

ASSIGNMENT

CSHO331CSP: Ethical Hacking

Topic 16: Detect Service Version with Nmap

BY

Reuben Sunish 2460429

3BTCS-A

Department of Computer Science and Engineering

School of Engineering and Technology

CHRIST (Deemed to be University)

Kumbalagodu, 560074

August, 2025

Introduction:

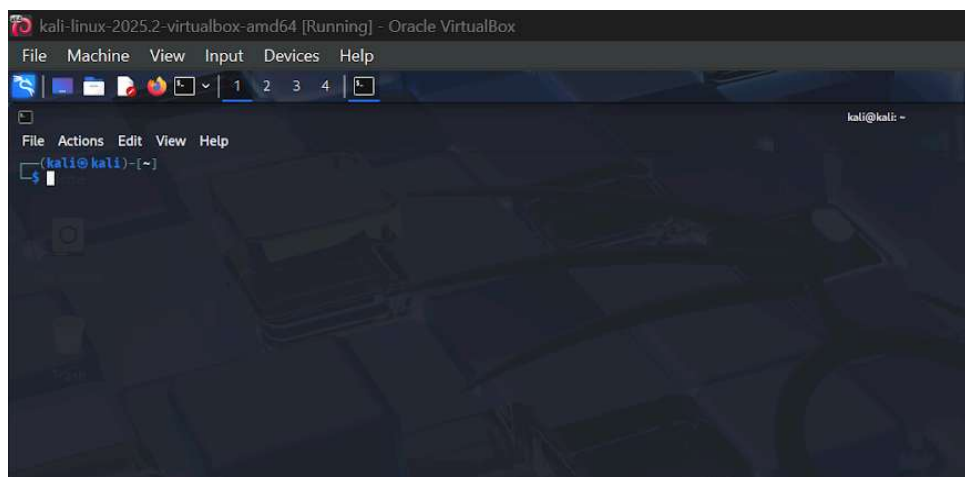
Nmap is short for Network Mapper. It is an open-source Linux command-line tool that is used to scan IP addresses and ports in a network and to detect installed applications.

Nmap allows network admins to find which devices are running on their network, discover open ports and services, and detect vulnerabilities.

Some of the reasons why Nmap is used are that it can quickly map out single or multiple networks, detecting all connected devices such as servers, routers, switches, and mobile devices. It helps identify running services (like web and DNS servers) along with their versions, detect operating systems and their details, and assist in vulnerability scanning through its scripting engine. Nmap also offers a graphical interface, Zenmap, for creating visual network maps to simplify analysis and reporting.

Conduction:

1. Kali Linux was launched and run



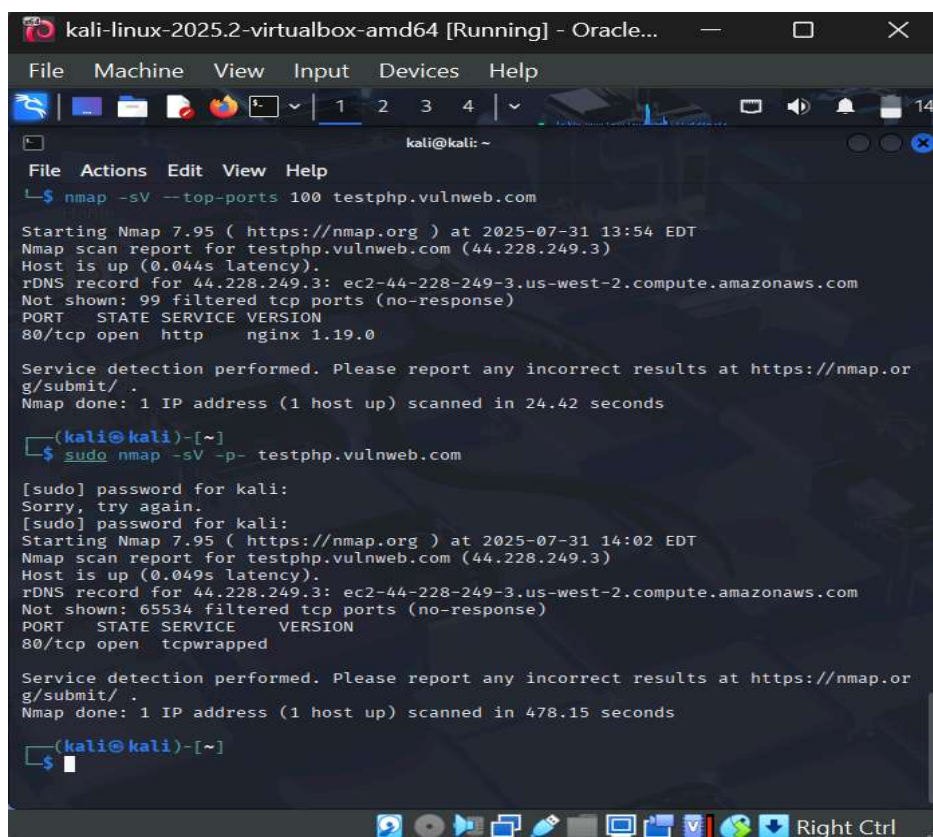
A few nmap commands were run but they did not return the expected results.

80/tcp open tcpwrapped was seen indicating that the host is using a security mechanism—such as TCP Wrappers, xinetd, or similar firewall-based filtering—to restrict or control access to the service. As a result, detailed service version detection is not possible on this port unless access is explicitly permitted.

But on running another command,

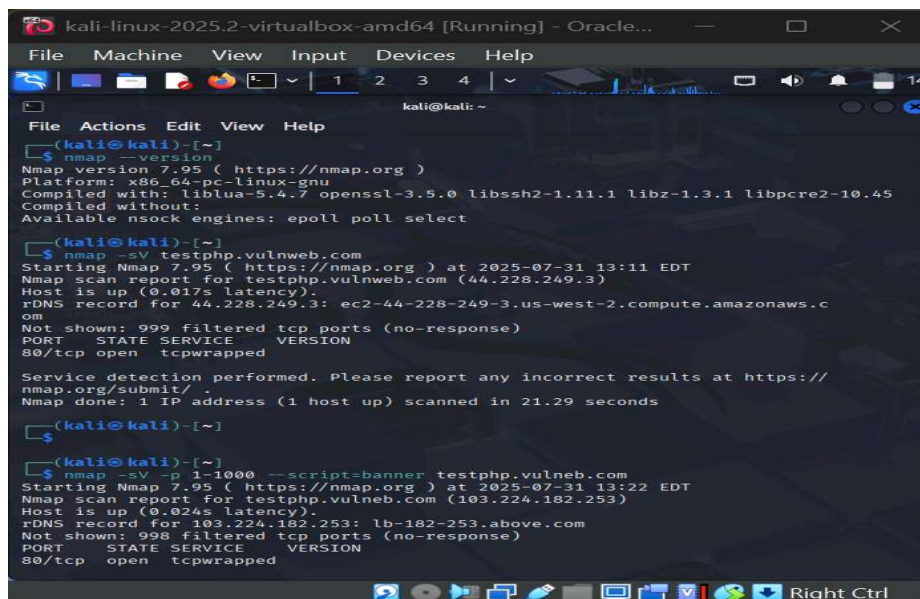
```
nmap -sV --top-ports 100 testphp.vulnweb.com
```

One service was obtained



```
kali@kali: ~  
File Actions Edit View Help  
$ nmap -sV --top-ports 100 testphp.vulnweb.com  
  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-31 13:54 EDT  
Nmap scan report for testphp.vulnweb.com (44.228.249.3)  
Host is up (0.044s latency).  
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.com  
Not shown: 99 filtered tcp ports (no-response)  
PORT      STATE SERVICE VERSION  
80/tcp    open  http      nginx 1.19.0  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 24.42 seconds  
  
(kali@kali)-[~]  
$ sudo nmap -sV -p- testphp.vulnweb.com  
  
[sudo] password for kali:  
Sorry, try again.  
[sudo] password for kali:  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-31 14:02 EDT  
Nmap scan report for testphp.vulnweb.com (44.228.249.3)  
Host is up (0.049s latency).  
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.com  
Not shown: 65534 filtered tcp ports (no-response)  
PORT      STATE SERVICE VERSION  
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 478.15 seconds  
  
(kali@kali)-[~]  
$
```

Attempted to look for 2 more services, however,



```
kali@kali: ~  
$ nmap -v testphp.vulnweb.com  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-31 13:11 EDT  
Nmap scan report for testphp.vulnweb.com (44.228.249.3)  
Host is up (0.017s latency).  
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.com  
Not shown: 999 filtered tcp ports (no-response)  
PORT      STATE SERVICE      VERSION  
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 21.29 seconds  
  
$ nmap -sV -p 1-1000 --script-banner testphp.vulnweb.com  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-31 13:22 EDT  
Nmap scan report for testphp.vulnweb.com (103.224.182.253)  
Host is up (0.024s latency).  
rDNS record for 103.224.182.253: lb-182-253.above.com  
Not shown: 998 filtered tcp ports (no-response)  
PORT      STATE SERVICE      VERSION  
80/tcp    open  tcpwrapped
```

From the results obtained, **only port 80** is accessible and is running an outdated version of Nginx.

Port 80/tcp: Running *nginx 1.19.0* (HTTP service)

Known vulnerabilities for this version include:

- **CVE-2021-23017:** Memory corruption via DNS resolver

Type: 1-byte memory overwrite (Buffer Overflow)

A carefully crafted DNS response can trigger a 1-byte buffer overwrite in the **resolver** component of nginx. This can potentially lead to a denial-of-service (crash), or under certain conditions, arbitrary code execution. Affected Versions: nginx 0.6.18 – 1.20.0

- **CVE-2020-11724:** HTTP/2 vulnerabilities

Type: NULL pointer dereference.

A bug in nginx's HTTP/2 implementation allowed for a NULL pointer dereference

when processing certain specially crafted requests. This leads to unexpected termination of worker processes. Affected Versions: nginx before 1.19.1 with the http2 module enabled

- **CVE-2021-3618:** General HTTP parsing issues

Type: Privilege escalation (via outdated packaging)

Found in **nginx Alpine Linux package**, where improper sandboxing and outdated builds led to a potential **privilege escalation** vector if used with specific container configurations. **Affected Versions:** nginx packaged with older Alpine Linux versions

Security Insight: The detected version of Nginx (**1.19.0**) is outdated.

These vulnerabilities could lead to denial-of-service or remote code execution under certain conditions. Running outdated versions like nginx 1.19.0 can leave the server open to remote exploits, memory corruption, and request manipulation. These could lead to denial-of-service or unauthorized access.

Conclusions and Understanding:

Through this activity, I learned to effectively use Nmap for network reconnaissance and security assessment. I gained skills in identifying network devices, detecting running services and their versions, and determining the operating systems of hosts. I also explored basic vulnerability scanning using the Nmap Scripting Engine and practiced working with the Nmap command-line tool. Additionally, I developed the basic ability to interpret scan results