTP.

* **DNS Enumeration**: DNS means Domain name service. DNS is used to store the record using the DNS database. In DNS, the most commonly used types of record are as follows:

Domain name aliases

IP Address

Nameservers

Start of authority

Pointers for reverse DNS lookups

Mail exchange

DNS works on TCP (Transmission control protocol) as well as UDP (User datagram protocol). It uses port number 53. In DNS, TCP is used for zone transfer, and UDP is used for resolving queries. The database's position can be replicated from the primary server to the secondary server using the DNS zone transfer. DNS enumeration is possible when the DNS primary server is requested by the zone transfer and pretends like a client. In response to the request, it reveals the sensitive information related to domain records.

* **Windows Enumeration**: Windows Os and Sysinternals tools can be enumerated together. You can download the many more Sysinternals tools using the URL https://technet.microsoft.com/en-in/sysinternals/bb545021.aspx.
* **LINUX/UNIX Enumeration**: Linux or Unix OS and Multiple command-line utilities can be enumerated together. The utilities are provided by the operating system.