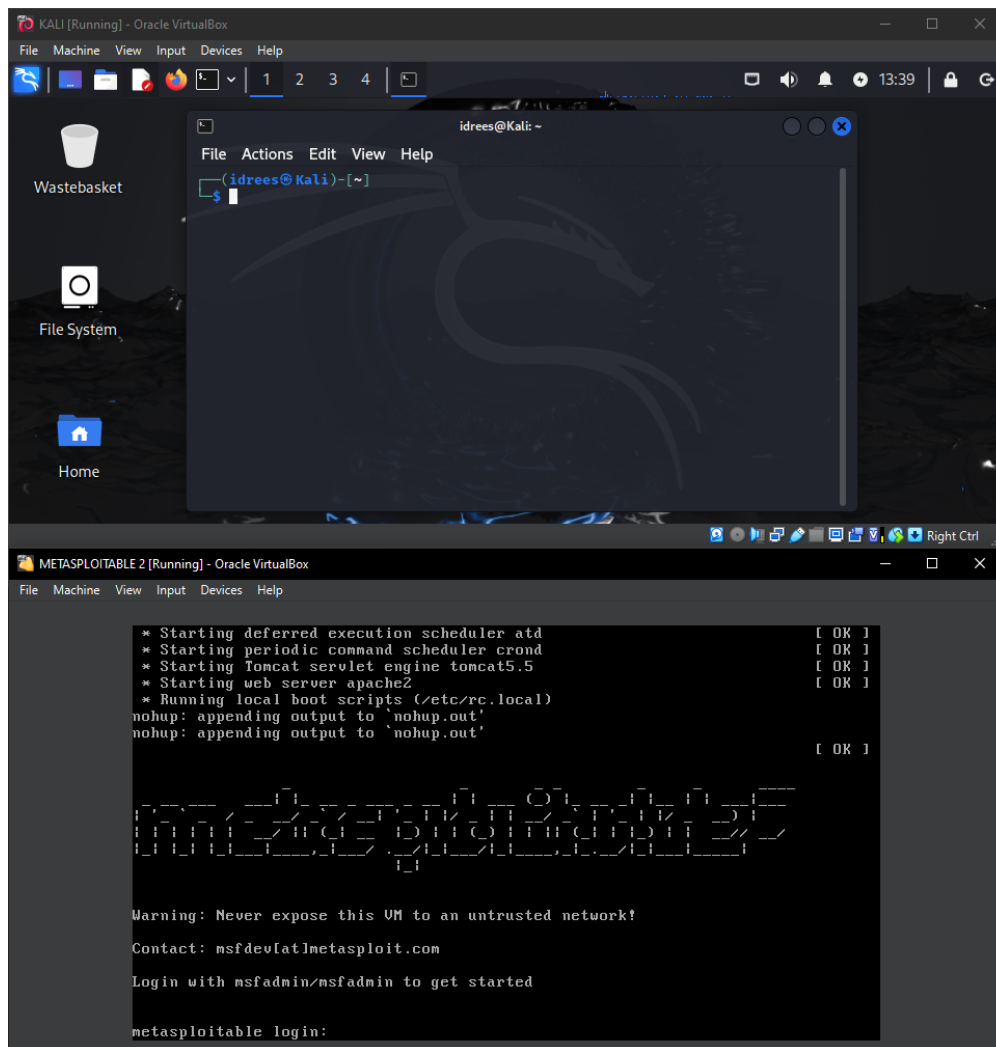


Project scenario:

- Penetration Tester.
- Test security posture of a multinational Aeronautical corporation called AeroTech.
- Identify vulnerabilities and rectify those weaknesses before an attack actually occurs

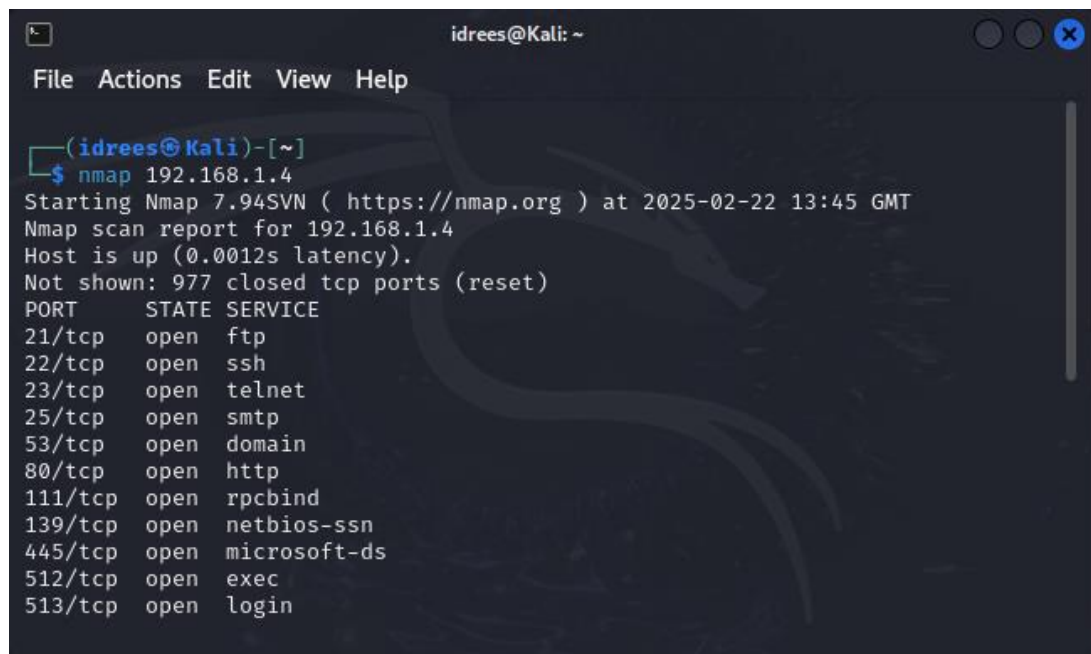
Task 1: Use Nmap to scan for vulnerability services

1. Begin by running our attacking machine and the victim machine. We are using metasploitable2 to attack the victim machine.



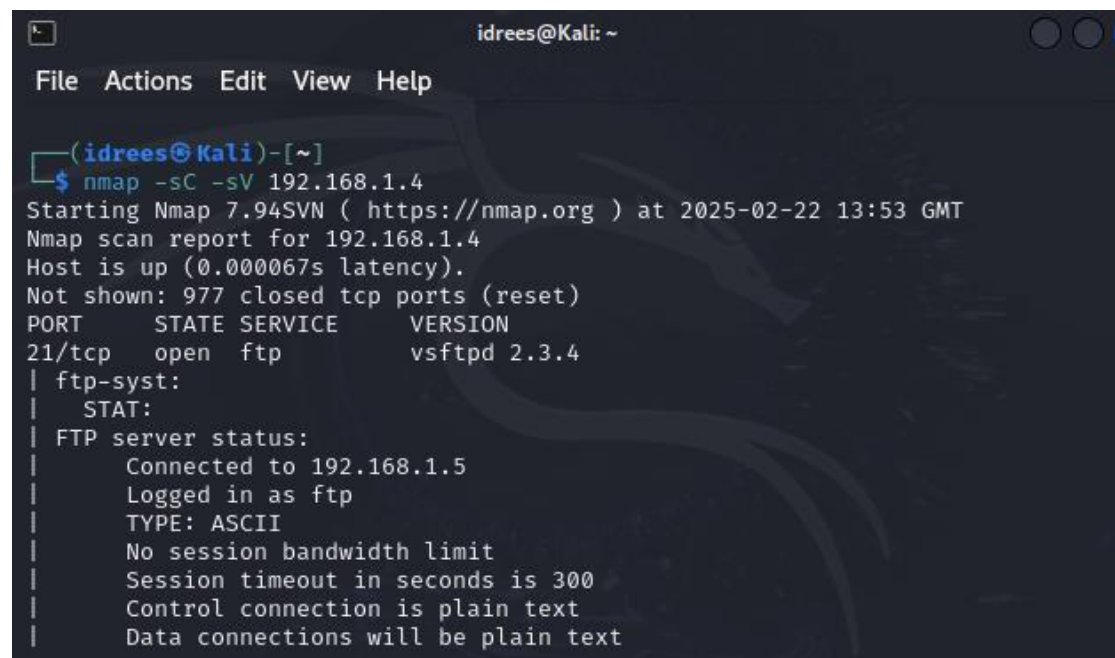
NOTE: The command 'nmap -h' will give help and provide the manual for nmap.

2. Run nmap using the Ip address of your victim machine



```
idrees@Kali: ~  
File Actions Edit View Help  
  
(idrees@Kali)-[~]  
$ nmap 192.168.1.4  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-22 13:45 GMT  
Nmap scan report for 192.168.1.4  
Host is up (0.0012s latency).  
Not shown: 977 closed tcp ports (reset)  
PORT      STATE SERVICE  
21/tcp    open  ftp  
22/tcp    open  ssh  
23/tcp    open  telnet  
25/tcp    open  smtp  
53/tcp    open  domain  
80/tcp    open  http  
111/tcp   open  rpcbind  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
512/tcp   open  exec  
513/tcp   open  login
```

NOTE: This will present all the ports that are open. The more ports that are open the larger the attack surface. The command 'nmap -sC [IP address]' will give a more detailed scan. Adding the -sV flag will provide the version number too so you can check if something is outdated.



```
idrees@Kali: ~  
File Actions Edit View Help  
  
(idrees@Kali)-[~]  
$ nmap -sC -sV 192.168.1.4  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-22 13:53 GMT  
Nmap scan report for 192.168.1.4  
Host is up (0.000067s latency).  
Not shown: 977 closed tcp ports (reset)  
PORT      STATE SERVICE      VERSION  
21/tcp    open  ftp          vsftpd 2.3.4  
| ftp-syst:  
|   STAT:  
| FTP server status:  
|   Connected to 192.168.1.5  
|   Logged in as ftp  
|   TYPE: ASCII  
|   No session bandwidth limit  
|   Session timeout in seconds is 300  
|   Control connection is plain text  
|   Data connections will be plain text
```

Conclusion:

- Pen testing requires a reconnaissance stage so that we can learn more about the system
- Nmap is a powerful tool for scanning vulnerable systems
- Ports with outdated services will often host vulnerabilities

