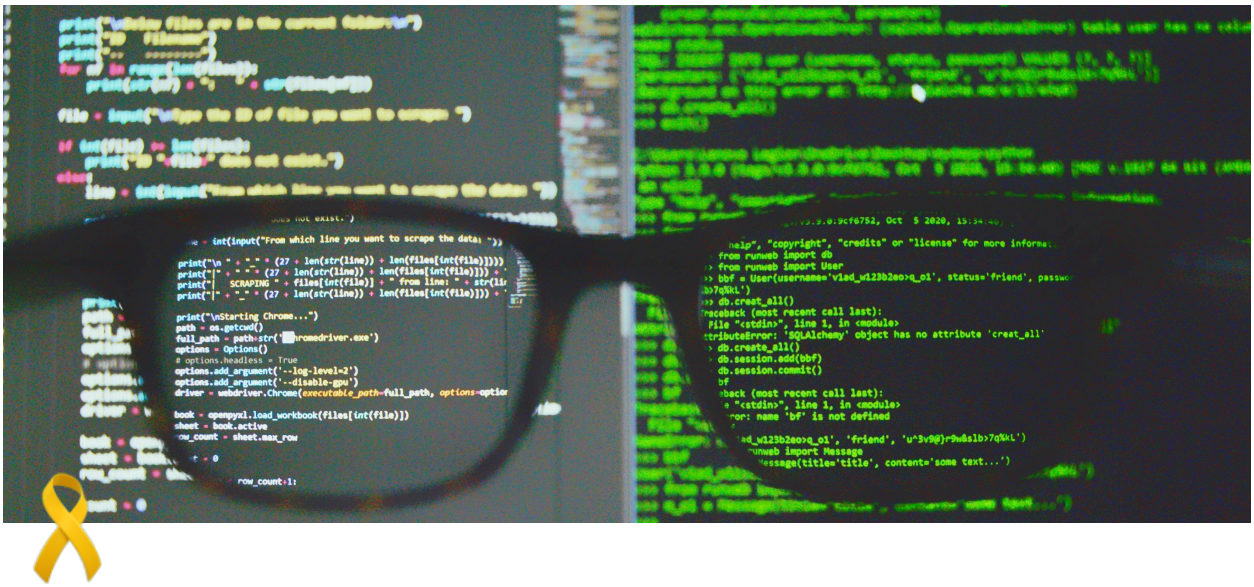


Assessment Methodologies Information Gathering

Passive Information Gathering:

No direct interaction with the target

- **Goal:** Stay stealthy, avoid detection
- **Sources:**WHOIS,DNS records,Google dorking,Social media,Job Postings,Public websites (e.g., LinkedIn, GitHub)
- **Tools:**Maltego,theHarvester,recon-ng,Google,Shodan,crt.sh (certificate transparency logs)

Active Information Gathering:

Direct interaction with the target system

- **Goal:** Collect detailed data (may trigger alerts)
- **Examples:** Port scanning (Nmap),Banner Grabbing, OS Detection ,DNS zone Transfers ,Service enumeration
- **Tools:** Nmap, Netcat, Dirb/Dirbuster, Nikto, Wappalyzer, WhatWeb

What Information Are We Looking For?

- Passive Information Gathering

  Identifying IP addresses & DNS information.

  + Identifying domain names and domain ownership information.

  + Identifying email addresses and social media profiles.

  + Identifying web technologies being used on target sites.

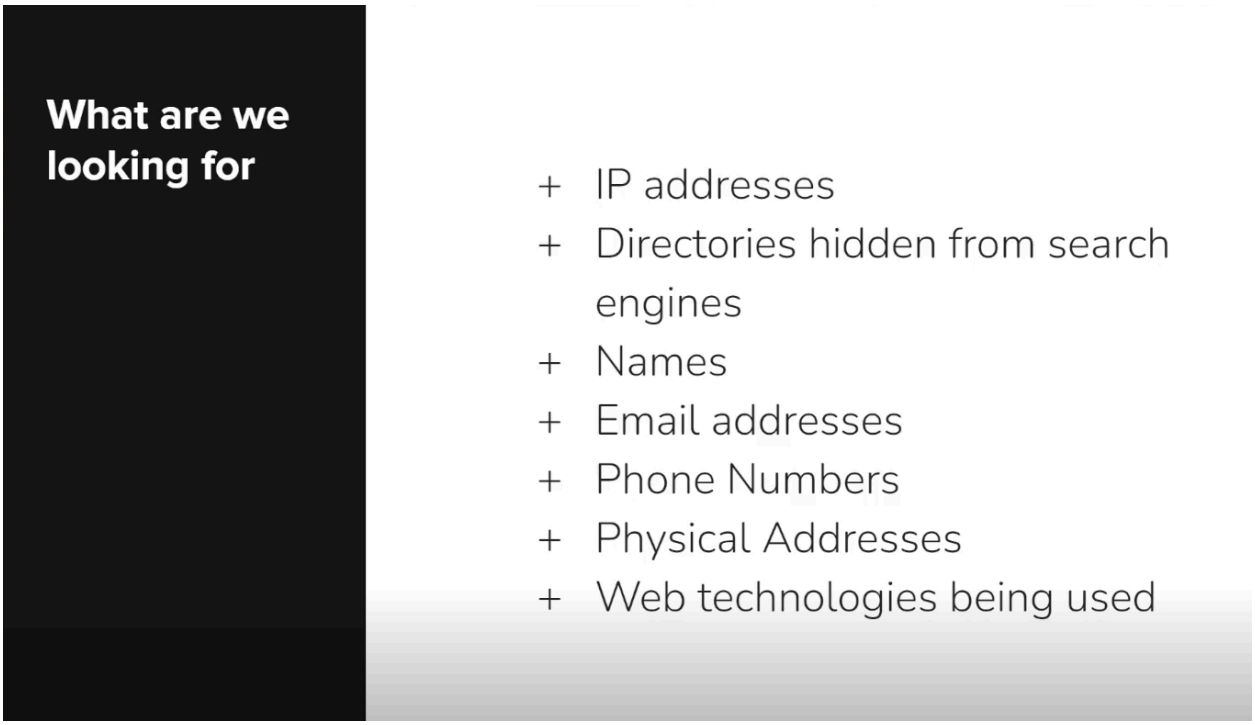
  + Identifying subdomains.

- Active Information Gathering

  + Discovering open ports on target systems.

  + Learning about the internal infrastructure of a target network/organization.

  + Enumerating information from target systems.



commands

- `host <target-website>` (get IPs v4/v6 & mail server)

- `curl -I <target-website>` (to see the https headers)
- `whois <command, eg. host>` (what to know about the tool or command)
- always look for `robots.txt & sitemap.xml`

web technology discovery

- Wappalyzer
- builtwith
- whatruns
- `whatweb <targeted-website>` (kali tool)

to download the website

- Webhttrack (Linux tool)

to get **registration info** about a domain name or IP address, registry domain id, registrar url, **organization that owns a domain/IP**

- `whois <targeted name>`

Finding the **organization that owns a domain/IP**

DNS Recon

- dnsrecon (used for get the name server & ips)
- dnsdumpster.com

detect firewalls or how to identify weather a website is being protected by proxy or firewall

- `Wafw00f <target-website>` (WAF Detection with Wafw00f tool of Linux)
- `Whatwaf -u <target.com>`
- `nmap -p 80,443 --script http-waf-detect --script-args http-waf-detect.uri=/ target.com`
- `dig target.com`

---

subdomain finder tools

- `sublist3r -d example.com -o subdomains.txt`
- `amass enum -passive -d example.com`
- `assetfinder --subs-only example.com`
- `crt.sh/Hunter.io` (online websites)

Google Dorks

Purpose	Dork Query Example
Find subdomains	site:*.example.com -www
List directories	site:example.com inurl:/admin
Exposed login pages	site:example.com inurl:login
Public exposed documents	site:example.com filetype:pdf
Discover config files	intitle:index.of config
Find cameras / CCTVs	inurl:/view/index.shtml
Discover email lists	intext:@example.com
Look for SQL error messages	intext:"you have an error in your sql syntax"
Find PHPMyAdmin access	intitle:"phpMyAdmin" "Welcome to phpMyAdmin"
Find backup files	intitle:index.of "backup" or filetype:bak
Sensitive files (env, log)	filetype:env OR filetype:log site:example.com
Git repositories	inurl:.git site:example.com

Filetype Dorks (Leak Detection)

site:example.com filetype:pdf

site:example.com filetype:xls

site:example.com filetype:log

site:example.com filetype:env

site:example.com filetype:sql

🛠️ Technology Detection

site:example.com inurl:wp-content # WordPress

site:example.com inurl:php? # PHP in use

site:example.com ext:jsp # Java server pages

wayback machine for tracking a website or see the older version of the website

- Google Hacking Database

 # Email Harvesting With theHarvester

- theHarvester -d example.com -b google

- It gathers valuable **enumeration data** like: Email addresses,Subdomains,Hosts,URLs,Open ports,Employee names

Leaked Password Databases

- Haveibeenpwned.com

⇐==========active information gathering==========⇒

#DNS Zone Transfers

use to get the dns-record (eg. Host's addresses,Name Servers,Mail (MX) Servers,Trying Zone Transfers and getting Bind Versions)or scan the internal network

- `dnsenum <targeted-website>`
- `deg axfr <name server> <targeted-website>` (eg. dig axfr @nsztm1.digi.ninja zonetransfer.me)
- `Fierce -dns <targeted-website>`

Nmap(Host Discovery With Nmap)

- Ip a or ifconfig (to get my own ip (my ip is under the 'eth0' , inet 192.168.146.183))
- `nmap -sn 192.168.146.183/24` or `arp-scan -l` or `netdiscover` (to find the active device IPs in the some network)

Port Scanning With Nmap

-

first lab CTF 1

- my ip 10.1.0.4

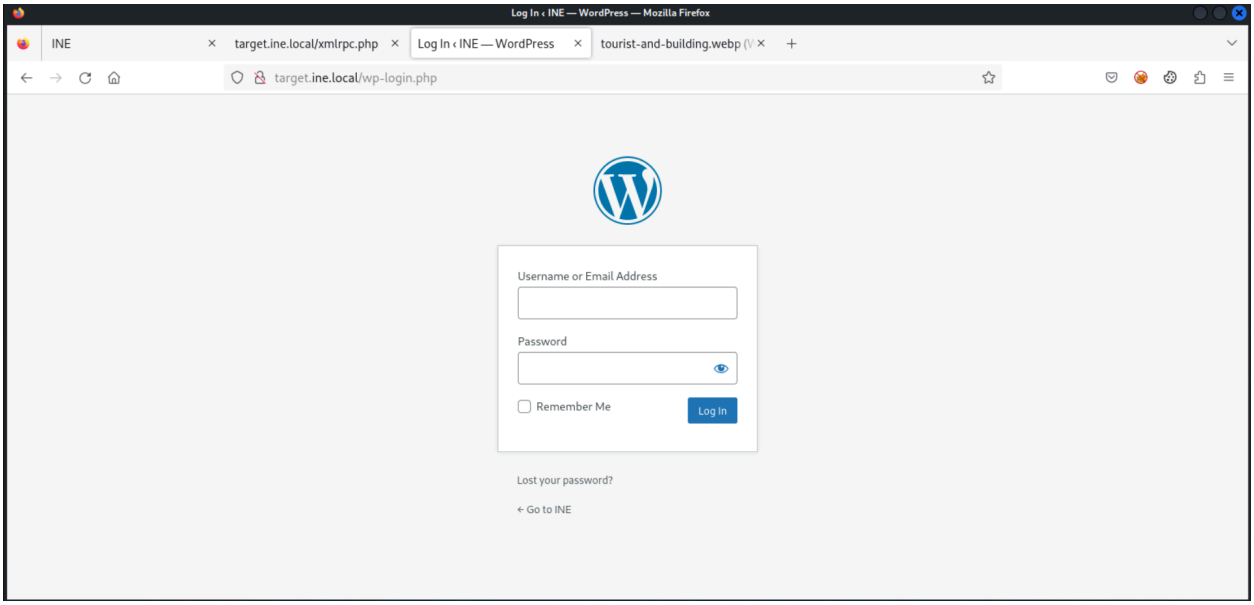
```
┌──(root㉿INE)-[~]
└─# nmap -sn 10.1.0.4/16
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-22 21:12 IST
Nmap scan report for 10.1.0.1
Host is up (0.000015s latency).
MAC Address: 02:42:78:C6:71:9B (Unknown)
Nmap scan report for traefik-proxy.no-internet (10.1.0.2)
Host is up (0.000019s latency).
MAC Address: 02:42:0A:01:00:02 (Unknown)
Nmap scan report for plrihfkteugv18sn4m6oz5q7p.no-internet (10.1.0.3)
Host is up (0.000055s latency).
MAC Address: 02:42:0A:01:00:03 (Unknown)
Nmap scan report for z9s0nyeq8ee1yuudctbuv54w8.no-internet (10.1.0.5)
Host is up (0.000030s latency).
MAC Address: 02:42:0A:01:00:05 (Unknown)
Nmap scan report for khdu2iy37v9m1csptbsr3lvpd.no-internet (10.1.0.6)
Host is up (0.000049s latency).
MAC Address: 02:42:0A:01:00:06 (Unknown)
Nmap scan report for c27xipaoq94gwuslmkhokaypi.no-internet (10.1.0.7)
Host is up (0.000042s latency).
MAC Address: 02:42:0A:01:00:07 (Unknown)
Nmap scan report for gvtdvv5gp7tdaqeu1ykvrjdhm.no-internet (10.1.0.8)
Host is up (0.000033s latency).
MAC Address: 02:42:0A:01:00:08 (Unknown)
Nmap scan report for INE (10.1.0.4)
Host is up.
```

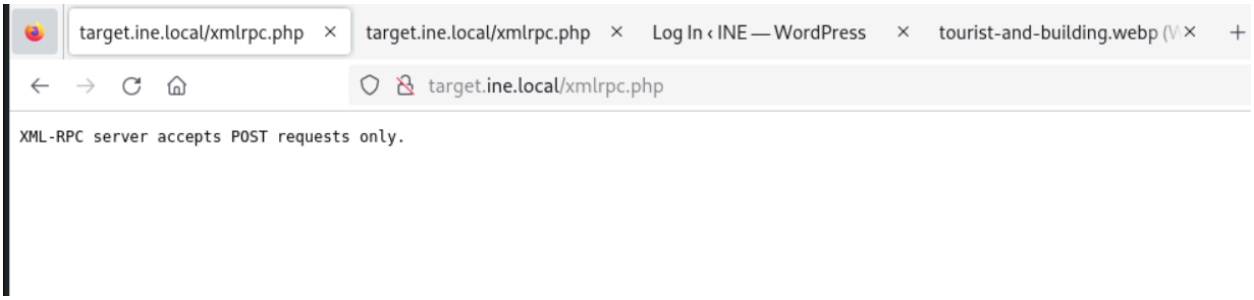
target.ine.local (192.85.46.3) || target.ine.local has address 192.47.84.3

- http://target.ine.local/wp-login.php

```
┌──(root㉿INE)-[~/hts-cache/http:/target.ine.local]
└─# ls
 index.php  '?p=2'        wp-admin     wp-includes   'wp-login.php?action=lostpassword'                                                    'xmlrpc.php?rsd'
'?p=1'       robots.txt   wp-content   wp-login.php  'wp-login.php?redirect_to=http%3A%2F%2Ftarget.ine.local%2Fwp-admin%2F%26reauth=1'
```

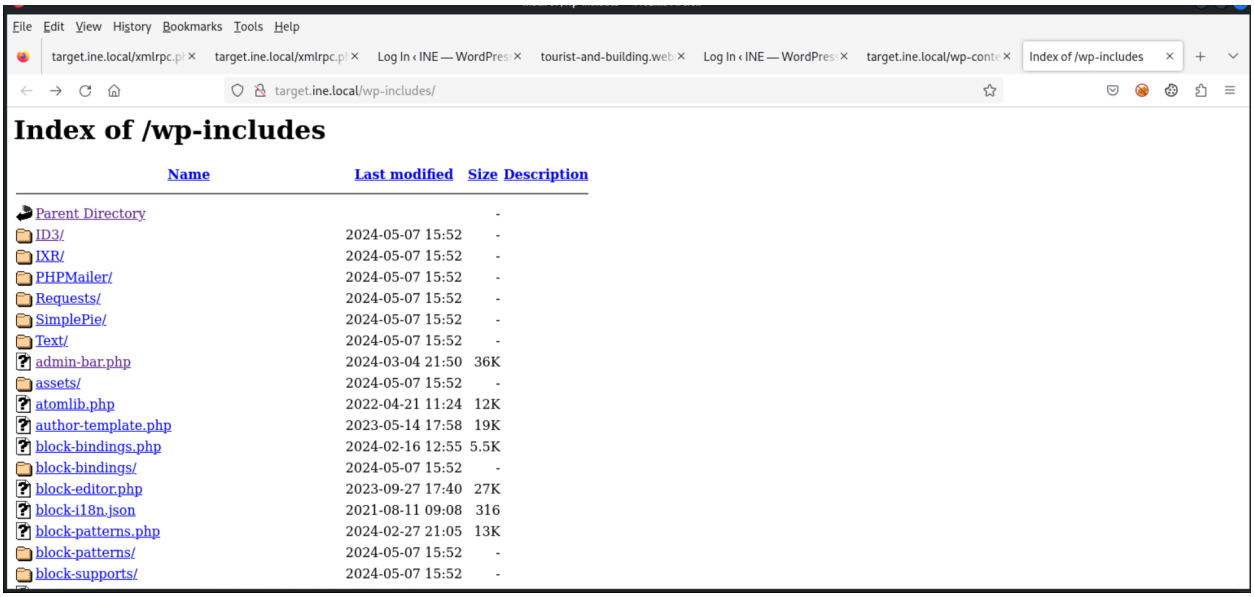
http://target.ine.local/wp-login.php

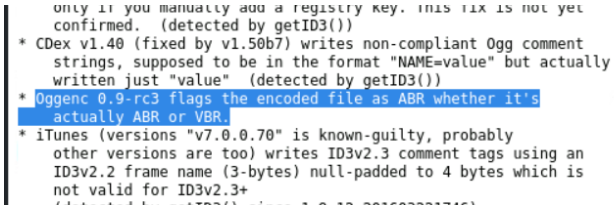

Log In ‹ INE — WordPress — Mozilla Firefox
INE
target.ine.local/xmlrpc.php
Log In ‹ INE — WordPress
tourist-and-building.webp
target.ine.local/wp-login.php
Username or Email Address
Password
Remember Me
Log In
Lost your password?
← Go to INE


target.ine.local/xmlrpc.php
target.ine.local/xmlrpc.php
Log In ‹ INE — WordPress
tourist-and-building.webp
target.ine.local/xmlrpc.php
XML-RPC server accepts POST requests only.

```
┌──(root㉿INE)-[~]
└─# gobuster dir -u http://target.ine.local/  -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://target.ine.local/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htaccess            (Status: 403) [Size: 281]
/.hta                 (Status: 403) [Size: 281]
/.htpasswd            (Status: 403) [Size: 281]
/index.php            (Status: 301) [Size: 0] [--> http://target.ine.local/]
/robots.txt           (Status: 200) [Size: 108]
/server-status        (Status: 403) [Size: 281]
/wp-admin             (Status: 301) [Size: 323] [--> http://target.ine.local/wp-admin/]
/wp-content           (Status: 301) [Size: 325] [--> http://target.ine.local/wp-content/]
/wp-includes          (Status: 301) [Size: 326] [--> http://target.ine.local/wp-includes/]
Progress: 4614 / 4615 (99.98%)
/xmlrpc.php           (Status: 405) [Size: 42]
===============================================================
Finished
===============================================================
```

http://target.ine.local/wp-includes/






```
┌──(root㉿INE)-[~]
└─# nmap -p-  10.1.0.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-23 12:35 IST
Nmap scan report for INE (10.1.0.4)
Host is up (0.000012s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE
3389/tcp  open  ms-wbt-server
45654/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 1.47 seconds
```

```
┌──(root㉿INE)-[~]
└─# nmap -Pn  -p-   192.35.21.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-23 12:37 IST
Nmap scan report for target.ine.local (192.35.21.3)
Host is up (0.000027s latency).
Not shown: 65534 closed tcp ports (reset)
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 02:42:C0:23:15:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 2.88 seconds

┌──(root㉿INE)-[~]
└─# nmap -Pn  -p-   192.35.21.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-23 12:38 IST
Nmap scan report for INE (192.35.21.2)
Host is up (0.000011s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE
3389/tcp  open  ms-wbt-server
45654/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 1.63 seconds

┌──(root㉿INE)-[~]
└─# nmap -Pn  -p-   10.1.0.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-23 12:38 IST
Nmap scan report for INE (10.1.0.4)
Host is up (0.000011s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE
3389/tcp  open  ms-wbt-server
45654/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 1.57 seconds

┌──(root㉿INE)-[~]
└─#
```

```
┌──(root㉿INE)-[~]
└─# nmap -Pn  -F -sV   192.35.21.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-23 12:53 IST
Nmap scan report for INE (192.35.21.2)
Host is up (0.000010s latency).
Not shown: 99 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
3389/tcp open  ms-wbt-server xrdp

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.33 seconds
```