## Active Information Gathering Lab

**Objective:**
The task was to conduct active reconnaissance to identify information a malicious actor could obtain about a target system.

**Scenario:**
A department seeks to improve its cybersecurity. As a penetration tester, your role is to assess potential risks through active information gathering.

**Scope:**

- Target: `ctf.wpk.tpu.fi` and its public IP.
- Public IP range: `195.148.56.130-190`.

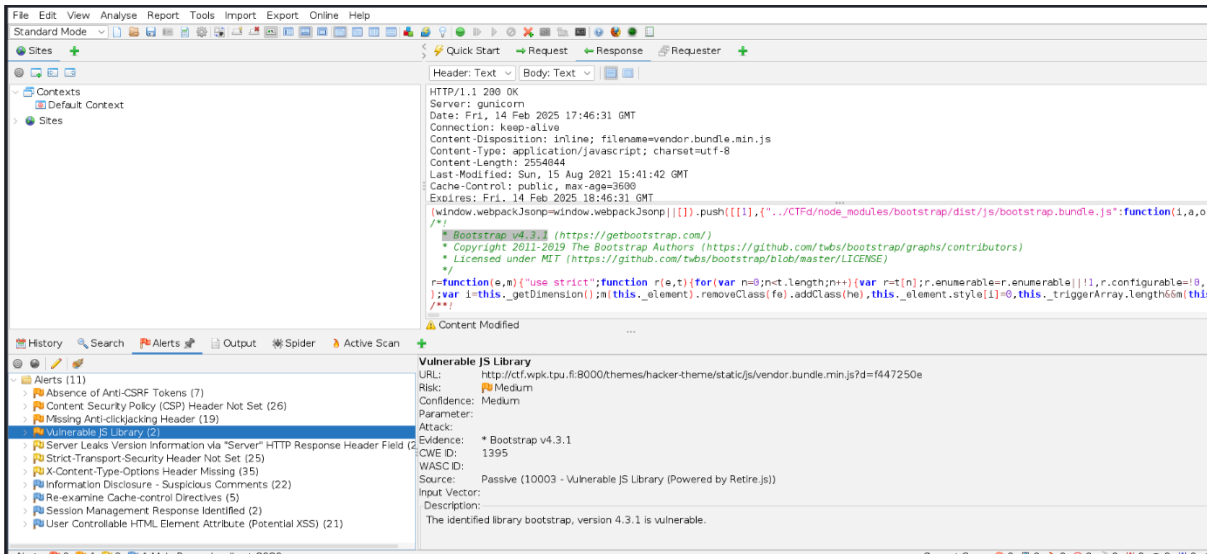
**Tools & Methods:**

- **Scanning & Enumeration:** `nmap`, `curl`, `wget`, SSL tools.
- **Vulnerability Assessment:** `nikto`, `zap`, GVM, and other suitable tools.
- **Ethical Considerations:** Avoid disruptive methods (e.g., brute force).

This lab builds on previous reconnaissance work and focuses on structured, ethical penetration testing techniques.

| Target IP | Hostname | Tool | OS | Port / Service | Version | Vulnerability |
|---|---|---|---|---|---|---|
| **193.167.167.56** | ctf.wpk.tpu.fi | Nmap-script | Linux | 443/tcp, https | Apache | CVE 2011-3192 |
| **193.167.167.56** | ctf.wpk.tpu.fi | ZAP | Linux | JS library | Bootsrap 4.3.1 | CVE-2024-6531 |
| **195.148.56.130** | ulkodns.wpk.tpu.fi | Nmap-script | | Ftp helper | | Firewall bypass through ftp helper |
| **195.148.56.189** | vpn.wpk.tpu.fi | Nmap-script | | 1723/pptp | | Pptp is heavily obsolete method |
| **193.167.167.56** | ctf.wpk.tpu.fi | Nmap-sript | Ubuntu | 80/http,443/ssl/http | nginx 1.14.0 | Obsolete version of the nginx / CVE-2018-16844 |

```
┌──(kali㉿kali)-[~]
└─$ nmap --script=vuln ctf.wpk.tpu.fi
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-05 09:31 EST
Stats: 0:00:08 elapsed; 0 hosts completed (0 up), 0 undergoing Script Pre-Scan
NSE Timing: About 0.00% done
Stats: 0:00:14 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 56.55% done; ETC: 09:32 (0:00:04 remaining)
Stats: 0:00:46 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 97.39% done; ETC: 09:32 (0:00:01 remaining)
Stats: 0:01:47 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.30% done; ETC: 09:33 (0:00:01 remaining)
Stats: 0:02:26 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.65% done; ETC: 09:34 (0:00:00 remaining)
Stats: 0:03:34 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.83% done; ETC: 09:35 (0:00:00 remaining)
Stats: 0:03:35 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.83% done; ETC: 09:35 (0:00:00 remaining)
Stats: 0:03:36 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.83% done; ETC: 09:35 (0:00:00 remaining)
Stats: 0:03:37 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.83% done; ETC: 09:35 (0:00:00 remaining)
Nmap scan report for ctf.wpk.tpu.fi (193.167.167.56)
Host is up (0.013s latency).
rDNS record for 193.167.167.56: pc167-56.guest.tpu.fi
Not shown: 994 filtered tcp ports (no-response)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
443/tcp  open  https
| http-vuln-cve2011-3192:
|   VULNERABLE:
|   Apache byterange filter DoS
|     State: VULNERABLE
|     IDs:  CVE:CVE-2011-3192  BID:49303
|       The Apache web server is vulnerable to a denial of service attack when numerous
|       overlapping byte ranges are requested.
|     Disclosure date: 2011-08-19
|     References:
|       https://www.tenable.com/plugins/nessus/55976
|       https://seclists.org/fulldisclosure/2011/Aug/175
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3192
|_      https://www.securityfocus.com/bid/49303
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
2000/tcp open  cisco-sccp
2222/tcp open  EtherNetIP-1
8000/tcp open  http-alt
```




```
Nmap scan report for vpn.wpk.tpu.fi (195.148.56.189)
Host is up (0.00028s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT     STATE SERVICE
53/tcp   open  domain
1723/tcp open  pptp
```

```
└─$ nmap -Pn --script=vuln 195.148.56.130
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-14 12:22 EST
Nmap scan report for ulkodns.wpk.tpu.fi (195.148.56.130)
Host is up.
All 1000 scanned ports on ulkodns.wpk.tpu.fi (195.148.56.130) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Host script results:
| firewall-bypass:
|_  Firewall vulnerable to bypass through ftp helper. (IPv4)

Nmap done: 1 IP address (1 host up) scanned in 214.72 seconds
```

kali@kali: ~

```
Nmap done: 1 IP address (1 host up) scanned in 4.21 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -sV -O ctf.wpk.tpu.fi
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-28 11:50 EST
Nmap scan report for ctf.wpk.tpu.fi (193.167.167.56)
Host is up (0.0046s latency).
rDNS record for 193.167.167.56: pc167-56.guest.tpu.fi
Not shown: 993 filtered tcp ports (no-response)
PORT     STATE SERVICE    VERSION
22/tcp   open  ssh        OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
80/tcp   open  http       nginx 1.14.0 (Ubuntu)
443/tcp  open  ssl/http   nginx 1.14.0 (Ubuntu)
2222/tcp open  ssh        OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
5060/tcp open  tcpwrapped
8000/tcp open  tcpwrapped
8443/tcp open  ssl/http   nginx 1.26.2
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: WAP|general purpose
Running: Actiontec embedded, Linux 2.4.X
OS CPE: cpe:/h:actiontec:mi424wr-gen3i cpe:/o:linux:linux_kernel cpe:/o:linux:linux_kernel:2.4.37
OS details: Actiontec MI424WR-GEN3I WAP, DD-WRT v24-sp2 (Linux 2.4.37)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 29.16 seconds
```