VULNERABILITIES FOR MAIN WEBSITE

TEAM NO.:7.4

TEAMMATES: N. HARIKA
P. MONISH
D. SRAVANI
M. LIKHITHA

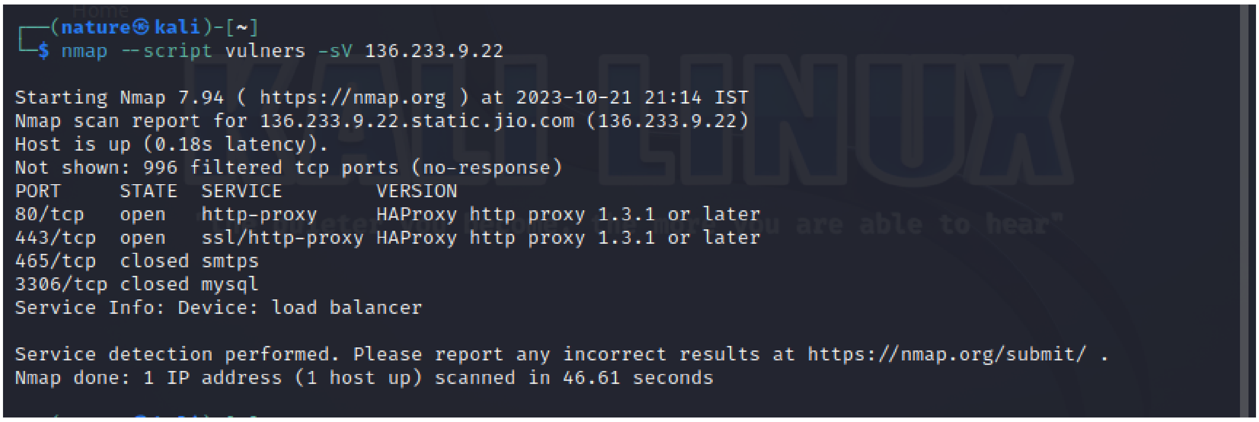
TOTAL VULNERABILITIES SCANNED: 5

Main website:

https://vtop.vit.ac.in/vtop/open/page

Open ports that we have find using nmap

Step-1:

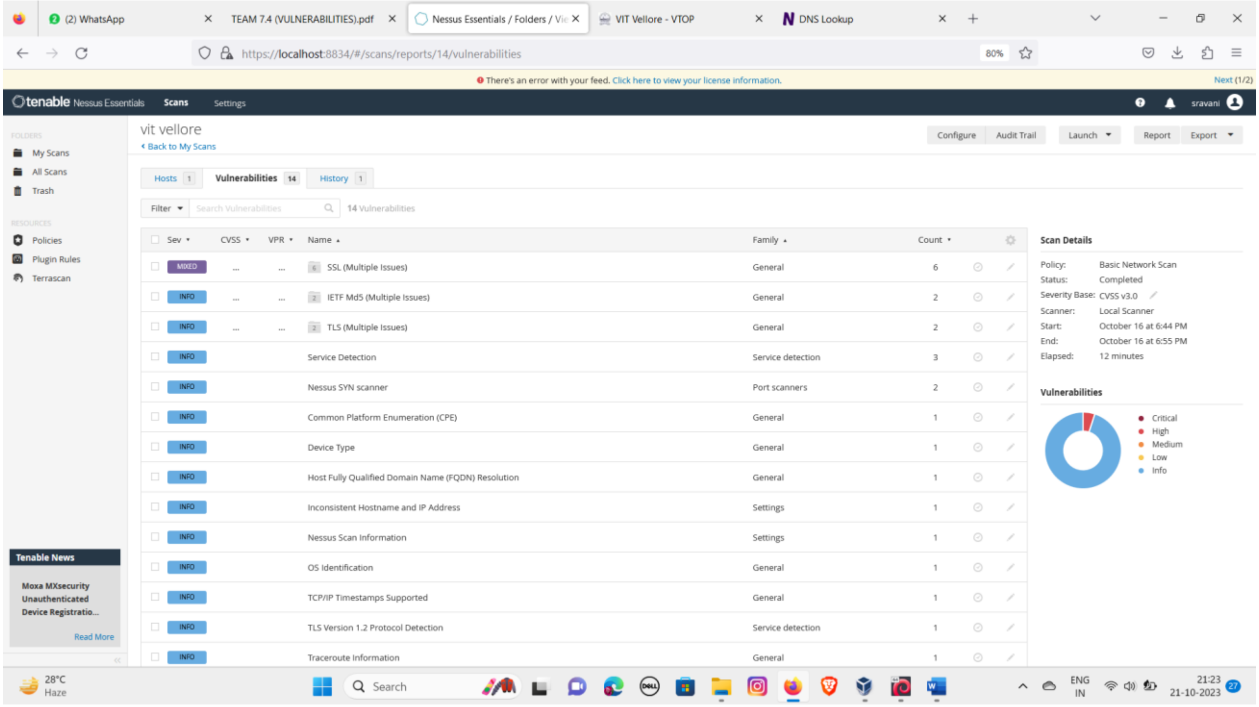


```
┌──(nature㉿kali)-[~]
└─$ nmap --script vulners -sV 136.233.9.22

Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-21 21:14 IST
Nmap scan report for 136.233.9.22.static.jio.com (136.233.9.22)
Host is up (0.18s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE  SERVICE        VERSION
80/tcp   open   http-proxy     HAProxy http proxy 1.3.1 or later
443/tcp  open   ssl/http-proxy HAProxy http proxy 1.3.1 or later
465/tcp  closed smtps
3306/tcp closed mysql
Service Info: Device: load balancer

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 46.61 seconds
```

we can see that port no. 80 and 443 are open so, they can be vulnerable.

Now by using Nessus tool we can find the vulnerabilities

As mentioned above we have find 14 vulnerabilities using Nessus



vit vellore

Back to My Scans

14 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count
MIXED	...	...	6 SSL (Multiple Issues)	General	6
INFO	...	...	2 IETF Md5 (Multiple Issues)	General	2
INFO	...	...	2 TLS (Multiple Issues)	General	2
INFO			Service Detection	Service detection	3
INFO			Nessus SYN scanner	Port scanners	2
INFO			Common Platform Enumeration (CPE)	General	1
INFO			Device Type	General	1
INFO			Host Fully Qualified Domain Name (FQDN) Resolution	General	1
INFO			Inconsistent Hostname and IP Address	Settings	1
INFO			Nessus Scan Information	Settings	1
INFO			OS Identification	General	1
INFO			TCP/IP Timestamps Supported	General	1
INFO			TLS Version 1.2 Protocol Detection	Service detection	1
INFO			Traceroute Information	General	1

Scan Details

Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	October 16 at 6:44 PM
End:	October 16 at 6:55 PM
Elapsed:	12 minutes

Vulnerabilities

1. Common Platform Enumeration:

Description

By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.

FIXING THE VULNERABILITY:

CPE is a structured naming scheme for information technology systems, software, and packages. Based upon the generic syntax for Uniform Resource

Identifiers (URI), CPE includes a formal name format, a method for checking names against a system, and a description format for binding text and tests to a name.

2. TCP/IP Timestamps Supported Description:

The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

FIXING THE VULNERABILITY:

TCP timestamps are enabled by default. If you disable TCP timestamps, the timestamps are not displayed in the traffic capture file. You can run the show tcp_timestamps command to determine whether the TCP timestamps are enabled or disabled before running set tcp_timestamps

3.TLS Version 1.2 Protocol Detection

Description:

The remote service accepts connections encrypted using TLS 1.2

HOW TO FIX IT:

Step to enable TLS 1.2 in Google Chrome

1. Open Google Chrome.
2. Press Alt + F and select Settings.
3. Select the Advanced tab.

4. Select the System category.
5. Select Open your computer's proxy settings.
6. Select Advanced tab.
7. Scroll down to Security category and tick the box for Use TLS 1.2.
8. Click OK.

4. SSL Medium Strength Cipher Suites Supported (SWEET32):

Description:

The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

Solution:

Reconfigure the affected application if possible to avoid use of medium strength ciphers.