**Foot printing & Social engineering-**

**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.

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:

* active footprinting
* passive footprinting

**active 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**

As the name implies, 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.

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.

**Advantages of footprinting-**

* 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.

**Social engineering-**

Social engineering refers to all techniques aimed at talking a target into revealing specific information or performing a specific action for illegitimate reasons.

Social engineering attacks are a type of cybercrime wherein the attacker fools the target through impersonation. They might pretend to be your boss, your supplier, someone from our IT team, or your delivery company. Regardless of who they're impersonating, their motivation is always the same — extracting money or data.

**Types of Social Engineering Attacks-**

Social engineering attacks come in many different forms and can be performed anywhere where human interaction is involved. The following are common forms of digital social engineering attacks.

* **Phishing:** The process of attempting to acquire sensitive information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity using bulk email, SMS text messaging, or by phone. Phishing messages create a sense of urgency, curiosity, or fear in the recipients of the message. The message will prod victims into revealing sensitive information, clicking on links to malicious websites, or opening attachments that contain malware
* **Baiting:** A type of social engineering attack where a scammer uses a false promise to lure a victim into a trap which may steal personal and financial information or inflict the system with malware. The trap could be in the form of a malicious attachment with an enticing name.
* The most common form of baiting uses physical media to disperse malware. For example, attackers leave the bait of a malware-infected flash drives in conspicuous areas where potential victims are certain to see them. When the victim inserts the flash drive into a work or home computer, the malware is automatically installed on the system. Baiting scams are also online in the form of tempting ads that lead to malicious sites or encourage users to download a malware-infected application.
* **Tailgating:** Also known as "piggybacking". A physical breach where an unauthorized person manipulates their way into a restricted or employee only authorized area through the use of social engineering tactics. The attacker might impersonate a delivery driver, or custodian worker. Once the employee opens the door, the attacker asks the employee to hold the door, thereby gaining access to the building.
* **Scareware:** Scareware involves victims being bombarded with false alarms and fictitious threats. Users are deceived to think their system is infected with malware, prompting them to install software that grants remote access for the criminal or to pay the criminal in a form of bitcoin in order to preserve sensitive video that the criminal claims to have.
* **Dumpster Diving:** A scammer will search for sensitive information e.g., bank statements, pre-approved credit cards, student loans, other account information, in the garbage when it hasn’t been properly sanitized or destroyed.
* **Quid Pro Quo:** Quid pro quo involves a criminal requesting the exchange of some type of sensitive information such as critical data, login credentials, or monetary value in exchange for a service. For example, a computer user might receive a phone call from the criminal who, posed as a technology expert, offers free IT assistance or technology improvements in exchange for login credentials. If an offer sounds too good to be true, it most likely a scam and not legitimate.

**Social Engineering Prevention-**

Don't open email attachments from suspicious sources. Even if you do know the sender and the message seems suspicious, it's best to contact that person directly to confirm the authenticity of the message.

* Use Multi-Factor Authentication (MFA). One of the most valuable pieces of information attackers seeks are user credentials. Using MFA helps to ensure your account's protection in the event of an account compromise. Follow Computing Services instructions for downloading DUO two-factor authentication to add another layer of protection for your Andrew account.
* Be wary of tempting offers. If an offer seems to good to be true, it's probably because it is. Use a search engine to look up the topic can help you quickly determine whether you're dealing with a legitimate offer or a trap.
* Clean up your social media. Social engineers scour the Internet searching for any kind of information they can find on a person. The more information you have posted about yourself, the more likely it is that a criminal can send you a targeted spear phishing attack.
* Install and update antivirus and other software. Make sure automatic updates are turned on. Periodically check to make sure that the updates have been applied and scan your system daily for possible infections. Visit Secure Your Computer on the Computing Services website for more instructions on using and updating antivirus software.
* Back up your data regularly. If you were to fall victim to a social engineering attack in which your entire hard drive was corrupted, it is essential that you have a backup on an external hard drive or saved in the cloud.
* Avoid plugging an unknown USB into your computer. When a USB drive is found unattended, please give it to a cluster consultant, the Computer Services Help Center, a residence assistant (RA), or to Carnegie Mellon campus police.
* You should also Disable Autorun on your machine. Autorun is a feature that allows Windows to automatically run the startup program when a CD, DVD, or USB device is inserted into a drive.
* Destroy sensitive documents regularly. All sensitive documents such as bank statements, student loan information, and other account information should be physically destroyed in a cross-shredder or placed in one of the blue or gray locked receptacles which are incinerated.