Name : Akash Arjun Sawant

Email ID : sawantakash106@gmail.com

Day 4 Assignment (Cyber Security Essentials)

Solution :

Q1) Find out the mail servers of the following domain:

- **Ibm.com**
- **Wipro.com**

Open -> PenTester VMware workstation

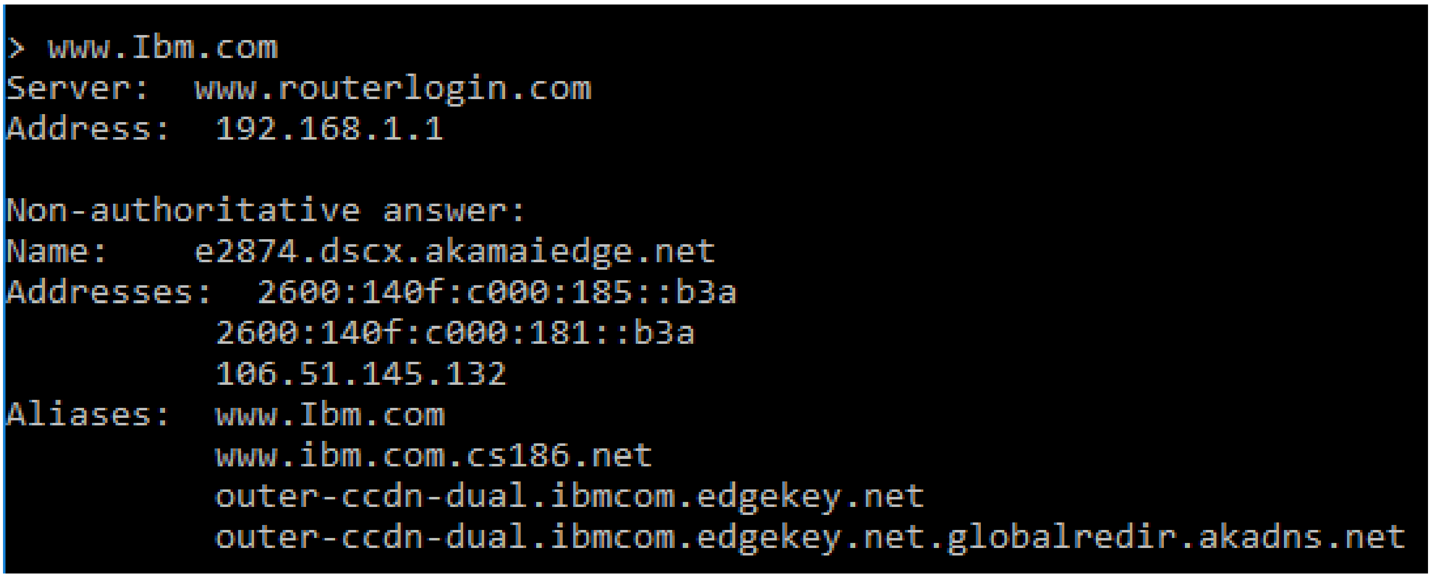
Open -> Command Prompt

Type

> ipconfig

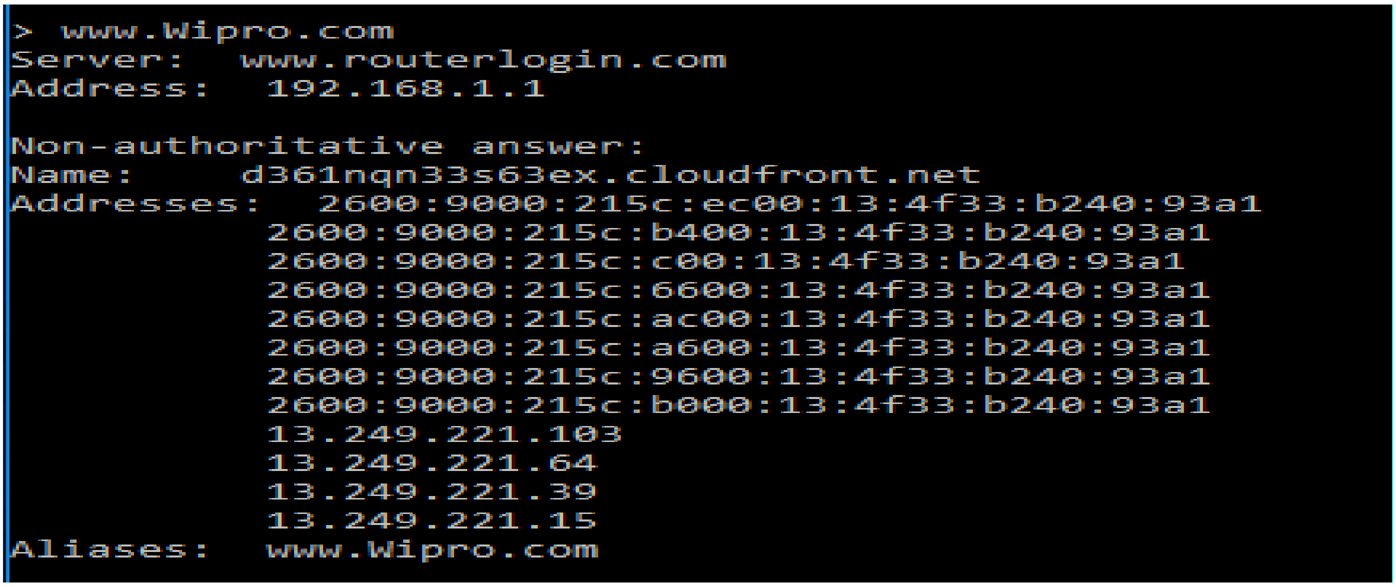
> nslookup

> www.Ibm.com



```
> www.Ibm.com
Server:  www.routerlogin.com
Address:  192.168.1.1

Non-authoritative answer:
Name:    e2874.dscx.akamaiedge.net
Addresses:  2600:140f:c000:185::b3a
          2600:140f:c000:181::b3a
          106.51.145.132
Aliases:  www.Ibm.com
          www.ibm.com.cs186.net
          outer-ccdn-dual.ibmcom.edgekey.net
          outer-ccdn-dual.ibmcom.edgekey.net.globalredir.akadns.net
```

> www.Wipro.com



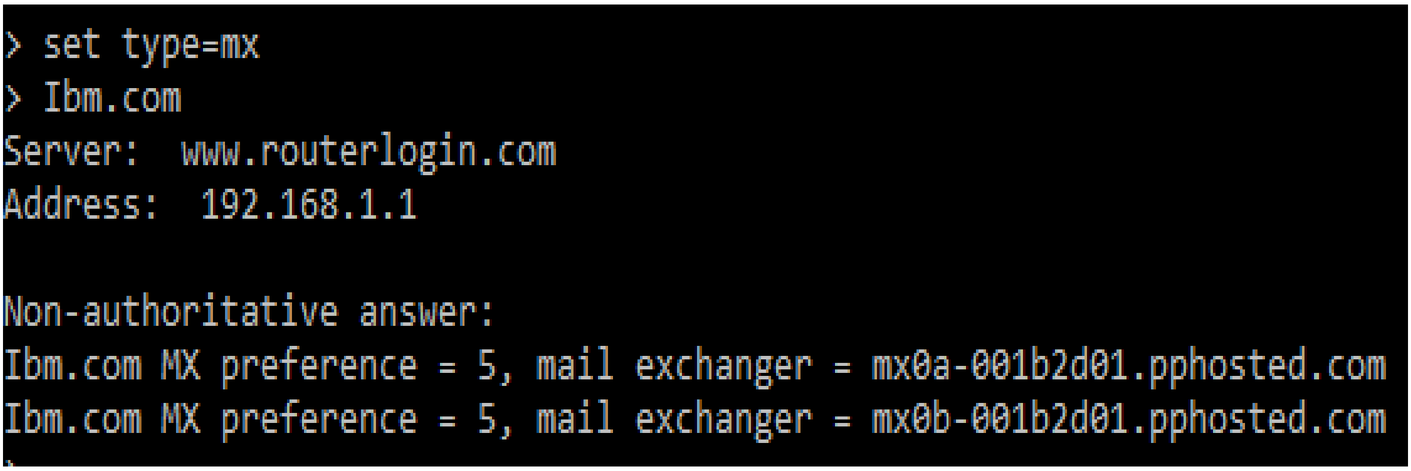
```
> www.Wipro.com
Server:  www.routerlogin.com
Address:  192.168.1.1

Non-authoritative answer:
Name:    d361nqn33s63ex.cloudfront.net
Addresses:  2600:9000:215c:ec00:13:4f33:b240:93a1
          2600:9000:215c:b400:13:4f33:b240:93a1
          2600:9000:215c:c00:13:4f33:b240:93a1
          2600:9000:215c:6600:13:4f33:b240:93a1
          2600:9000:215c:ac00:13:4f33:b240:93a1
          2600:9000:215c:a600:13:4f33:b240:93a1
          2600:9000:215c:9600:13:4f33:b240:93a1
          2600:9000:215c:b000:13:4f33:b240:93a1
          13.249.221.103
          13.249.221.64
          13.249.221.39
          13.249.221.15
Aliases:  www.Wipro.com
```

Q2) Find the locations, where these email servers are hosted.

Type

> set type=mx

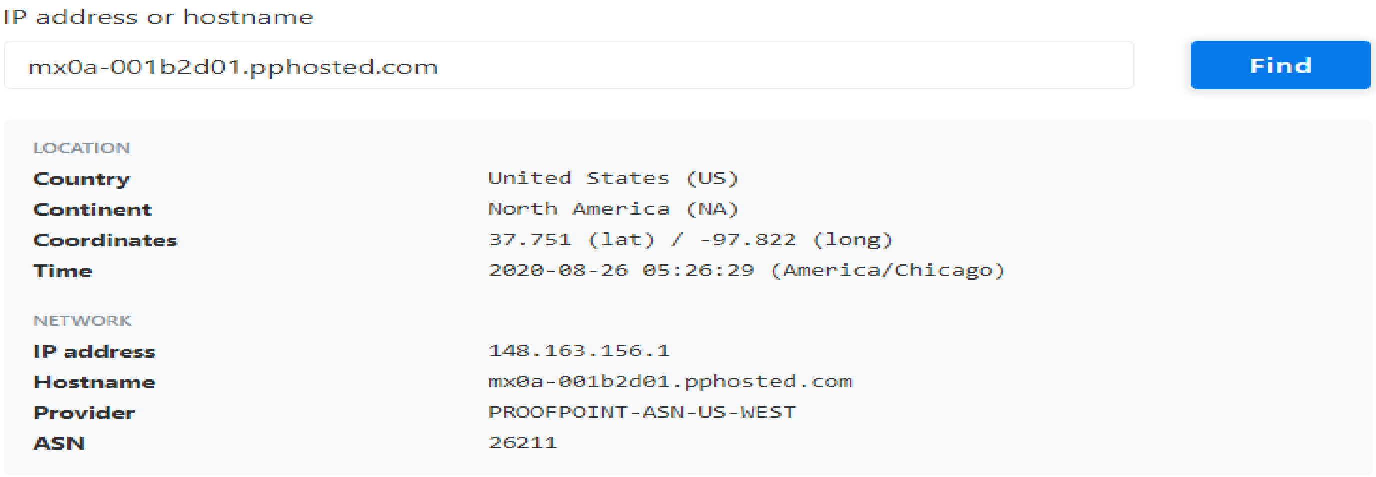
> Ibm.com



```
> set type=mx
> Ibm.com
Server:  www.routerlogin.com
Address:  192.168.1.1

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

Location

Address 1



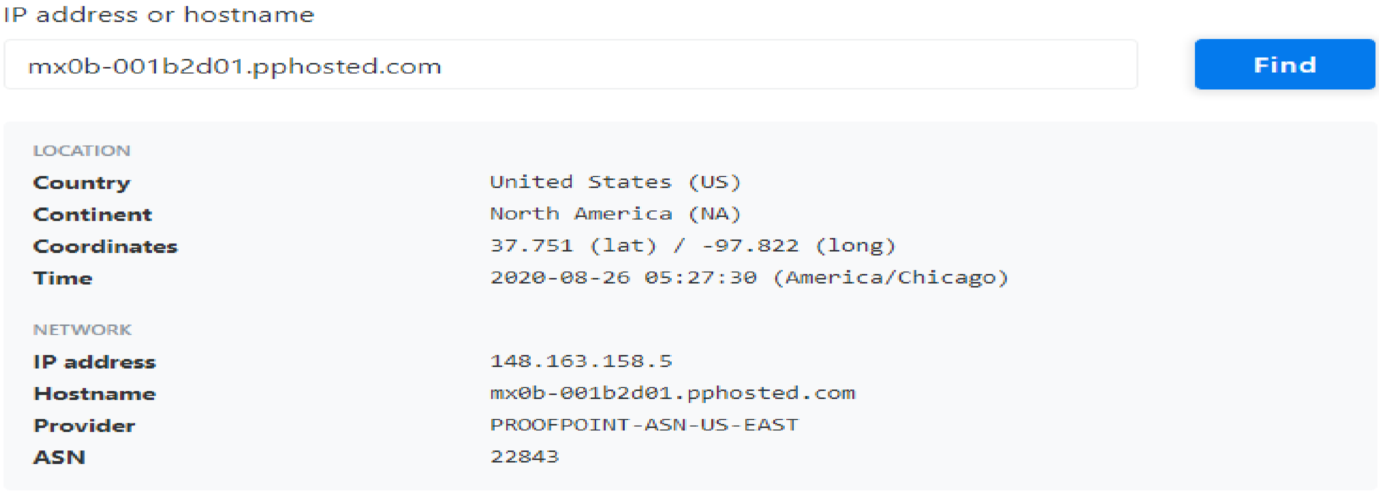
IP address or hostname

mx0a-001b2d01.pphosted.com

LOCATION	
Country	United States (US)
Continent	North America (NA)
Coordinates	37.751 (lat) / -97.822 (long)
Time	2020-08-26 05:26:29 (America/Chicago)

NETWORK	
IP address	148.163.156.1
Hostname	mx0a-001b2d01.pphosted.com
Provider	PROOFPOINT-ASN-US-WEST
ASN	26211

Address 2



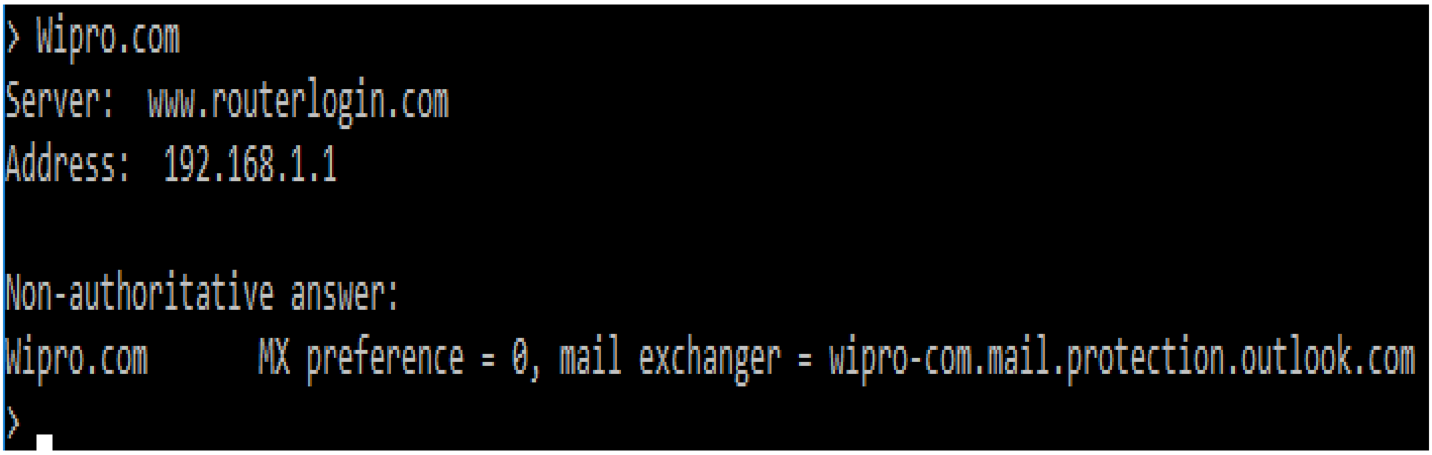
IP address or hostname

mx0b-001b2d01.pphosted.com

LOCATION	
Country	United States (US)
Continent	North America (NA)
Coordinates	37.751 (lat) / -97.822 (long)
Time	2020-08-26 05:27:30 (America/Chicago)

NETWORK	
IP address	148.163.158.5
Hostname	mx0b-001b2d01.pphosted.com
Provider	PROOFPOINT-ASN-US-EAST
ASN	22843

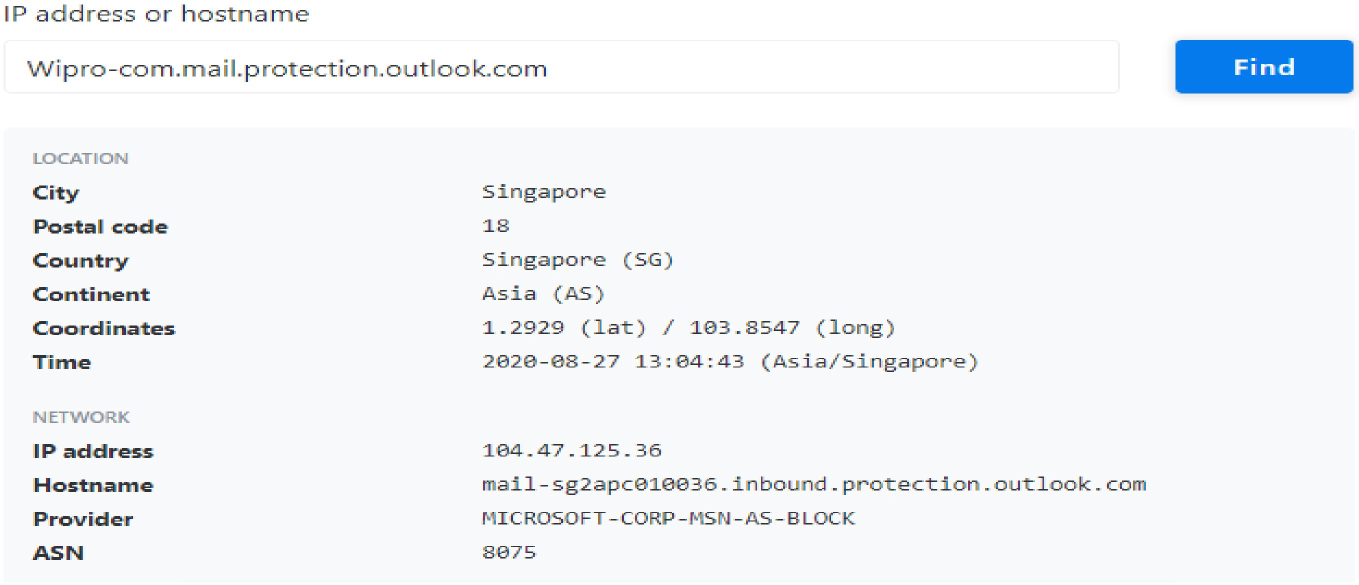
> Wipro.com



```
> Wipro.com
Server:  www.routerlogin.com
Address:  192.168.1.1

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

Location

Address



Wipro-com.mail.protection.outlook.com

LOCATION

City	Singapore
Postal code	18
Country	Singapore (SG)
Continent	Asia (AS)
Coordinates	1.2929 (lat) / 103.8547 (long)
Time	2020-08-27 13:04:43 (Asia/Singapore)

NETWORK

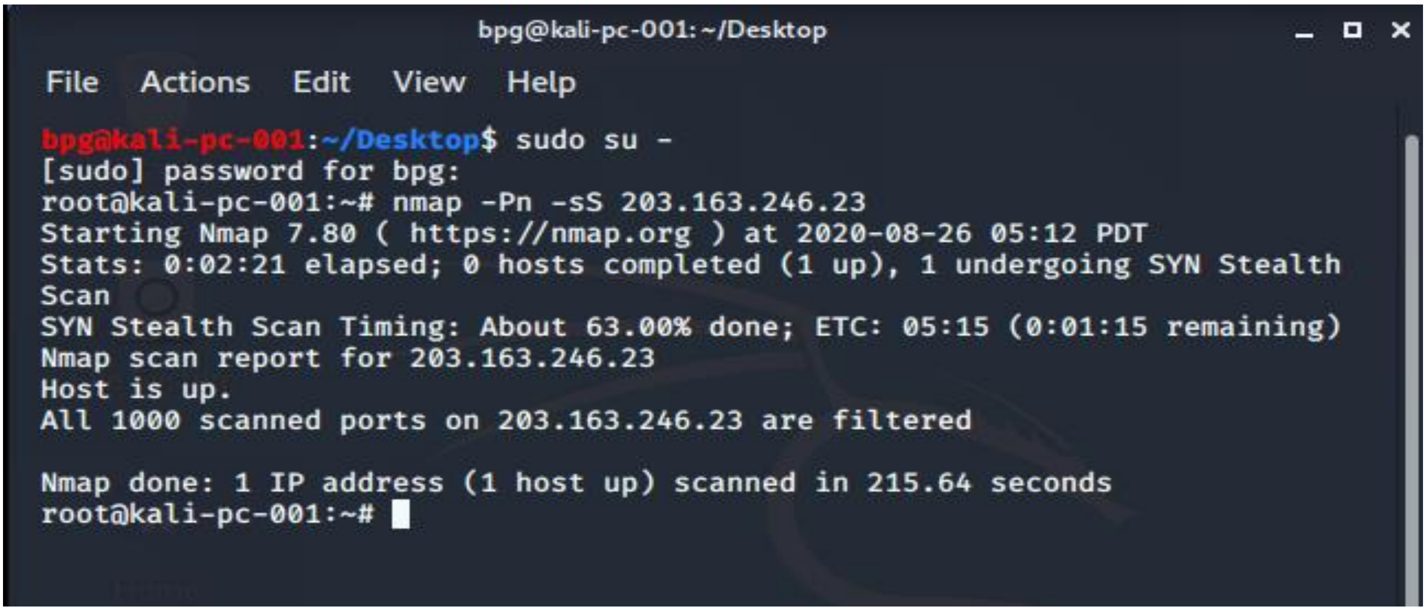
IP address	104.47.125.36
Hostname	mail-sg2apc010036.inbound.protection.outlook.com
Provider	MICROSOFT-CORP-MSN-AS-BLOCK
ASN	8075

Q3) Scan and find out port numbers open 203.163.246.23

Use -> Kali

Type

> sudo su –
> Enter password
> nmap –Pn –sS 203.163.246.23



```
bpg@kali-pc-001:~/Desktop$ sudo su -
[sudo] password for bpg:
root@kali-pc-001:~# nmap -Pn -sS 203.163.246.23
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-26 05:12 PDT
Stats: 0:02:21 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth
Scan
SYN Stealth Scan Timing: About 63.00% done; ETC: 05:15 (0:01:15 remaining)
Nmap scan report for 203.163.246.23
Host is up.
All 1000 scanned ports on 203.163.246.23 are filtered

Nmap done: 1 IP address (1 host up) scanned in 215.64 seconds
root@kali-pc-001:~# 
```

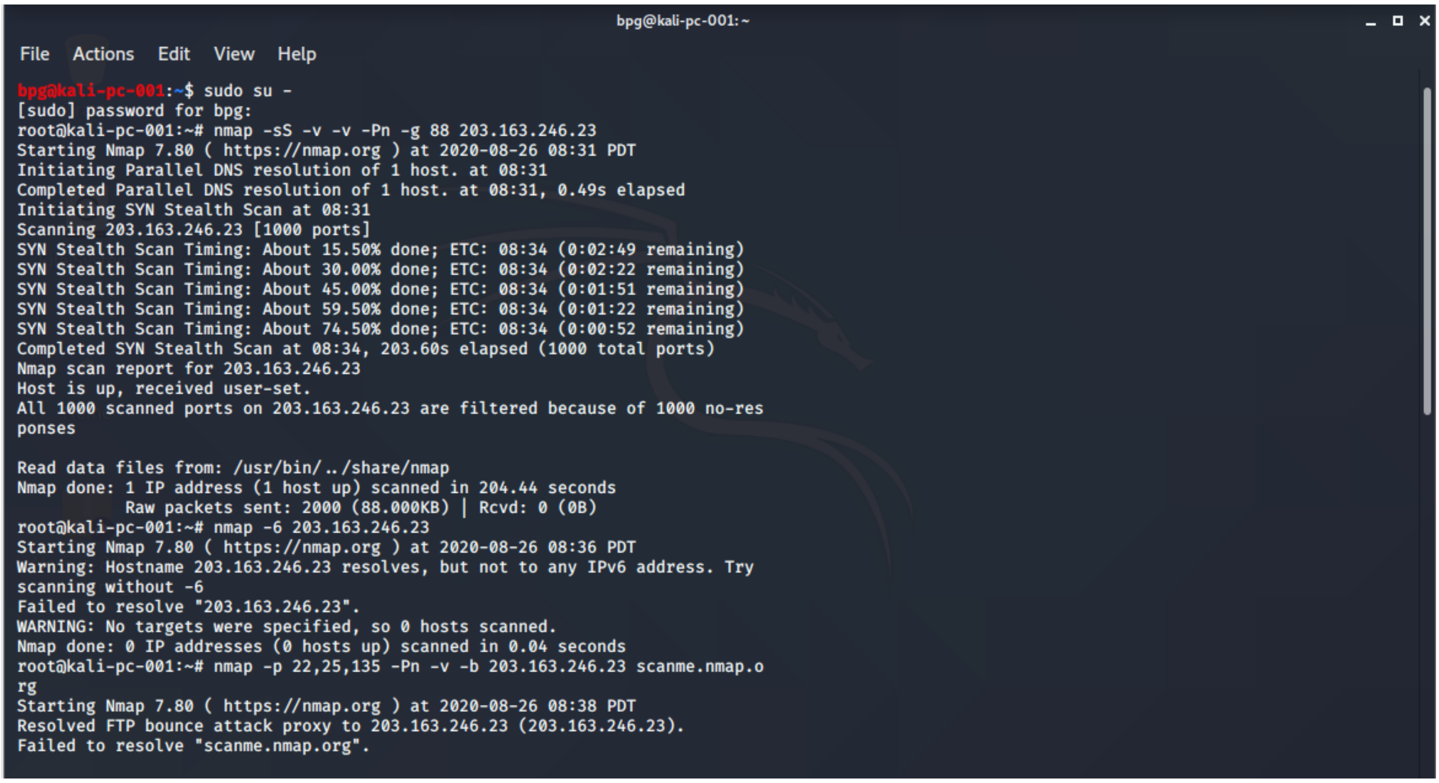
Some extra alternative commands

> -sS -v -v -Pn 203.163.246.23

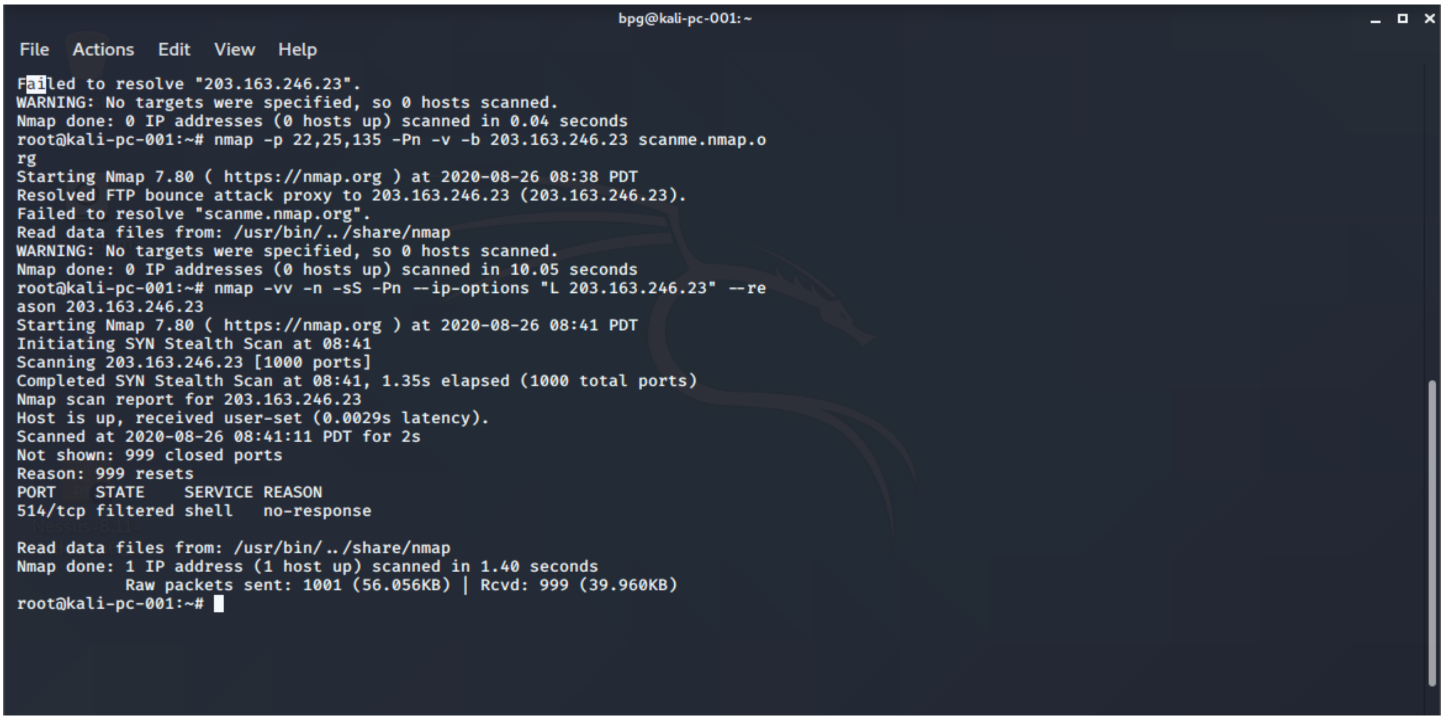
> nmap -6 203.163.246.23

> nmap -p 22,25,135 -Pn -v –b 203.163.246.23 scanme.nmap.org

> nmap -vv -n -sS -Pn --ip-options "L 203.163.246.23 " --reason 203.163.246.23

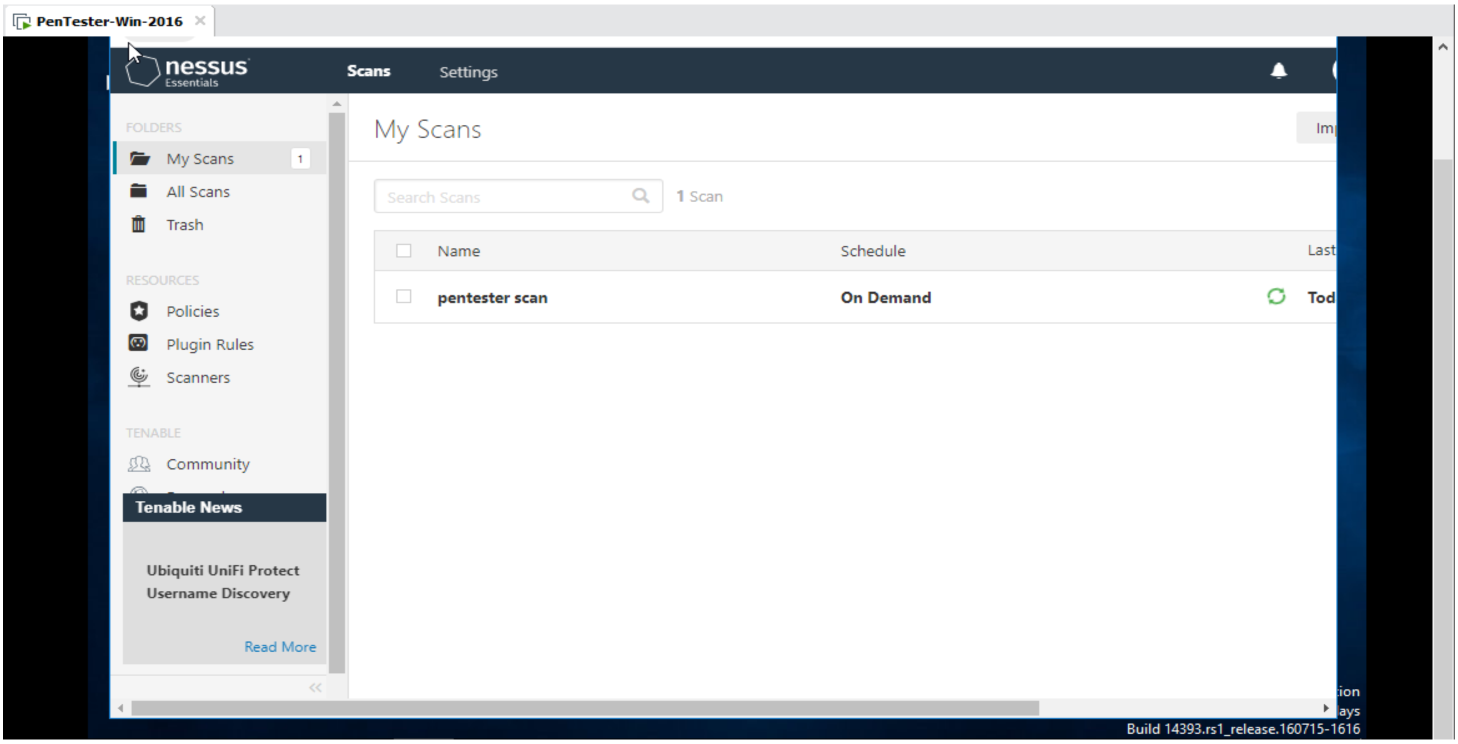


```
bpg@kali-pc-001:~$ sudo su -
[sudo] password for bpg:
root@kali-pc-001:~# nmap -sS -v -v -Pn -g 88 203.163.246.23
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-26 08:31 PDT
Initiating Parallel DNS resolution of 1 host. at 08:31
Completed Parallel DNS resolution of 1 host. at 08:31, 0.49s elapsed
Initiating SYN Stealth Scan at 08:31
Scanning 203.163.246.23 [1000 ports]
SYN Stealth Scan Timing: About 15.50% done; ETC: 08:34 (0:02:49 remaining)
SYN Stealth Scan Timing: About 30.00% done; ETC: 08:34 (0:02:22 remaining)
SYN Stealth Scan Timing: About 45.00% done; ETC: 08:34 (0:01:51 remaining)
SYN Stealth Scan Timing: About 59.50% done; ETC: 08:34 (0:01:22 remaining)
SYN Stealth Scan Timing: About 74.50% done; ETC: 08:34 (0:00:52 remaining)
Completed SYN Stealth Scan at 08:34, 203.60s elapsed (1000 total ports)
Nmap scan report for 203.163.246.23
Host is up, received user-set.
All 1000 scanned ports on 203.163.246.23 are filtered because of 1000 no-res
ponses

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 204.44 seconds
           Raw packets sent: 2000 (88.000KB) | Rcvd: 0 (0B)
root@kali-pc-001:~# nmap -6 203.163.246.23
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-26 08:36 PDT
Warning: Hostname 203.163.246.23 resolves, but not to any IPv6 address. Try
scanning without -6
Failed to resolve "203.163.246.23".
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.04 seconds
root@kali-pc-001:~# nmap -p 22,25,135 -Pn -v -b 203.163.246.23 scanme.nmap.o
rg
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-26 08:38 PDT
Resolved FTP bounce attack proxy to 203.163.246.23 (203.163.246.23).
Failed to resolve "scanme.nmap.org".
```



```
Failed to resolve "203.163.246.23".
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.04 seconds
root@kali-pc-001:~# nmap -p 22,25,135 -Pn -v -b 203.163.246.23 scanme.nmap.o
rg
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-26 08:38 PDT
Resolved FTP bounce attack proxy to 203.163.246.23 (203.163.246.23).
Failed to resolve "scanme.nmap.org".
Read data files from: /usr/bin/../share/nmap
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 10.05 seconds
root@kali-pc-001:~# nmap -vv -n -sS -Pn —ip-options "L 203.163.246.23" —re
ason 203.163.246.23
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-26 08:41 PDT
Initiating SYN Stealth Scan at 08:41
Scanning 203.163.246.23 [1000 ports]
Completed SYN Stealth Scan at 08:41, 1.35s elapsed (1000 total ports)
Nmap scan report for 203.163.246.23
Host is up, received user-set (0.0029s latency).
Scanned at 2020-08-26 08:41:11 PDT for 2s
Not shown: 999 closed ports
Reason: 999 resets
PORT    STATE    SERVICE REASON
514/tcp filtered shell   no-response

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.40 seconds
           Raw packets sent: 1001 (56.056KB) | Rcvd: 999 (39.960KB)
root@kali-pc-001:~# 
```

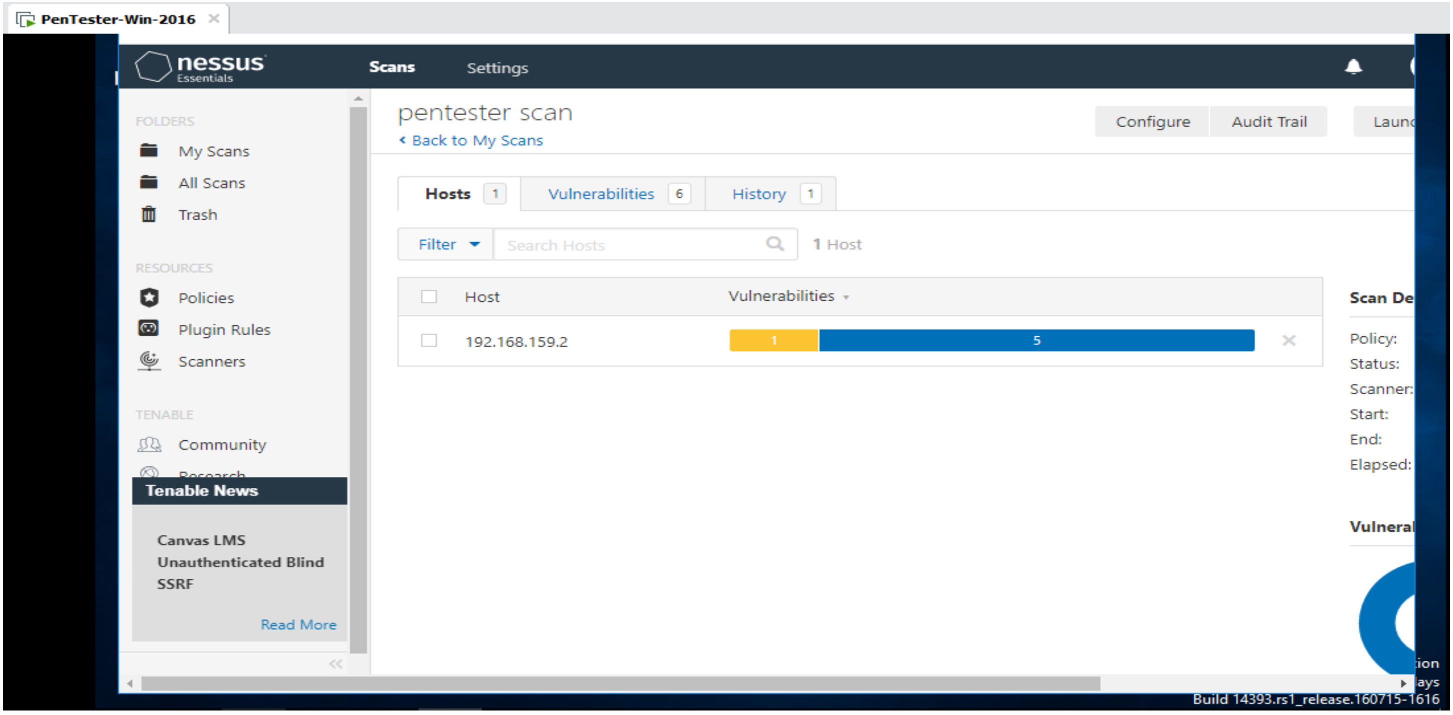
Q4) Install nessus in a VM and scan your laptop/desktop for CVE



My Scans

1 Scan

□	Name	Schedule	Last
□	pentester scan	On Demand	Tod



pentester scan

‹ Back to My Scans

Hosts 1 | Vulnerabilities 6 | History 1

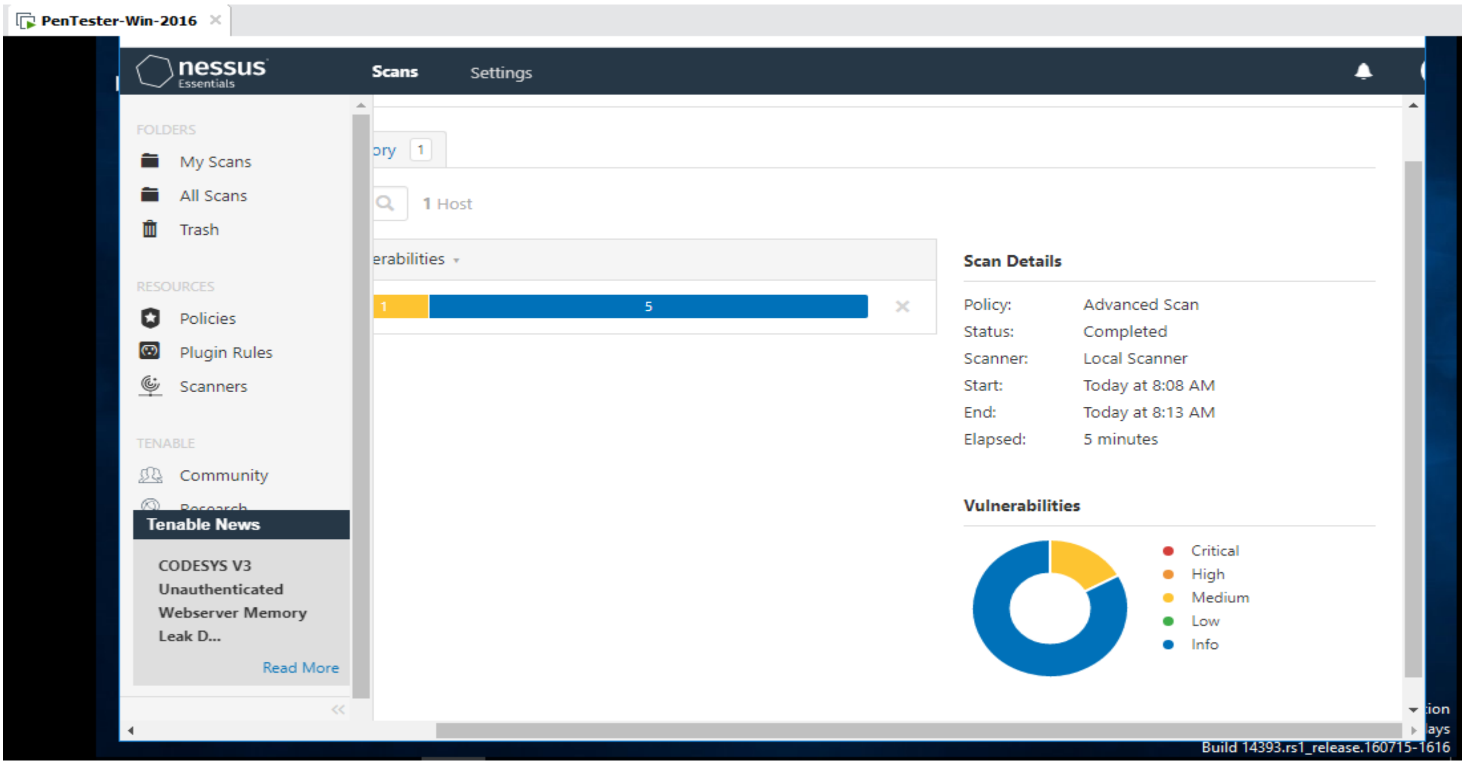
1 Host

□	Host	Vulnerabilities
□	192.168.159.2	1 5

Scan De

Policy:
Status:
Scanner:
Start:
End:
Elapsed:

Vulneral



Tenable News

CODESYS V3 Unauthenticated Webserver Memory Leak D...

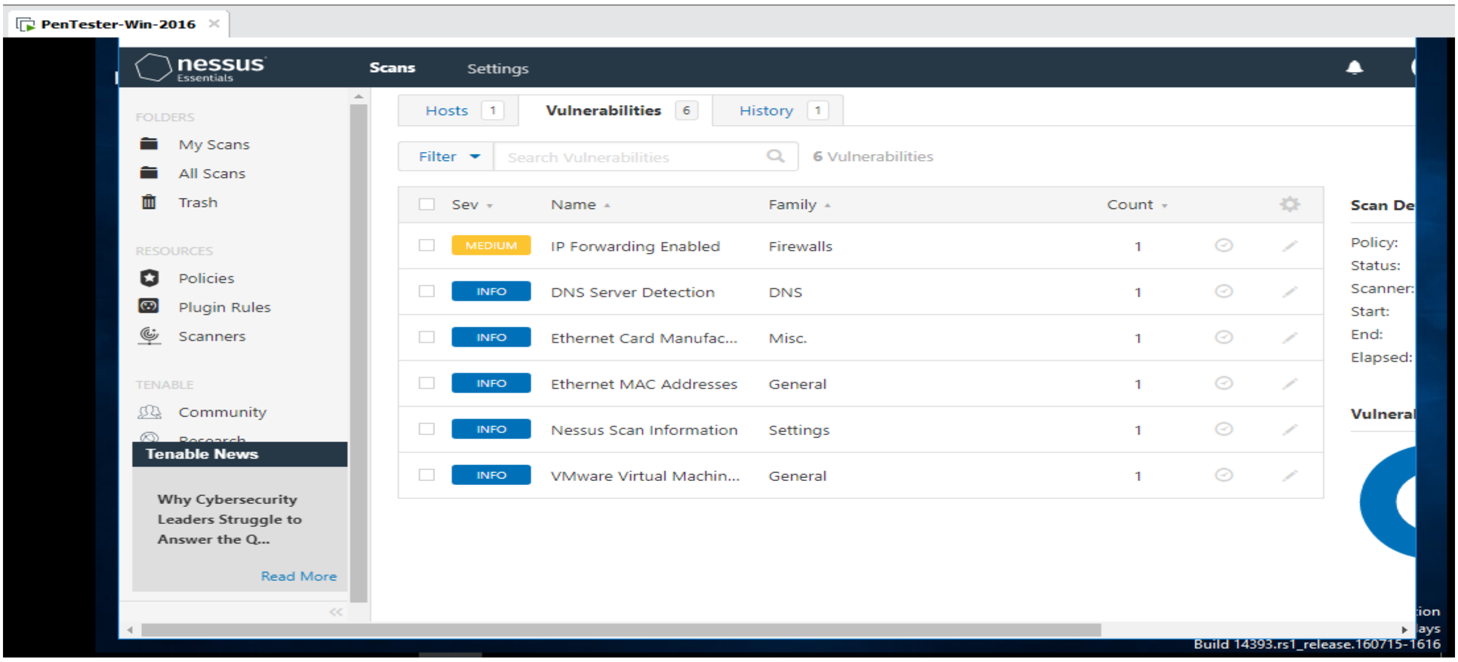
Read More

Scan Details

Policy:	Advanced Scan
Status:	Completed
Scanner:	Local Scanner
Start:	Today at 8:08 AM
End:	Today at 8:13 AM
Elapsed:	5 minutes

Vulnerabilities

- ● Critical
- ● High
- ● Medium
- ● Low
- ● Info



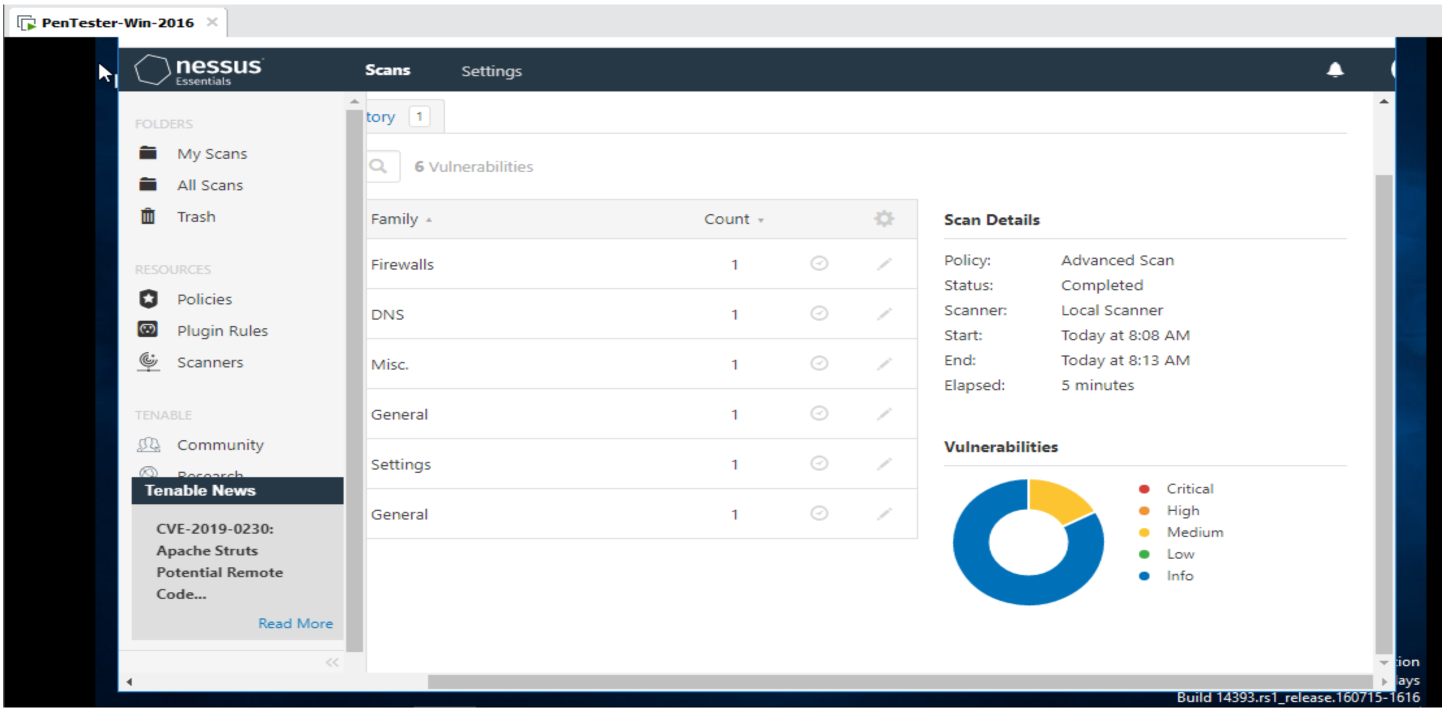
Tenable News

Why Cybersecurity Leaders Struggle to Answer the Q...

Read More

6 Vulnerabilities

□	Sev	Name	Family	Count
□	MEDIUM	IP Forwarding Enabled	Firewalls	1
□	INFO	DNS Server Detection	DNS	1
□	INFO	Ethernet Card Manufac...	Misc.	1
□	INFO	Ethernet MAC Addresses	General	1
□	INFO	Nessus Scan Information	Settings	1
□	INFO	VMware Virtual Machin...	General	1



Tenable News

CVE-2019-0230: Apache Struts Potential Remote Code...

Read More

6 Vulnerabilities

Family	Count
Firewalls	1
DNS	1
Misc.	1
General	1
Settings	1
General	1

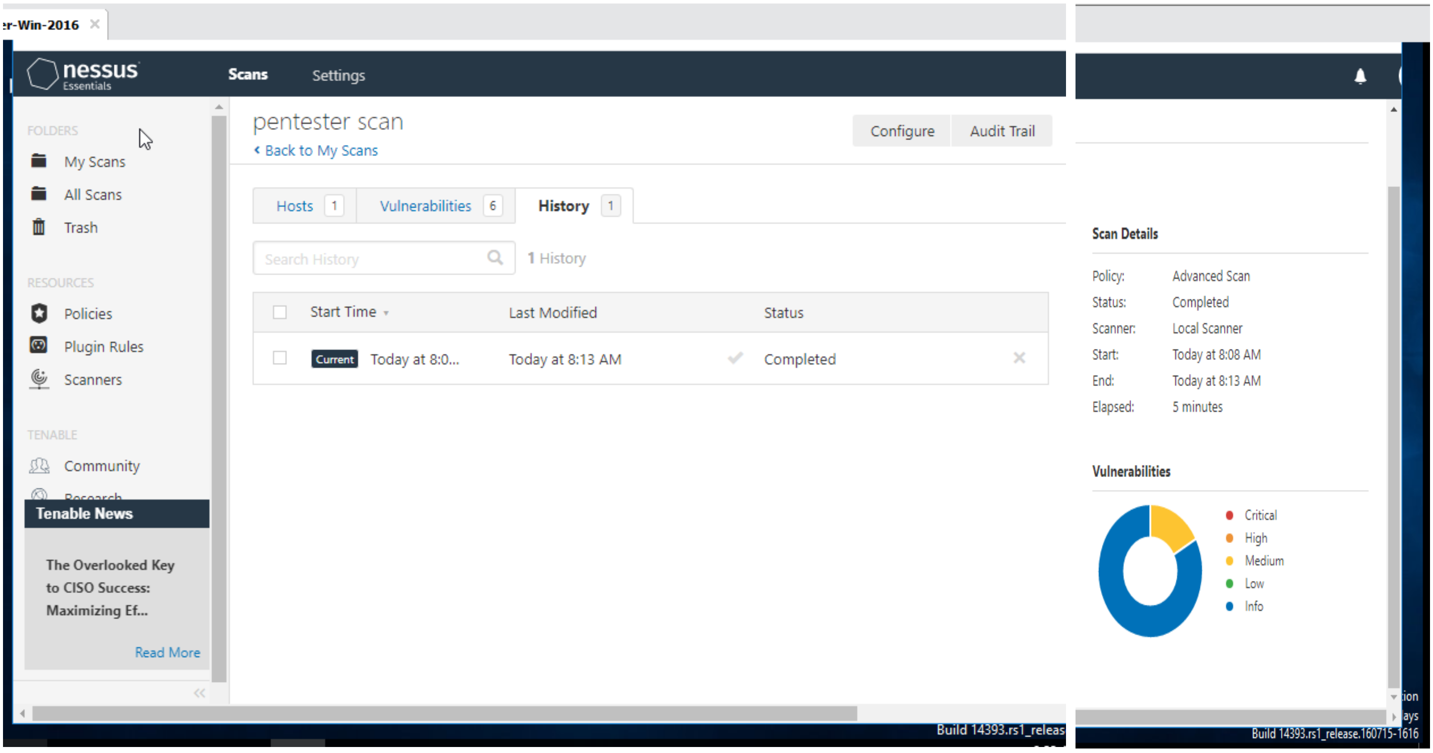
Scan Details

Policy:	Advanced Scan
Status:	Completed
Scanner:	Local Scanner
Start:	Today at 8:08 AM
End:	Today at 8:13 AM
Elapsed:	5 minutes

Vulnerabilities

- ● Critical
- ● High
- ● Medium
- ● Low
- ● Info

Build 14393.rs1_release.160715-1616



pentester scan

‹ Back to My Scans

Tenable News

The Overlooked Key to CISO Success: Maximizing Ef...

Read More

1 History

	Start Time	Last Modified	Status
□	Current Today at 8:0...	Today at 8:13 AM	✓ Completed

Scan Details

Policy:	Advanced Scan
Status:	Completed
Scanner:	Local Scanner
Start:	Today at 8:08 AM
End:	Today at 8:13 AM
Elapsed:	5 minutes

Vulnerabilities

- ● Critical
- ● High
- ● Medium
- ● Low
- ● Info

Build 14393.rs1_releas

Build 14393.rs1_release.160715-1616