CHRIST
(DEEMED TO BE UNIVERSITY)
BANGALORE · INDIA

ASSIGNMENT

CSHO331CSP: Ethical Hacking

Topic 16: Detect Service Version with Nmap

BY

Nikshitha P 2460415

3BTCS-B

Department of Computer Science and Engineering
School of Engineering and Technology
CHRIST (Deemed to be University)
Kumbalagodu, 560074
August, 2025

INTRODUCTION:

Nmap is like a scanner tool for networks. It helps us discover what devices are running, what services (like web servers, FTP, SSH) they're offering, and which ports are open. Security professionals use it for network mapping, vulnerability scanning, and penetration testing. It's super flexible — from simply checking if a system is online to running complex scans with scripts for deeper insights.

Nmap works by sending specially crafted packets to a target and then analyzing the responses. Based on this, it can figure out things like the operating system, the software version of services, and possible misconfigurations or vulnerabilities. It's super widely used because it's lightweight, fast, and reliable — making it a go-to tool for both system admins who want to secure their networks and ethical hackers who want to test defenses.

CONDUCTION:

Target IP: `44.228.249.3`
Domain: `testphp.vulnweb.com`
Purpose: Reconnaissance scan on a deliberately vulnerable website for ethical hacking practice.

Command:

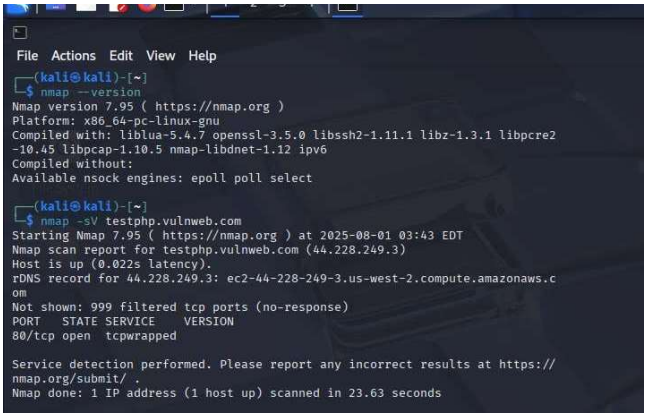
```
nmap -sV -p 80 testphp.vulnweb.com
```

Description:

- `-sV`: Attempts to detect the version of the service running on port 80.
- `-p 80`: Scans only port 80 (HTTP).

Result:

- **PORT 80/tcp: filtered**
- Meaning: Port 80 was not responsive or blocked by a firewall, preventing service detection.



Second Attempt with Adjusted Flags

Command:

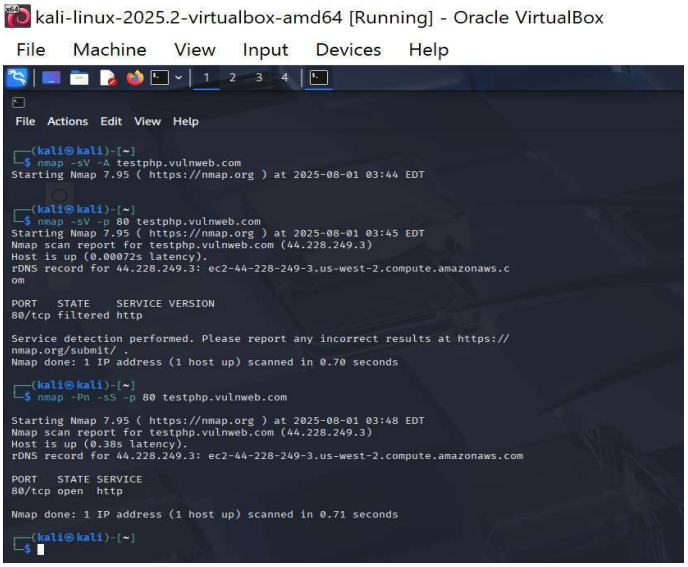
```
nmap -Pn -sS -p 80 testphp.vulnweb.com
```

Description:

- `-Pn`: Disables host discovery (skips ping). Useful when ICMP is blocked.
- `-sS`: Performs a stealth SYN scan to check for open ports.
- `-p 80`: Scans port 80.

Result:

```
PORT  STATE SERVICE
80/tcp open  http
```



- Port 80 is open, confirming the presence of an active HTTP service.
- The first scan failed to detect the service due to filtered port (possibly blocked ICMP or TCP handshake attempts).
- The second scan succeeded by bypassing ping and using a stealth method, confirming port 80 is open.
- The active HTTP service indicates potential attack surface for testing vulnerabilities like SQLi, XSS, LFI, etc.

CONCLUSION:

In short, Nmap is more than just a network scanner — it's a versatile toolkit for discovering, monitoring, and securing systems. Whether used for simple host detection or advanced vulnerability assessment, it plays a vital role in cybersecurity by giving professionals the visibility they need to strengthen defenses and respond quickly to threats.