

Assignment Day 4 | 23rd August 2020

Submitted By: Piyush Choudhary [choudharypiyush08@gmail.com]

Ques 1: Find out the mail servers of the following domain:

- **lbn.com**
- **Wipro.com**

Sol 1:

Opened CMD in the host machine.

Used the command **nslookup** to open nslookup tool.

Set the type to mail exchange server to search only for mail servers using **set type=mx**

Next, the domain name to be searched for is given.

Mail servers of the given domains are as follows:

```
C:\WINDOWS\system32\cmd.exe - nslookup
C:\Users\Rony>nslookup
Default Server:  csp1.zte.com.cn
Address:  fe80::1

> set type=mx
> lbn.com
Server:  csp1.zte.com.cn
Address:  fe80::1

Non-authoritative answer:
lbn.com MX preference = 5, mail exchanger = mx0b-001b2d01.pphosted.com
lbn.com MX preference = 5, mail exchanger = mx0a-001b2d01.pphosted.com

lbn.com nameserver = ns1-99.akam.net
lbn.com nameserver = ns1-206.akam.net
lbn.com nameserver = usc2.akam.net
lbn.com nameserver = asia3.akam.net
lbn.com nameserver = eur2.akam.net
lbn.com nameserver = eur5.akam.net
lbn.com nameserver = usc3.akam.net
lbn.com nameserver = usw2.akam.net
usc3.akam.net internet address = 96.7.50.64
ns1-206.akam.net internet address = 193.108.91.206
ns1-206.akam.net AAAA IPv6 address = 2600:1401:2::ce
asia3.akam.net internet address = 23.211.61.64
eur2.akam.net internet address = 95.100.173.64
usc2.akam.net internet address = 184.26.160.64
ns1-99.akam.net internet address = 193.108.91.99
ns1-99.akam.net AAAA IPv6 address = 2600:1401:2::63
eur5.akam.net internet address = 23.74.25.64
```

Fig 1.1 Search Results for lbn.com

```

C:\WINDOWS\system32\cmd.exe - nslookup
IBM.COM nameserver = usc2.akam.net
IBM.COM nameserver = asia3.akam.net
IBM.COM nameserver = eur2.akam.net
IBM.COM nameserver = eur5.akam.net
IBM.COM nameserver = usc3.akam.net
IBM.COM nameserver = usw2.akam.net
usc3.akam.net internet address = 96.7.50.64
ns1-206.akam.net internet address = 193.108.91.206
ns1-206.akam.net AAAA IPv6 address = 2600:1401:2::ce
asia3.akam.net internet address = 23.211.61.64
eur2.akam.net internet address = 95.100.173.64
usc2.akam.net internet address = 184.26.160.64
ns1-99.akam.net internet address = 193.108.91.99
ns1-99.akam.net AAAA IPv6 address = 2600:1401:2::63
eur5.akam.net internet address = 23.74.25.64
usw2.akam.net internet address = 184.26.161.64
> wipro.com
Server: csp1.zte.com.cn
Address: fe80::1

Non-authoritative answer:
wipro.com MX preference = 0, mail exchanger = wipro-com.mail.protection.outlook.com

wipro.com nameserver = ns1.webindia.com
wipro.com nameserver = ns2.webindia.com
wipro.com nameserver = ns4.webindia.com
ns1.webindia.com internet address = 50.16.170.116
ns2.webindia.com internet address = 34.235.29.171
ns4.webindia.com internet address = 54.66.0.69

```

Fig 1.2 Search Results for ibm.com

Ques 2: Find the locations, where these email servers are hosted.

Sol 2: Locations for the servers mail@ibm.com and mail@wipro.com are as follows:

mail@ibm.com	
Mailbox Domain	mx0b-001b2d01.pphosted.com
IP	148.163.158.5
Country	United States
City	Sunnyvale
Latitude	37.424900054932
Longitude	-122.0074005127
ISP	N/A

Fig 2.1 Location for the mail@ibm.com

mail@wipro.com	
Mailbox Domain	wipro-com.mail.protection.outlook.com
IP	104.47.126.36
Country	Korea, Republic of
City	Busan
Latitude	35.102798461914
Longitude	129.04029846191
ISP	N/A

Fig 2.2 Location for the mail@wipro.com

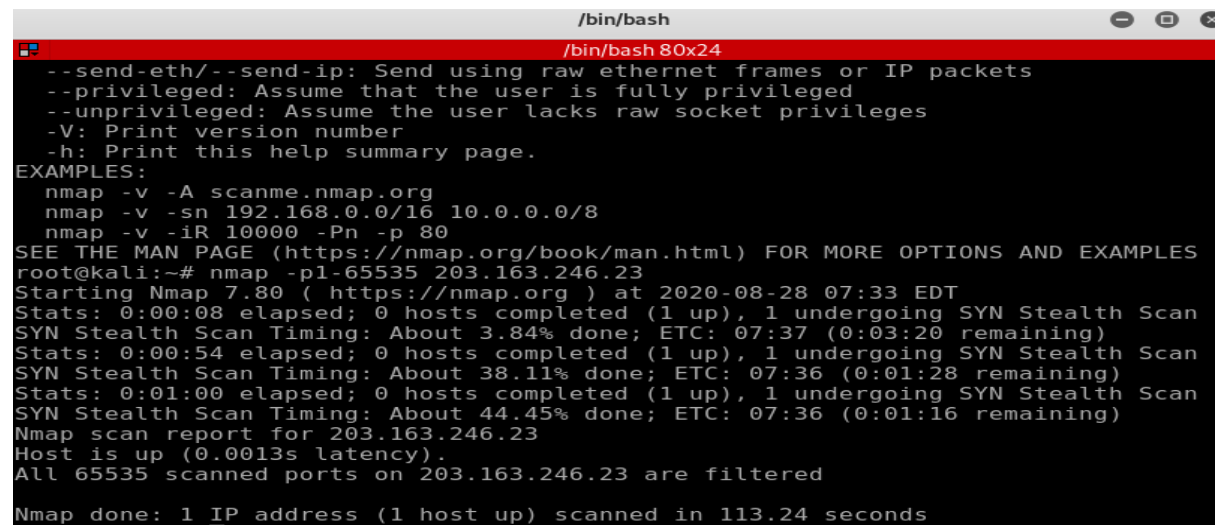
Ques 3: Scan and find out port numbers open for 203.163.246.23

Sol 3:

Opened Terminal in Kali VM.

Used the command `nmap -p1-65535 203.163.246.23` to start the scan for the given IP.

All the 65535 ports for the given IP are filtered thus NMAP is unable to detail it as Open or Closed. Scan report for the given IP is as follows:



```
/bin/bash
--send-eth/--send-ip: Send using raw ethernet frames or IP packets
--privileged: Assume that the user is fully privileged
--unprivileged: Assume the user lacks raw socket privileges
-V: Print version number
-h: Print this help summary page.
EXAMPLES:
nmap -v -A scanme.nmap.org
nmap -v -sn 192.168.0.0/16 10.0.0.0/8
nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
root@kali:~# nmap -p1-65535 203.163.246.23
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-28 07:33 EDT
Stats: 0:00:08 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 3.84% done; ETC: 07:37 (0:03:20 remaining)
Stats: 0:00:54 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 38.11% done; ETC: 07:36 (0:01:28 remaining)
Stats: 0:01:00 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 44.45% done; ETC: 07:36 (0:01:16 remaining)
Nmap scan report for 203.163.246.23
Host is up (0.0013s latency).
All 65535 scanned ports on 203.163.246.23 are filtered
Nmap done: 1 IP address (1 host up) scanned in 113.24 seconds
```

Fig 3.1 Scan Results for 203.163.246.23

Ques 4: Install Nessus in a VM and scan your laptop/desktop for CVE.

Sol 4:

Opened Windows10 VM.

Downloaded Nessus and Installed it.

Scanned the host machine for CVE using Nessus in VM as follows:

Setting up an advanced scan for the target **10.0.2.13** -

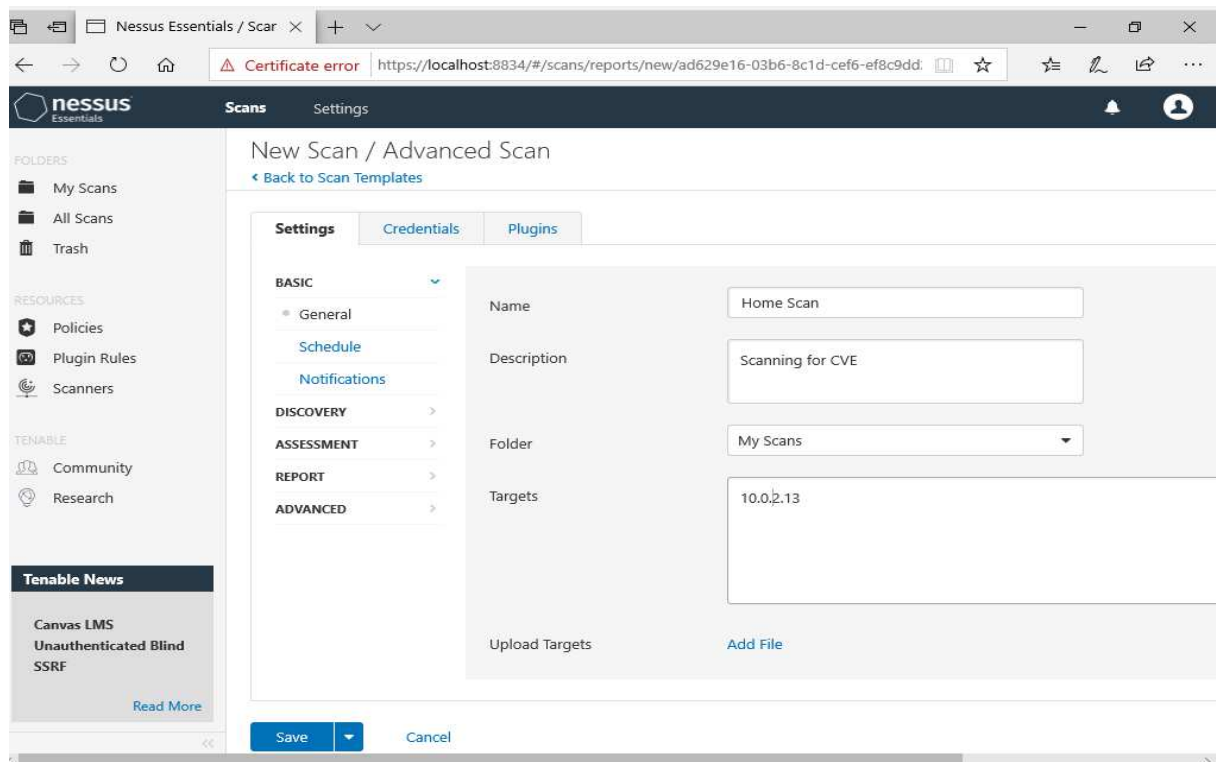


Fig 4.1 Setting up an advanced scan

Scan Generated -

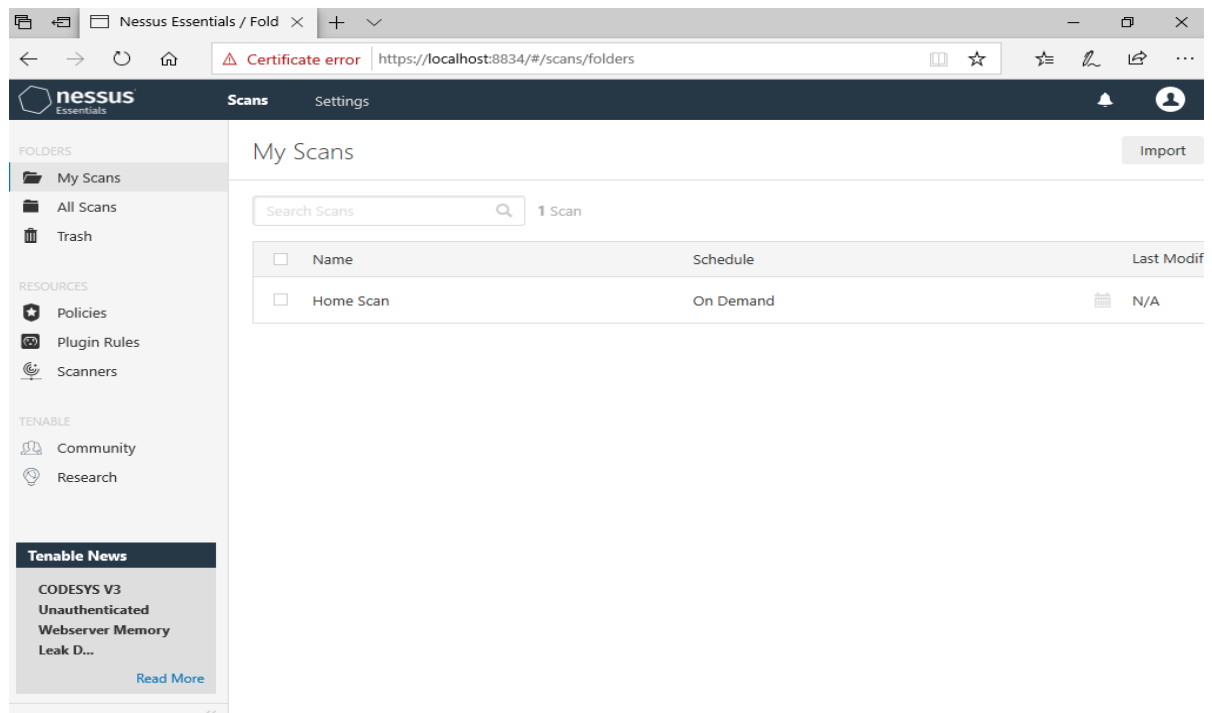


Fig 4.2 Scan Generated

Scan Initiated -

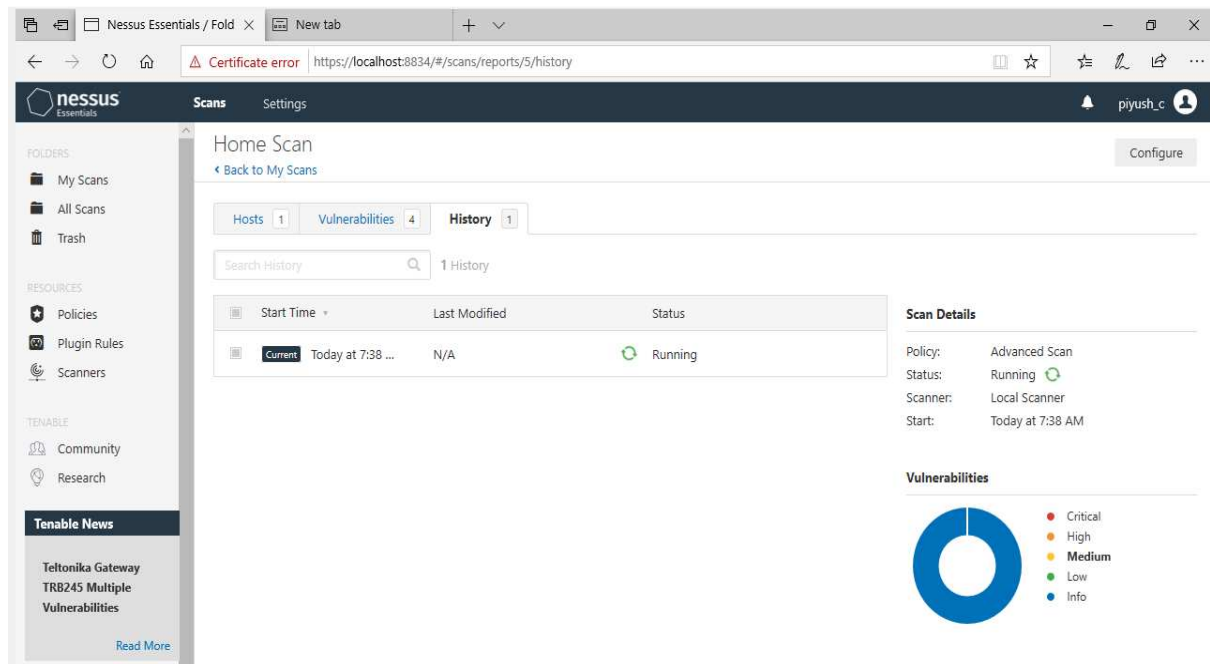


Fig 4.3 Scan Initiated

Scan Completed -

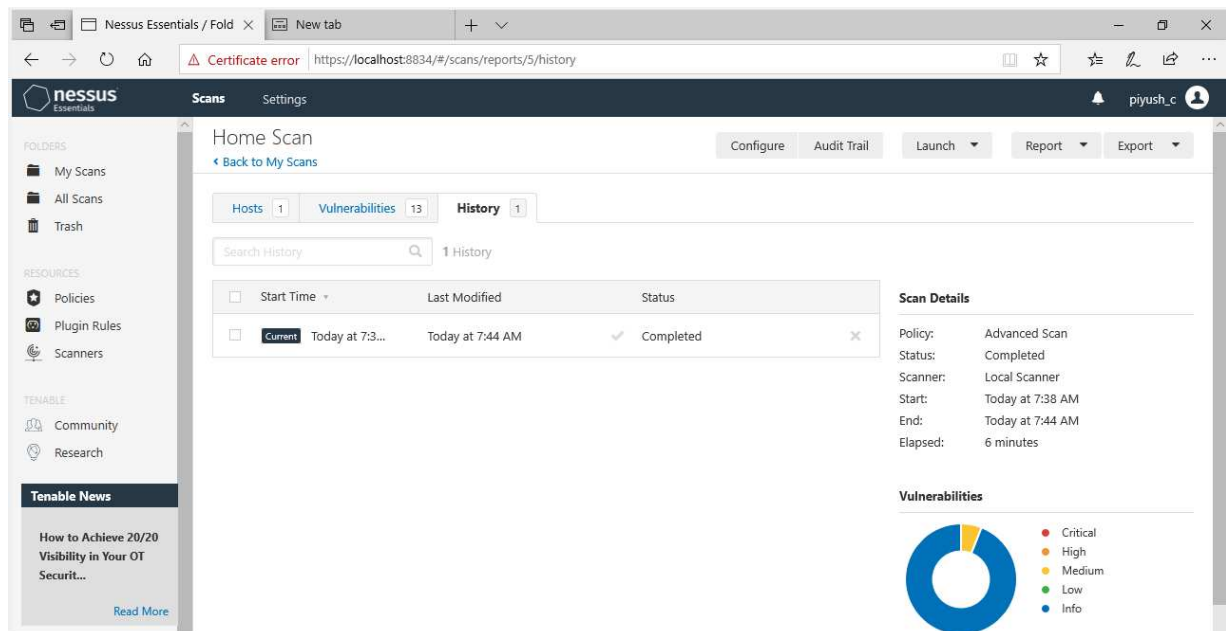


Fig 4.4 Scan Completed

Vulnerabilities Found – Total = 13

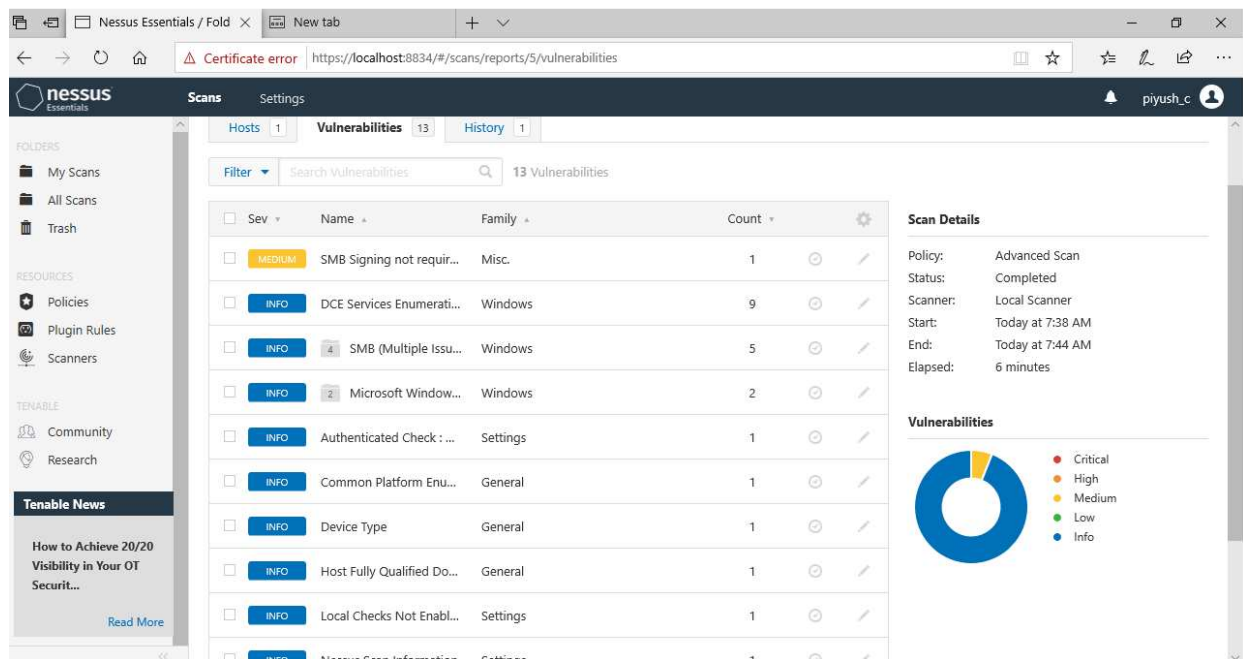


Fig 4.5 Vulnerabilities Found

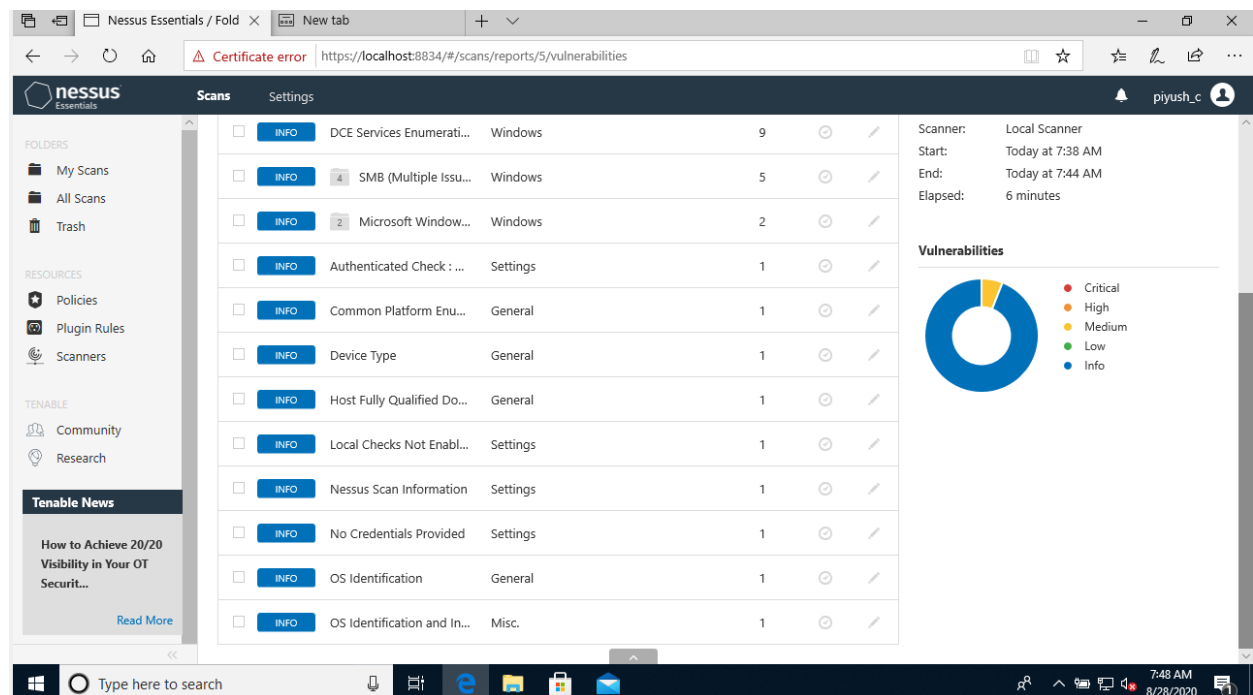


Fig 4.6 Vulnerabilities Found