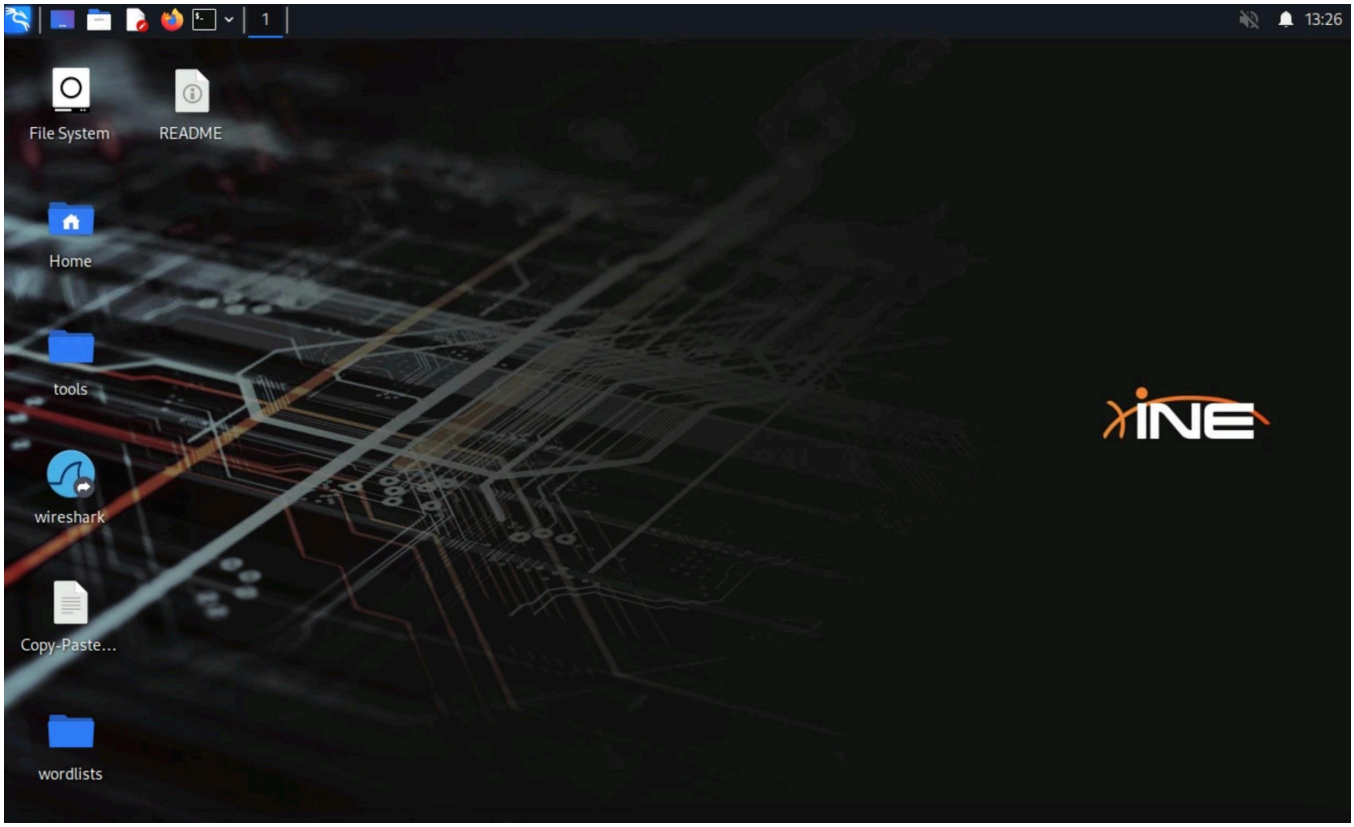
Lab -

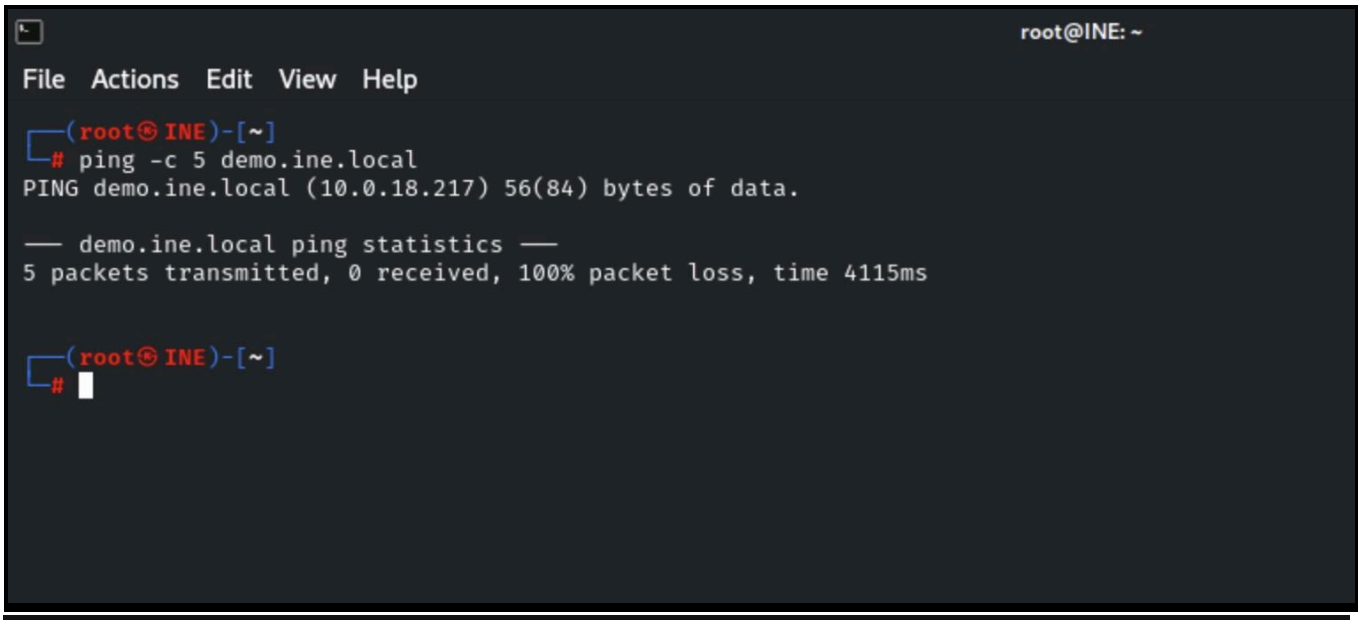
1 Nmap Host Discovery-

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



Command:

```
ping -c 5 demo.ine.local
```

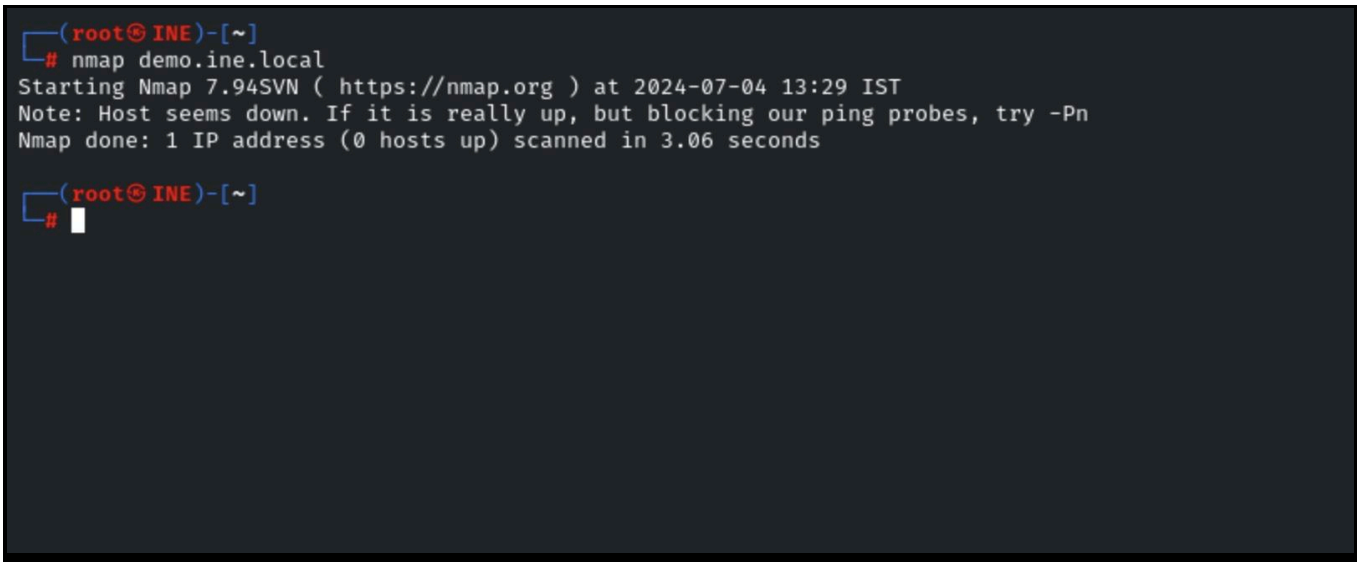


We can observe that the target is not responding to the ping requests, so this does not confirm if it's alive or down.

Step 3: Run a Nmap scan against the target.

Command:

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



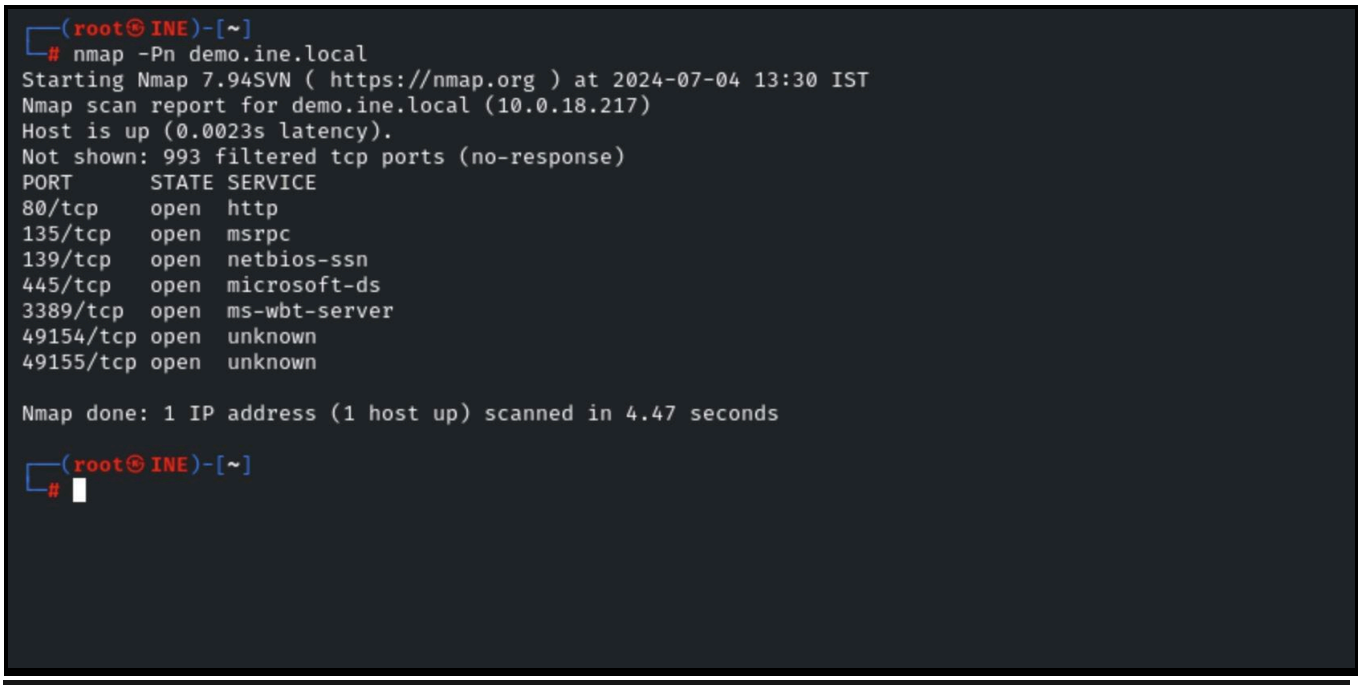
Nmap also could not detect whether the host was up or not. Many security tools first ping the host before they start scanning or exploiting the target. In that case, one has to use advanced Nmap options, i.e., -A or -T5, etc., in order to get the correct output.

In the nmap, there is one option, i.e., -Pn (Treat all hosts as online; skip host discovery). This option will force the scanning even if it has detected the target as down in host discovery.

Step 4: Running Nmap using the -Pn option to discover all alive ports.

Command:

```
nmap -Pn demo.ine.local
```

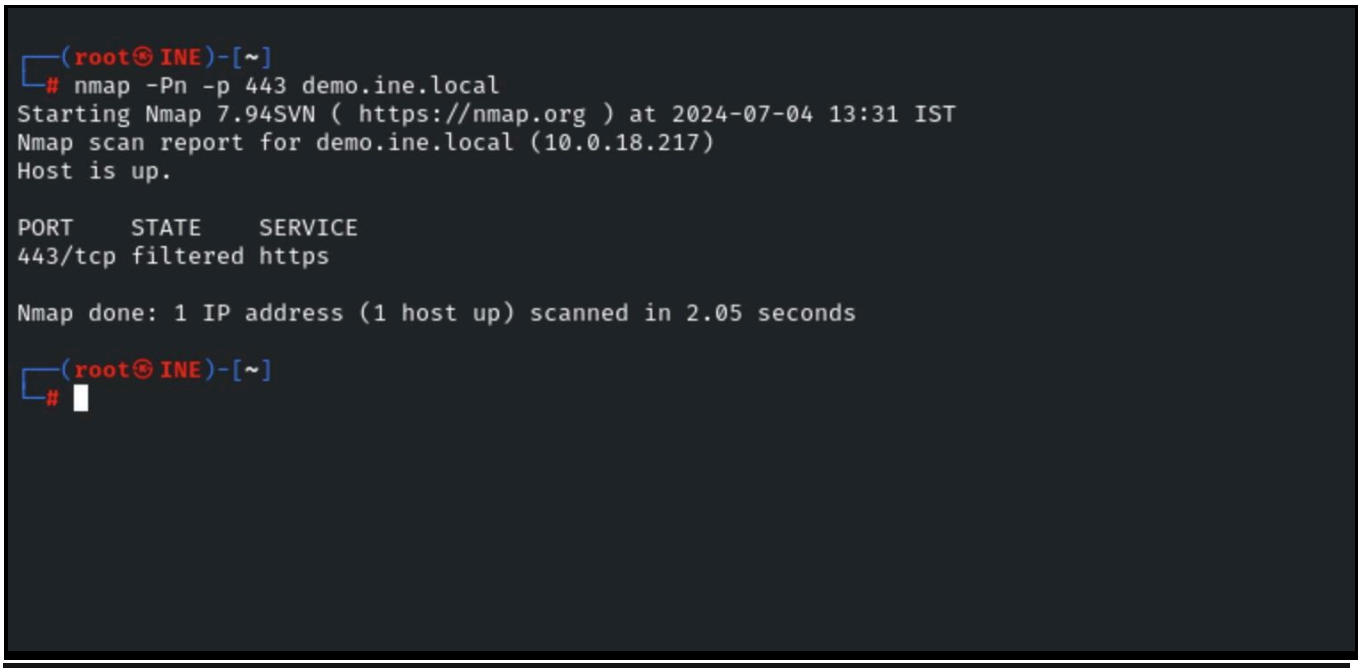


We can see multiple ports are open on the target machine.

Now, we will scan any random port that isn't open. In this case, scan port 443. If the port is not open, we would receive "filtered" output from that port.

Command:

```
nmap -Pn -p 443 demo.ine.local
```



We can observe in the Nmap output that the host is up, but port 443 is filtered.

About Filtered port:

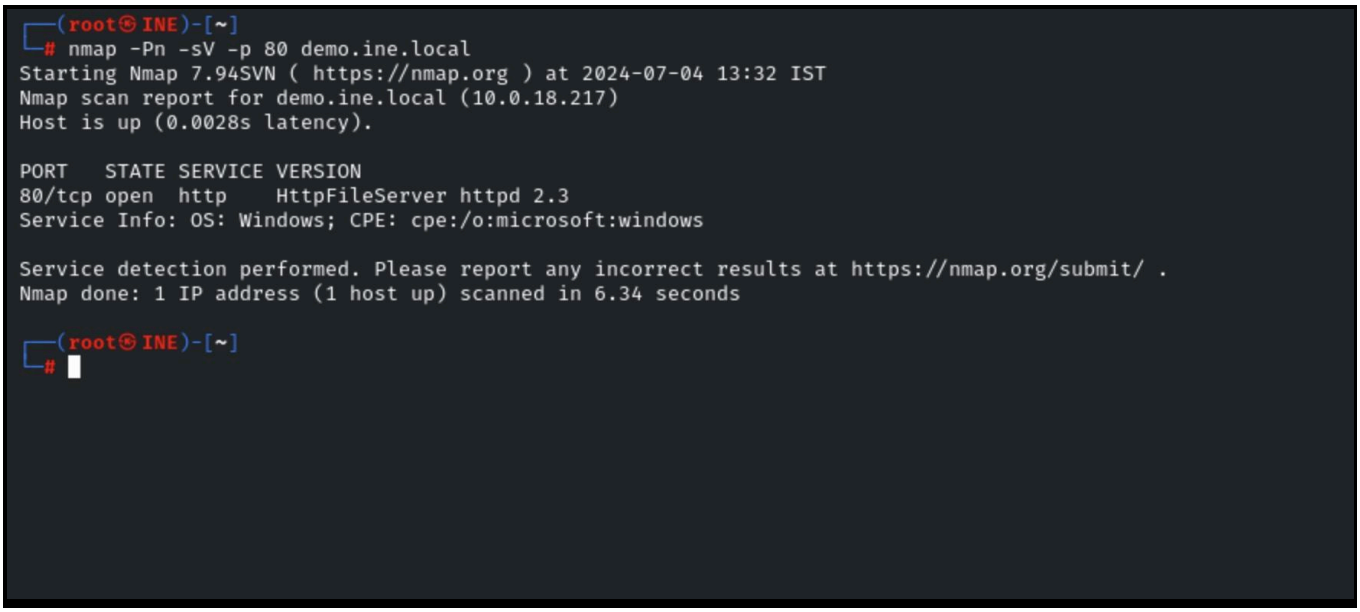
Nmap cannot determine whether the port is open because packet filtering prevents its probes from reaching the port. The filtering could be from a dedicated firewall device, router rules, or host-based firewall software. These ports frustrate attackers because they provide so little information. Sometimes they respond with ICMP error messages such as type 3 code 13 (destination unreachable: communication administratively prohibited), but filters that simply drop probes without responding are far more common. This forces Nmap to retry several times just in case the probe was dropped due to network congestion rather than filtering. This slows down the scan dramatically.

Source: https://nmap.org/book/man-port-scanning-basics.html

Step 5: Similarly, if we want to discover the running application on port 80, we could use option -sV, and this option is used to determine the application version information.

Command:

```
nmap -Pn -sV -p 80 demo.ine.local
```



This is one of the ways we can discover a machine that is behind a firewall, forcing tools for scanning.

Conclusion

In this lab, we saw a standard method to discover hosts using Nmap, which is behind a firewall.

References

- Nmap