## **horizontal line**

**Footprinting and Phases of Hacking**

**Before attacking a system we have to plan things logically -**

**There are 5 phases of attacking into a system -**

**1 - Reconnaissance/Information Gathering/Footprinting - is collecting information about target like where is target? why we are attacking? what we want? when we do? how we do?**

**(i) Most time consuming**

**(ii) Obtain as much info about the target as possible**

**2 - Scanning - is finding weeknesses that can be exploited**

**(i) Goal-Identify weaknesses that can be exploited**

**(ii) Obtain as much info about the target as possible**

**There is three types of scans -**

**Ping Scans - Pings a range of IP addresses to finding out the which machine is responding**

**TCP scans - Check for open-listening TCP ports looking for services**

**OS footprinting - identifies the operating system by using different signatures**

**3 - Gaining Access - Accesing the system**

**For gaining access we can launch exploits -**

**(i) Web attacks - Owasp Top 10 and Sans 25**

**(ii) Other exploits - Failure to maintain up-to-date software**

**Haven't patched common exploited vulnerabilities**

**4 - Maintaining Access - Maintain the access or can enter again in system**

**(i) Maintain access and continually escalate the privilegas**

**(ii) Be careful in this phase the longer you maintain access the more chances that you can be caught**

**(iii) Ultimately a backdoor can be uploaded so we can acces the system again at any time**

**5 - Covering Tracks - Clear the logs and exit the system without leaving any evidence**

**(i) Erase evidence on targeted system**

**Footprinting is first step of hacking In this process the main purpose is to gather information about the target.**

**Types of footprinting :**

**Active Footprinting – in active footprinting we make direct connection with the target through tools.**

**Passive Footprinting – in passive footprinting we don’t make direct connection with the target. For example – Social Media**

**In Passive footprinting we use social media for gather information about the target some are the website which are helpful for gather information about the target are –**

**http://whois.domaintools.com**

**Internet Archive(Wayback Machine) is the website to see your target website looks like in the very first version and we can extract website links too.**

**https://archive.org/**

**Foot-Printing Methodology**

**1. Foot-printing through Search Engine --> Google, Yahoo, Bing etc**

**2. Foot-printing through Advanced google Hacking Techniques --> Using of Google Dorking methods ex - intitle:, filetype:, inurl:**

**https://www.exploit-db.com/google-hacking-database - In this website we will get all latest dorks.**

**site: etc https://securitytrails.com/blog/google-hacking-techniques**

**3. Foot-printing through Social Networking platforms --> Facebook, Twitter, Linkedin etc**

**4. Foot-printing through Websites --> their own sites**

**5. Foot-printing through Email --> whatever email id they are using or provided(ultratools)Hunter.io**

**6. Foot-printing through WHOIS --> you can use tools also or use website i.e = HYPERLINK "https://who.is/"https://who.is/**

**7. Foot-printing through DNS --> getting information about domain by DNSdumpster.com**

**8. Foot-printing through Network --> all information about network such as ip address, ports, info about network map.**

**9. Foot-printing through Social Engineering --> getting information from people by manipulating them.**

**10. Foot-Printing through Competitive intelligence --> Competitive intelligence gathering is the process of gathering information about the competitors from resources such as the Internet.**

**Eg: company website, search engine, internet, online databases, press releases, annual**

**+reports, trade journals**

**OS Fingerprinting & Banner Grabbing :**

**One method for determining the information about the operating system running on a target machine is called OS fingerprinting.**

**Two types of OS Fingerprinting :**

**1. Active OS Fingerprinting**

**2. Passive OS Fingerprinting**

**Active OS Fingerprinting and Banner Grabbing :**

**Nmap can easily perform Active Banner Grabbing. For OS Detection nmap allows to send TCP & UDP packets & observe the response from the targeted host ip.**

**Command:-**

**#nmap -O <ip address>**

**Passive OS Fingerprinting or Banner Grabbing :**

**Passive OS Fingerprinting perform by the Analysing Network Traffic along with the special inspection of Time to Live (TTL) value & Window Size.**

**Banner Grabbing :**

**Banner Grabbing is similar to OS fingerprinting, but actually, Banner Grabbing is determining the service that are running on the target machine.**

**Tools and Technique**

**Wappalyzer - it’s a extension to show which technology website using.**

**Builtwith - A advanced website for showing all the technology website use.**

**Who is - For Domain and website infomation.**

**Database Information**

**Name of the Registrar etc**

**Web site or web Application :**

**IP Address: Ping > "ip address"**

**Server Information**

**Dedicated or shared**

**https://www.yougetsignal.com --> reverse IP DOMAIN CHEKUP**

**http://reverseip.domaintools.com/**

**https://viewdns.info/reverseip/**

**White list and Black List**

**- robots.txt**

**Grabify Ip Logger - For device and public ip location.**

**Some useful websites where we can get list of vulnerabilities -**

**1 : Exploit-DB**

**2 : CVE- details**

**3 : us-cert.gov**

**3 : cve.mitre.org**