

Lab Objective:

scanning a host using Nmap and understanding the results.

Lab Purpose:

Nmap (Network Mapper) is one of the most common tools used among hackers and system administrators. It is used to scan a host, which can be a server, pc, network, etc. When running an Nmap scan, the goal is usually to discover various pieces of information about a target system or network. Examples of such information include: the devices that are connected to a network, the ports that are open on a device, the services that are running on these ports, whether the device is up, and whether there is a firewall protecting the device, among others.

Lab Tool:

Kali Linux

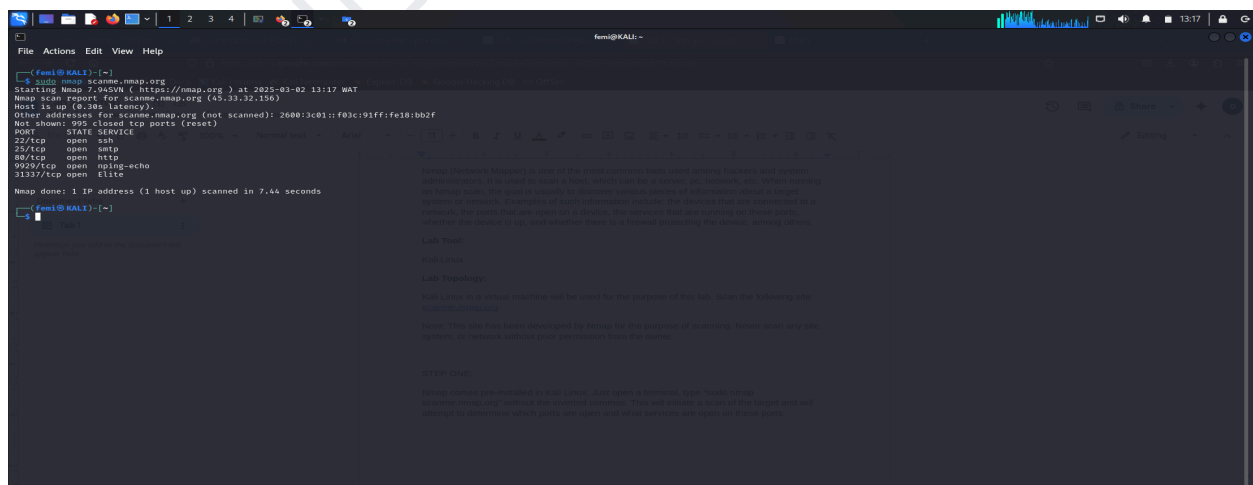
Lab Topology:

Kali Linux in a virtual machine will be used for the purpose of this lab. Scan the following site: scanme.nmap.org

Note: This site has been developed by Nmap for the purpose of scanning. Never scan any site, system, or network without prior permission from the owner.

STEP ONE:

Nmap comes pre-installed in Kali Linux. Just open a terminal, type “sudo nmap scanme.nmap.org” without the inverted commas. This will initiate a scan of the target and will attempt to determine which ports are open and what services are open on these ports.



```
femi@kali:~$ sudo nmap scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-02 13:17 WAT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.38s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f83c:91ff:fe18:bb2f
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    open  smtp
80/tcp    open  http
9929/tcp  open  nsling-echo
31337/tcp  open  elite

Nmap done: 1 IP address (1 host up) scanned in 7.44 seconds
femi@kali:~$
```

Lab Tools:

Lab Linux:

Lab Topology:

Kali Linux in a virtual machine will be used for the purpose of this lab. Scan the following site: scanme.nmap.org

Note: This site has been developed by Nmap for the purpose of scanning. Never scan any site, system, or network without prior permission from the owner.

STEP ONE:

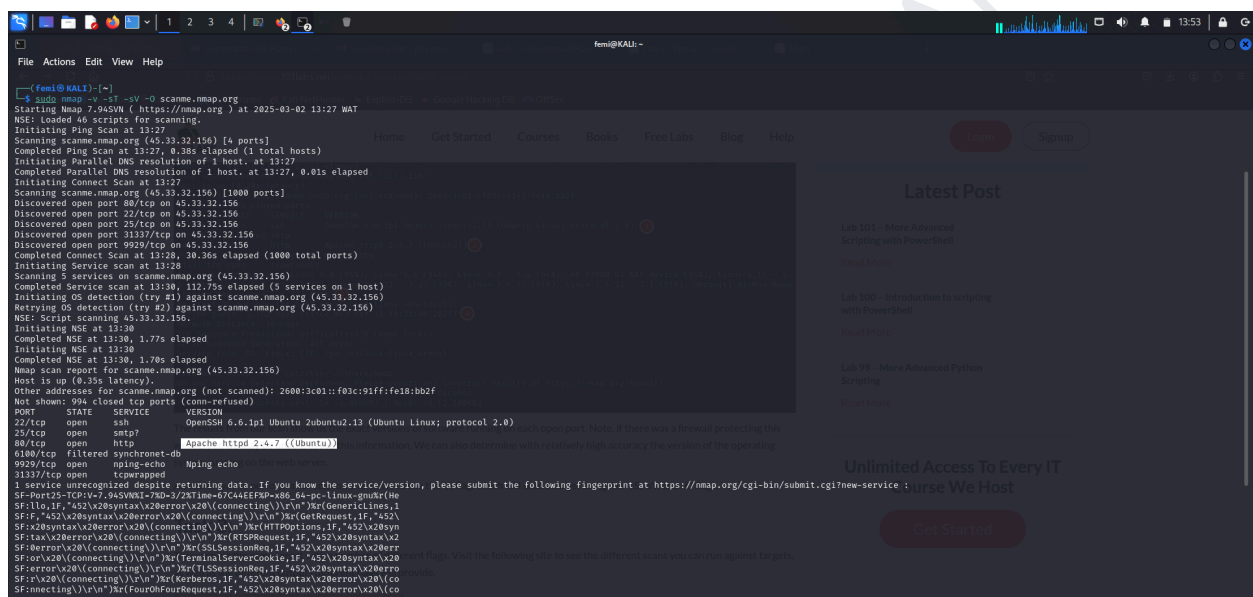
Nmap comes pre-installed in Kali Linux. Just open a terminal, type “sudo nmap scanme.nmap.org” without the inverted commas. This will initiate a scan of the target and will attempt to determine which ports are open and what services are open on these ports.

STEP TWO:

scanning the same target, scanme.nmap.org, but with a more advanced scan. Let's say we want to determine the versions for the services running on each port, so that we can determine if they are out of date and potentially vulnerable to exploitation. We also want to determine the operating system of the webserver running the target site. We will run the following scan to determine this information:

Type in **`sudo nmap -v -sT -sV -O scanme.nmap.org`**

The above command uses administrative privileges to run the Nmap program, provide verbose output, perform a TCP connect scan, detect service versions, and attempt to determine the operating system of the host **`scanme.nmap.org`**.

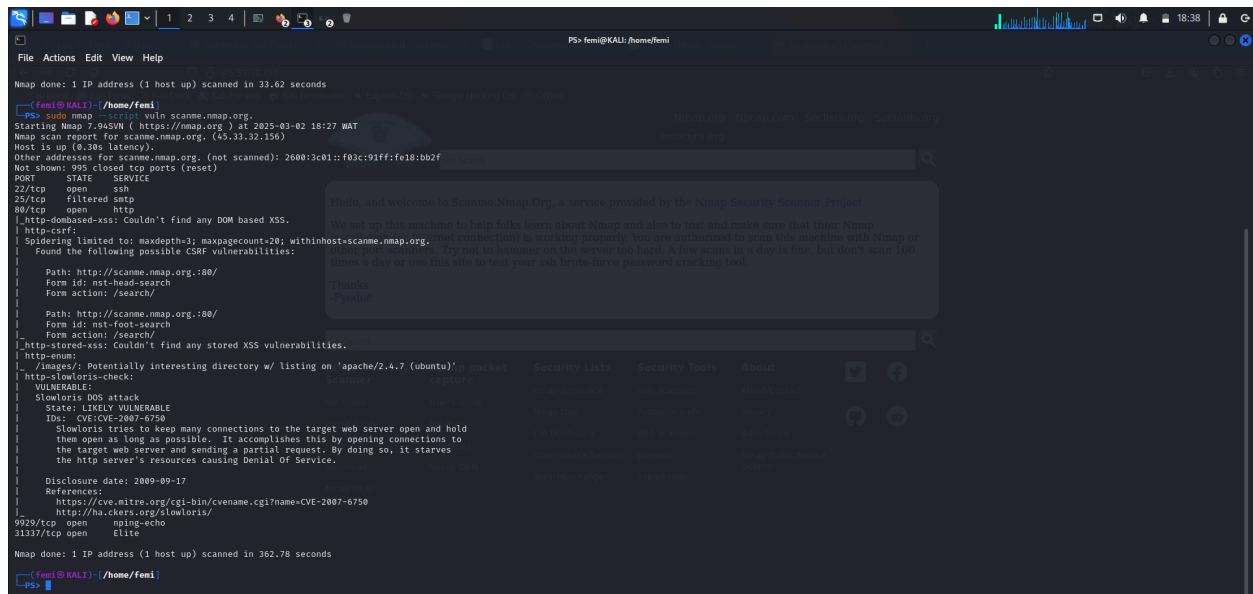


```
(femi@KALI)-[~]
$ sudo nmap -v -sT -sV -O scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-02 13:27 WAT
NSE: Loaded 46 scripts for scanning.
Initiating Ping Scan at 13:27
Scanning scanme.nmap.org (45.33.32.156) [4 ports]
Completed Ping Scan at 13:27, 0.38s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:27
Completed Parallel DNS resolution of 1 host. at 13:27, 0.01s elapsed
Initiating Connect Scan at 13:27
Scanning scanme.nmap.org (45.33.32.156) [1000 ports]
Discovered open port 80/tcp on 45.33.32.156
Discovered open port 22/tcp on 45.33.32.156
Discovered open port 25/tcp on 45.33.32.156
Discovered open port 31337/tcp on 45.33.32.156
Discovered open port 9929/tcp on 45.33.32.156
Completed Connect Scan at 13:28, 30.36s elapsed (1000 total ports)
Initiating Service scan at 13:28
Scanning 5 services on scanme.nmap.org (45.33.32.156)
Completed Service scan at 13:30, 112.75s elapsed (5 services on 1 host)
Initiating OS detection (try #1) against scanme.nmap.org (45.33.32.156)
Retrying OS detection (try #2) against scanme.nmap.org (45.33.32.156)
NSE: Script scanning 45.33.32.156.
Initiating NSE at 13:30
Completed NSE at 13:30, 1.77s elapsed
Initiating NSE at 13:30
Completed NSE at 13:30, 1.70s elapsed
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.35s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 996 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
25/tcp    open  smtp     Apache httpd 2.4.7 ((Ubuntu))
80/tcp    open  http     Nginx 1.18.0
9929/tcp  filtered synchroet-db
31337/tcp open  tcpwrapped
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service:
_
SF:Port25-TCP:V=7.94SVN:W=72D-3/25Time=6C44EEF4P=486_64-pc-linux-gnu:He
SF:|lo,if,"452\\x28syntax\\x28error\\x20\\(connecting\\)\\r\\n"\\r(GenericLines,1
SF:|F,"452\\x28syntax\\x28error\\x20\\(connecting\\)\\r\\n"\\r(GetRequest,1F,"452\\
SF:|x28syntax\\x28error\\x20\\(connecting\\)\\r\\n"\\r(HTTPOptions,1F,"452\\x28syn
SF:|x\\x28error\\x20\\(connecting\\)\\r\\n"\\r(RTSPRequest,1F,"452\\x28syntax\\x2
SF:|8error\\x20\\(connecting\\)\\r\\n"\\r(S2SessionReq,1F,"452\\x28syntax\\x28erro
SF:|or\\x20\\(connecting\\)\\r\\n"\\r(TerminalServerCookie,1F,"452\\x28syntax\\x20
SF:|error\\x20\\(connecting\\)\\r\\n"\\r(TLSSessionReq,1F,"452\\x28syntax\\x28erro
SF:|x\\x20\\(connecting\\)\\r\\n"\\r(Header,1F,"452\\x28syntax\\x28error\\x20\\(co
SF:|nnecting\\)\\r\\n"\\r(FourOHFourRequest,1F,"452\\x28syntax\\x28error\\x20\\(co
```

STEP THREE:

Checking for vulnerabilities on scanme.nmap.org.

Type in **`sudo nmap -script vuln scanme.nmap.org`**.



```
(femi@KALI) ~/home/femi
PS> sudo nmap -script vuln scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-02 18:27 WAT
Nmap scan report for scanme.nmap.org. (45.33.32.150)
Host is up (0.38s latency).
Other addresses for scanme.nmap.org. (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    filtered smtp
80/tcp    open  http
|_ http-dombased-xss: Couldn't find any DOM based XSS.
|_ http-csrf:
|   Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=scanme.nmap.org.
|   Found the following possible CSRF vulnerabilities:
|
|   Path: http://scanme.nmap.org:80/
|   Form id: nst-head-search
|   Form action: /search/
|
|   Path: http://scanme.nmap.org:80/
|   Form id: nst-foot-search
|   Form action: /search/
|_ http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_ http-slowloris-check:
|   - /images/: Potentially interesting directory w/ listing on 'apache/2.4.7 (ubuntu)'
|_ http-vuln-cvss:
|   - CVE-2007-6750: Slowloris DDoS attack
|     State: LIKELY VULNERABLE
|     IDs: CVE:CVE-2007-6750
|     Slowloris tries to keep many connections to the target web server open and hold
|     them open as long as possible. It accomplishes this by opening connections to
|     the target web server and sending a partial request. By doing so, it starves
|     the http server's resources causing Denial Of Service.
|
|   Disclosure date: 2009-09-17
|   References:
|     https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|     http://ha.ckers.org/slowloris/
|_ 9929/tcp open  nping-echo
|_ 31337/tcp open  elite
Nmap done: 1 IP address (1 host up) scanned in 362.78 seconds
(femi@KALI) ~/home/femi
PS>
```

Vulnerability Analysis

1. HTTP Vulnerabilities

- **DOM-based XSS:** Not found.
 - No DOM-based Cross-Site Scripting (XSS) vulnerabilities were detected.
- **CSRF (Cross-Site Request Forgery):**
 - Two potential CSRF vulnerabilities were identified:
 - **Form IDs:** nst-head-search and nst-foot-search
 - **Form Action:** /search/
 - **Implication:** If an attacker can trick a user into submitting a malicious request (e.g., via a crafted link or form), they could perform unauthorized actions on behalf of the user. This is a moderate risk and should be mitigated by implementing anti-CSRF tokens.
- **Stored XSS:** Not found.
 - No stored XSS vulnerabilities were detected.
- **Directory Enumeration:**
 - The /images/ directory is accessible and allows directory listing.

- **Implication:** Directory listing can expose sensitive files or information. It's recommended to disable directory listing unless explicitly required.
 - **Slowloris DoS Vulnerability:**
 - The server is **likely vulnerable** to the Slowloris Denial of Service (DoS) attack (CVE-2007-6750).
 - **Implication:** An attacker could exploit this vulnerability to exhaust server resources, causing a denial of service. This is a serious issue and should be addressed by:
 - Applying patches or updates to the web server (e.g., Apache).
 - Configuring the server to limit the number of concurrent connections or timeouts.
-

Summary of Risks

1. **High Risk:**
 - **Slowloris DoS Vulnerability:** The server is likely vulnerable to a denial of service attack. Immediate action is recommended to patch or mitigate this issue.
 2. **Moderate Risk:**
 - **CSRF Vulnerabilities:** The web application may be susceptible to CSRF attacks. Implement anti-CSRF tokens to mitigate this risk.
 - **Directory Listing:** The `/images/` directory allows listing, which could expose sensitive information. Disable directory listing unless necessary.
 3. **Low Risk:**
 - **Open Ports (22, 9929, 31337):** These ports are open but do not show any vulnerabilities. Ensure they are properly secured and monitored.
-

Recommendations

1. **Patch the Web Server:**
 - Update Apache (or the web server in use) to the latest version to address the Slowloris vulnerability.
 - Configure the server to limit the number of concurrent connections and set appropriate timeouts.
2. **Mitigate CSRF:**
 - Implement anti-CSRF tokens in all forms and actions.
 - Validate and sanitize all user inputs.
3. **Disable Directory Listing:**

- Modify the server configuration to disable directory listing for the /images/ directory and any other sensitive directories.

4. **Harden SSH:**

- Ensure SSH is configured securely (e.g., disable root login, use key-based authentication, and limit access to trusted IPs).

5. **Monitor Unusual Ports:**

- Investigate the purpose of ports 9929 and 31337. If they are not needed, consider closing them.

6. **Regular Vulnerability Scanning:**

- Perform regular vulnerability scans to identify and address new risks.