



# 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.

```
File Actions Edit View Help
(kali@kali)-[~]
└─$ nmap --version
Nmap version 7.95 ( https://nmap.org )
Platform: x86_64-pc-linux-gnu
Compiled with: liblua-5.4.7 openssl-3.5.0 libssh2-1.11.1 libz-1.3.1 libpcre2
-10.45 libpcap-1.10.5 nmap-libdnet-1.12 ipv6
Compiled without:
Available nsock engines: epoll poll select

(kali@kali)-[~]
└─$ nmap -sV testphp.vulnweb.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-01 03:43 EDT
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.022s latency).
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.c
om
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  tcpwrapped

Service detection performed. Please report any incorrect results at https://
nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 23.63 seconds
```

## 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
```

```
kali-linux-2025.2-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help

(kali@kali)-[~]
└─$ nmap -sV testphp.vulnweb.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-01 03:44 EDT

(kali@kali)-[~]
└─$ nmap -sV -p 80 testphp.vulnweb.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-01 03:45 EDT
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.00072s latency).
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.c
om

PORT      STATE SERVICE
80/tcp    filtered http

Service detection performed. Please report any incorrect results at https://
nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 0.70 seconds

(kali@kali)-[~]
└─$ nmap -Pn -sS -p 80 testphp.vulnweb.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-01 03:48 EDT
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.38s latency).
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.com

PORT      STATE SERVICE
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 0.71 seconds

(kali@kali)-[~]
```

- 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.