PRACTICAL: 3

AIM:

Footprinting is the process of accumulating data regarding a specific network environment, usually for the purpose of finding ways to intrude into the environment. Footprinting can reveal system vulnerabilities and improve the ease with which they can be exploited. It is also known as reconnaissance. Study practical approach to implement Footprinting: Gathering Target Information by making use of the following tools: Recon-ng, Maltego ,OSRFramework , BillCipher , and OSINT Framework.

THEORY:

Footprinting and Reconnaissance:

Reconnaissance and footprinting are two essential processes in any security assessment .They can help a corporation develop a security posture strategy and detect potential risks.

The practise of locating and evaluating the security hazards inherent within an organisation is known as network footprinting. Similar to reconnaissance, it entails learning as much as you can about the target, including information that might not be easily accessible online. The security posture of the organisation may then be profiled using this data, and any possible weak areas can be found. In the aftermath of a hack or data breach, it may be used as proof. A business may more readily demonstrate that it followed all essential steps to safeguard its data by keeping an accurate record of its security posture.

Footprinting is a part of reconnaissance, a more thorough strategy. Reconnaissance is the stage of ethical hacking where you learn about the target system. This data may comprise everything from network architecture to employee contact information. Locating as many possible attack routes as is practicable is the goal of reconnaissance.

Recon-ng:

On GitHub, there is a free and open-source programme called reconng. The most fundamental and effective reconnaissance instrument, Open-Source Intelligence (OSINT), is the foundation of Reconng. Contextual assistance and command completion are only a couple of the useful features offered by the interactive interface.

Features-

- Recon-ng is a free and open-source utility, so you can download and use it without spending any money.
- Recon-ng is a comprehensive collection of modules for information collecting. You can use so many of its components to acquire information.
- Recon-ng functions as a website/web application scanner.
- simplest and most effective tools

Maltego:

Maltego is an open source information collecting and graphical link analysis tool for tasks related to conducting investigations. Operating systems for Windows, Macs, and Linux are all compatible with the Java application Maltego. Many different types of people utilise Maltego, such as security experts, forensic detectives, investigative journalists, and researchers. It will provide you with timely information mining, easily understandable information depiction, and information gathering.

Features-

- Information from scattered data sources can be easily gathered.
- Create a graph that automatically connects and combines all the data.
- Investigate relationships in your data visually.

OSR Framework:

The OSRFramework is the most often used method for acquiring information about an organization's target domain or employee from open-source or publicly accessible sources. This technique is mostly used by malicious hackers in attacks like phishing and social engineering. On the plus side, though, we can use this OSINT technique to comprehend the scope and become accustomed to our target area.

BillCipher:

The most popular technique for obtaining data from open-source or publicly available sources on a target domain or employee of a business is the OSRFramework. Malicious hackers mostly employ this tactic in social engineering and phishing assaults. On the bright side, we may utilise this OSINT method to comprehend the extent and become acquainted with our target region.

OSINT Framework:

Open-source intelligence, or OSINT, is any information about a person or organisation that has been legally gathered from unpaid, public sources. Data that may be accessible in a range of media types is also included in OSINT. Even while we typically think of information as text-based, it may also be in the form of pictures, movies, webinars, lectures, and conferences.

OUTPUT:

```
The Actions Ear Wess Hop
whateveb is already the newest version (0.5.5-1).
whateveb is already the newest version (0.5.5-1).
whateveb is already the newest version (0.5.5-1).
whateveb is to manually installed.
Suggested puckers
webbitrack hierack-doc
The following New packages will be installed:
hitrack libhtrack2
0 upgraded, 2 newly installed, 9 to remove and 1617 not upgraded.
Need to get 309 & No of archives.
After this operation, 924 kB of additional disk space will be used.
Get: http://http.kali.org/kali kali-rolling/main amd64 bibhtrack2 amd64 3.49.2-1.1+b1 [269 kB]
Get: 2 http://http.kali.org/kali kali-rolling/main amd64 bibhtrack2 amd64 3.49.2-1.1+b1 [40.0 kB]
Fetched 309 kB of a (50.6 kB/s)
Selecting previously unselected package libhtrack2.
(Reading database ... 33365 files and directories currently installed.)
Preparing to unpack .../libhtrack2 3.49.2-1.1+b1 amd64.deb ...
Unpacking libhtrack2 (3.49.2-1.1+b1) ...
Selecting previously unselected package hitrack.
Preparing to unpack .../libhtrack 3.49.2-1.1+b1 ...
Setting up libhtrack2 (3.49.2-1.1+b1) ...
Setting up libhtrack2 (3.49.2-1.1+b1) ...
Setting up libhtrack3 (3.49.2-1.1+b1) ...
Setting up libhtrack4 (3.49.2-1.1+b1) ...
Frocessing triggers for man-db (2.10.2-1) ...
Processing triggers for Mall-senu (2022.3.1) ...

(kali@kali)-[-/Desktop]

$\frac{\text{kali} kali}{\text{kal}} \text{-foskitop}
$\text{kal} \text{-foskitop}
$\text{kal} \text{-foskitop}
$\text{-foskitop} \text{-f
```

Created a file in Desktop and added dependencies and git clone



DNS lookup command for geeksforgeeks

HTTP Header for geeksforgeeks

```
| Section 1 2 3 4 | Section 1
```

Reserve IP lookup:- no DNS found as it is secure website

```
| Description | 12 3 4 | Description | 12 4 | Description | 12
```

Same as above but use for charusat.ac.in

```
| Second Processing Continues | Seco
```

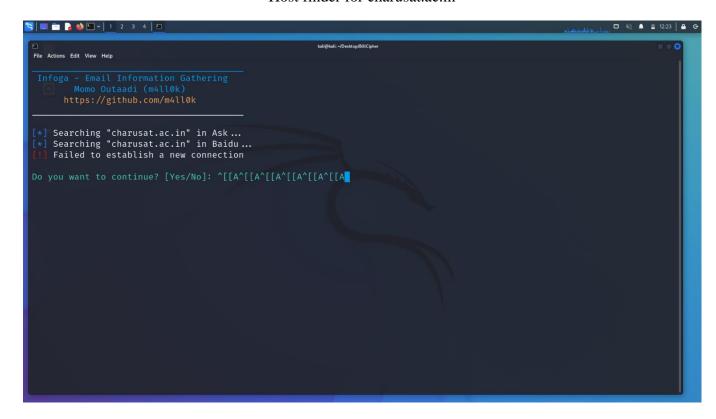
GeoIp lookup of charusat.ac.in

About zone transfer information

HTTP header info for charusat.ac.in

```
| Section | Sect
```

Host finder for charusat.ac.in



E-mail gathering for charusat.ac.in

```
# Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for charusat.ac.in
[-] Searching now in Baidu...
[-] Searching now in Windoo...
[-] Searching now in Nabou...
[-] Searching now in Bing...
[-] Searching now in Naboumpster...
[-] Searching now in NbSdumpster...
[-] Searching now in Virustotal...
[-] Searching now in ThreatCrowd...
[-] Searching now in SSL Certificates...
[-] Searching now in PassiveDNS...
Process Netcraftnum-7:
Traceback (most recent call last):
File "/inome/kali/Desktop/BillCipher/modules/Sublist3r/sublist3r.py", line 264, in run domain_list = self_enumerate()
File "/home/kali/Desktop/BillCipher/modules/Sublist3r/sublist3r.py", line 561, in enumerate cookies * self_egt_cookies
```

Subdomain listing for charusat.ac.in



It will check and bypass cloudflare

```
| Image: | I
```

Website copier for charusat.ac.in

```
🔾 📖 🛅 🍃 😂 🖭 🗸 📋 2 3 4 📗
                                                                                                                               □ 🔌 🛕 🖺 12:27 | 🖴 G
File Actions Edit View Help
Status
           : 301 Moved Permanently
            : <None>
IP
            : <Unknown>
Country
          : RedirectLocation[https://charusat.ac.in/], UncommonHeaders[x-cdn-cache-status,x-via]
Summary
Detected Plugins:
[ RedirectLocation ]
         HTTP Server string location. used with http-status 301 and
                         : https://charusat.ac.in/ (from location)
         String
[ UncommonHeaders ]
         Uncommon HTTP server headers. The blacklist includes all
          the standard headers and many non standard but common ones.
         Interesting but fairly common headers should have their own plugins, eg. x-powered-by, server and x-aspnet-version.

Info about headers can be found at www.http-stats.com
                         : x-cdn-cache-status,x-via (from headers)
         String
HTTP Headers:
         HTTP/1.1 301 Moved Permanently
         content-length: 0
          location: https://charusat.ac.in/
```

Host info scanner 1.1

```
😽 | 📖 🛅 🍃 🍪 🕒 🗸 | 1 | 2 | 3 | 4 | 🗈
                                                                                                                                                            □ 🔌 💄 12:28 | 🖴 G
               : CHARUSAT | Best Private University in Gujarat
Summary : Apache, Bootstrap, Email[info@charusat.ac.in], Frame, HTML5, HTTPServer[Apache], JQuery, Meta-Author[CHARUSAT Web Team], MetaGenerator[Powered by Visual Composer - drag and drop page builder for WordPress.], Open-Graph-Protocol[homepage], PHP[7.0.33], PoweredBy[Visual], Script[text/html,text/javascript], UncommonHeaders[x-cache-status,x-cdn-cache-status,x-via], probably WordPress, X-Powered-By[PHP/7.0.33], X-UA-Compatible[ie=edge]
Detected Plugins:
 [ Apache ]
            The Apache HTTP Server Project is an effort to develop and
            maintain an open-source HTTP server for modern operating
            systems including UNIX and Windows NT. The goal of this
            project is to provide a secure, efficient and extensible server that provides HTTP services in sync with the current
            HTTP standards.
            Google Dorks: (3)
                            : http://httpd.apache.org/
            Website
 [ Bootstrap ]
            Bootstrap is an open source toolkit for developing with
            HTML, CSS, and JS.
            Website
                            : https://getbootstrap.com/
 [ Email
            Extract email addresses. Find valid email address and
            syntactically invalid email addresses from mailto: link
```

Host info scanner 1.2

```
🔻 📖 🛅 🍃 🐞 🖭 v | 1 2 3 4 | 🗈
                                                                                                                          □ 🦚 🛕 🖺 12:28 🗎 🙃 G
                                                               kali@kali: =/Deckton/BillCinha
File Actions Edit View Help
[ X-Powered-By ]
         X-Powered-By HTTP header
                       : PHP/7.0.33 (from x-powered-by string)
         String
[ X-UA-Compatible ]
         This plugin retrieves the X-UA-Compatible value from the
         HTTP header and meta http-equiv tag. - More Info:
         http://msdn.microsoft.com/en-us/library/cc817574.aspx
HTTP Headers:
         HTTP/1.1 200 OK
         date: Thu, 05 Jan 2023 17:27:17 GMT content-type: text/html; charset=UTF-8
         transfer-encoding: chunked
         server: Apache
         x-powered-by: PHP/7.0.33
         cache-control: max-age=2592000
         expires: Sat, 04 Feb 2023 17:27:20 GMT vary: Accept-Encoding
         x-cache-status: MISS
         content-encoding: gzip
         x-cdn-cache-status: MISS
         x-via: SIN1
```

Host info scanner 1.3

LATEST APPLICATIONS:

- Students or new graduates can use and apply to test their websites.
- Also to find the loopholes in several websites of clients.
- Also used in several smalls bug bounties programs for security purposes.

LEARNING OUTCOME:

This practical helped me better understand footprinting and how attackers may employ it to get information about our devices. We also studied software that may help us get information like an email address or the IP address of a website, among other things. You should be aware that some of these tools can be used maliciously.

REFERENCES:

1. About footprinting and reconnaissance:

https://www.eccouncil.org/cybersecurityexchange/ethical-hacking/basics-footprintingreconnaissance

- 2. Recon-ng: https://www.geeksforgeeks.org/recon-ng-installation-on-kali-linux/
- 3. Maltego: https://www.maltego.com/
- 4. OSR Framework: https://www.kali.org/tools/osrframework/
- 5. BillCipher: https://github.com/bahatiphill/BillCipher
- 6. OSI Framework:

https://www.asktheeu.org/en/request/5762/response/18627/attach/8/9.OSINT%20Documentation.pdf

7. Lab Module: https://www.youtube.com/watch?v=JWF3bkUclQE