Certified Ethical Hacker Labs

1)Footprinting and Reconnaissance Techniques

This stage focuses on gathering information about the target in order to assess their security posture and identify potential vulnerabilities. Reconnaissance is either done passively or actively. Passive reconnaissance uses publicly available information found on news articles or websites while active reconnaissance utilizes more intrusive techniques such as actively probing a system or applying social engineering attacks. There are various methods and tools we can use to perform reconnaissance on our target.

Using search engines

Search engines provide a wealth of information about companies and organizations. Our search engine results can further be refined and filtered to only mention specific information. Google offers advanced search operators that can help us narrow down our results when retrieving information found on the Internet.

-You can use the **site:** keyword to restrict the search results to a specific website.
-You can use the **allinurl** keyword to find a string of words in the url.
-You can also restrict the search to specific file types using **filetype:**
-You can also look for definitions using the **define:** keyword

Using social media sites and applications

Sites like Linkedin, Twitter, and Instagram can provide a lot of information about your target company or organization.

Using web services

There are various web services such as opencorporates to collect data about the target company such as their location, email address, and contact number.

Website footprinting using source code and archive.org

Website footprinting techniques can help us gather a wide array of information about our targets and their computer systems such as operating systems and their versions, software and their versions, and programming and scripting languages used.

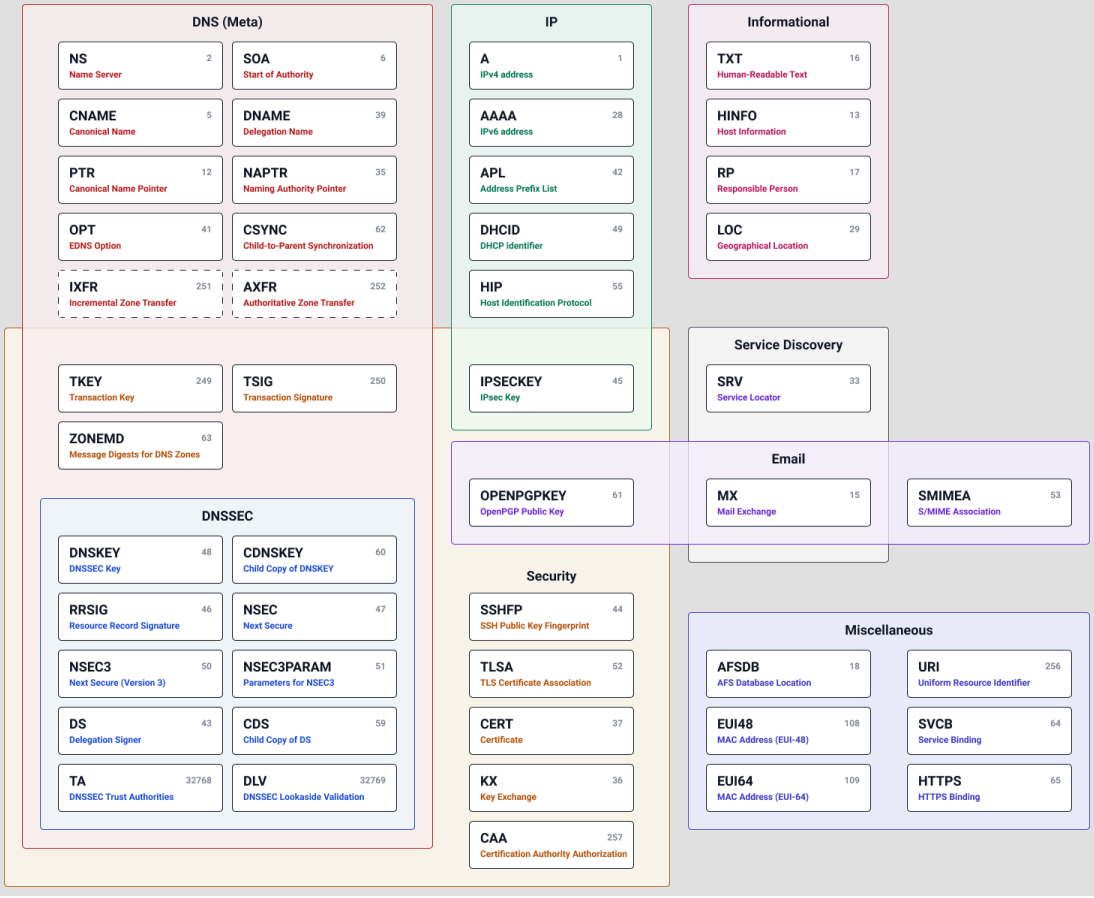
For instance, by right clicking anywhere on a web page and selecting view page source, you can find out the language being used above in the code.
Also, the website archive.org keeps a track of all the updates or changes to a website since its launch.

DNS footprinting using Nslookup and dnsenum

DNS footprinting techniques allow an attacker to obtain information about the DNS zone data which includes DNS domain names, IP addresses, and other network related data.

Nslookup is a network administration command line tool used to query the Domain Name System to obtain the mapping between a domain name and its IP address or other DNS records.

```
nslookup <target domain>
nslookup -type=<recordtype> <target domain>
```



Dnsenum is a DNS enumeration tool that is used to determine which DNS information is publicly available.

2) Network Reconnaissance Techniques

Network scanning is a technique that helps attackers identify hosts and computers on a network as well as ports, applications, and services running on these hosts.

Hping3 is a tool that is used to perform layers 3 and 4 scanning.

Use

sudo hping3 <IP address> –icmp

You can limit the count of packages by using -c <count number>

Dmitry is an information gathering tool that can help hackers obtain subdomains, email addresses, uptime information, tcp port scans, and whois lookups.

```
Deepmagic Information Gathering Tool

"There be some deep magic going on"


Usage: dmitry [-winsepfb] [-t 0-9] [-o %host.txt] host

  -o  Save output to %host.txt or to file specified by -o file

  -i  Perform a whois lookup on the IP address of a host

  -w  Perform a whois lookup on the domain name of a host

  -n  Retrieve Netcraft.com information on a host

  -s  Perform a search for possible subdomains

  -e  Perform a search for possible email addresses

  -p  Perform a TCP port scan on a host

* -f  Perform a TCP port scan on a host showing output reporting
filtered ports

* -b  Read in the banner received from the scanned port

* -t 0-9 Set the TTL in seconds when scanning a TCP port (
Default 2 )

*Requires the -p flagged to be passed
```

Nmap is a network mapper tool that is used to identify active hosts on a network and the ports and applications they're running. There are multiple kinds of scans that can be run using Nmap. In order to avoid getting detected, hackers usually perform a 'stealth' scan. A Stealth scan doesn't complete the three way handshake.

Command:

nmap -sS <target>

Note: You can also choose the speed of your stealth scan. For example, you choose paranoid, sneaky, polite, normal, aggressive, and insane.

These are defined as T0 to T5, where T5 is the fastest

Fping can be used to check if a host is alive

Command:

fping <target>

Zenmap is the graphical user interface of nmap.

. The top section has three key fields:

- Target: this is the system that you want to scan.
- Profile: is a predefined scan method. The default is an Intense scan.
- Command: this is entered based on the profile selection. You can choose to type a command manually.

Mylanviewer is a network and IP scanner. It can also search the whois database.

Metasploit framework is a tool used for exploiting vulnerabilities. It is also used in penetration testing. Aside from that, it contains modules that can be used for several types of scans including UDP scans, TCP stealth scans, and full connect scans.

3)Enumeration Reconnaissance Techniques

NetBIOS enumeration

NetBIOS is an old networking discovery protocol. It is used to find other endpoints on the same LAN.

Using Nbtstat

NBTstat is a utility that allows you to obtain a machine's NetBIOS information using cmd on Windows.

Command :

nbtstat -a <target>

Using Nmap

Nmap contains a Nmap Scripting Engine (NSE) that is used to execute ready-made scripts within it. One of these scripts can help you obtain NetBIOS information.

Command :

nmap - - script nbtstat.nse <target>

Using snmp check

Snmp check is a tool available on kali linux that is used to enumerate devices running the SNMP service.

Command:

snmp-check <target>