**Winter Semester 22-23**

**Regno:20BCE2404**

**Name: Kirit Govindaraja Pilla**

**Slot: L25+L26**

**Subject: CSE3502 Information Security Management**

**Faculty: Prof.Kathiravan S**

**LABFAT**

**SET -2**

i)Consider the class C subnet to identify the available web servers and determine whether they present an interesting attack surface. Using Nmap and other essentials tools, perform a scan for the port 8080 in this entire subnet to determine the open web services.

ii)Deploy Nikto perform a web content scan (maxtime = 45 seconds) for the following vulnerable web application: http://testphp.vulnweb.com/artists.php?artist=1

Question 2) i.

Aim

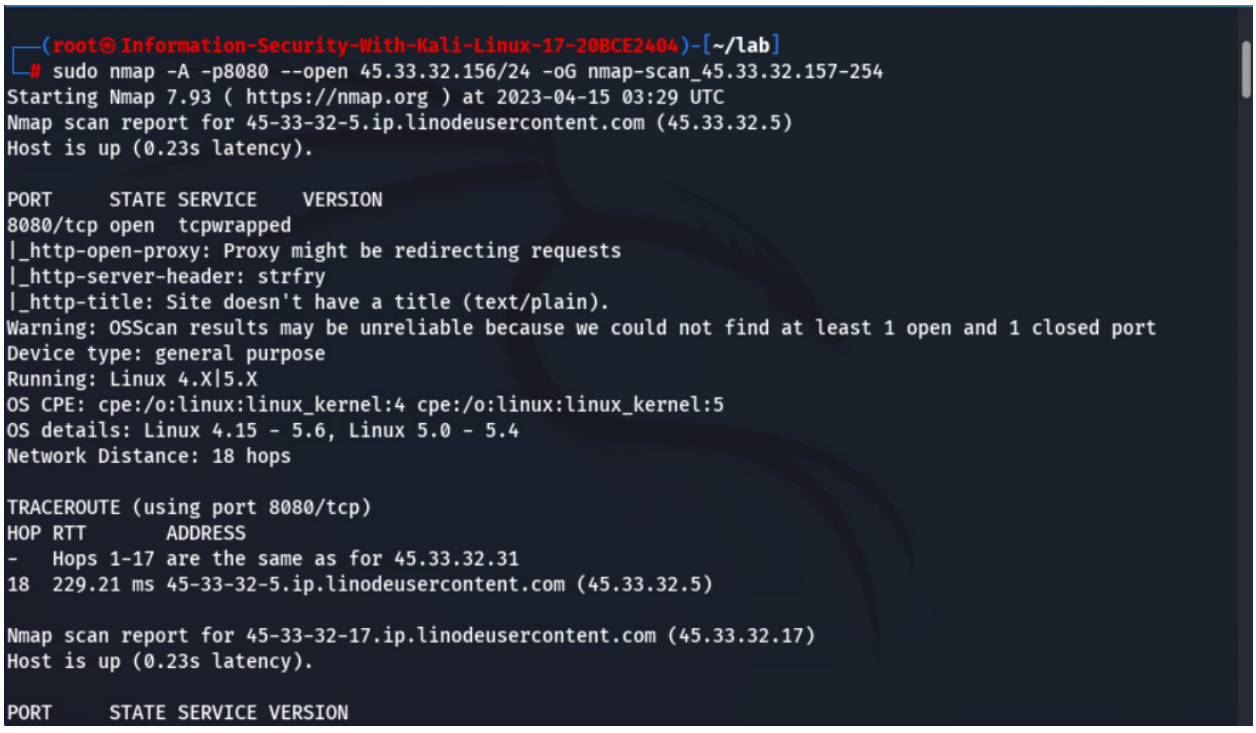
To perform a scan for the port 8080 in this entire subnet to determine the open web services.

Procedure

- Create a lab folder for the exercise.
- Use "cd" to enter the temporary folder directory.
- Scan the class C subnet using nmap with "-A" option for aggressive scanning, "-p" for port 8080, "--open" to return machines with open ports, and "-oG" to save the scan results in greppable format.
- Use "cat" command to view the output file format.

- Notice that each IP address is repeated twice, with the first line displaying the machine status and the second displaying the port number being scanned.
- Use "grep" to filter for lines containing port 8080.
- Use "grep -v" to exclude the first line containing the case-sensitive keyword "Nmap".
- Use "awk" to print the second field, which is the IP addresses, using space as a delimiter.
- Use a Bash one-liner to loop through the IP address list and run cutycapt with "--url" to specify the target web site and "--out" to specify the name of the output file.
- Use "ls -1" to list the output files created by the Bash one-liner.
- Use scripting knowledge and basic HTML knowledge to create a Bash script that builds an HTML file (web.html), inserts each .PNG file name into an HTML IMG tag, appends this to our web.html file, and appends HTML end tags into the file.
- Make the script executable and view it in the browser to see a view of each web server's main page.

**Observation**



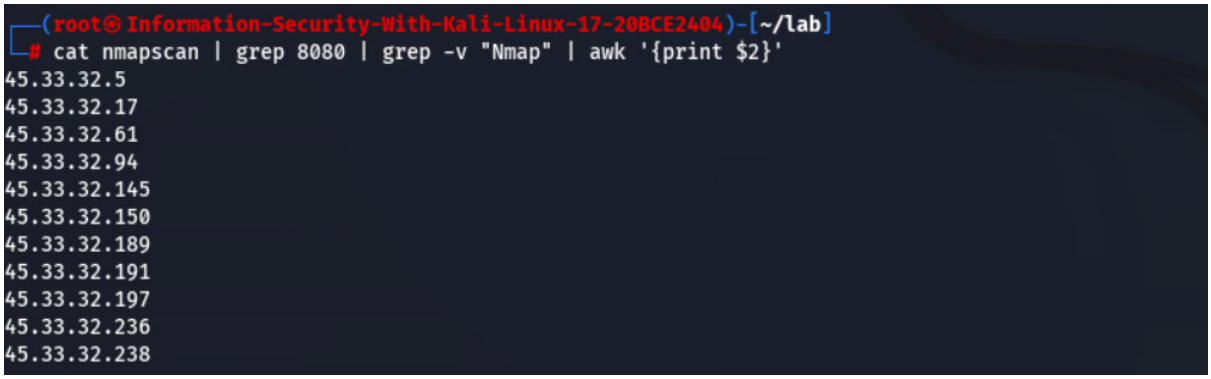
```
PORT     STATE SERVICE VERSION
8080/tcp open  http    Apache httpd 2.4.29 ((Ubuntu) mod_fcgid/2.3.9 OpenSSL/1.1.1)
|_http-title: Site doesn't have a title (text/html).
| http-methods:
|_  Potentially risky methods: TRACE
|_http-open-proxy: Proxy might be redirecting requests
|_http-server-header: Apache/2.4.29 (Ubuntu) mod_fcgid/2.3.9 OpenSSL/1.1.1
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 5.X
OS CPE: cpe:/o:linux:linux_kernel:5.4
OS details: Linux 5.4
Network Distance: 18 hops

TRACEROUTE (using port 8080/tcp)
HOP RTT       ADDRESS
-   Hops 1-17 are the same as for 45.33.32.10
18  225.12 ms 45-33-32-17.ip.linodeusercontent.com (45.33.32.17)

Nmap scan report for li982-61.members.linode.com (45.33.32.61)
Host is up (0.23s latency).

PORT     STATE SERVICE    VERSION
8080/tcp open  http-proxy
| fingerprint-strings:
|   DNSStatusRequestTCP, DNSVersionBindReqTCP, RPCCheck, RTSPRequest, Socks4, Socks5:
|     HTTP/1.1 400 Bad Request
|     Content-Length: 65
```

```
root@Information-Security-With-Kali-Linux-17-20BCE2404: ~/lab
File  Edit  View  Search  Terminal  Help
Service Info: Host: localhost

TRACEROUTE (using port 8080/tcp)
HOP RTT       ADDRESS
-   Hops 1-17 are the same as for 45.33.32.31
18  225.12 ms 45-33-32-236.ip.linodeusercontent.com (45.33.32.236)

Nmap scan report for 45-33-32-238.ip.linodeusercontent.com (45.33.32.238)
Host is up (0.23s latency).

PORT     STATE SERVICE         VERSION
8080/tcp open  ssl/http-proxy?
|_http-trane-info: ERROR: Script execution failed (use -d to debug)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6, Linux 5.0 - 5.4
Network Distance: 18 hops

TRACEROUTE (using port 8080/tcp)
HOP RTT       ADDRESS
-   Hops 1-17 are the same as for 45.33.32.9
18  225.65 ms 45-33-32-238.ip.linodeusercontent.com (45.33.32.238)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (206 hosts up) scanned in 196.84 seconds
```

```
┌──(root㉿Information-Security-With-Kali-Linux-17-20BCE2404)-[~/lab]
└─# cat nmapscan
# Nmap 7.93 scan initiated Sat Apr 15 03:43:28 2023 as: nmap -A -p8080 --open -oG nmapscan 45.33.32.156/24
Host: 45.33.32.5 (45-33-32-5.ip.linodeusercontent.com)  Status: Up
Host: 45.33.32.5 (45-33-32-5.ip.linodeusercontent.com)  Ports: 8080/open/tcp//tcpwrapped///     OS: Linux 4.15 - 5.6|Linux 5.0 - 5.4    Se
q Index: 261    IP ID Seq: All zeros
Host: 45.33.32.17 (45-33-32-17.ip.linodeusercontent.com)        Status: Up
Host: 45.33.32.17 (45-33-32-17.ip.linodeusercontent.com)        Ports: 8080/open/tcp//http//Apache httpd 2.4.29 ((Ubuntu) mod_fcgid|2.3.9
OpenSSL|1.1.1)/ OS: Linux 5.4   Seq Index: 255  IP ID Seq: All zeros
Host: 45.33.32.61 (li982-61.members.linode.com) Status: Up
Host: 45.33.32.61 (li982-61.members.linode.com) Ports: 8080/open/tcp//http-proxy///     OS: Linux 3.2 - 4.9|Linux 5.1   Seq Index: 262  IP
 ID Seq: All zeros
Host: 45.33.32.94 (li982-94.members.linode.com) Status: Up
Host: 45.33.32.94 (li982-94.members.linode.com) Ports: 8080/open/tcp//http-proxy///     OS: Linux 4.15 - 5.6|Linux 5.0 - 5.4    Seq Index:
 260    IP ID Seq: All zeros
Host: 45.33.32.145 (45-33-32-145.ip.linodeusercontent.com)      Status: Up
Host: 45.33.32.145 (45-33-32-145.ip.linodeusercontent.com)      Ports: 8080/open/tcp//http//Apache httpd 2.4.29 ((Ubuntu) mod_fcgid|2.3.9
OpenSSL|1.1.1)/ OS: Linux 4.15 - 5.6|Linux 5.4  Seq Index: 258  IP ID Seq: All zeros
Host: 45.33.32.150 (unifi.tonythedeveloper.cloud)       Status: Up
Host: 45.33.32.150 (unifi.tonythedeveloper.cloud)       Ports: 8080/open/tcp//http-proxy///     OS: Linux 5.4   Seq Index: 259  IP ID Seq:
 All zeros
Host: 45.33.32.189 (li982-189.members.linode.com)       Status: Up
Host: 45.33.32.189 (li982-189.members.linode.com)       Ports: 8080/open/tcp//http-proxy///     OS: Linux 4.15 - 5.6    Seq Index: 263  IP
 ID Seq: All zeros
```

```
┌──(root㉿Information-Security-With-Kali-Linux-17-20BCE2404)-[~/lab]
└─# cat nmapscan | grep 8080
# Nmap 7.93 scan initiated Sat Apr 15 03:43:28 2023 as: nmap -A -p8080 --open -oG nmapscan 45.33.32.156/24
Host: 45.33.32.5 (45-33-32-5.ip.linodeusercontent.com)  Ports: 8080/open/tcp//tcpwrapped///     OS: Linux 4.15 - 5.6|Linux 5.0 - 5.4    Se
q Index: 261    IP ID Seq: All zeros
Host: 45.33.32.17 (45-33-32-17.ip.linodeusercontent.com)        Ports: 8080/open/tcp//http//Apache httpd 2.4.29 ((Ubuntu) mod_fcgid|2.3.9
OpenSSL|1.1.1)/ OS: Linux 5.4   Seq Index: 255  IP ID Seq: All zeros
Host: 45.33.32.61 (li982-61.members.linode.com) Ports: 8080/open/tcp//http-proxy///     OS: Linux 3.2 - 4.9|Linux 5.1   Seq Index: 262  IP
 ID Seq: All zeros
Host: 45.33.32.94 (li982-94.members.linode.com) Ports: 8080/open/tcp//http-proxy///     OS: Linux 4.15 - 5.6|Linux 5.0 - 5.4    Seq Index:
 260    IP ID Seq: All zeros
Host: 45.33.32.145 (45-33-32-145.ip.linodeusercontent.com)      Ports: 8080/open/tcp//http//Apache httpd 2.4.29 ((Ubuntu) mod_fcgid|2.3.9
OpenSSL|1.1.1)/ OS: Linux 4.15 - 5.6|Linux 5.4  Seq Index: 258  IP ID Seq: All zeros
Host: 45.33.32.150 (unifi.tonythedeveloper.cloud)       Ports: 8080/open/tcp//http-proxy///     OS: Linux 5.4   Seq Index: 259  IP ID Seq:
 All zeros
Host: 45.33.32.189 (li982-189.members.linode.com)       Ports: 8080/open/tcp//http-proxy///     OS: Linux 4.15 - 5.6    Seq Index: 263  IP
 ID Seq: All zeros
Host: 45.33.32.191 (movetoapple.com)    Ports: 8080/open/tcp//http//Apache httpd 2.4.12 ((Ubuntu))/     OS: Linux 4.15 - 5.6|Linux 5.0 - 5
.4      Seq Index: 261  IP ID Seq: All zeros
Host: 45.33.32.197 (li982-197.members.linode.com)       Ports: 8080/open/tcp//http//Jetty 9.4.z-SNAPSHOT/       OS: Linux 4.15 - 5.6    Se
q Index: 260    IP ID Seq: All zeros
Host: 45.33.32.236 (45-33-32-236.ip.linodeusercontent.com)      Ports: 8080/open/tcp//http//Apache httpd 2.4.55/        OS: Linux 4.15 - 5
.6      Seq Index: 264  IP ID Seq: All zeros
Host: 45.33.32.238 (45-33-32-238.ip.linodeusercontent.com)      Ports: 8080/open/tcp//ssl|http-proxy?///        OS: Linux 4.15 - 5.6    Se
q Index: 260    IP ID Seq: All zeros

┌──(root㉿Information-Security-With-Kali-Linux-17-20BCE2404)-[~/lab]
└─#
```

```
┌──(root㉿Information-Security-With-Kali-Linux-17-20BCE2404)-[~/lab]
└─# cat nmapscan | grep 8080 | grep -v "Nmap"
Host: 45.33.32.5 (45-33-32-5.ip.linodeusercontent.com)  Ports: 8080/open/tcp//tcpwrapped///     OS: Linux 4.15 - 5.6|Linux 5.0 - 5.4    Se
q Index: 261    IP ID Seq: All zeros
Host: 45.33.32.17 (45-33-32-17.ip.linodeusercontent.com)        Ports: 8080/open/tcp//http//Apache httpd 2.4.29 ((Ubuntu) mod_fcgid|2.3.9
OpenSSL|1.1.1)/ OS: Linux 5.4   Seq Index: 255  IP ID Seq: All zeros
Host: 45.33.32.61 (li982-61.members.linode.com) Ports: 8080/open/tcp//http-proxy///     OS: Linux 3.2 - 4.9|Linux 5.1   Seq Index: 262  IP
 ID Seq: All zeros
Host: 45.33.32.94 (li982-94.members.linode.com) Ports: 8080/open/tcp//http-proxy///     OS: Linux 4.15 - 5.6|Linux 5.0 - 5.4    Seq Index:
 260    IP ID Seq: All zeros
Host: 45.33.32.145 (45-33-32-145.ip.linodeusercontent.com)      Ports: 8080/open/tcp//http//Apache httpd 2.4.29 ((Ubuntu) mod_fcgid|2.3.9
OpenSSL|1.1.1)/ OS: Linux 4.15 - 5.6|Linux 5.4  Seq Index: 258  IP ID Seq: All zeros
Host: 45.33.32.150 (unifi.tonythedeveloper.cloud)       Ports: 8080/open/tcp//http-proxy///     OS: Linux 5.4   Seq Index: 259  IP ID Seq:
 All zeros
Host: 45.33.32.189 (li982-189.members.linode.com)       Ports: 8080/open/tcp//http-proxy///     OS: Linux 4.15 - 5.6    Seq Index: 263  IP
 ID Seq: All zeros
Host: 45.33.32.191 (movetoapple.com)    Ports: 8080/open/tcp//http//Apache httpd 2.4.12 ((Ubuntu))/     OS: Linux 4.15 - 5.6|Linux 5.0 - 5
.4      Seq Index: 261  IP ID Seq: All zeros
Host: 45.33.32.197 (li982-197.members.linode.com)       Ports: 8080/open/tcp//http//Jetty 9.4.z-SNAPSHOT/       OS: Linux 4.15 - 5.6    Se
q Index: 260    IP ID Seq: All zeros
Host: 45.33.32.236 (45-33-32-236.ip.linodeusercontent.com)      Ports: 8080/open/tcp//http//Apache httpd 2.4.55/        OS: Linux 4.15 - 5
.6      Seq Index: 264  IP ID Seq: All zeros
Host: 45.33.32.238 (45-33-32-238.ip.linodeusercontent.com)      Ports: 8080/open/tcp//ssl|http-proxy?///        OS: Linux 4.15 - 5.6    Se
q Index: 260    IP ID Seq: All zeros
```




**Inference**

We have scanned a class C subnet 45.33.32.156 to identify web servers and determine whether or not they present an interesting attack surface. The procedure involves using nmap to scan the subnet and filter for machines with open port 8080. The IP addresses are then extracted and used to generate screenshots of the web pages using cutycapt. The use of aggressive scanning with nmap helps to identify potential attack vectors by detecting what services are running on the target machines. By filtering for machines with open port 8080, the focus is on identifying web servers that may present an interesting attack surface. Overall, the procedure outlined in the scenario provides a systematic and effective way to scan a class C subnet and identify potential attack surfaces.

Question 2) ii.

**Aim**

To perform a web content scan (maxtime = 45 seconds) for the web application: http://testphp.vulnweb.com/artists.php?artist=1

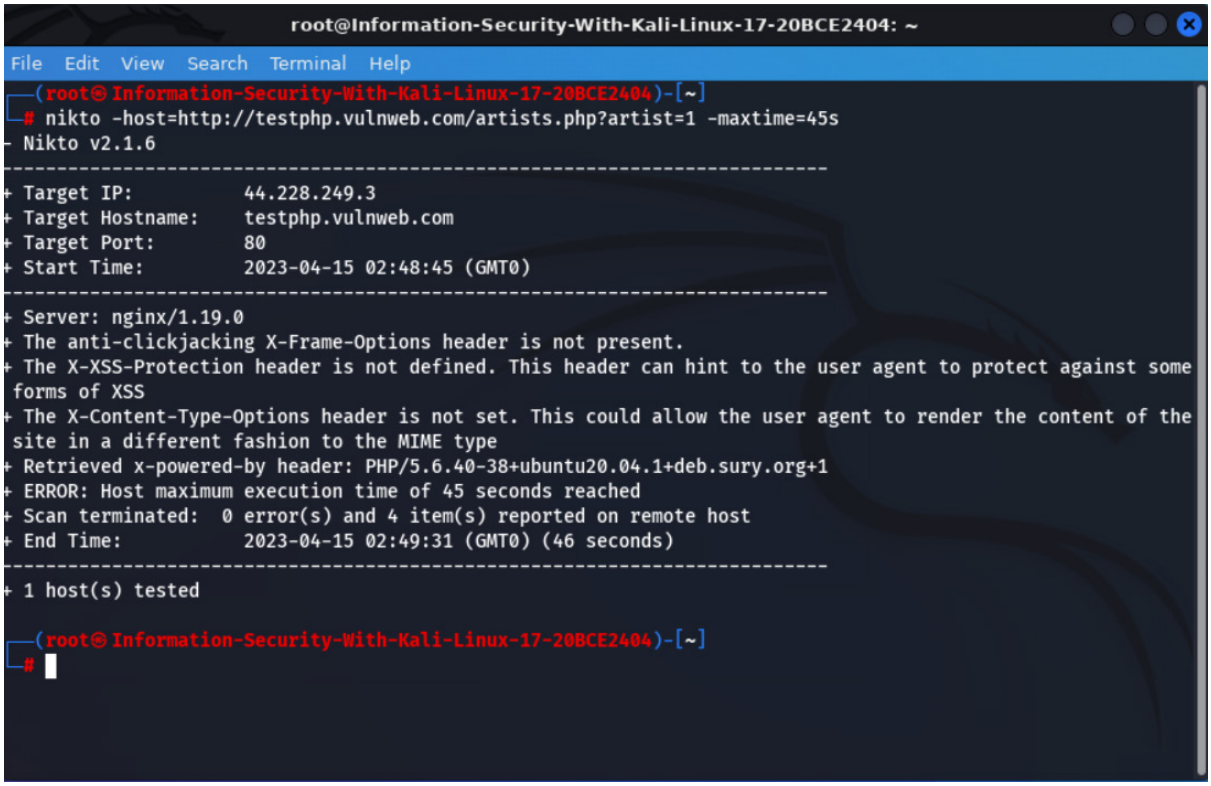
**Procedure**

- Nikto is not designed for stealth as it will send many requests and embed information about itself in the User-Agent header.
- Set the -maxtime option, which will halt the scan after the specified time limit.
- -T option is used to tune and control which types of tests to run.
- Nikto is especially useful for catching low-hanging fruit, reporting non-standard server headers, and catching server configuration errors.
- To run Nikto against a host, specify the host to scan
  **nikto -host=http://testphp.vulnweb.com/artists.php?artist=1 -maxtime=45s**

or -T option to control the scan duration and test types.

- Record the obtained Output and the data from the given scan.

Observation




**Inference**

The experiment aimed to analyze http://testphp.vulnweb.com/artists.php?artist=1 using Nikto in Kali Linux. Nikto was used to scan multiple servers and pages, reporting non-standard server headers, catching server configuration errors and identifying low-hanging fruit. The scan was not designed for stealth and the -maxtime and -T options were used to control the scan duration and types of tests run. The aim was to assess the website's security vulnerabilities and identify potential risks.