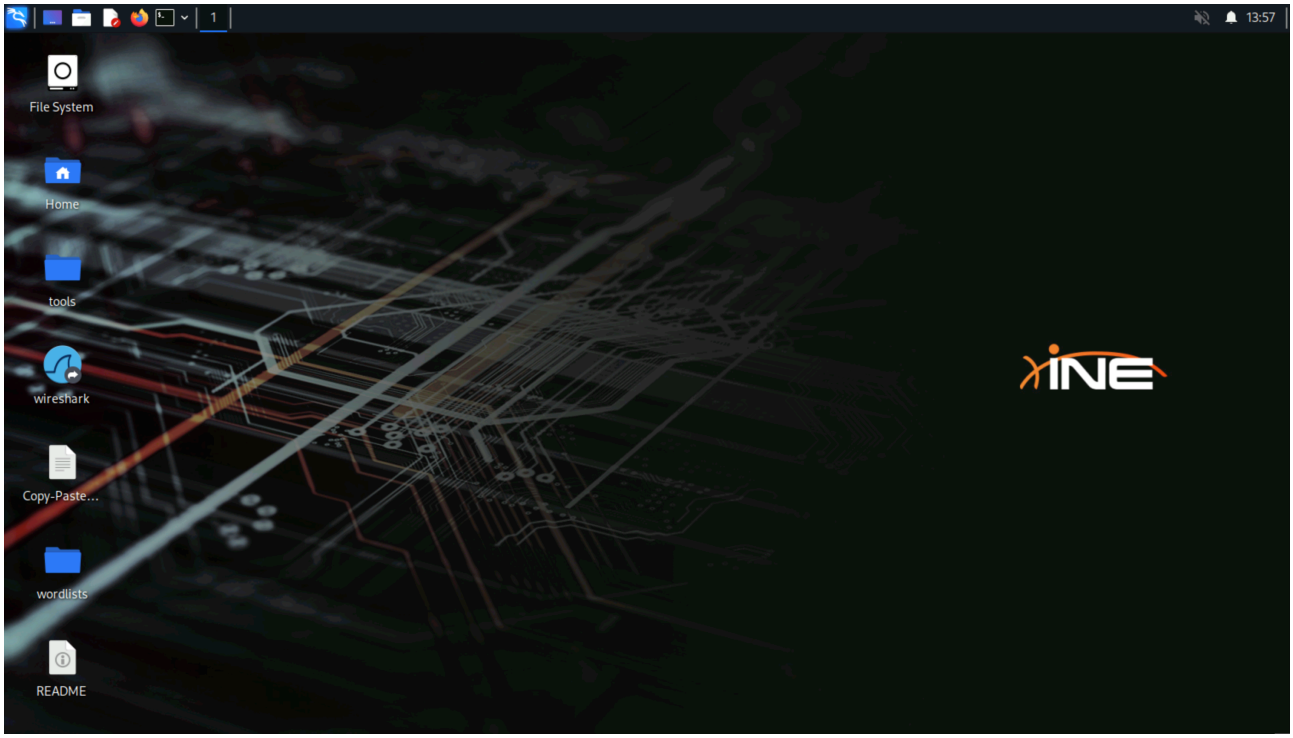
Lab-2

Scan the server 1

Step 1: Open the lab link to access the Kali machine.



Step 2: Check if the target machine is reachable:

Command:

```
ping -c 4 demo.ine.local
```

```
┌──(root㉿INE)-[~]
└─# ping -c 4 demo.ine.local
PING demo.ine.local (192.39.148.3) 56(84) bytes of data.
64 bytes from demo.ine.local (192.39.148.3): icmp_seq=1 ttl=64 time=0.091 ms
64 bytes from demo.ine.local (192.39.148.3): icmp_seq=2 ttl=64 time=0.057 ms
64 bytes from demo.ine.local (192.39.148.3): icmp_seq=3 ttl=64 time=0.043 ms
64 bytes from demo.ine.local (192.39.148.3): icmp_seq=4 ttl=64 time=0.041 ms

── demo.ine.local ping statistics ──
4 packets transmitted, 4 received, 0% packet loss, time 3091ms
rtt min/avg/max/mdev = 0.041/0.058/0.091/0.020 ms

┌──(root㉿INE)-[~]
└─#
```

The target is reachable.

Step 3: Port scanning with Nmap

We can now perform a default Nmap port scan on the target to identify the open ports on the target system, this can be done by running the following command:

Command:

```
nmap demo.ine.local
```

As shown in the following screenshot, the default Nmap scan does not reveal any open ports. This is because the default Nmap scan profile only scans 1000 of the most commonly used ports.

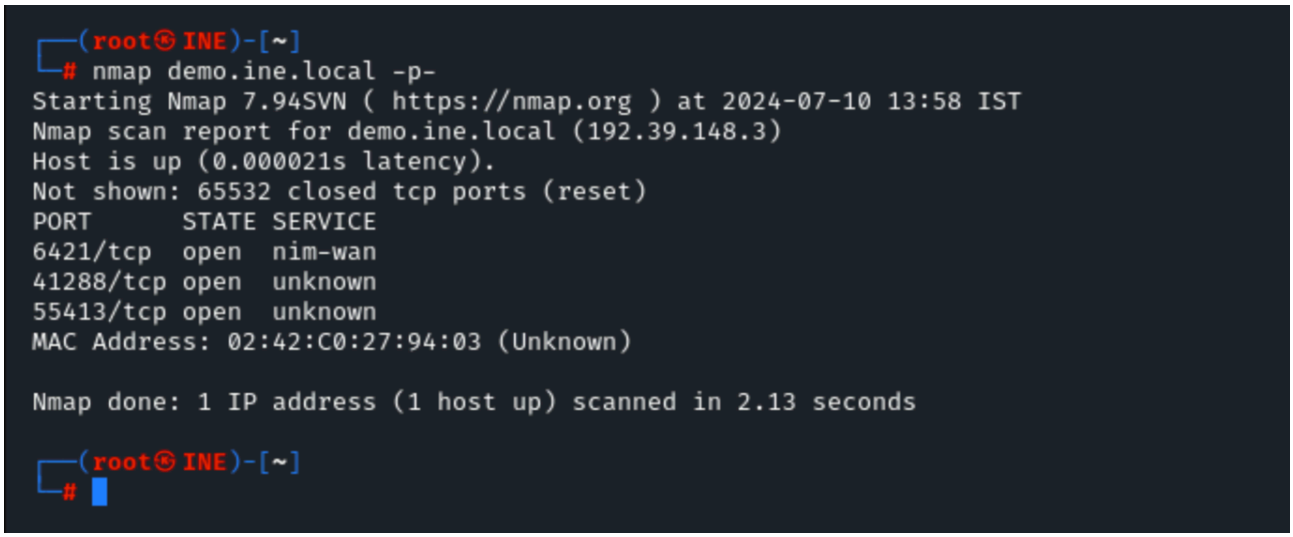
```
┌──(root㉿INE)-[~]
└─# nmap demo.ine.local
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-10 13:58 IST
Nmap scan report for demo.ine.local (192.39.148.3)
Host is up (0.000023s latency).
All 1000 scanned ports on demo.ine.local (192.39.148.3) are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 02:42:C0:27:94:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds

┌──(root㉿INE)-[~]
└─#
```

In order to get an accurate idea of the open ports on the target system, we will need to scan the entire TCP port range (65,535 ports). This can be done by running the following command:

Command:

```
nmap demo.ine.local -p-
```

As shown in the following screenshot, the Nmap scan reveals that the target system has 3 open ports.



Step 4: Service detection with Nmap

Now that we have identified the open ports on the target, we can learn more about the services running on the open ports by performing a service detection scan with Nmap.

This can be done by running the following command:

Command:

```
nmap demo.ine.local -p 6421,41288,55413 -sV
```

As shown in the following screenshot, the Nmap service detection scan reveals the names and versions of the services running on the open ports on the target system.

```
┌──(root㉿INE)-[~]
└─# nmap demo.ine.local -p 6421,41288,55413 -sV
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-10 13:59 IST
Nmap scan report for demo.ine.local (192.39.148.3)
Host is up (0.000048s latency).

PORT      STATE SERVICE   VERSION
6421/tcp  open  mongodb   MongoDB 2.6.10
41288/tcp open  memcached Memcached
55413/tcp open  ftp       vsftpd 3.0.3
MAC Address: 02:42:C0:27:94:03 (Unknown)
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.31 seconds

┌──(root㉿INE)-[~]
└─#
```

Conclusion

In this lab, we explored the process of performing port scanning and service detection with Nmap.