FOOTPRINTING & RECONNAISSANCE

🕵️ Lesson: Footprinting & Reconnaissance (Full Breakdown)

Module 3 – Ethical Hacking Essentials

🧠 What is Footprinting?

> Footprinting is the first step in hacking — where you collect as much information as possible about the target system or network.

Imagine you're a thief planning a bank robbery (purely metaphorical here 😄). You don't barge in blindly. First, you:

- Observe the building
- Count security cameras
- Note guard timings
- Understand the blueprint

  That’s exactly what footprinting is in hacking.

🔎 What is Reconnaissance?

Reconnaissance, or **recon**, is the process of **actively or passively gathering information** about a target before launching an attack.

Footprinting = subset of Reconnaissance ✅

Recon is broader and includes **scanning** and **enumeration** as well.

🎯 Why Footprinting & Recon is Important?

- Helps attackers **map the target’s digital footprint**.
- Reveals **vulnerabilities** without alerting the target.
- Saves time during actual exploitation.
- Allows ethical hackers to report flaws **before attackers find them**.

🧩 Types of Footprinting

🔵 1. Passive Footprinting

- No direct interaction with the target.
- 100% stealthy.
- Sources: Public websites, social media, search engines, DNS, WHOIS, job listings, PDF metadata, etc.

Example:

- Searching `site:target.com filetype:pdf` on Google to find hidden documents.

🔴 2. Active Footprinting

- Involves **direct engagement** with the target system.
- May be detectable in logs.
- Tools: Ping, traceroute, Nmap, theHarvester, DNS Interrogation.

Example:

- Running an Nmap scan to find open ports on the target server.

📦 Types of Information Gathered During Recon:

Type	Example
Domain info	`target.com` , WHOIS data
IP addresses	Public/Private IP ranges
DNS records	A, MX, CNAME, TXT records
Subdomains	`admin.target.com` , `mail.target.com`
Employee details	Found via LinkedIn, GitHub
Tech stack	Apache, PHP, CMS like WordPress

Type	Example
Emails	contact@target.com, hr@target.com
Physical location	From address, geo-IP, job posts
File metadata	Author name, software used
Security gaps	Outdated software, open ports

🔧 Techniques in Footprinting

📌 Passive Techniques:

- **Google Hacking (Google Dorks)**

  Example:

  `intitle:index.of site:target.com` – To find exposed directories.

- **WHOIS Lookup**

  Use sites like who.is to get domain ownership, admin contact, registration dates, etc.

- **Social Media Mining**

  LinkedIn → Find employees

  GitHub → Find developers and leaked code

  Twitter → Insider info & company tools

- **DNS Interrogation**

  Tools like `nslookup`, `dig` can reveal internal domains and mail servers.

- **Job Listings**

  Often reveal internal tech: "Looking for Django developer" → Uses Django!

- **Website Enumeration**

  Use `whatweb`, `wappalyzer`, or `builtwith.com` to detect tech stack.

📌 Active Techniques:

- **Ping and Traceroute**
  - Discover live systems and how data travels.
- **Nmap Scanning**

    - To find open ports and services on a host.
- **theHarvester**
    - Collects emails, subdomains, hostnames from search engines.
- **Netcraft**
    - Gives server details, uptime, and hosting provider.

🛠️ Common Tools for Recon & Footprinting

Tool	Use
`theHarvester`	Email, domain & host gathering
`Recon-ng`	Recon automation framework
`Google Dorks`	Smart searches for hidden info
`WHOIS Lookup`	Domain ownership & contacts
`Shodan`	Finds internet-connected devices
`Maltego`	Visual link analysis of people, domains, networks
`Censys/ZoomEye`	Device & port discovery
`Nmap`	Active scanning, service detection

🧪 Real-World Hacking Scenario (Example):

Imagine you're targeting `targetcorp.com` for a bug bounty.

1. Use `whois targetcorp.com` to get admin email.
2. Use `theHarvester` to collect emails like `admin@targetcorp.com`.
3. Find `.pdf` files with Google Dorks → Extract author names from metadata.
4. Discover subdomains like `dev.targetcorp.com`, which runs outdated WordPress.
5. Use `Shodan` to see public-facing servers.
6. Bingo! A server is running FTP with anonymous login enabled.

Result: You now have a complete map of the organization without touching their firewall.

⚠️Perform Footprinting Through Search Engines

https://mattw.io/youtube-metadata/

> YouTube Metadata tool collects singular details of a video, its uploader, playlist and its creator or channel.

TinEye Reverse Image Search

FTP Search Engines:

- https://www.searchftps.net/
- https://www.freewareweb.com/

IoT Search Engines:

- https://www.shodan.io/
- https://search.censys.io/

Domains and Sub-domains:

- https://www.netcraft.com/tools/
- https://github.com/aboul3la/Sublist3r

theHarvester:

> This tool gathers emails, subdomains, hosts, employee names, open ports, and banners from different public sources such as search engines, PGP key servers, and the SHODAN computer database as well as uses Google, Bing, SHODAN, etc.

```
theHarvester -d eccouncil -l 200 -b linkedin
```

> -d specifies the domain or company name to search (here, eccouncil), -l specifies the number of results to be retrieved, and -b specifies the data source as LinkedIn.

Deep and Dark Web Searching:

- The Hidden Wiki

- FakeID is an onion site for creating fake passports
- Cardshop is an onion site that sells cards with good balances
- ExoneraTor
- OnionLand Search engine,

Information from Various Social Networking Sites:

- Sherlock:

  > Sherlock is a python-based tool that is used to gather information about a target person over various social networking sites. Sherlock searches a vast number of social networking sites for a given target user, locates the person, and displays the results along with the complete URL related to the target person.

- Social Searcher
- Followerwonk

  > Followerwonk is an online tool that helps you explore and grow your social graph, digging deeper into Twitter analytics; for example, Who are your followers? Where are they located? When do they tweet? This can be used to gather Twitter information about any target organization or individual.

Gather Information about a Target Website:

- Photon

  > Photon is a Python script used to crawl a given target URL to obtain information such as URLs (in-scope and out-of-scope), URLs with parameters, email addresses, social media accounts, files, secret keys and subdomains. The

> extracted information can further be exported in the JSON format.

- Central Ops

> CentralOps (centralops.net) is a free online network scanner that investigates domains and IP addresses, DNS records, traceroute, nslookup, whois searches, etc.

- https://github.com/digininja/CeWL
- https://whois.domaintools.com/

DNS Footprinting

- nslookup
- http://www.kloth.net/services/nslookup.php
- https://dnsdumpster.com/
- https://www.broadbandsearch.net/network-tools
- https://www.yougetsignal.com/
- https://securitytrails.com/

Locate the Network Range

- tracert ← windows
- traceroute ← linux

Recon-ng:

> Recon-ng is a web reconnaissance framework with independent modules and database interaction that provides an environment in which open-source web-based reconnaissance can be conducted. Here, we will use Recon-ng to perform network reconnaissance, gather personnel information, and gather target information from social networking sites.

Maltego:

> Maltego is a footprinting tool used to gather maximum information for the purpose of ethical hacking, computer forensics, and pentesting. It provides a library of transforms to discover data from open sources and visualizes that information in a graph format, suitable for link analysis and data mining. Maltego provides you with a graphical interface that makes seeing these relationships instant and accurate, and even making it possible to see hidden connections.

OSRFramework:

> OSRFramework is a set of libraries that are used to perform Open Source Intelligence tasks. They include references to many different applications related to username checking, DNS lookups, information leaks research, deep web search, regular expressions extraction, and many others. It also provides a way of making these queries graphically as well as several interfaces to interact with such as OSRFConsole or a Web interface.

domainfy :

- `domainfy -n [Domain Name] -t all`
- n: specifies a nickname or a list of nicknames to be checked. -t: specifies a list of top-level domains where nickname will be searched.

searchfy:

> check for the existence of a given user details on different social networking platforms such as Github, Instagram and Keyserverubuntu. Type searchfy -q "target user name or profile name"

BillCipher:

> BillCipher is an information gathering tool for a Website or IP address. Using this tool, you can gather information such as DNS Lookup, Whois lookup, GeoIP Lookup, Subnet Lookup, Port Scanner, Page Links, Zone Transfer, HTTP Header, etc. Here, we will use the BillCipher tool to footprint a target website URL.

OSINT Framework:

- https://osintframework.com/

📝 Summary

Feature	Passive Recon	Active Recon
Stealth	100% invisible	Can be detected
Safety	Safe, legal	Needs permission
Speed	Slower	Faster
Tools	Google, WHOIS	Nmap, theHarvester