Steps to perform Practical 1

There are two kinds of ports on each computer – TCP, and UDP – and 65,536 of each.

The first 1024 TCP ports are the well-known ports like FTP(21), HTTP(80), or SSH(22). Anything above 1024 is available for use by services or applications.

How to Scan Nmap Ports
To **scan Nmap ports** on a remote system, enter the following in the terminal:

```
sudo nmap 192.168.0.1
```

Replace the IP address with the IP address of the system you're testing. This is the basic format for **Nmap**, and it will return information about the ports on that system.

In addition to scanning by IP address, you can also use the following commands to specify a target:

To scan a host:

```
nmap www.hostname.com
```

To scan a range of IP addresses (.1 – .10):

```
nmap 192.168.0.1-10
```

To run **Nmap** on a subnet:

```
nmap 192.168.0.1/13
```

To scan targets from a text file:

```
nmap –iL textlist.txt
```

Scan a Single Port, All Ports, or Series
Nmap commands can be used to scan a single port or a series of ports:

Scan port 80 on the target system:

```
nmap –p 80 192.168.0.1
```

Scan ports 1 through 200 on the target system:

```
nmap –p 1-200 192.168.0.1
```

Scan (Fast) the most common ports:

```
nmap –F 192.168.0.1
```

To scan all ports (1 – 65535):

```
nmap –p– 192.168.0.1
```

Other Types of Nmap Port Scans
Different types of scans can be performed:

To scan using TCP connect (it takes longer, but is more likely to connect):

```
nmap –sT 192.168.0.1
```

To perform the default SYN scan (it tests by performing only half of the TCP handshake):

```
nmap –sS 192.168.0.1
```

To instruct Nmap to scan UDP ports instead of TCP ports (the **–p switch** specifies ports 80, 130, and 255 in this example):

```
nmap –sU –p 80,130,255 192.168.0.1
```

Run a fast scan on the target system, but bypass host discovery. (Host discovery uses **ping**, but many server firewalls do not respond to **ping** requests. This option forces the test without waiting for a reply that may not be coming):

```
nmap –Pn –F 192.168.0.1
```

The **nmap** utility can be used to detect the operating system of a particular target:

```
nmap –A 192.168.0.1
```

It can also be used to probe for the services that might be using different ports:

```
nmap –sV 192.168.0.1
```

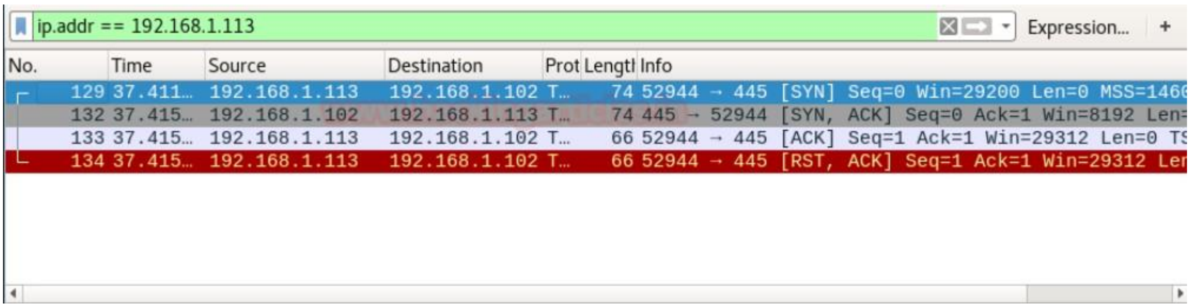
Understanding Nmap Scan with Wireshark

TCP Scan

Tcp scan will scan for TCP port like port 22, 21, 23, 445 etc and ensure for listening port (open) through 3-way handshake connection between the source and destination port. If the port is open then source made request with **SYN** packet, a response destination sent **SYN, ACK** packet and then source sent **ACK** packets, at last source again sent **RST, ACK** packets.

Type following NMAP command for TCP scan as well as start Wireshark on another hand to capture the sent Packet.

```
nmap -sT -p 445 192.168.1.102
```

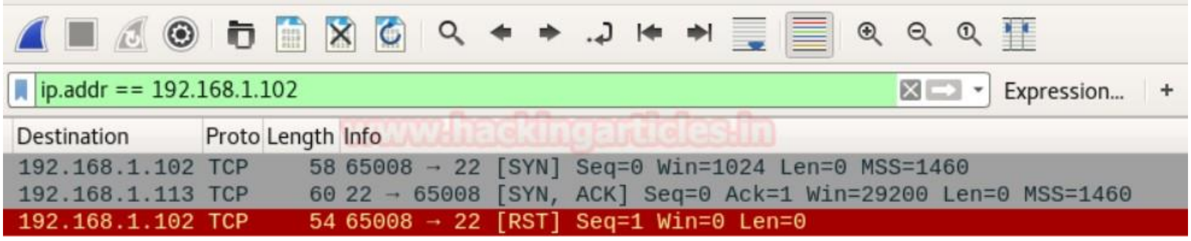


```
ip.addr == 192.168.1.113

No.   Time       Source          Destination     Prot Lengtl Info
  129 37.411…  192.168.1.113   192.168.1.102 T…   74 52944 → 445 [SYN] Seq=0 Win=29200 Len=0 MSS=146
  132 37.415…  192.168.1.102   192.168.1.113 T…   74 445 → 52944 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=
  133 37.415…  192.168.1.113   192.168.1.102 T…   66 52944 → 445 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TS
  134 37.415…  192.168.1.113   192.168.1.102 T…   66 52944 → 445 [RST, ACK] Seq=1 Ack=1 Win=29312 Len
```

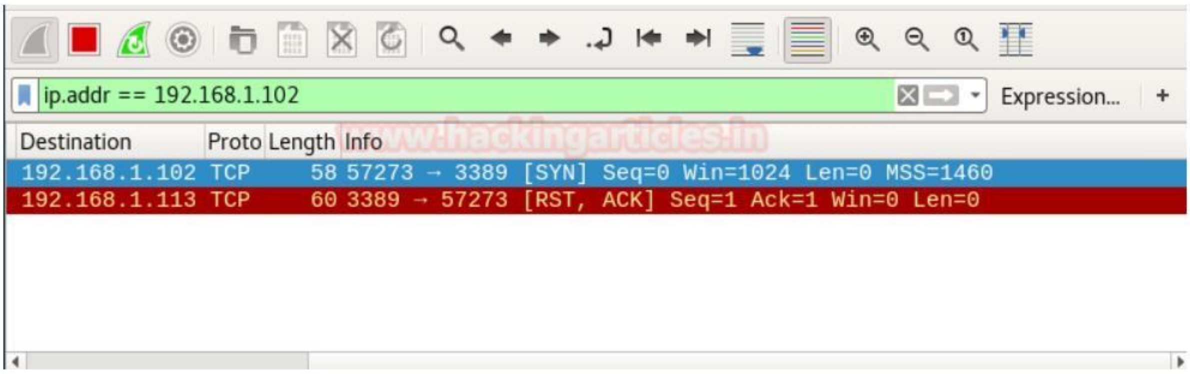
Stealth Scan

SYN scan is the default and most popular scan option for good reasons. It can be performed quickly, scanning thousands of ports per second on a fast network not hampered by restrictive firewalls. It is also relatively typical and stealthy since it never completes TCP connections.

```
nmap -sS -p 22 192.168.1.102
```



```
ip.addr == 192.168.1.102

Destination    Proto Length Info
192.168.1.102 TCP      58 65008 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
192.168.1.113 TCP      60 22 → 65008 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
192.168.1.102 TCP      54 65008 → 22 [RST] Seq=1 Win=0 Len=0
```



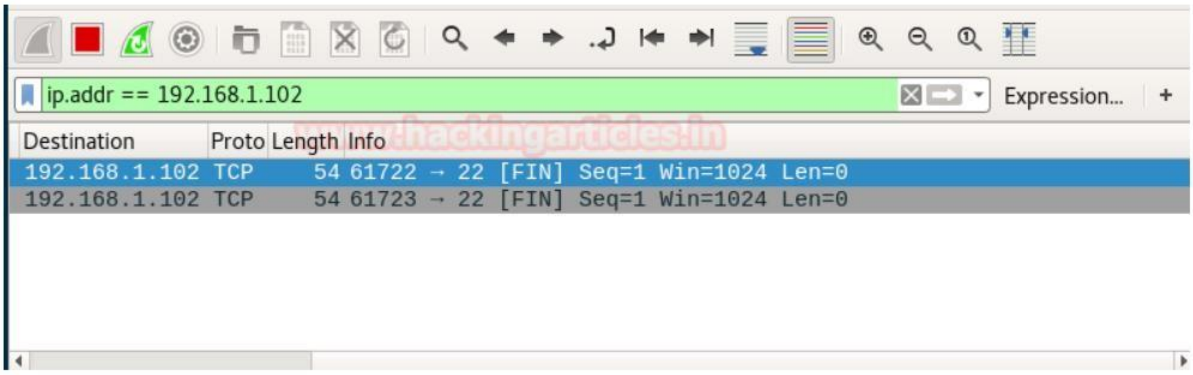
```
ip.addr == 192.168.1.102

Destination    Proto Length Info
192.168.1.102 TCP      58 57273 → 3389 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
192.168.1.113 TCP      60 3389 → 57273 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
```

Fin Scan

A FIN packet is used to terminate the TCP connection between the source and destination port typically after the data transfer is complete. In the place of an SYN packet, Nmap starts a FIN scan by using a FIN packet. If the port is open then no response will come from destination port when FIN packet is sent through source port.

Type following NMAP command for TCP scan as well as start Wireshark on another hand to capture the sent Packet.

```
nmap -sF -p 22 192.168.1.102
```



ip.addr == 192.168.1.102

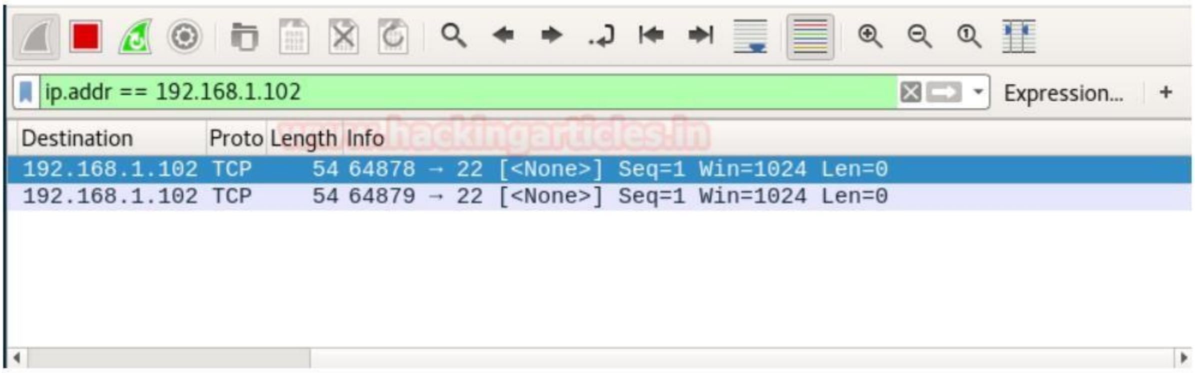
```
Destination    Proto Length Info
192.168.1.102  TCP      54 61722 → 22 [FIN] Seq=1 Win=1024 Len=0
192.168.1.102  TCP      54 61723 → 22 [FIN] Seq=1 Win=1024 Len=0
```

Null Scan

A Null Scan is a series of TCP packets which hold a sequence number of “zeros” (0000000) and since there are none flags set, the destination will not know how to reply the request. It will discard the packet and no reply will be sent, which indicate that the port is open.

Type following NMAP command for TCP scan as well as start Wireshark on another hand to capture the sent Packet.

```
nmap -sN -p 22 192.168.1.102
```

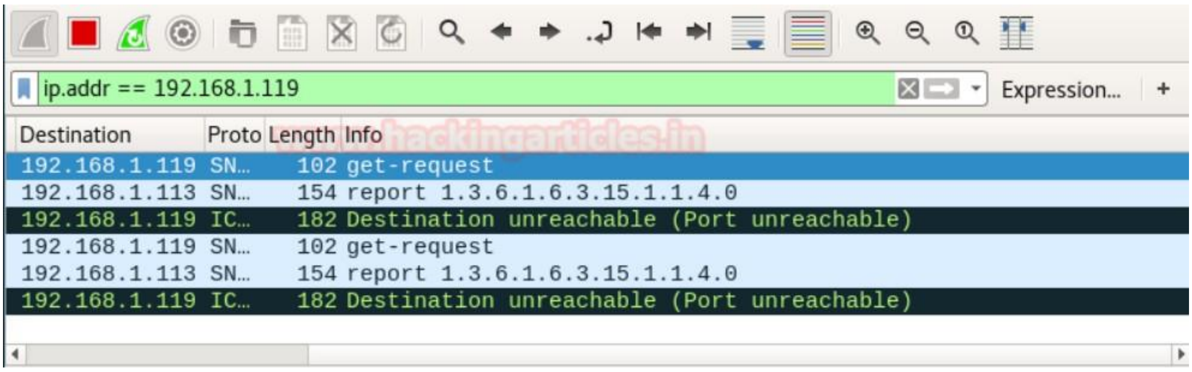


ip.addr == 192.168.1.102

```
Destination    Proto Length Info
192.168.1.102  TCP      54 64878 → 22 [<None>] Seq=1 Win=1024 Len=0
192.168.1.102  TCP      54 64879 → 22 [<None>] Seq=1 Win=1024 Len=0
```

UDP Scan

```
nmap -sU -p 161 192.168.1.119
```

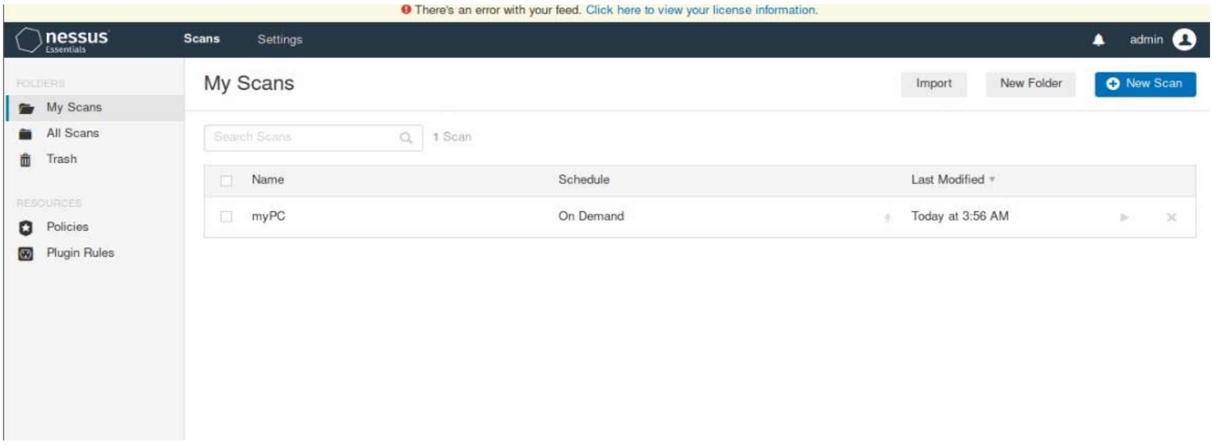


```
Destination   Proto Length Info
192.168.1.119 SN…   102 get-request
192.168.1.113 SN…   154 report 1.3.6.1.6.3.15.1.1.4.0
192.168.1.119 IC…   182 Destination unreachable (Port unreachable)
192.168.1.119 SN…   102 get-request
192.168.1.113 SN…   154 report 1.3.6.1.6.3.15.1.1.4.0
192.168.1.119 IC…   182 Destination unreachable (Port unreachable)
```

Conclusion:

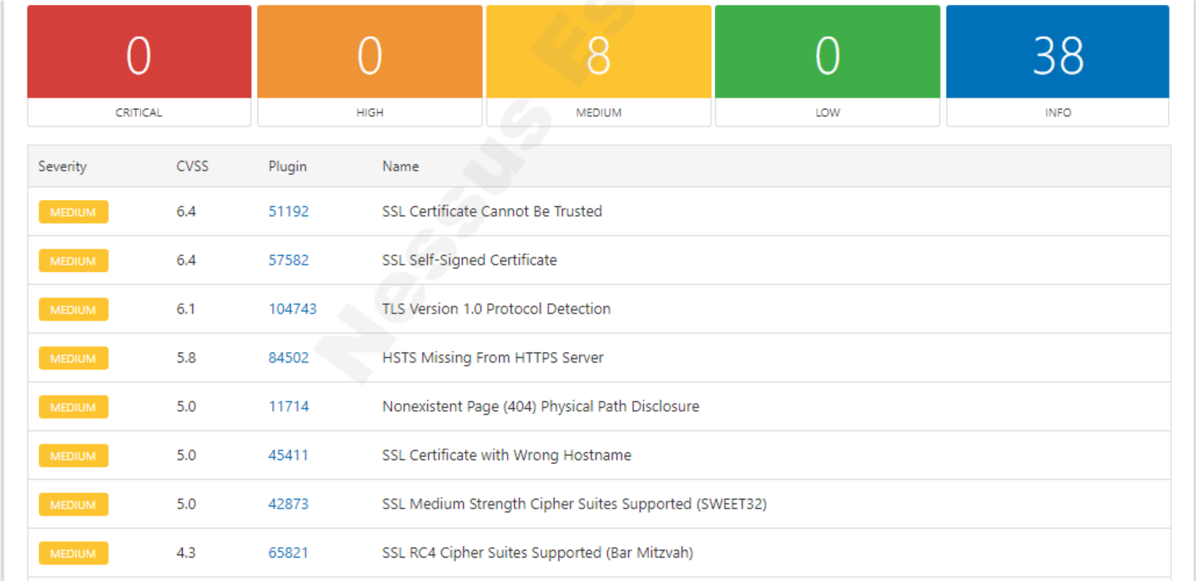
By the above practical we were able to perform 5 different types of (port) scanning using nmap on a single port and capture the packets using Wireshark and analyse the output.

Steps to perform Practical 2



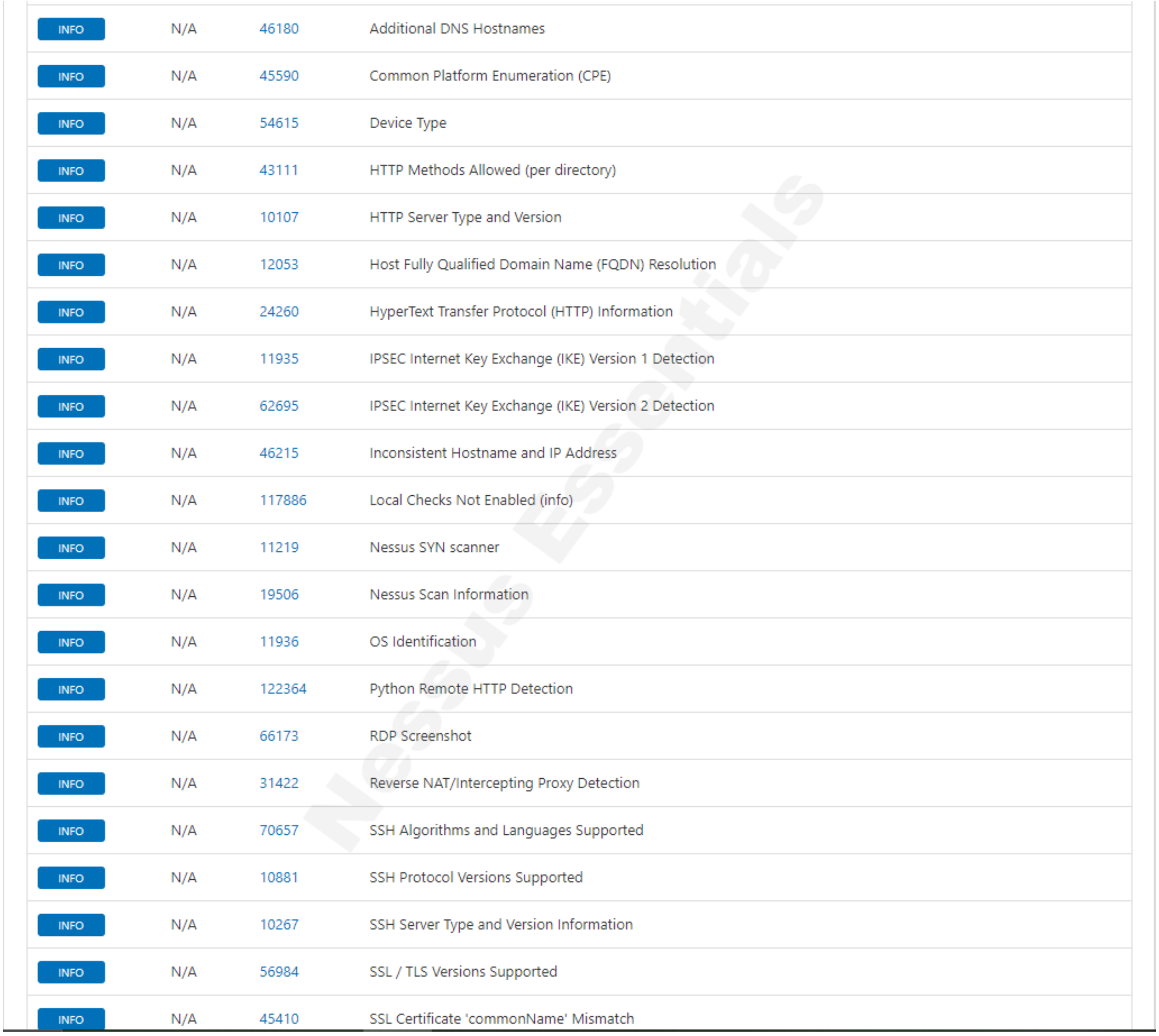
There's an error with your feed. Click here to view your license information.

Name	Schedule	Last Modified
myPC	On Demand	Today at 3:56 AM

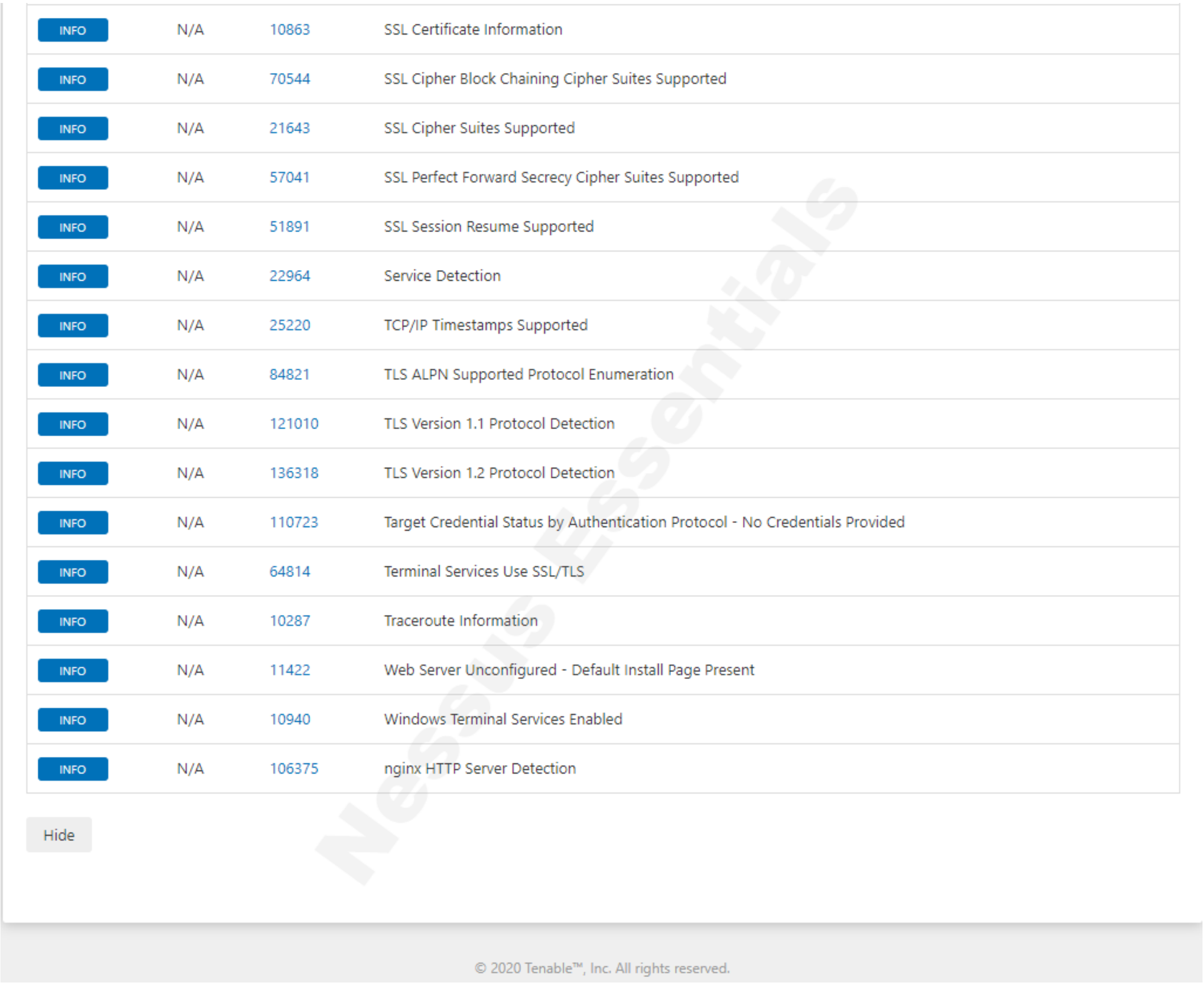


CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	8	0	38

Severity	CVSS	Plugin	Name
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	6.1	104743	TLS Version 1.0 Protocol Detection
MEDIUM	5.8	84502	HSTS Missing From HTTPS Server
MEDIUM	5.0	11714	Nonexistent Page (404) Physical Path Disclosure
MEDIUM	5.0	45411	SSL Certificate with Wrong Hostname
MEDIUM	5.0	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	4.3	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)



INFO	N/A	46180	Additional DNS Hostnames
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	54615	Device Type
INFO	N/A	43111	HTTP Methods Allowed (per directory)
INFO	N/A	10107	HTTP Server Type and Version
INFO	N/A	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	11935	IPSEC Internet Key Exchange (IKE) Version 1 Detection
INFO	N/A	62695	IPSEC Internet Key Exchange (IKE) Version 2 Detection
INFO	N/A	46215	Inconsistent Hostname and IP Address
INFO	N/A	117886	Local Checks Not Enabled (info)
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	11936	OS Identification
INFO	N/A	122364	Python Remote HTTP Detection
INFO	N/A	66173	RDP Screenshot
INFO	N/A	31422	Reverse NAT/Intercepting Proxy Detection
INFO	N/A	70657	SSH Algorithms and Languages Supported
INFO	N/A	10881	SSH Protocol Versions Supported
INFO	N/A	10267	SSH Server Type and Version Information
INFO	N/A	56984	SSL / TLS Versions Supported
INFO	N/A	45410	SSL Certificate 'commonName' Mismatch



INFO	N/A	10863	SSL Certificate Information
INFO	N/A	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	21643	SSL Cipher Suites Supported
INFO	N/A	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	51891	SSL Session Resume Supported
INFO	N/A	22964	Service Detection
INFO	N/A	25220	TCP/IP Timestamps Supported
INFO	N/A	84821	TLS ALPN Supported Protocol Enumeration
INFO	N/A	121010	TLS Version 1.1 Protocol Detection
INFO	N/A	136318	TLS Version 1.2 Protocol Detection
INFO	N/A	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	64814	Terminal Services Use SSL/TLS
INFO	N/A	10287	Traceroute Information
INFO	N/A	11422	Web Server Unconfigured - Default Install Page Present
INFO	N/A	10940	Windows Terminal Services Enabled
INFO	N/A	106375	nginx HTTP Server Detection