**Practical – 1**

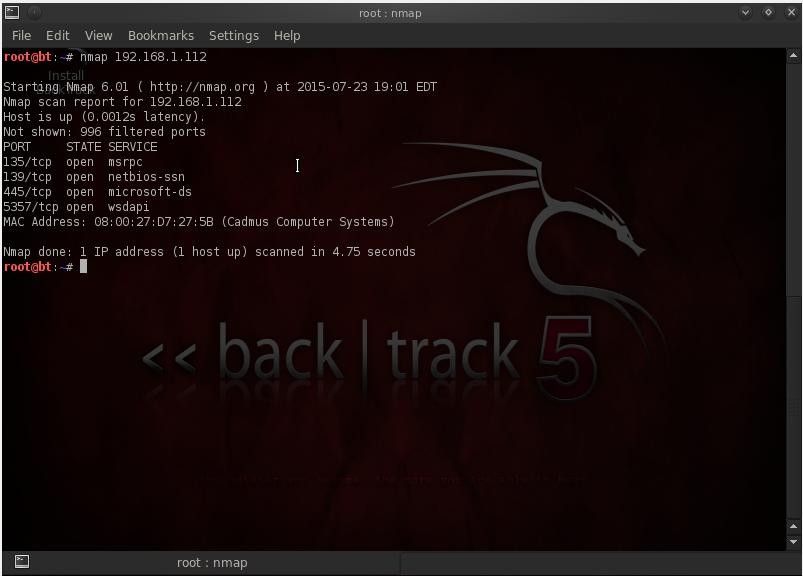
**Aim:** Vulnerability Assessment of a system using NMAP 1. TCP SYN Scan 2.TCP FIN Scan 3. Port Scan.

Nmap is short for Network Mapper. It is an open-source security to ol for network exploration, security scanning and auditing. However, nmap command comes w ith lots of options that can make the utility more robust and difficult to follow for new users.

The purpose of this post is to introduce a user to the nmap command line tool to scan a host and/or network, so to find out the possible vulnerable points in the hosts. Y ou will also slearn how to use Nmap for offensive and defensive purposes.

1. **Scan a single host or an IP address (IPv4)**

# nmap 192.168.1.112

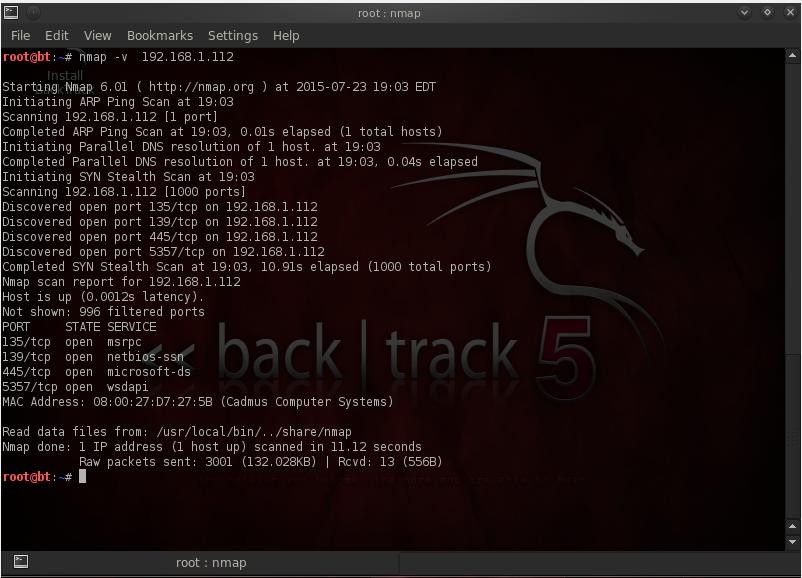
**Output:**

1. **Scan using “-v” option.**

command with “-v” option is giving more detailed information about the remote machine.

# nmap -v 192.168.1.112

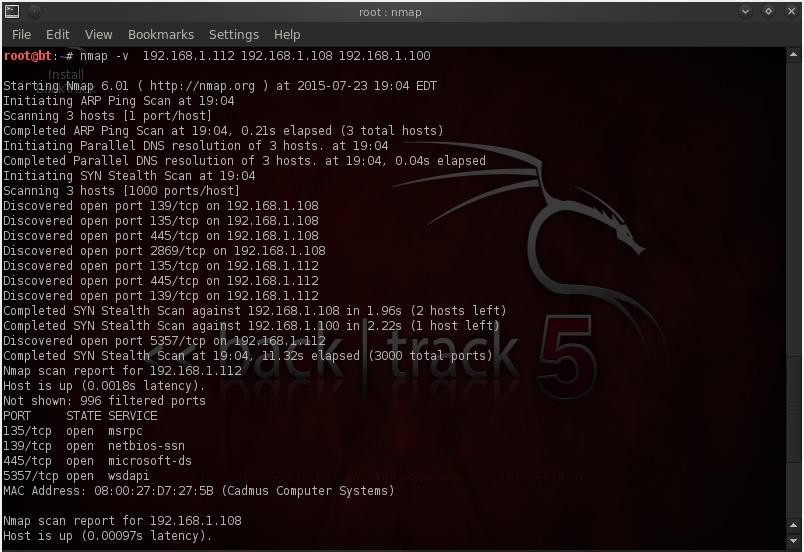
**Output:**

****

1. **Scan Multiple Hosts.**

# nmap –v 192.168.1.112 192.168.1.108 192.168.1.100

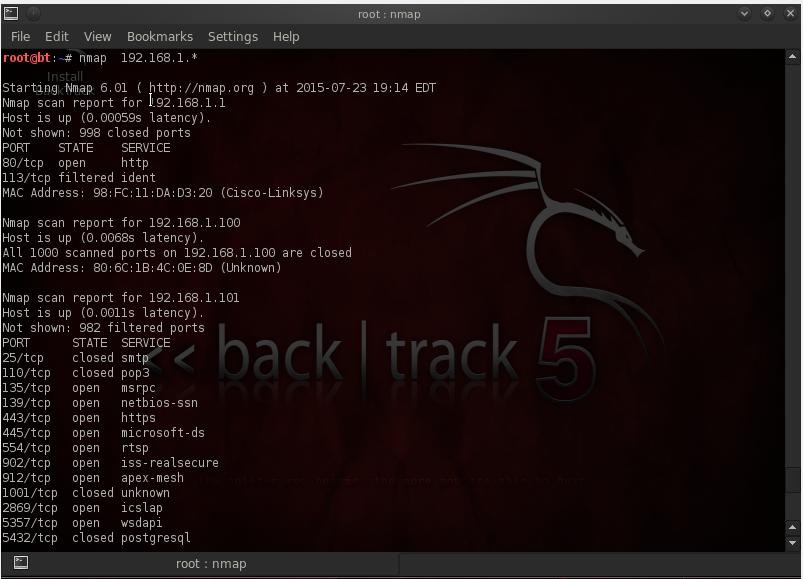
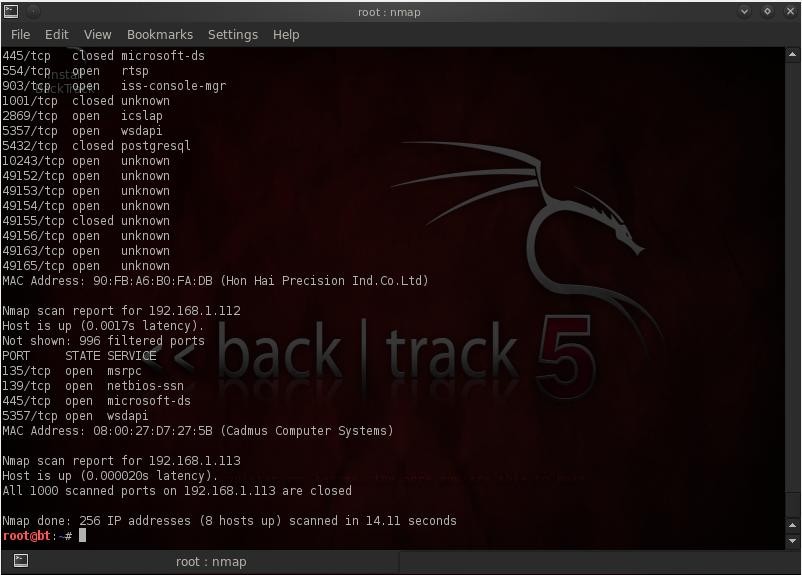
**Output:**

****

1. **Scan a whole Subnet**

# nmap –v 192.168.1.\*

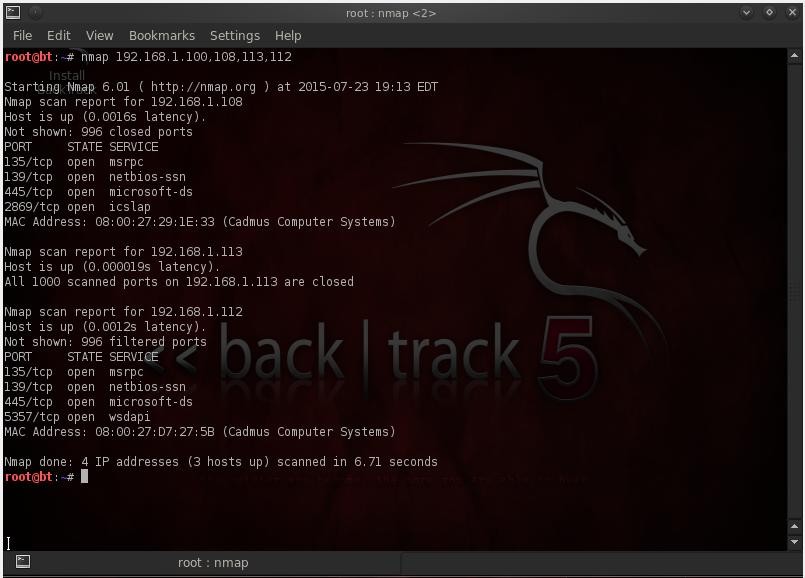
**Output:**

****

1. **Scan Multiple Servers using last octet of IP address.**

# nmap –v 192.168.1.1,108,113,112

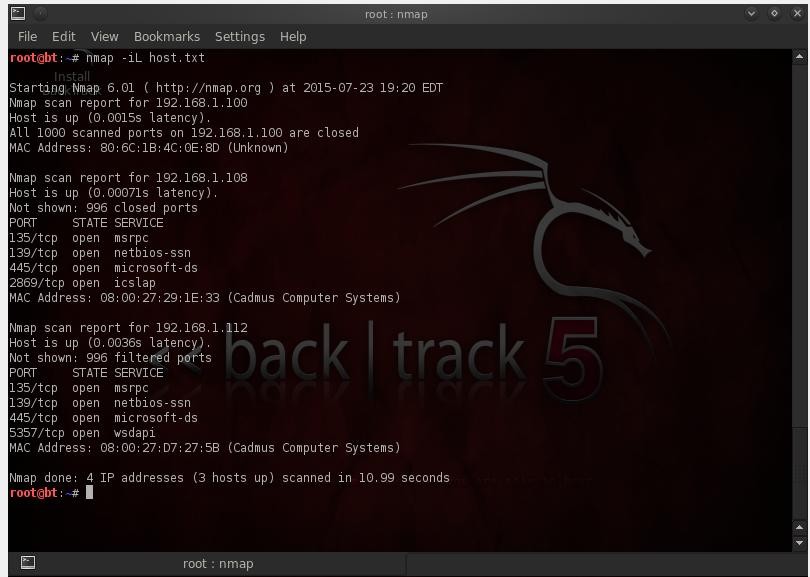
**Output:**

****

1. **Scan list of Hosts from a File.**

# nmap –iL host.txt

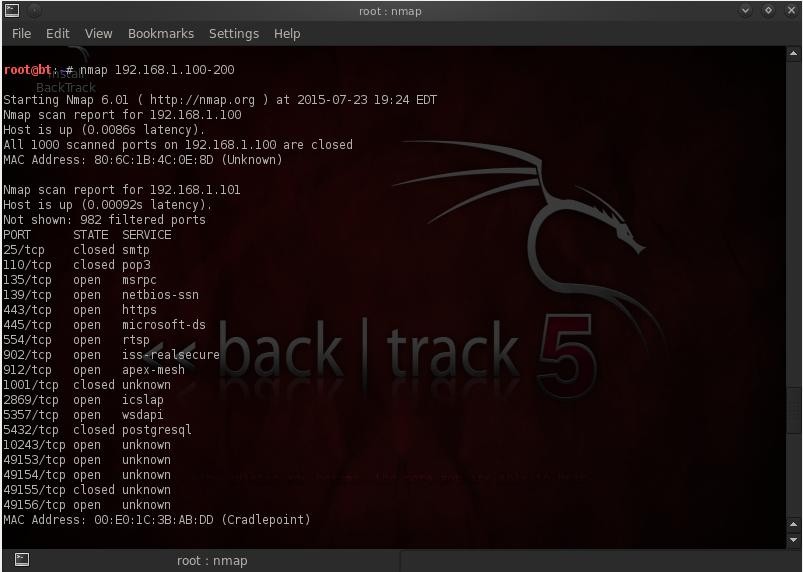
**Output:**

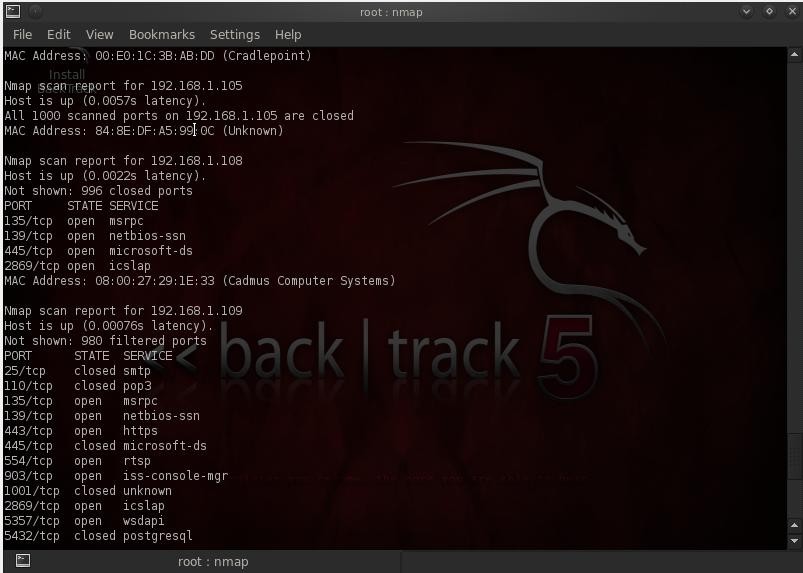
****

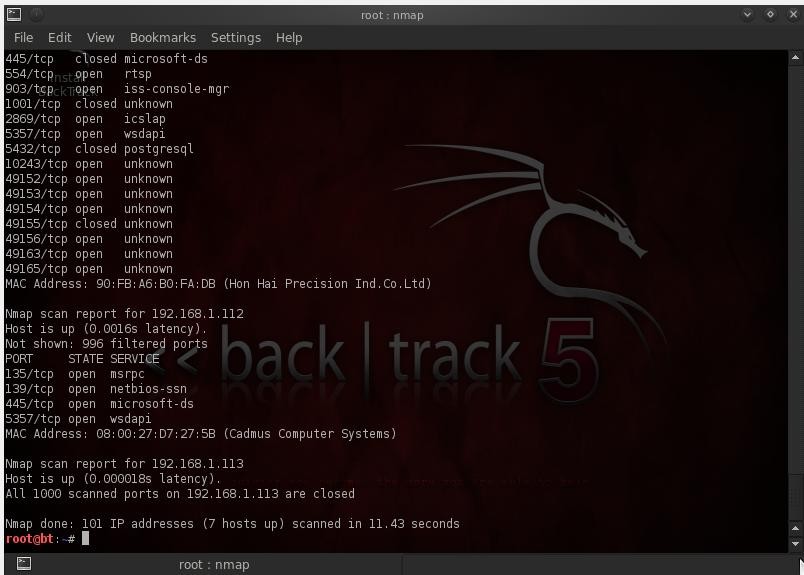
1. **Scan an IP Address Range**

# nmap 192.168.1.1,100-200

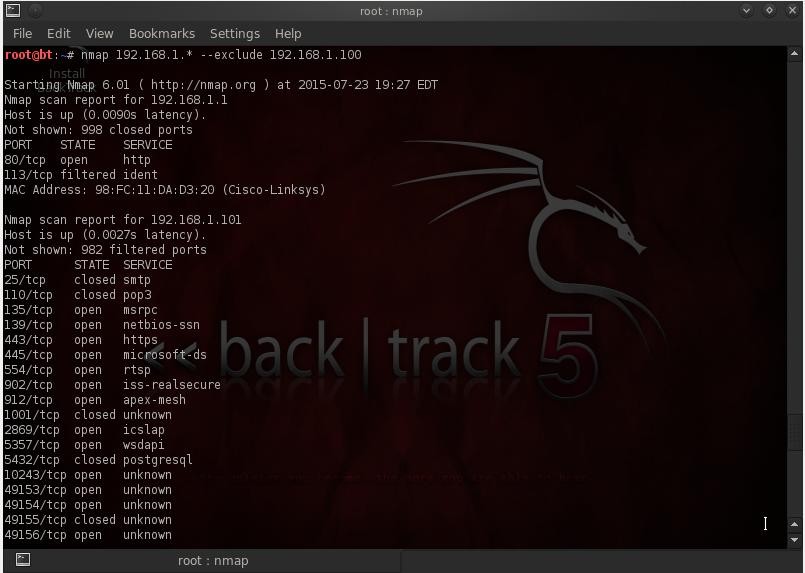
**Output:**

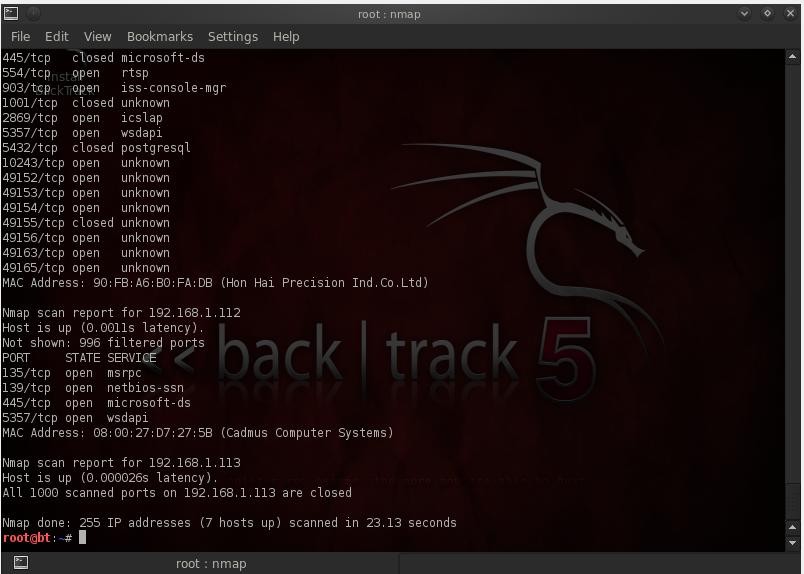
****

****



1. **Scan Network Excluding Remote Hosts.**

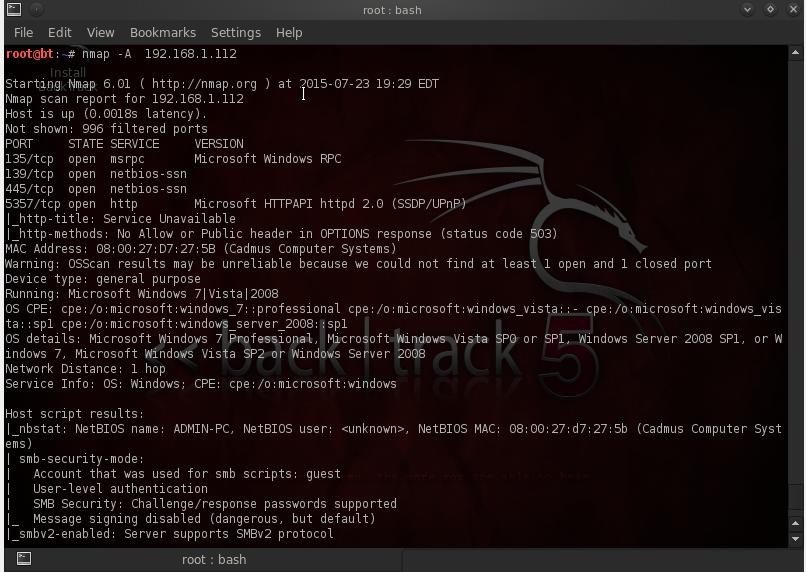
**** # nmap 192.168.1.\* --exclude 192.168.1.100 **Output:**

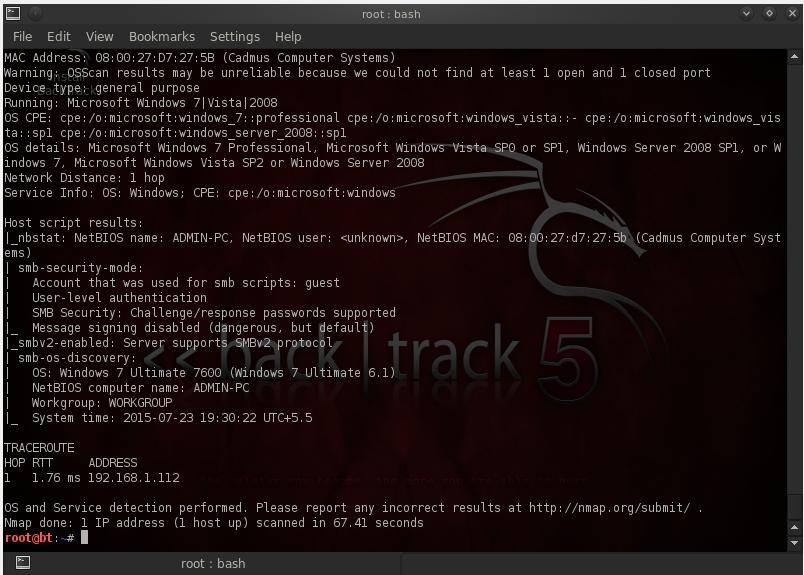


1. **Scan OS information and Trace route.**

# nmap -A 192.168.1.112

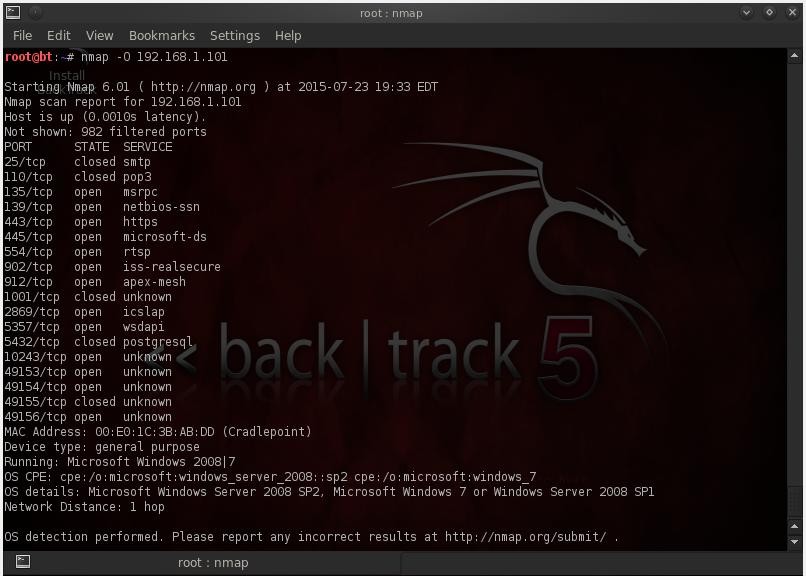
**Output:**

****



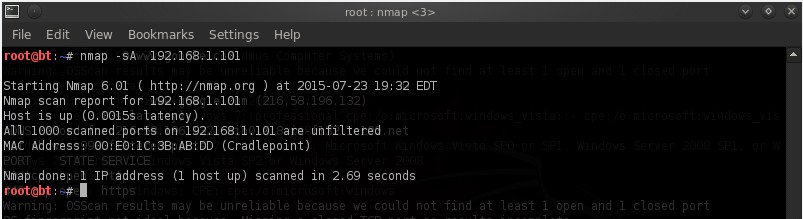
1. **Enable OS Detection with Nmap.**

# nmap -O 192.168.1.101

**Output:**

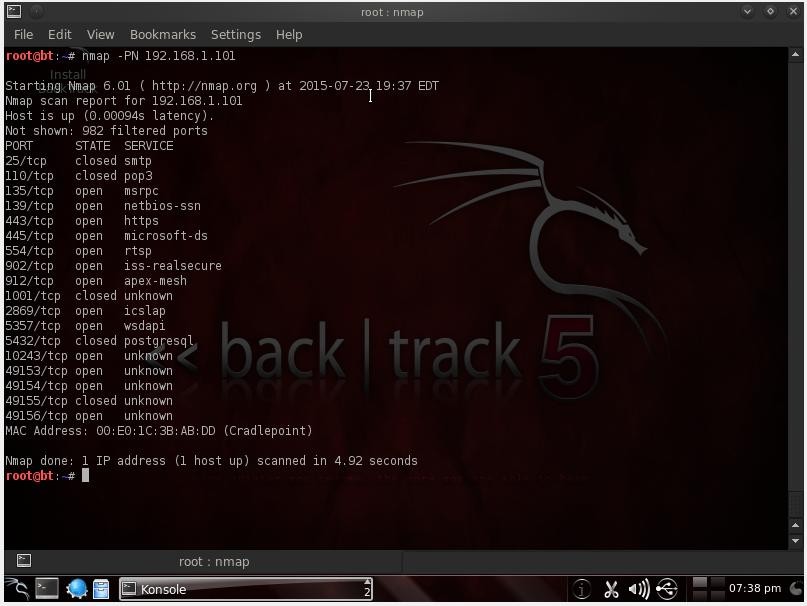
1. **Scan a Host to Detect Firewall.**

# nmap -sA 192.168.1.101

**Output:**

1. **Scan a Host to check its protected by Firewall.**

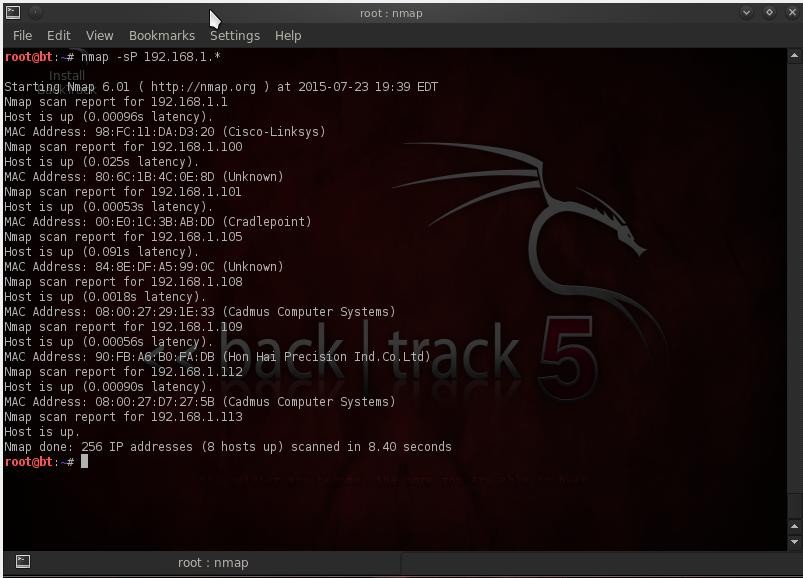
# nmap -PN 192.168.1.101

**Output:**

1. **Find out Live hosts in a Network**

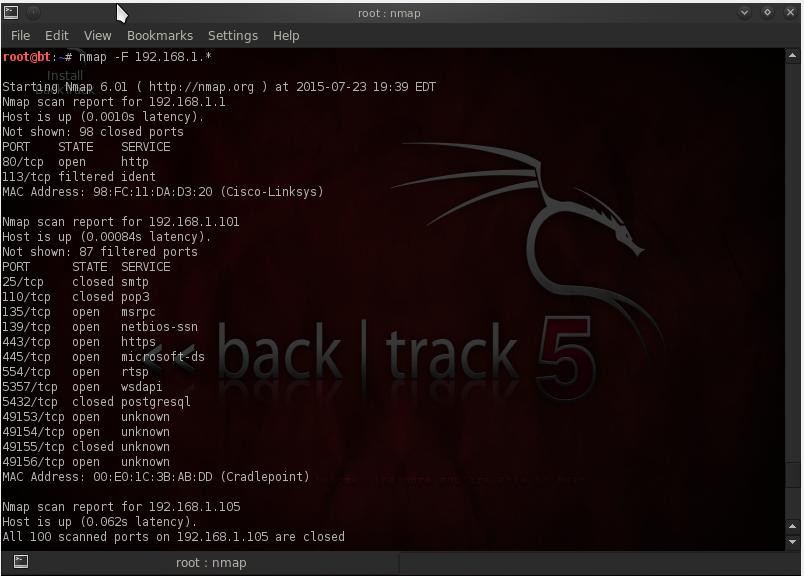
# nmap -sP 192.168.1.\*

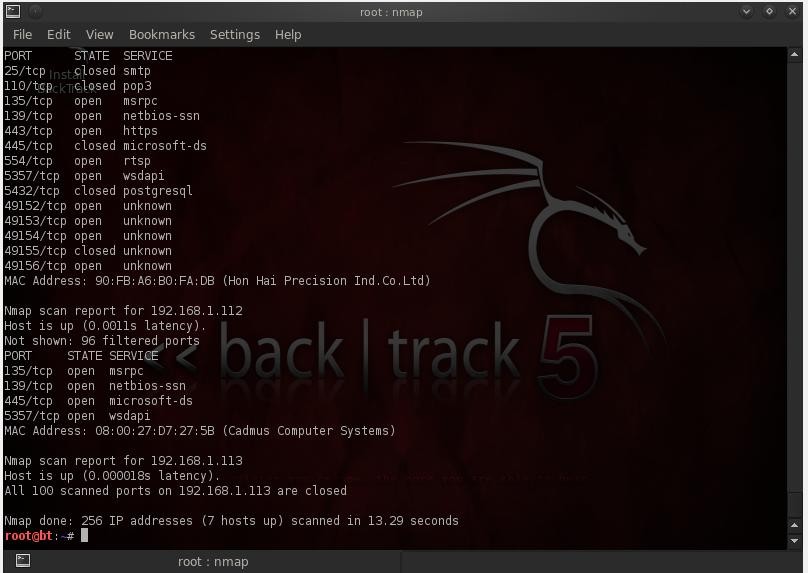
**Output:**

****

1. **Perform a Fast Scan.**

# nmap -F 192.168.1.\*

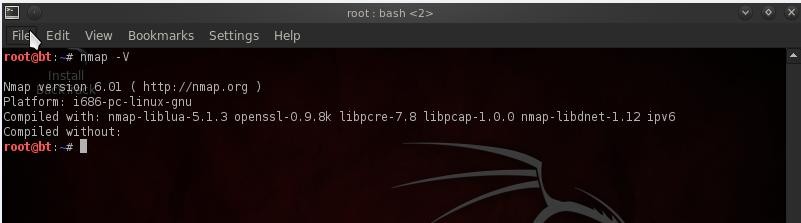
**Output**



1. **Find Nmap version.**

# nmap -V

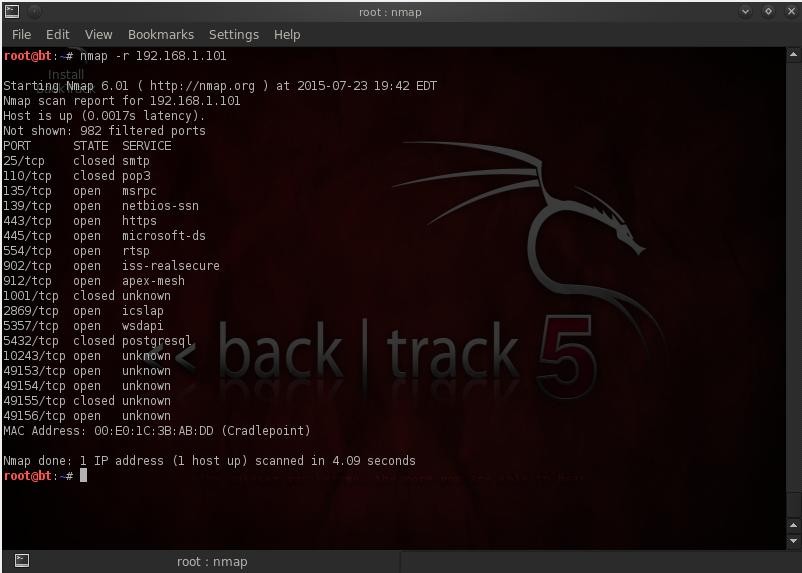
**Output:**

****

1. **Scan Ports Consecutively.**

# nmap -r 192.168.1.101

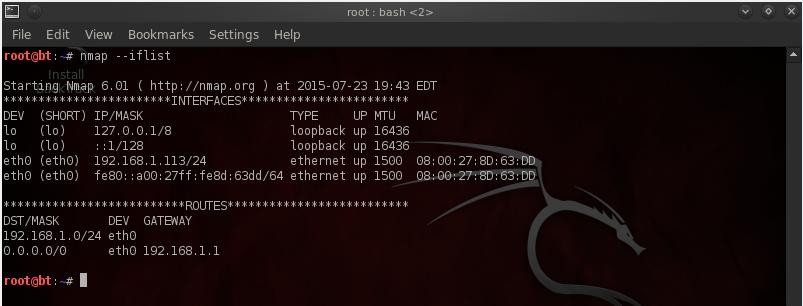
**Output:**

****

1. **Print Host interfaces and Routes.**

# nmap -- iflist

**Output:**

****

1. **Scan for specific Port.**

There are various options to discover ports on remote machine with Nmap. We can specify the port we want nmap to scan with **-p** option, by default nmap scans only TCP ports.

# namp –p 25 192.168.1.101

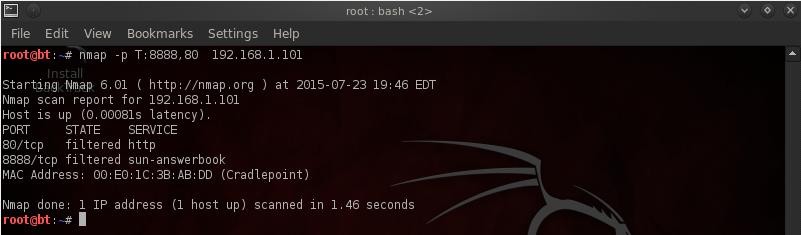
**Output:**

****

1. **Scan a TCP Port.**

# nmap –p T:8080,80 192.168.1.101

**Output:**

****

1. **Scan a UDP Port.**

# nmap –sU 192.168.1.101

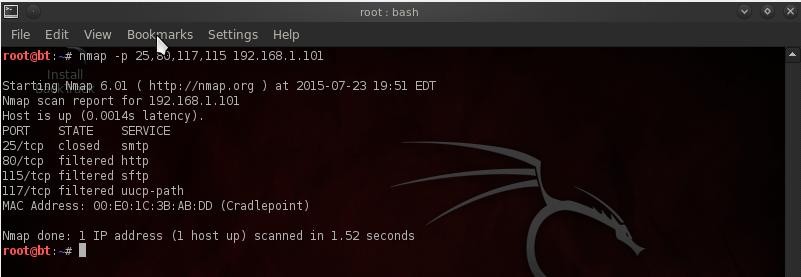
**Output:**

****

1. **Scan Multiple Ports.**

# nmap –p 25,80,117,115 192.168.1.101

**Output:**

****

1. **Scan Ports by Network Range.**

# nmap –p 1-300 192.168.1.101

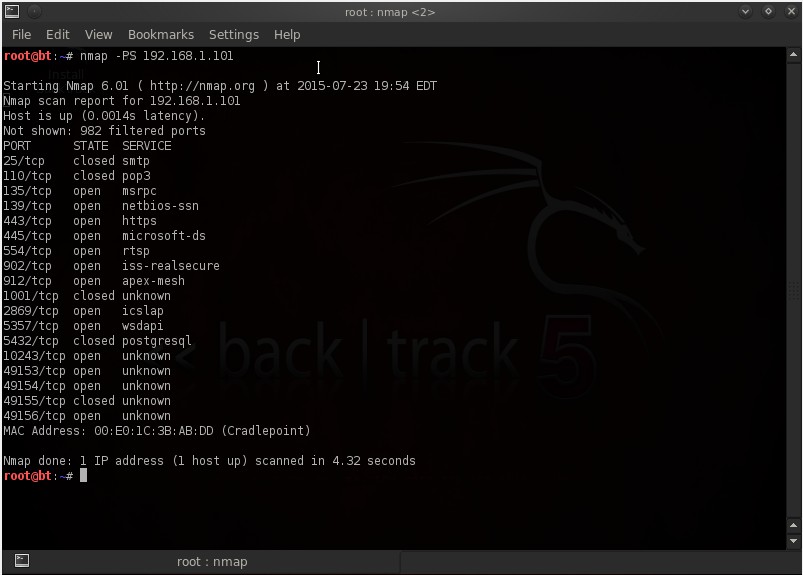
**Output:**

****

1. **Scan remote hosts using TCP ACK (PA) and TCP Syn (PS).**

# nmap –PS 192.168.1.101

**Output:**

****

1. **Scan Remote host for specific ports with TCP ACK.**

# nmap –PA –p 80 192.168.1.101

**Output:**

****

1. **Scan Remote host for specific ports with TCP Syn.**

# nmap –PA –p 80 192.168.1.101

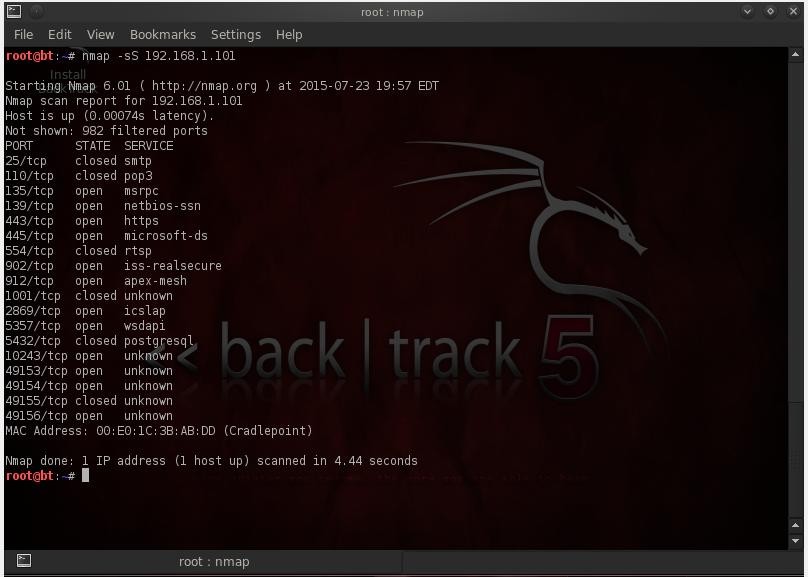
**Output:**

****

1. **Perform a stealthy Scan.**

# nmap –sS 192.168.1.101

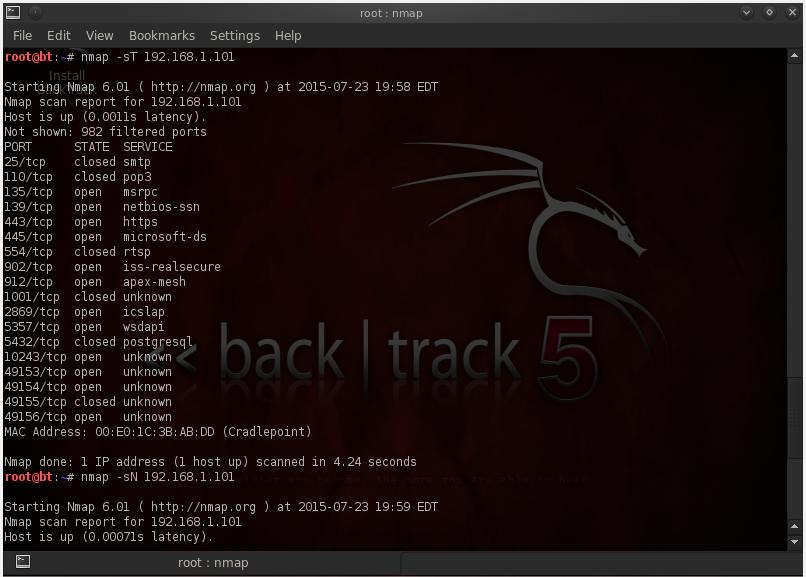
**Output:**

****

1. **Check most commonly used Ports with TCP Syn**

# nmap –sT 192.168.1.101

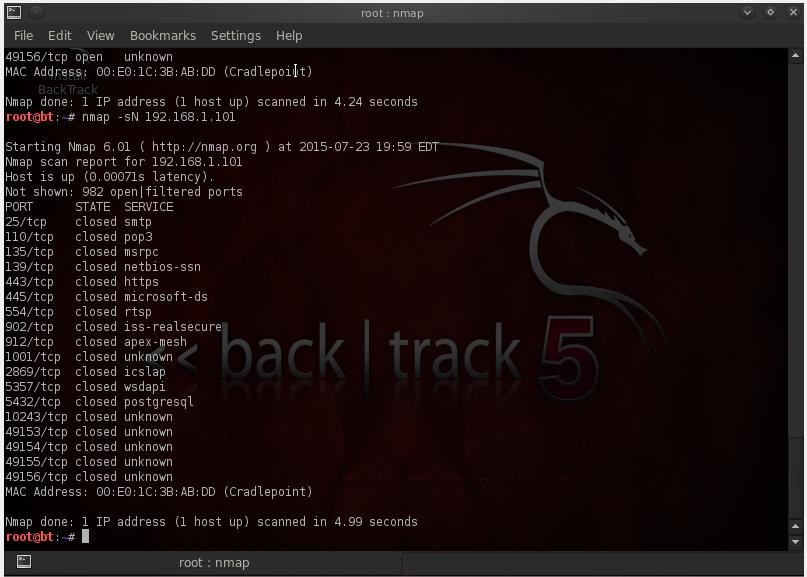
**Output:**

****

1. **Perform a tcp null scan to fool a firewall.**

# nmap –sN 192.168.1.101

**Output:**

****

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Port no.** | **Services** | **Application** | **Vulnerability** | **Exploit** |
| 80: TCP, UDP | HTTP, WWW | Hyper Text Transfer Protocol (HTTP) - port used for web traffic.  Hypertext Transfer Protocol (HTTP) (official) | Weak | Trojan(711 trojan, AckCmd BlueFire Cafeini Duddie Executor, God Message Seeker Slapper WebServerCT (WebDownlo ader) |
| 25: TCP, UDP | SMTP | SMTP (Simple Mail Transfer Protocol). Many worms contain their own SMTP engine and use it to propagate by mass- mailing the payload, often also spoofing the "From: ..." field in emails. | Weak | Antigen Barok BSE  EmailPasswordSender EPSII  Gip Gris Happy99 Hpteammail Hybris Iloveyou Kuang2 MagicHorse MBTMailBombingTrojan |
| 110: TCP, UDP | POP3 | POP3 (Post Office Protocol - Version 3) Re-usable cleartext password, no auditing of connections & attempts thus subject to grinding. Some POP3 server versions have had buffer overflow problems. | Weak | Trojan Pro-MailTrojan Bancos  Civcat |
| 135: TCP, UDP | Loc-srv Msrpc Epmap | Remote Procedure Call (RPC) port 135 is used in client/server applications (might be on a single machine) such as Exchange clients, the recently exploited messenger service, as well as other Windows NT/2K/XP software. | weak | W32.Kiman Femot  W32.Blaster.Worm W32.Francette.Worm W32.Mytob |
| 139: TCP, UDP | Net-Bios ss | NetBIOS is a protocol used for File and Print Sharing under all current versions of Windows. While this in itself is not a problem, the way that the protocol is implemented can be.  There are a number of vulnerabilities associated with leaving this port open.  **NetBios services:** NETBIOS Session | Weak | Trojan: Chode, God Message Worm Msinit Network Qaz Sadmind SMB Relay |
| 443: TCP, SCTP | HTTPS  Games Application (AIMVIDEIM  ,Battlefieldetc) | HTTPS / SSL - encrypted web traffic. ASUS AiCloud routers file sharing service uses ports 443 and 8082. | Weak | Civcat Tabdim W32.Kelvir |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Port no.** | **Services** | **Application** | **Vulnerability** | **Exploit** |
| 445 | Microsoft- ds | TCP port 445 is used for direct TCP/IP MS Networking access without the need for a NetBIOS layer. This service is only implemented in the more recent verions of Windows (e.g. Windows 2K / XP). The SMB  (Server Message Block) protocol is used among other things for file sharing in Windows NT/2K/XP. | weak | Otinet Rtkit Secefa W32.Aizu  W32.Bobax W32.Bolgi.Worm W32.Cissi W32.Cycle W32.Explet  W32.HLLW.Deborms W32.HLLW.Deloder W32.HLLW.Gaobot W32.HLLW.Lioten W32.HLLW.Moega  W32.HLLW.Nebiwo W32.HLLW.Polybot |
| 902 | ideafarm- door ideafarm- chat  iss- realsecure | self-documenting Telnet Door  self-documenting Door: send 0x00 for info IDEAFARM-CHAT ISS RealSecure Sensor | Weak | Trojan(Net Devil Pest) |
| 903  Tcp,udp | ideafarm- door ideafarm- chat  iss- realsecure | self documenting Telnet Door  self documenting Door: send 0x00 for info IDEAFARM-CHAT ISS RealSecure Sensor | Weak | Trojan(Net Devil Pest) |