Name: Prathmesh baviskar
Roll no: 5020106
Name: Joshua Dabhi
Roll no: 5020167

Experiment 2

Aim: Study of packet sniffer tools like Wireshark and Nmap.

Theory:

A network observer, commonly known as a network scrutinizer or network analyzer, serves as a valuable tool for network administrators to oversee and troubleshoot network traffic. This tool captures data packets, allowing administrators to identify faulty packets and address network congestion to ensure smooth data transmission. In its basic form, a packet sniffer captures all data packets traversing a specific network interface. However, when a malicious intruder deploys a packet sniffer in promiscuous mode, they can intercept and scrutinize all network traffic.

Wireshark stands out as a leading network packet analyzer. Its primary function is to capture and display network packets in meticulous detail. Wireshark is open-source and freely available, making it one of the most esteemed packet analysis tools in use today. Its capabilities include:

- Compatibility with UNIX and Windows operating systems.

- Real-time packet data capture from network interfaces.

- In-depth protocol information displayed for packets.

- The ability to save captured packet data.

- Utilization by QA engineers for network application verification.

- Utilization by developers for debugging protocol implementations.

- A resource for individuals interested in learning about network protocol intricacies.

Nmap, also known as Network Mapper, is a security scanning tool originally created by Gordon Lyon. It serves the purpose of discovering hosts and services within a computer network. Nmap is an open-source, free tool employed for vulnerability scanning and network exploration. Network administrators leverage Nmap to identify active devices on their systems, discover available hosts and their services, identify open ports, and detect potential security vulnerabilities. Nmap's versatility extends to monitoring individual hosts as well as extensive networks encompassing numerous devices and subnetworks. Essentially, Nmap is a network scanning utility that employs IP packets to identify all devices connected to a network, revealing information about their services and operating systems.

Wireshark Usage Steps:

I. Download and install Wireshark.

II. Initiate scanning using Ethernet or Wi-Fi.

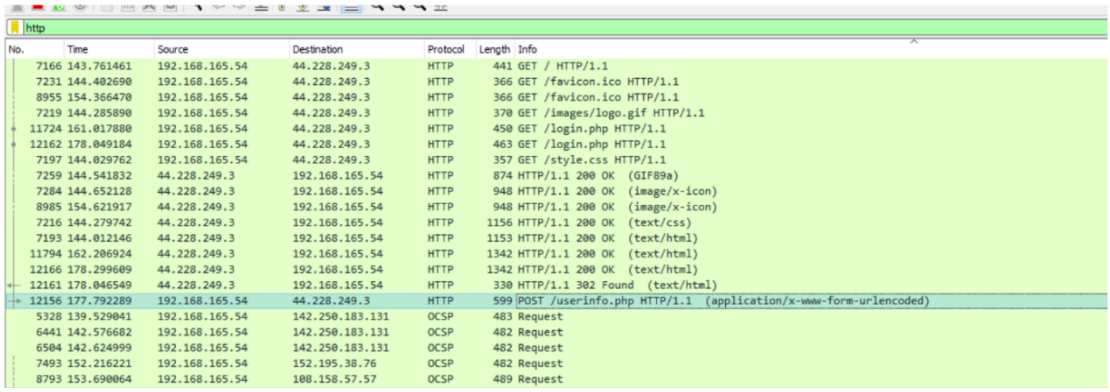
Name: Prathmesh baviskar
Roll no: 5020106
Name: Joshua Dabhi
Roll no: 5020167

III. Access a vulnerable login website, such as http://testphp.vulnweb.com/login.php.

IV. Inspect Wireshark for HTTP protocols.

V. The entered credentials will be clearly visible in Wireshark's captured data.

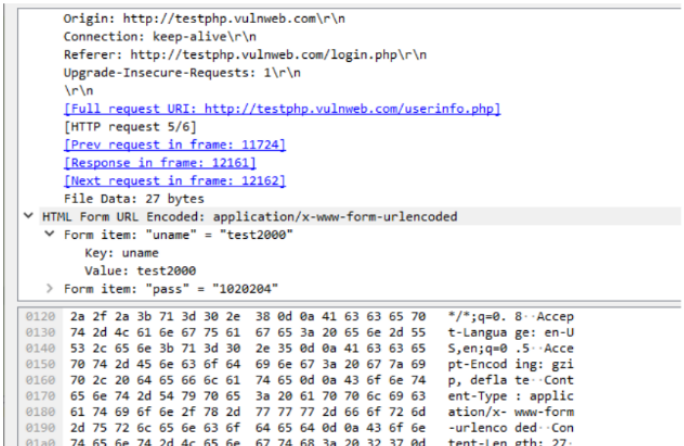
Outputs:



http

No.	Time	Source	Destination	Protocol	Length	Info
7166	143.761461	192.168.165.54	44.228.249.3	HTTP	441	GET / HTTP/1.1
7231	144.402690	192.168.165.54	44.228.249.3	HTTP	366	GET /favicon.ico HTTP/1.1
8955	154.366470	192.168.165.54	44.228.249.3	HTTP	366	GET /favicon.ico HTTP/1.1
7219	144.285890	192.168.165.54	44.228.249.3	HTTP	370	GET /images/logo.gif HTTP/1.1
11724	161.017880	192.168.165.54	44.228.249.3	HTTP	450	GET /login.php HTTP/1.1
12162	178.049184	192.168.165.54	44.228.249.3	HTTP	463	GET /login.php HTTP/1.1
7197	144.029762	192.168.165.54	44.228.249.3	HTTP	357	GET /style.css HTTP/1.1
7259	144.541832	44.228.249.3	192.168.165.54	HTTP	874	HTTP/1.1 200 OK (GIF89a)
7284	144.652128	44.228.249.3	192.168.165.54	HTTP	948	HTTP/1.1 200 OK (image/x-icon)
8985	154.621917	44.228.249.3	192.168.165.54	HTTP	948	HTTP/1.1 200 OK (image/x-icon)
7216	144.279742	44.228.249.3	192.168.165.54	HTTP	1156	HTTP/1.1 200 OK (text/css)
7193	144.012146	44.228.249.3	192.168.165.54	HTTP	1153	HTTP/1.1 200 OK (text/html)
11794	162.206924	44.228.249.3	192.168.165.54	HTTP	1342	HTTP/1.1 200 OK (text/html)
12166	178.299609	44.228.249.3	192.168.165.54	HTTP	1342	HTTP/1.1 200 OK (text/html)
12161	178.046549	44.228.249.3	192.168.165.54	HTTP	330	HTTP/1.1 302 Found (text/html)
12156	177.792289	192.168.165.54	44.228.249.3	HTTP	599	POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
5328	139.529041	192.168.165.54	142.250.183.131	OCSP	483	Request
6441	142.576682	192.168.165.54	142.250.183.131	OCSP	482	Request
6504	142.624999	192.168.165.54	142.250.183.131	OCSP	482	Request
7493	152.216221	192.168.165.54	152.195.38.76	OCSP	482	Request
8793	153.690064	192.168.165.54	108.158.57.57	OCSP	489	Request

Found Data:

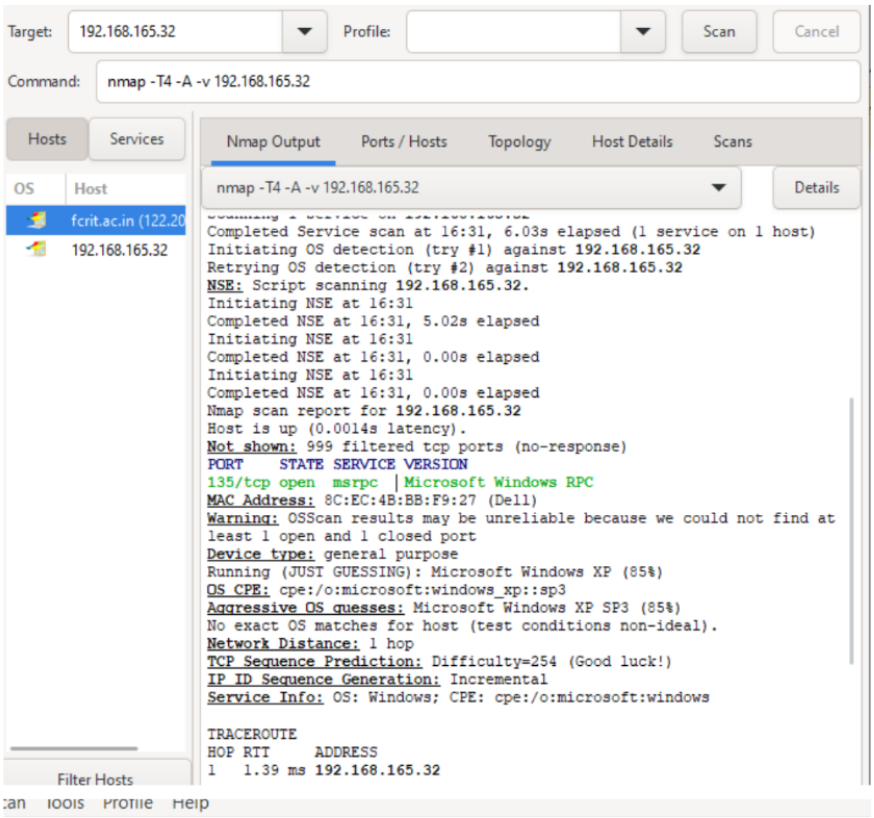


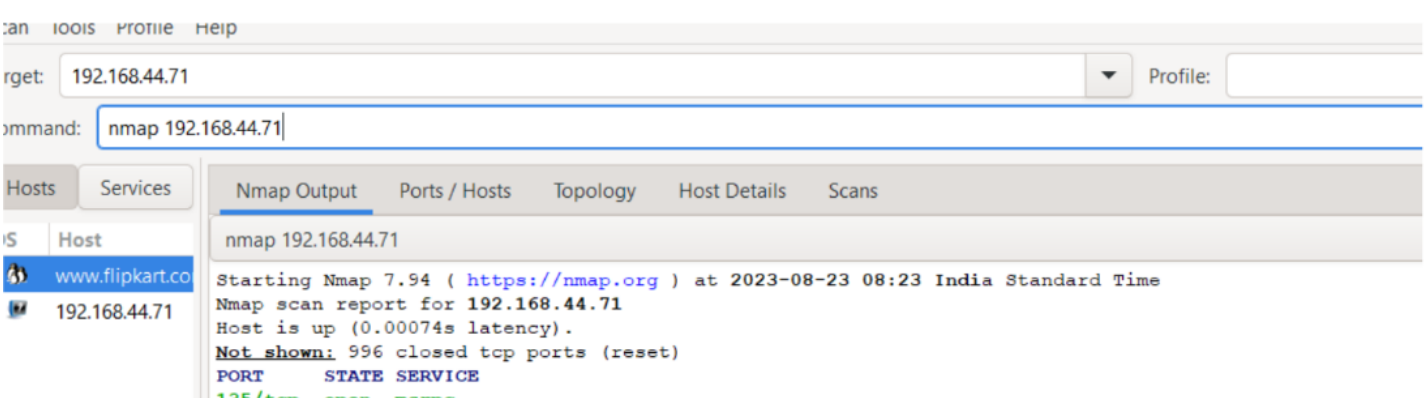
```
Origin: http://testphp.vulnweb.com\r\n
Connection: keep-alive\r\n
Referer: http://testphp.vulnweb.com/login.php\r\n
Upgrade-Insecure-Requests: 1\r\n
\r\n
[Full request URI: http://testphp.vulnweb.com/userinfo.php]
[HTTP request 5/6]
[Prev request in frame: 11724]
[Response in frame: 12161]
[Next request in frame: 12162]
File Data: 27 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded
  Form item: "uname" = "test2000"
    Key: uname
    Value: test2000
  Form item: "pass" = "1020204"

0120  2a 2f 2a 3b 71 3d 30 2e  38 0d 0a 41 63 63 65 70   */*;q=0. 8··Accep
0130  74 2d 4c 61 6e 67 75 61  67 65 3a 20 65 6e 2d 55   t-Langua ge: en-U
0140  53 2c 65 6e 3b 71 3d 30  2e 35 0d 0a 41 63 63 65   S,en;q=0 .5··Acce
0150  70 74 2d 45 6e 63 6f 64  69 6e 67 3a 20 67 7a 69   pt-Encod ing: gzi
0160  70 2c 20 64 65 66 6c 61  74 65 0d 0a 43 6f 6e 74   p, defla te··Cont
0170  65 6e 74 2d 54 79 70 65  3a 20 61 70 70 6c 69 63   ent-Type : applic
0180  61 74 69 6f 6e 2f 78 2d  77 77 77 2d 66 6f 72 6d   ation/x- www-form
0190  2d 75 72 6c 65 6e 63 6f  64 65 64 0d 0a 43 6f 6e   -urlenco ded··Con
01a0  74 65 6e 74 2d 4c 65 6e  67 74 68 3a 20 32 37 0d   tent-Len gth: 27·
```

Name: Prathmesh baviskar
Roll no: 5020106
Name: Joshua Dabhi
Roll no: 5020167

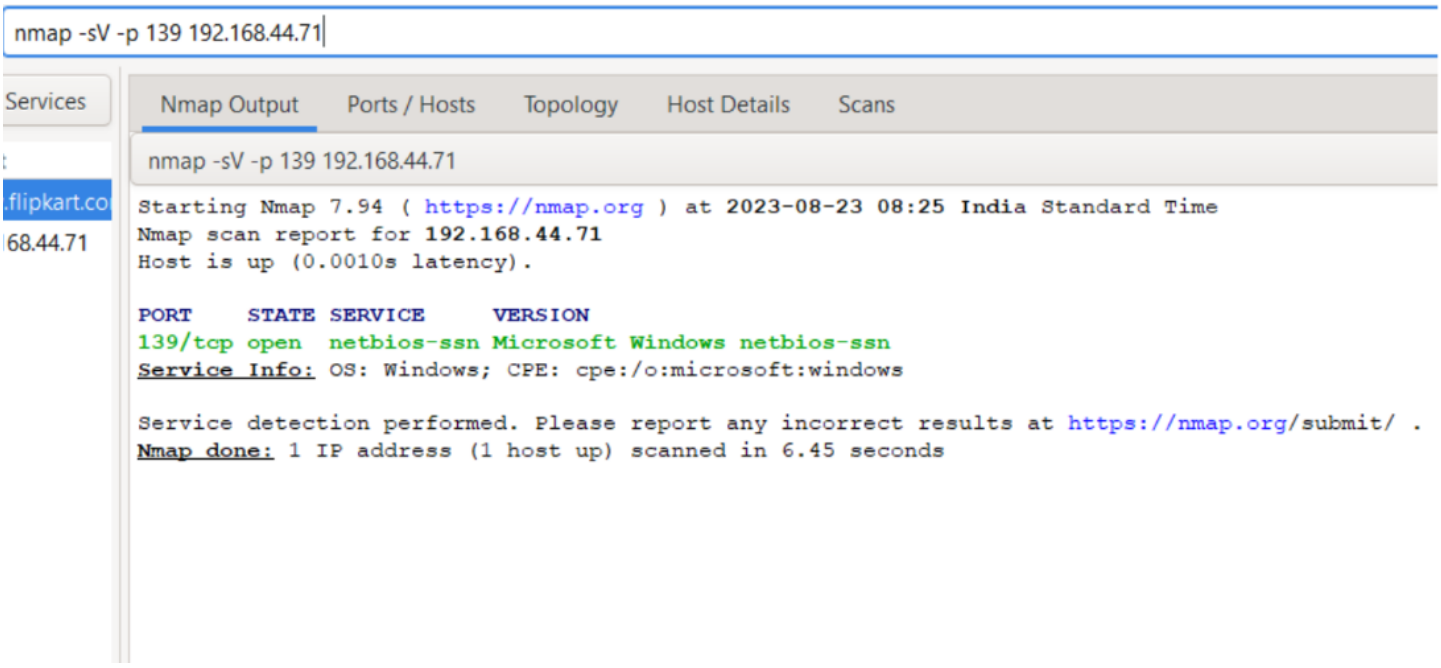
Nmap steps:

1. Install Nmap/zenmap
2. Scan for open ports
3. Os scanning
4. Traceroute command scan

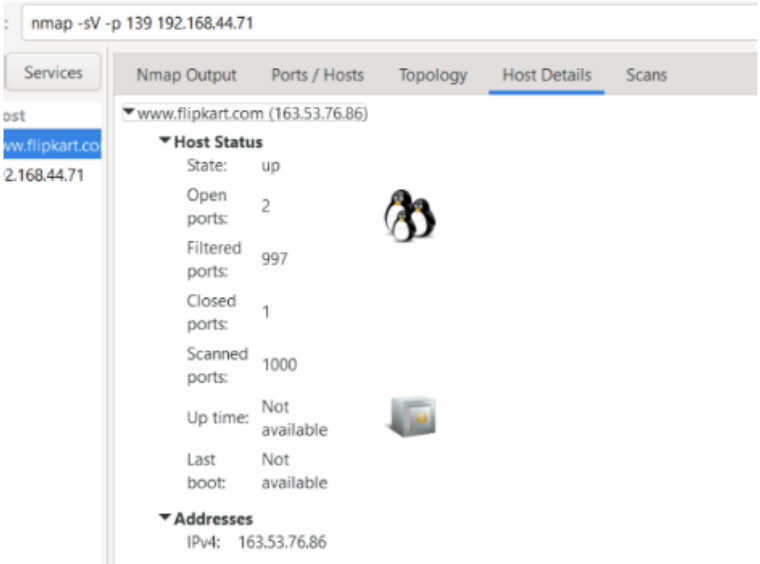




Name: Prathmesh baviskar
Roll no: 5020106
Name: Joshua Dabhi
Roll no: 5020167

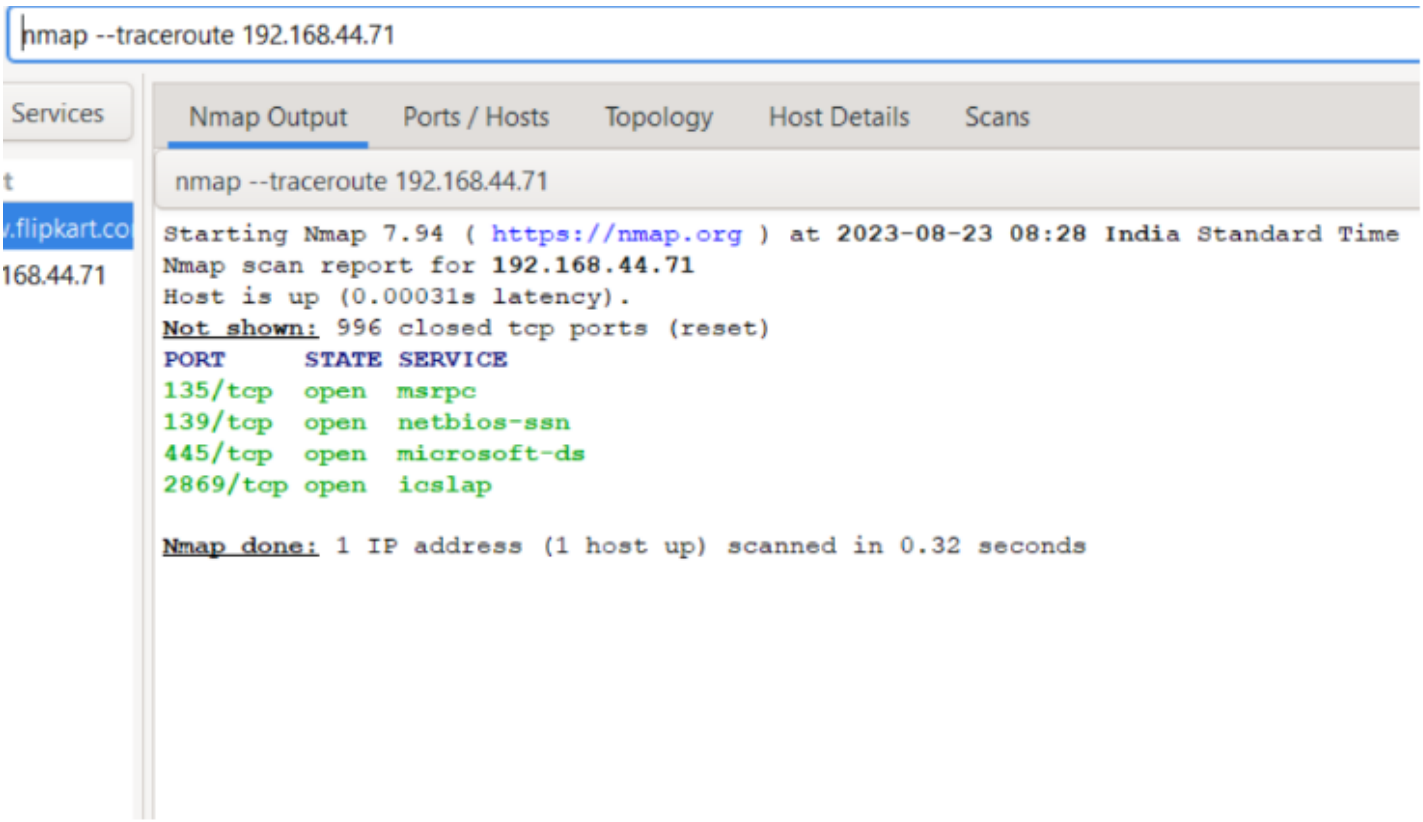


OS Scan:



Name: Prathmesh baviskar
Roll no: 5020106
Name: Joshua Dabhi
Roll no: 5020167

Traceroute:



Conclusion: Thus, we have successfully performed packet sniffing using Wireshark and port scanning.