MODULE 2

Tools for Foot Printing

- Footprinting is an ethical hacking technique used to gather as much data as possible about a specific targeted computer system, an infrastructure and networks to identify opportunities to penetrate them. It is one of the best methods of finding vulnerabilities.
- The process of cybersecurity footprinting involves profiling organizations and collecting data about the network, host, employees and third-party partners. This information includes the OS used by the organization, firewalls, network maps, IP addresses, domain name system information, security configurations of the target machine, URLs, virtual private networks, staff IDs, email addresses and phone numbers.
- There are two types of footprinting in ethical hacking:
  1) *Active footprinting*
  2) *Passive footprinting*
  3) *DNA footprinting*
  4) *Ecological footprinting*
  5) *Digital footprinting*

- ***Active footprinting*** describes the process of using tools and techniques, like using the traceroute commands or a ping sweep -- Internet Control Message Protocol sweep -- to collect data about a specific target. This often triggers the target's intrusion detection system (IDS). It takes a certain level of stealth and creativity to evade detection successfully.
- ***Passive footprinting*** involves collecting data about a specific target using innocuous methods, like performing a Google search, looking through Archive.org, using NeoTrace, browsing through employees' social media profiles, looking at job sites and using Whois, a website that provides the domain names and associated networks fora specific organization. It is a stealthier approach to footprinting because it does not trigger the target's IDS.
- ***DNA footprinting*** is the method used to identify the nucleic acid sequence that binds with proteins.
- An ***ecological footprint*** is an approach to measuring human demand for natural capital or resources. It calculate the amount of natural resources required to support people or an economy. Ecological footprinting uses an ecological accounting system to keep track of this demand.

- A ***digital footprint*** describes one's unique, traceable digital activities. These include actions, communications and contributions expressed on the internet or digital services. Digital footprints can be either active or passive.
- Footprinting processes start with determining the location and objective of an intrusion. Once ethical hackers identify a specific target, they gather information about the organization using nonintrusive methods, such as accessing the organization's own webpage, personnel directory or employee bios.
- Ethical hackers collect this information and initiate social engineering campaigns to identify security vulnerabilities and achieve ethical hacking goals.
- Footprinting techniques in ethical hacking help businesses identify and secure IT infrastructure before a threat actor exploits a vulnerability.
- Users can also build a database of known vulnerabilities and loopholes.
- Footprinting also helps companies better understand their current security posture through analysis of data gathered about the firewall, security configuration and more.
- Users can update this list periodically and use it as a reference point during security audits.
- Drawing a network map helps cover all trusted routers, servers and other network topologies.
- Users can pursue a reduced attack surface by narrowing it down to a specific range of systems.
- ***Tools for footprinting includes:***
  - ***Conducting Competitive Intelligence:***
    - ✓ *Competitive intelligence is the process of gathering and analyzing information about competitors to gain insights into their strategies, strengths, weaknesses, and market positioning.*
    - ✓ *It involves monitoring competitors' online presence, marketing campaigns, pricing, product offerings, and customer feedback.*
    - ✓ *Understanding the competitive landscape, businesses can make informed decisions, identify opportunities to gain a competitive advantage in the market.*
    - ✓ *The key to competitor intelligence is that second word – intelligence. Information gathered however formally or informally won't help a company unless it is analyzed thoughtfully or carefully.*
    - ✓ *You can use the insights gained through competitive intelligence to improve your current marketing strategy and respond appropriately to the current competitive landscape.*

- ***Google Hacking***
  - ✓ *Google hacking or Google dorks is the process in which information is gathered by creating search queries with the help of Google operators.*
  - ✓ *This type of footprinting stores information like passwords or information relevant to any topic or competitor.*
  - ✓ *Google Dorking involves using advanced search operations in Google to search for specific keywords, file types, or website parameters.*
  - ✓ *These operators can be combined to create more powerful search queries that can reveal information that would not be easily accessible otherwise.*
  - ✓ *While Google Dorking can be used for legitimate purposes such as researching a website's security vulnerabilities, hackers use this technique maliciously to find sensitive information such as usernames, passwords, and other potential information. As a result, it is important for website owners to secure their websites and avoid exposing sensitive information in publicly accessible directories.*
  - ✓ *In addition, internet users should also be careful about the information they share online and use strong, unique passwords for each of their online accounts to avoid falling victim to a cyberattack.*
  - ✓ *Overall, Google Dorking is a powerful technique that can be used for both good and bad purposes. Website owners and internet users should be aware of its potential risks and take steps to protect themselves from any potential security breaches.*
- ***Scanning & Enumeration***
  - ✓ *Scanning and enumeration is the phase where the attacker begins to "touch" the systems. Attackers will scan networks to discover live hosts and open port. They will then enumerate the live hosts and ports to discover services, machine names, and other network resources.*
  - ✓ *there are several more types of scanning:*
    - ***Network Scanning***

      As discussed above, network scanning is the technique of scanning the devices and systems in a network for vulnerabilities and inconsistencies. Its role is to help admins and ethical hackers find and fix vulnerabilities so that hacking attacks on the network can be avoided.

- ***Port Scanning***

  Penetration testers use port scanning techniques to identify the open ports or doors in a system that can be compromised by attackers. If compromised, the hackers can find the live hosts, firewalls, OS, and devices connected to the system.

- ***Vulnerability Scanning***

  It is the automated scanning of the systems in a network to find whether there are any vulnerabilities or loopholes.

- ***TCP Scanning***

  TCP scanning uses the port scanning method. It scans all the ports in a system or network to find the ones that are open, half-open or closed. In case a port is found open, the OS will perform the TCP three-way handshake. The scanner will end the connection so that DoS attacks can be avoided.

- ***UDP Scanning***

  UDP port scanners are used for finding the open ports in the user datagram protocol. If a port is found open, there will be an ICMP port unreachable response. However, it also considers those ports open which are blocked by firewalls or the 'port unreachable' message is blocked.

- ***SYN Scanning***

  SYN scanning is a part of TCP scanning. In this method, the port scanner doesn't use the network functions of the OS, but creates new IP packets and checks the responses. SYN scanning doesn't fully open the TCP connection. Hence, it is also referred to as half-open scanning. An SYN packet is created and sent to all the ports. For open ports, there will be an SYN-ACK response. For closed and unfiltered ports, there will be an RST response.

- ***ICMP Scanning***

  The role of ICMP scanning is to map network topology. It stands for Internet Control Message Protocol. When ICMP scanning is attempted, it receives three types of responses- normal, possibly suspicious, and highly suspicious.

✓ *Enumeration is the stage where the attacker begins compromising the vulnerabilities in the target system. Here, the details of the victim are extracted from open ports.*

- ✓ *These details can include usernames, user groups, network sources, routing tables, machine names, banners, SNMP details, DNS details, applications, etc.*
- ✓ *Various methods and techniques of enumeration.*

1. NetBIOS Enumeration

The full form of NetBIOS is Network Basic Input Output System. The communication between devices on a LAN is enabled using NetBIOS. Hackers can enumerate NetBIOS to find the list of computers, individual hosts, policies and passwords, etc., on the network. Poisoning attacks are the primary way to enumerate NetBIOS. Here, the hacker accesses the network and spoofs the devices to gain control and misdirect traffic. He can also get the hashed passwords of users to crack these later. For NetBIOS enumeration in ethical hacking, NBTScan is one of the prominent command-line tools in use. It scans the networks and finds NetBIOS shares and name information. NBTScan is available for Windows, Unix, and Kali Linux.

2. SNMP Enumeration

The full form of SNMP is a Simple Network Management Protocol. Based on the UDP protocol, SNMP is used to manage the devices on the IP network, including routers, hubs, and switches. The authentication method of the SNMP is weak and prone to spoofing. Hackers can use it to enumerate the accounts of the users, groups, systems, as well as devices on the network.

3. SMTP Enumeration

The full form of SMTP is the Simple Mail Transport Protocol. Its role is to send emails. Mail Exchange servers are used by SMTP to direct and send emails. SMTP enumeration can be used to get access to usernames using EXPN and VRFY commands (unless disabled by the network admins). EXPN shows the list of emails and the address of the user, whereas VRFY confirms the names of valid users.

4. NFS Enumeration

Network File System (NFS) is used to enable remote data sharing between systems on a network. These systems are based on Unix. The communication between machines on a network makes use of server-client architecture. Hackers perform

NFS enumeration using Nmap scan. The Nmap scan helps in finding the NFS ports that are open and can be targeted.

5. DNS Enumeration

DNS enumeration means finding the DNS servers and related records of the target company or system. Hackers can enumerate usernames, computer names, and IP addresses. With DNS enumeration, they can get an idea about the database records in use, zone files of the domain name system, etc.

- ***Trojan & Backdoor***
  - ✓ *A Trojan Horse is any type of malware that misleads users of its intent, like a destructive program that appears as a genuine application or software program.*
  - ✓ *Trojan Horses are named after the Ancient Greek story of the deceptive Trojan Horse that took down the city of Troy.*
  - ✓ *Unlike viruses, Trojan Horses do not replicate themselves, but they can be just as destructive.*
  - ✓ *Trojans also open a backdoor entry to your computer, giving command to malicious actor or allowing malicious users/programs access to your system. This leads to confidential and personal information being stolen.*
  - ✓ *A backdoor is a means of bypassing an organization's existing security systems. While a company may have various security solutions in place, there may be mechanisms in place that allow a legitimate user or attacker to evade them.*
  - ✓ *If an attacker can identify and access these backdoors, they can gain access to corporate systems without detection.*
  - ✓ *Backdoors can come in various different forms. A few of the most common types include:*
    - ***Trojans**: Most backdoor malware is designed to slip past an organization's defenses, providing an attacker with a foothold on a company's systems. For this reason, they are commonly trojans, which pretend to be a benign or desirable file while containing malicious functionality, such as supporting remote access to an infected computer.*
    - ***Built-in Backdoors**: Device manufacturers may include backdoors in the form of default accounts, undocumented remote access systems, and similar features. While these systems are typically only intended for the use of the manufacturer, they are*

often designed to be impossible to disable and no backdoor remains secret forever, exposing these security holes to attackers.

- ***Web Shells**: A web shell is a web page designed to take user input and execute it within the system terminal. These backdoors are commonly installed by system and network administrators to make it easier to remotely access and manage corporate systems.*
- ***Supply Chain Exploits**: Web applications and other software often incorporate third-party libraries and code. An attacker may incorporate backdoor code into a library in the hope that it will be used in corporate applications, providing backdoor access to systems running the software.*

✓ *Some best practices for protecting against exploitation of backdoors include:*

- ***Changing Default Credentials**: Default accounts are some of the most common types of backdoors. When setting up a new device, disable the default accounts if possible, and, if not, change the password to something other than the default setting.*
- ***Deploying Endpoint Security Solutions**: Backdoors are commonly implemented as trojan malware. An endpoint security solution may detect and block known malware or identify novel threats based on unusual behavior.*
- ***Monitoring Network Traffic**: Backdoors are designed to provide remote access to systems via alternative means that bypass authentication systems. Monitoring for unusual network traffic may enable the detection of these covert channels.*
- ***Scanning Web Applications**: Backdoors may be deployed as web shells or integrated into third-party libraries or plugins. Regular vulnerability scanning can help to identify these backdoors in an organization's web infrastructure.*

Virus & Worms

Sl.No.	***Basis of Comparison***	***WORMS***	***VIRUS***
1.	***Definition***	***A Worm is a form of malware that replicates itself and can spread to different computers via Network.***	***A Virus is a malicious executable-code attached to another executable file which***

			can be harmless or can modify or delete data.
2.	*Objective*	*The main objective of worms is to eat the system resources. It consumes system resources such as memory and bandwidth and made the system slow in speed to such an extent that it stops responding.*	*The main objective of viruses is to modify the information.*
3.	*Host*	*It doesn't need a host to replicate from one computer to another.*	*It requires a host is needed for spreading.*
4.	*Harmful*	*It is less harmful as compared.*	*It is more harmful.*
5.	*Detection and Protection*	*Worms can be detected and removed by the Antivirus and firewall.*	*Antivirus software is used for protection against viruses.*
6.	*Controlled by*	*Worms can be controlled by remote.*	*Viruses can't be controlled by remote.*
7.	*Execution*	*Worms are executed via weaknesses in the system.*	*Viruses are executed via executable files.*
8.	*Comes from*	*Worms generally comes from the downloaded files or through a network connection.*	*Viruses generally comes from the shared or downloaded files.*

9.	*Symptoms*	*Hampering computer performance by slowing down it* *Automatic opening and running of programs* *Sending of emails without your knowledge* *Affected the performance of web browser* *Error-messages concerning to system and operating system*	*Pop-up windows linking to malicious websites* *Hampering computer performance by slowing down it* *After booting, starting of unknown programs.* *Passwords get changed without your knowledge*
10.	*Prevention*	*Keep your operating system and system in updated state* *Avoid clicking on links from untrusted or unknown websites* *Avoid opening emails from unknown sources* *Use antivirus software and a firewall*	*Installation of Antivirus software* *Never open email attachments* *Avoid usage of pirated software* *Keep your operating system updated* *Keep your browser updated as old versions are vulnerable to linking to malicious websites*
11.	*Types*	*Internet worms, Instant messaging worms, Email worms, File sharing worms,*	*Boot sector virus, Direct Action-virus, Polymorphic virus,*

		Internet relay chat (IRC) worms are different types of worms.	*Macro virus, Overwrite-virus, File Infector virus are different types of viruses*
12.	*Examples*	*Examples of worms include Morris worm, storm worm, etc.*	*Examples of viruses include Creeper, Blaster, Slammer, etc.*
13.	*Interface*	*It does not need human action to replicate.*	*It needs human action to replicate.*
14.	*Speed*	*Its spreading speed is faster.*	*Its spreading speed is slower as compared to worms.*

- ***Proxy & Packet Filtering***

Criteria	Proxy Server	Packet Filtering Firewall
Connectivity	**Acts as an intermediary between the client and the external server, forwarding requests and responses.**	**Monitors and filters incoming and outgoing traffic within a local network.**
Blocking	**Blocks or allows specific websites or content.**	**Blocks or allows network traffic under predefined rules.**
Content Filtering	**Filters client-side requests to connect to the network at the application layer.**	**Filters data by monitoring packets at the network and transport layers.**

Security	**Bypass restrictions by hiding the client's IP address.**	**It prevents unauthorized access by controlling packet flow.**
Traffic Level	**Operates on the application protocol level to manage client-side requests.**	**Operates on the packet level to analyze and control network traffic.**

- ***Deniel of service***

✓ *A Denial-of-Service (DoS) attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users.*

✓ *DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash. In both instances, the DoS attack deprives legitimate users (i.e. employees, members, or account holders) of the service or resource they expected.*

✓ *Victims of DoS attacks often target web servers of high-profile organizations such as banking, commerce, and media companies, or government and trade organizations.*

✓ *Though DoS attacks do not typically result in the theft or loss of significant information or other assets, they can cost the victim a great deal of time and money to handle.*

✓ *There are two general methods of DoS attacks: flooding services or crashing services.*

✓ *Flood attacks occur when the system receives too much traffic for the server to buffer, causing them to slow down and eventually stop. Popular flood attacks include:*

- ***Buffer overflow attacks*** *– the most common DoS attack. The concept is to send more traffic to a network address than the programmers have built the system to handle. It includes the attacks listed below, in addition to others that are designed to exploit bugs specific to certain applications or networks*
- ***ICMP flood*** *– leverages misconfigured network devices by sending spoofed packets that ping every computer on the targeted network, instead of just one specific machine. The network is then triggered to amplify the traffic. This attack is also known as the smurf attack or ping of death.*
- ***SYN flood*** *– sends a request to connect to a server, but never completes the handshake. Continues until all open ports are saturated with requests and none are available for legitimate users to connect to.*

✓ *Other DoS attacks simply exploit vulnerabilities that cause the target system or service to crash. In these attacks, input is sent that takes advantage of bugs in the target that*

subsequently crash or severely destabilize the system, so that it can't be accessed or used.

- ✓ *An additional type of DoS attack is the Distributed Denial of Service (DDoS) attack. A DDoS attack occurs when multiple systems orchestrate a synchronized DoS attack to a single target.*
- ✓ *The essential difference is that instead of being attacked from one location, the target is attacked from many locations at once.*

- ***Sniffers***
  - ✓ *works by capturing internet traffic and analyzing the data streams to uncover the nature — or even the specific contents — of data sent across a network.*
  - ✓ *Just as cars make up road traffic, internet traffic consists of packets of data traveling through a network.*
  - ✓ *Although you generally ignore most cars driving by, you're likely to investigate if a truck pulls up in your driveway. Similarly, your computer ignores most traffic flowing through a network, and only inspects the specific packets of data that are sent to it.*
  - ✓ *Sniffers, then, are like a tollbooth — they are set up to inspect all cars driving down the road, not just those that park in one driveway.*
  - ✓ *Unfiltered sniffers inspect every car, harvesting all traffic traveling through a network. Filtered sniffers are configured to inspect only certain types of traffic.*

Social engineering

- Social engineering is a manipulation technique that exploits human error to gain private information, access, or valuables.
- In cybercrime, these "human hacking" scams tend to lure unsuspecting users into exposing data, spreading malware infections, or giving access to restricted systems. Attacks can happen online, in-person, and via other interactions.
- Scams based on social engineering are built around how people think and act. As such, social engineering attacks are especially useful for manipulating a user's behavior.
- Once an attacker understands what motivates a user's actions, they can deceive and manipulate the user effectively.
- In addition, hackers try to exploit a user's lack of knowledge.Users also may not realize the full value of personal data, like their phone number. As a result, many users are unsure how to best protect themselves and their information.

- Generally, social engineering attackers have one of two goals:
  - ✓ ***Sabotage****: Disrupting or corrupting data to cause harm or inconvenience.*
  - ✓ ***Theft:*** *Obtaining valuables like information, access, or money****.***
- Most social engineering attacks rely on actual communication between attackers and victims. The attacker tends to motivate the user into compromising themselves, rather than using brute force methods to breach your data.
- The attack cycle gives these criminals a reliable process for deceiving you. Steps for the social engineering attack cycle are usually as follows:
  - ✓ *Prepare by gathering background information on you or a larger group you are a part of.*
  - ✓ *Infiltrate by establishing a relationship or initiating an interaction, started by building trust.*
  - ✓ *Exploit the victim once trust and a weakness are established to advance the attack.*
  - ✓ *Disengage once the user has taken the desired action.*
- This process can take place in a single email or over months in a series of social media chats. It could even be a face-to-face interaction. But it ultimately concludes with an action you take, like sharing your information or exposing yourself to malware.
- It's important to beware of social engineering as a means of confusion. Many employees and consumers don't realize that just a few pieces of information can give hackers access to multiple networks and accounts.
- By masquerading as legitimate users to IT support personnel, they grab your private details — like name, date of birth or address. From there, it's a simple matter to reset passwords and gain almost unlimited access. They can steal money, disperse social engineering malware, and more.
- Types of social engineering attacks are:
  - ***Shoulder Surfing:***
    - ✓ *A shoulder surfing attack describes a situation where the attacker can physically view the device screen and keypad to obtain personal information.*
    - ✓ *It is one of the few attack methods requiring the attacker to be physically close to the victim to succeed.*
    - ✓ *While it might be as simple as looking over the victim's shoulder as the name suggests, some attackers will use binoculars, miniature video cameras, or other optical devices to spy on their victims.*

- ✓ *The goal is to obtain information such as usernames and passwords, personally identifiable or sensitive information, and credit card numbers.*
- ✓ *Most shoulder surfing attacks are straightforward: the attacker positions himself so that they can view the victim's device screen and the keyboard or keypad if necessary. As the victim enters and views information on the device, the attacker records this data.*
- ✓ *The attacker is likely writing or typing the information somewhere in an equally straightforward manner. Still, more sophisticated attacks may use optical devices, so they don't need to be looking over the victim's shoulder and aren't as easily detected.*
- ✓ *An attack where the user has installed some kind of reading device to steal information (such as a skim reader on an ATM) or attacks where the hacker can view your screen, and your entries are not shoulder surfing attacks, since these attacks happen remotely.*
- ✓ *To protect Yourself from Shoulder Surfing Attacks:*
  - ***Eliminate passwords**: The ONLY way to ensure the prevention of password-based attacks is through eliminating passwords. Learn more about passwordless authentication today and keep your most critical applications secure.*
  - ***Add a privacy screen to your devices**: Using devices with attached privacy screens dramatically lessens the risk of data disclosure. Some glass protector manufacturers have versions with a privacy screen included, which not only protects your phone's glass but the information on your phone, too.*
  - ***Always be aware of your surroundings**: In public places, don't let your guard down. Attackers gravitate to those that they see as the easiest. If you're distracted, you may not notice someone is watching you and what you're entering into the device or the ATM.*
  - ***Use biometric authentication instead:** Biometric authentication, either using your fingerprint or face, can offer additional security that a PIN cannot. Since the attacker never sees you enter a physical PIN, they can't log into the device.*

- ***Dumpster Diving:***
  - ✓ *Dumpster diving is the process of searching trash to obtain useful information about a person/business that can later be used for the hacking purpose.*

- ✓ *This attack mostly targets large organizations or business to carry out phishing (mostly) by sending fake emails to the victims that appear to have come from a legitimate source.*
- ✓ *The information obtained by compromising the confidentiality of the victim is used for Identity frauds.*
- ✓ *Through this process a hacker looks for*
  - ***Email address/address***
  - ***Phone numbers to carry out Vishing***
  - ***Passwords and other social security numbers that we might have written on sticky notes for our convenience***
  - ***Bank statements/financial statements***
  - ***Medical records***
  - ***Important documents***
  - ***Account login credentials***
  - ***Business secrets***
  - ***Marketing secrets***
  - ***Information of the employee base***
  - ***Information about the software/tools/technologies that is being used at the company***

✓ *Preventive measures:*

- *Destroy any CDs/DVDs containing personal data.*
- *In case you no longer need your PC, make sure you have deleted all the data so that it can't be recovered.*
- *Use of firewalls can prevent suspicious Internet users from accessing the discarded data.*
- *Paper documents should be permanently destroyed/shredded.*
- *Companies should lock waste bins and should have a safe disposal policy.*

- ***Piggybacking***

✓ *Piggybacking is a social engineering attack in which an attacker uses another person's legitimate access to a physical or electronic location to gain unauthorized access themselves.*

✓ *This type of attack is often seen in office buildings, where an attacker will follow someone with an access badge into a secured area.*

- ✓ *It can also be seen in IT systems, where an attacker may log into a system using another user's credentials.*
- ✓ *Piggybacking can also be used as a form of eavesdropping, where an attacker uses another person's access to a location in order to listen in on conversations or harvest sensitive information.*
- ✓ *Piggybacking attacks are relatively easy to carry out and are often very hard to detect. However, there are several steps that organizations can take in order to protect themselves against this type of attack.*
- ✓ *For example, they can limit access to sensitive areas only to authorized individuals with proper credentials or set up a system for detecting unauthorized access attempts.*
- ✓ *Overall, piggybacking is a serious security threat that can have serious consequences for organizations. Therefore, it is important for organizations to be aware of this type of attack and take measures to protect themselves against it.*
- ✓ *In contrast, piggybacking is a social engineering attack in which an attacker uses another person's legitimate access to a physical or electronic location to gain unauthorized access themselves. This type of attack can occur in both physical and digital spaces and often requires some level of technical knowledge.*
- ✓ *Overall, piggybacking is more serious threat than tailgating because it can be used to gain unauthorized access to sensitive information or locations, while tailgating is typically used only for physical access.*