MODULE - 2
Footprinting & Reconnaissance

1. **Concepts**: Process of collecting information on the target.

2. **Objectives**:

•**Know Security Posture**: Footprinting allows attackers to know the external security posture of the target organization.
•**Reduce Focus Area**: It reduces the attacker's focus area to a specific range of IP addresses, networks, domain names, remote access, etc.
• **Identify Vulnerabilities**: It allows attackers to identify vulnerabilities in the target systems in order to select appropriate exploits.
• **Draw Network Map**: It allows attackers to draw a map or outline the target organization's network infrastructure to know about the actual environment that they are going to break

3. **Types of Footprinting** :
   1. Passive : It Involves gathering Information about the target without direct Interaction.
   2. Active : It Involves gathering Information about the target with direct Interaction.

4. **Information Obtained in footprinting** :
   1. Organization Information : Such information about an organization is available from its website.
   2. Network Information : Network information by performing whois database analysis, trace routing, Domain and sub Domain, ip address, network block, DNS records.
   3. System information : Gather system information by performing network footprinting, DNS footprinting

5. **Footprinting Threats** :
   1. Social Engineering
   2. System and Network Attacks
   3. Information Leakage
   4. Privacy loss
   5. Corporate Espionage
   6. Business Loss

6. **Footprinting Methodology** :
   1. Footprinting through search engines
   2. Footprinting through web services
   3. Footprinting through Social Networking sites
   4. WebSite Footprinting
   5. Email Footprinting
   6. Whois Footprinting
   7. DNS Footprinting
   8. Network Footprinting
   9. Footprinting through social engineering

7. **Google Dorking** :
   1. Site : This operator restrict search results to the specified site or domain
   2. Allinurl : restrict results to only the pages containing all the query terms specified in the URL
   3. Inurl : restricts the result to only the pages containing the specified word in the URL
   4. Allintitle : restrict results to only the pages containing all the query term specified in the title
   5. Intitle: restricts the result to only the pages containing the specified term in the title
   6. Filetype

8. **Other Technique for Footprinting through Search Engine** :

1. Gathering Information Using Google Advance Search, Advance Image Search, and Reverse Image Search.
2. Gathering Information from video search Engine
3. Gathering Information from meta search engines : They use other search engines to produce their own search indexes.
4. Gathering Information from FTP search engine.
5. Gathering information using IoT Search Engine

9. **Footprinting through web services** :

1. Tools to find Sub-domains :
   1. Netcraft
   2. Sublist3r
   3. Pentest-Tools Find Subdomain
2. Tools for Finding the Geographical Location :
   1. Google Earth
   2. Google maps
   3. Yahoo maps
3. Tools for people search :
   1. Intelius
   2. pipl
   3 Anywho

- attackers can use “theHarvester” tool to perform enumeration on linkedin
- harvesting email list using “theHarvester”

Gathering Information from Financial Services :

Google Finance

Footprinting through Job Sites

Deep and dark Web Footprinting

- Tor Browser
- Exonera

Detemining Operating Systems :

1. Netcraft
2. SHODAN Search Engine
3. Censys

Tools :

1. OSRFramework : Uses open source intelligence to get information about target
2. Web Spiders : Obtain information from the website such as pages, etc.
3. Recon-Ng
4. Metasploit Framework
5. theHarvester

```
theHarvester -d www.hackthissite.org -n -b google
```

6. Sublist3r

```
python3 sublist3r.py -d hackthissite.org
```

7. DIRB :

```
dirb https://www.hackthissite.org/ /usr/share/wordlists/dirb/small.txt
```

8. Maltego (OSINT tool)
9. Social Engineering Framework (SEF) :

generate phishing attacks and fake emails

Web Based Recon :

1. Netcraft :
   1. Background
   2. Network
   3. SSL/TLS
   4. Hosting History
   5. Sender Policy Framework (SPF)
   6. DMARC
   7. Web Trackers

DMARC : **DMARC** (Domain-based Message Authentication, Reporting and Conformance) is an email authentication protocol. It is designed to give email domain owners the ability to protect their domain from unauthorized use, commonly known as email spoofing.

2. Shodan :
   use Web crawlers to traverse your entire site
3. Censys
   Alternative for Shodan

ShortForms :

1. Search Engine Result Pages (SERPs)
2. Google Hacking Database (GHDB) - a database of queries, to identify sensitive data.
3. Supervisory Control and data acquistion (SCADA)
4. NNTP : Network News Transfer Protocol

Topics :

1. EDGAR :

FOOTPRINTING LABS :

1. Footprinting Basics with windows command line
   1. Ping
      - find the maximum frame size on the network
        ping www.certifiedhacker.com -f -l 1500
      - Investigate the TTL

   2. Nslookup
      - > set type=a
      -> www.certifiedhacker.com

   3. Tracert , Traceroute
      - tracert www.certifiedhacker.com

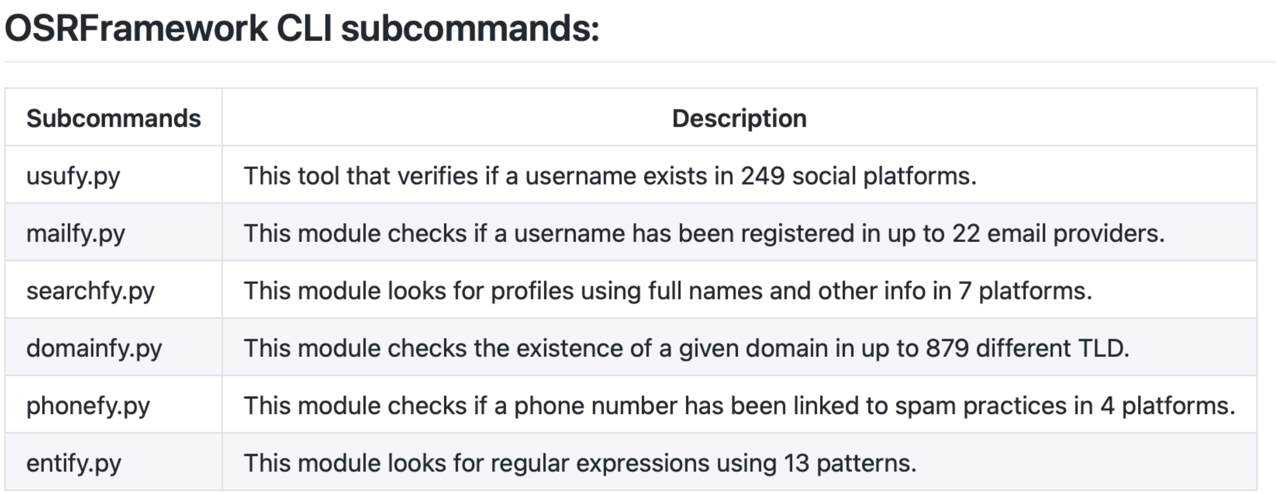
Authoritative Name Server : The Authoritative is a name server that has the original source files of a domain zone files. To obtain the Authoritative name server, set the **type** to **CNAME** record and query the target
Authoriative name(primary nameserver) server stores the records associated with the respective domain
-> set type=cname
-> certifiedhacker.com

2. Footprinting Using Maltego :
   1. All Transforms-> To Server Technologies [BuiltWith]
   2. All Transforms -> To Domains [DNS]
   3. All Transforms -> To DNS Name - SOA (Start of Authority).
   4. All Transforms -> To DNS Name - MX (mail server)
   5. All Transforms -> To DNS Name - NS (name server)
   6. All Transforms -> To IP address [DNS]
   7. All Transforms -> To Location [city, country]
   8. All Transforms -> To entities from whois [IBM Watson]

3. Recon-ng :
4. Open Source Intelligence gathering using OSRFramework :
   apt update && apt -y install osrframework
   1. Usufy.py
      -> check for the existence of a profile for a given user detail in different platform

2. Searchfy.py

-> checks with the existing users of pages/handlers for a given details in the all social network.



OSRFramework CLI subcommands:

Subcommands	Description
usufy.py	This tool that verifies if a username exists in 249 social platforms.
mailfy.py	This module checks if a username has been registered in up to 22 email providers.
searchfy.py	This module looks for profiles using full names and other info in 7 platforms.
domainfy.py	This module checks the existence of a given domain in up to 879 different TLD.
phonefy.py	This module checks if a phone number has been linked to spam practices in 4 platforms.
entify.py	This module looks for regular expressions using 13 patterns.

5. Information Gathering using Metasploit :

6. Information Gathering using theHarvester :

- theHarvester gathers emails, subdomains, hosts, employee names, open ports and banners from different public sources like search engines, PGP key servers and SHODAN computer database.
- theHarvester -d certifiedHacker.com -l 300 -b all

7. Another Tool for Recon :

1. Sublist3r : Sublist3r is a python tool designed to enumerate subdomains of websites using OSINT.
- sublist3r -d google.com -t 3 -e bing

8. Web Data Extractor :

1. HTTrack :
2. Tracing Emails
3. Whois Lookup
4. Automated footprinting using FOCA :

- Fingerprinting Organizations with Collected Archives (FOCA) is a tool that reveals metadata and shrouded data. These archives may be on site pages, and can be downloaded and dissected with FOCA.