TRAINING DAY 17 REPORT:

- ## Wget Mirroring

  Wget is a command-line utility used to download files or entire websites from the internet.

  ### Mirroring with Wget:

  1. You can use it to **create a local copy of a website**
  2. It downloads HTML pages, images, stylesheets, etc.
  3. It can follow links recursively to capture the site structure

  ### Purpose in cybersecurity:

  - Offline analysis of a website
  - Identifying structure, potential vulnerabilities, or exposed data

- ## Mirroring With HTTrack

  HTTrack is a GUI-based tool similar to Wget, but more user-friendly.

  ### Key Features:

  1. Downloads a full copy of a website
  2. Preserves the directory structure
  3. Can be used to inspect JavaScript files, form inputs, etc.

  ### Steps:

1. Install and launch HTTrack
2. Enter the website URL
3. Set mirroring options (depth, media files, filters)
4. Download and browse the mirror offline

  ### Use in hacking:

  - Analyzing how the website is structured

- Discovering exposed admin panels or sensitive paths

- ## HTTrack in Windows

  HTTrack is cross-platform and works well on Windows.

  ### Benefits on Windows:

  1. Easy-to-use wizard interface
  2. Suitable for beginners
  3. Saves websites into browsable folders

  ### Common Use:

  1. Used in ethical hacking training to replicate sites for practice
  2. Reverse engineering website layout or client-side scripting

- ## Temp Mails

  Temporary or **disposable emails** are used to:

  - Register on websites without revealing your real email
  - Avoid spam and tracking
  - Bypass mandatory email verification during reconnaissance

  ### Popular Temp Mail Services:

  1. temp-mail.org
  2. guerrillamail.com
  3. 10minutemail.com

  ### Use in hacking:

  1. Create anonymous accounts
  2. Sign up for tools/websites while doing recon
  3. Reduce your digital footprint

- ## Whois Lookup

  Whois is a query/response protocol to retrieve:

  - Domain name registrant information

  - Registration and expiry dates

  - Name servers and DNS details

  - Email/phone of the domain owner (if not private)

  Command Example (Linux):

  ```
  whois example.com
  ```

  ### Online Tools:

  - whois.domaintools.com

  - whois.net

  ### Why hackers use it:

  1. Identify organization behind a domain

  2. Gather contact details for social engineering

  3. Discover other associated domains

- ## DNS Resource Records

  DNS (Domain Name System) maps domain names to IP addresses.

  ### Common Resource Records:

  1. A: Maps domain to IPv4 address

  2. AAAA: Maps domain to IPv6 address

  3. MX: Mail server info

  4. NS: Nameservers

  5. CNAME: Alias to another domain

  6. TXT: Can contain SPF, verification strings

Purpose in hacking:

1. Get server IPs and configurations
2. Understand email routes
3. Reveal internal hostnames or subdomains

- ## DNS Footprinting - DNSDumpster Tool

DNSDumpster is an online reconnaissance tool that collects DNS data.

What it reveals:

- Subdomains
- IP addresses
- Host records
- MX (mail) records
- TXT entries

Steps:

1. Visit dnsdumpster.com
2. Enter domain name
3. View all discovered DNS information in a graph format

Use case:

1. Visual mapping of the network
2. Finding exposed servers or devices
3. Tracing internal IT infrastructure

- ## Chatroom

In ethical hacking, **chatrooms** may be:

- Forums or IRC channels used for gathering public data
- Places where users leak sensitive company information

- Open group discussions that give OSINT data

What to collect:

1. Usernames
2. Email addresses
3. Technical issues faced (can hint about tech stack)
4. Internal tool mentions

- ## Important search engines

General Search Engines

Used for surface web data collection.

Search Engine	Details
Google	Most powerful search engine. Supports advanced search operators (dorks) like `site:`, `inurl:`, `filetype:` for information gathering.
Bing	Microsoft's search engine. Good for finding content that Google may filter or miss.
DuckDuckGo	Privacy-focused. Doesn't track users, good for anonymous searches. May give different results from Google.
Yahoo	Older engine. Sometimes shows older or cached results useful in OSINT.
Yandex	Russian search engine, useful for image and deep searches, often shows data missed by Google.

Specialized Search Engines (For Hacking / OSINT)

Search Engine	Purpose
Shodan	Finds internet-connected devices (e.g., CCTV, routers, servers). Shows open ports, software, IPs.
Censys	Similar to Shodan. Helps in scanning hosts, certificates, services

Search Engine	Purpose
	on the internet.
ZoomEye	Chinese tool like Shodan. Used for discovering vulnerable hosts.
GreyNoise	Identifies IPs that are scanning the internet—useful to avoid honeypots.
PublicWWW	Searches source code, analytics IDs, emails, scripts inside websites.
Hunter.io	Finds email addresses related to a domain—helpful in email footprinting.
Wayback Machine	Internet archive. Lets you view past versions of websites (useful for deleted info or older data).

- # What is Network Footprinting?

  Network Footprinting is the **first step** in ethical hacking or cybersecurity testing. It involves **gathering information about a target's network** to understand its structure, devices, and potential vulnerabilities **without alerting the target**.

  ## Purpose

  1. Identify IP addresses, domain names, and servers

  2. Discover open ports, services, and subdomains

  3. Understand network security posture before an attack (or test)

  ## What Information is Collected?

  - IP address ranges

  - Domain names and subdomains

  - DNS records (MX, A, NS)

  - OS and software versions (via banners)

  - Network paths (using Traceroute)

  - Open ports/services (via scanners)

Common Tools

Tool	Use
WHOIS	Domain/IP ownership & registrar info
DNSDumpster	DNS records & subdomains
Shodan	Find internet-connected devices
Nmap	Scan open ports (active)
Traceroute	Shows path to a network destination

Why It's Important

1. Maps the **attack surface**
2. Helps ethical hackers plan tests
3. Shows organizations what is publicly exposed
4. Essential for both **offensive** (Red Team) and **defensive** (Blue Team) roles