Ethical HAcking Notes.

Phases of Penetration testing-

1. Information Gathering.
   ->OSINT
   ->MApping network
   Host discovery
   Port discovery
   Service & OS detection

2. Enumeration & Recon
   Service Enumeration
   User enumeration
   Share Enumeration

3. Exploitation(Initial)
   Vuln analysis
   Vuln Threat Modeling
   Vuld Identification

4. Post Exploitation
   Local enum
   Privilage escallation
   Creds access
   Persistence
   Lateral movement

5. Reporting
   Report

CIA Triad

C- Confidentiality

I- Integrity

A- Accessibility

The CIA triad refers to a set of functionalities. If one of them gets affected then it is considered as a bug. Confidentiality refers when any confidential or private info gets penetrated, which will leak the info that the owner does not want.

Integrity refers to the functionality of the the website or software.

Availability refers to the resources that are given to the users.

STEP-!

IFORMATION GATHERING

It is the first step of any type ofpenetration testing it is used to know abouyt your target what the target is. The more info you collect th more it will help you to penetrate in the system.

1.Passive

2. Active

PSSIVE=

It involves the collection of info through open sources like osint . You can collect this info by their websites or social media handles.

Ways -- Check the robots.txt and sitemap.sql

Use wapappalyzer to collect the info about what technologies the website is running.

ACTIVE=

It uses techniques in which we intract with the services of the server.

We collect the as much as urls and subdomains and ip adresses you can do this by using arin whois and mx toolbox and other tools

You have to collect their ASN no. To get their IPv4 ranges which will help you later in testing.

The info you need to collect is-

IP adresses

DNS info

Domain name and ownership

Email adresses

Social MEdia

Web technologis

Directories

Subdomain info

And as much as information possible even their employees dog name.

Now you need to discover open ports in the server and mapp the entire network using tools like namp and burpsuite.

Remember you have to take notes of everything ou find. You can use notion or obsidinor or anything esle its your choice.

Footprintin--

This method involves footprinting their websites which will help you find the contact info of the servers

Google Dorking=

You can use dorking to find find urls related to the website of the org.

FOOTPRINTING THROUGH WEB SERVICES

Through web services you can extract variety of information about your target organization. Web services such as social networking sites, people search services, alerting services, financial services, & job sites etc. provide information about a target organization. You can extract critical information such as a target organization's domains, subdomains, operating systems, geographic locations, employee details, emails, financial information, infrastructure details, hidden web pages and content, etc. Using this information, you can build a hacking strategy to break into the target organization's network and can carry out other types of advanced system attacks.

Groups, forums, and blogs may also provide sensitive information about a target organization such as public network information, system information, and personal information.

FOOTPRINTING THROUGH SOCIAL NETWORKING SITES

During information gathering, you need to gather personal information about employees working in critical positions in the target organization, for example, the Chief Information Security Officer, Security Architect, or Network Administrator. Social networking sites are online services or platforms that allow people to connect and build interpersonal relations. People usually maintain profiles on social networking sites & provides basic information about themselves that help to make and maintain connections with others. The profile generally contains information such as name, contact information (cellphone number, email address), friends information, information about family members, their interests, activities, etc. On social networking sites, people may also post their personal information such as date of birth, educational information, employment background, spouse's names, etc. Organizations often post information such as potential partners, websites, and upcoming news about the company. Social networking sites often prove to be valuable information resources. Examples of such sites include LinkedIn, Facebook, Instagram, Twitter, Pinterest, YouTube, etc

Using Netcraft In footprinting

It provides info about site title, site rank, date first seen, primary language , domain, IP adress, name server, TLD , ssl cert, hosting history.

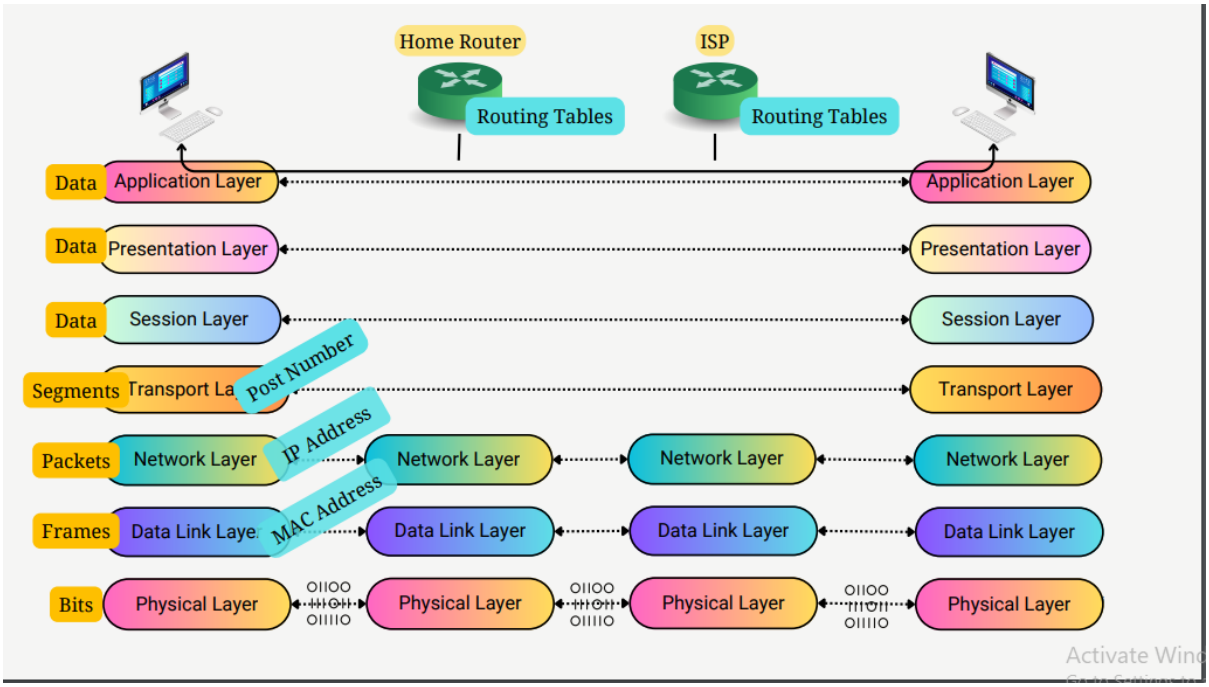
You can also use shodan to collect info.

NMAP = the most used tool in cybersecurity.

It is a port scanner and network mapping tools.

We will perform active info gathering with this tools. To further proceed on this step you must need to know about networking.

The basic structure of OSI model



NMAP===

Used for

Host discovery

Port scanning

Service version detection

Os fingerprinting

Etc

1. Host Discovery -

Host discovery is a process in which we find the the host which are live and remove the dead ones. We can do that by using httpx or httpx-toolkit.

Techniques and methods-

Ping sweeps

ARP scanning

TCP SYN Ping

UDP ping

TCP ACK ping

SYN/ACK ping

You might often see these techniques in the nmap cheatsheet we do this to identify that is the server running any of these technologies which we failed to find before.

Professional notes of trainer--

In the same folder.