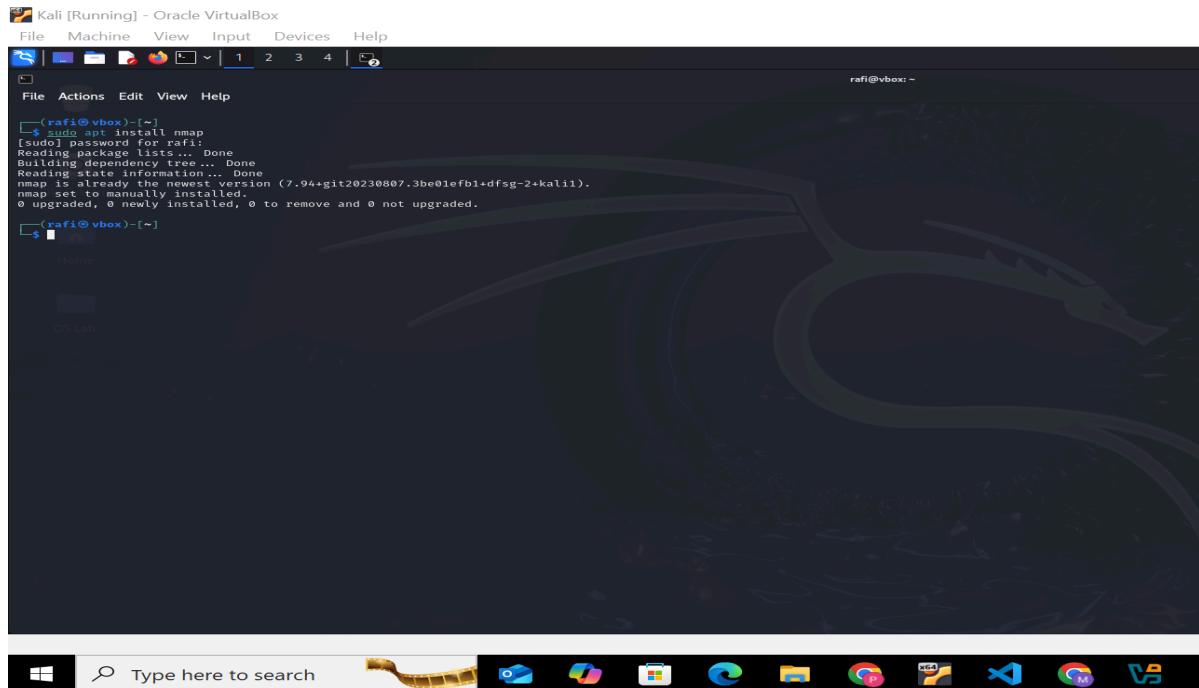


Basic Vulnerability Scan By nmap

Objective

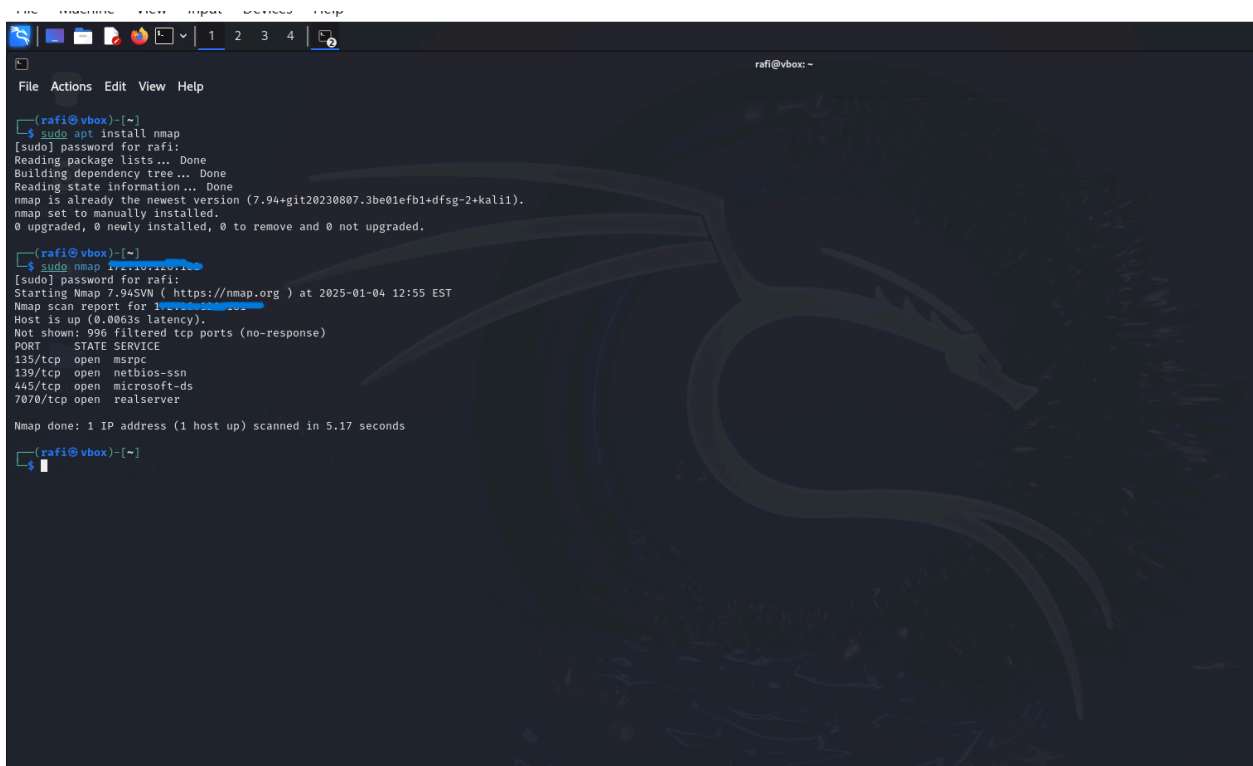
To perform a basic vulnerability scan on a target system to identify potential risks and vulnerabilities.

1. Setting Up the Environment

A screenshot of a Kali Linux virtual machine running in Oracle VM VirtualBox. The terminal window shows the command 'sudo apt install nmap' being executed. The output indicates that nmap is already installed at version 7.94, but it is being updated to the latest version (7.94+git20230807.3be01efb1+dfsg-2+kali1). The terminal also shows the password for the user 'rafi' and the confirmation to proceed with the installation. The background of the terminal window features a large, stylized dragon logo, which is the Kali Linux logo. The window title is 'Kali [Running] - Oracle VirtualBox'. The bottom of the image shows the Windows taskbar with various application icons and a search bar.

Nmap, a powerful network scanning tool, is installed and configured on Kali Linux. This tool is essential for scanning and analyzing the target system.

2. Scanning the Target IP:



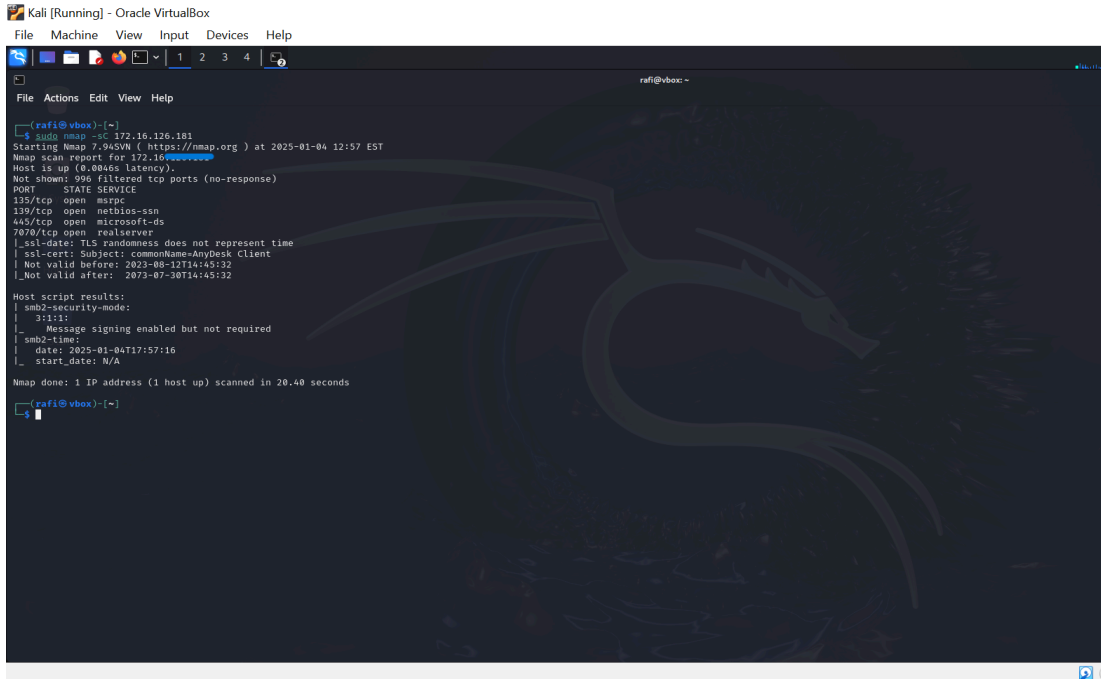
```
rafi@vbox: ~  
File Actions Edit View Help  
[rafi@vbox]~  
$ sudo apt install nmap  
[sudo] password for rafi:  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
nmap is already the newest version (7.94+git20230807.3be01efb1+dfsg-2+kali1).  
nmap set to manually installed.  
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.  
[rafi@vbox]~  
$ sudo nmap 192.168.100.100  
[sudo] password for rafi:  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-04 12:55 EST  
Nmap scan report for 192.168.100.100  
Host is up (0.0063s latency).  
Not shown: 996 filtered tcp ports (no-response)  
PORT      STATE SERVICE  
135/tcp   open  msrpc  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
7070/tcp  open  realserver  
Nmap done: 1 IP address (1 host up) scanned in 5.17 seconds  
[rafi@vbox]~  
$
```

The target system is scanned to check if it is active and to identify any open ports. This provides an initial view of the system's exposure.

Here we can see several ports are open as 135,139,445

3. Testing for Vulnerabilities:

Using Nmap's built-in vulnerability scripts, the target system is analyzed for known vulnerabilities, including SMB-related issues.



```
(rafi@vbox)-[~]
$ sudo nmap -SC 172.16.126.181
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-04 12:57 EST
Nmap scan report for 172.16.126.181
Host is up (0.0046s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  metbios-ssn
445/tcp    open  microsoft-ds
7070/tcp   open  realserver
|_ssl-date: TLS randomness does not represent time
|_ssl-cert: Subject: commonName=AnyDesk Client
|_Not valid before: 2023-08-12T14:45:32
|_Not valid after:  2072-07-30T14:45:32
Host script results:
|_smb2-security-mode:
|_  31:11:
|_    Message signing enabled but not required
|_smb2-time:
|_  date: 2025-01-04T17:57:16
|_  start_date: N/A
Nmap done: 1 IP address (1 host up) scanned in 20.40 seconds
(rafi@vbox)-[~]
$
```

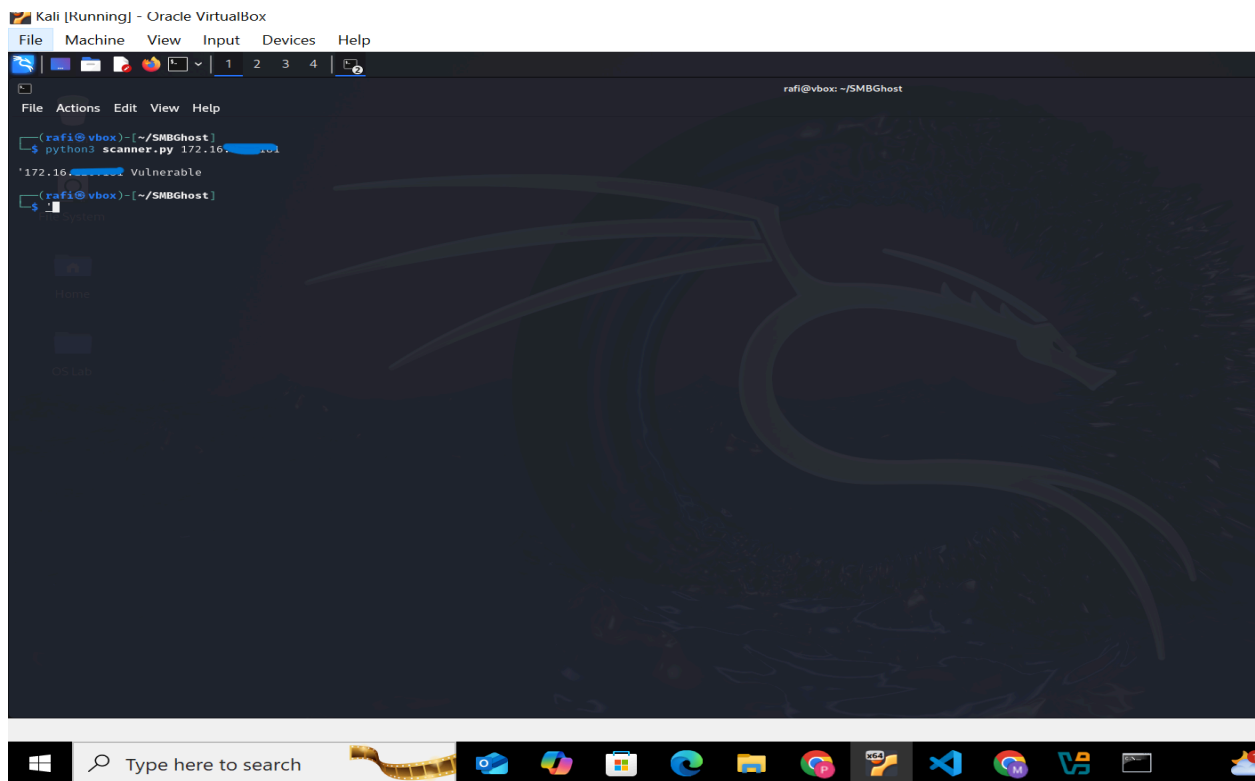
Also, there are a lot of built-in scripts available in Nmap that we can use specifically for specific vulnerability findings.

4.1 Summary of Open Ports

The scan reveals the following open ports, which provide insights into the services running on the target system:

- **Port 135:** Microsoft RPC
- **Port 139:** NetBIOS-SSN
- **Port 445:** SMB

4.2 Vulnerability Findings:



- **SMBGhost (CVE-2020-0796):**
 - A critical vulnerability in SMBv3 that could allow remote code execution or denial of service.
 - This issue has a high impact and requires immediate attention.

5. Recommendations;

1. **Apply Security Patches:** Ensure that all critical updates are applied to mitigate vulnerabilities like SMBGhost.
2. **Restrict Access:** Limit access to sensitive ports, especially from untrusted networks.
3. **Monitor SMB Traffic:** Use appropriate tools to detect and respond to suspicious activities.

6. Conclusion

The vulnerability scan highlights potential risks, including open ports and SMBGhost. Immediate remediation steps are recommended to secure the target system.