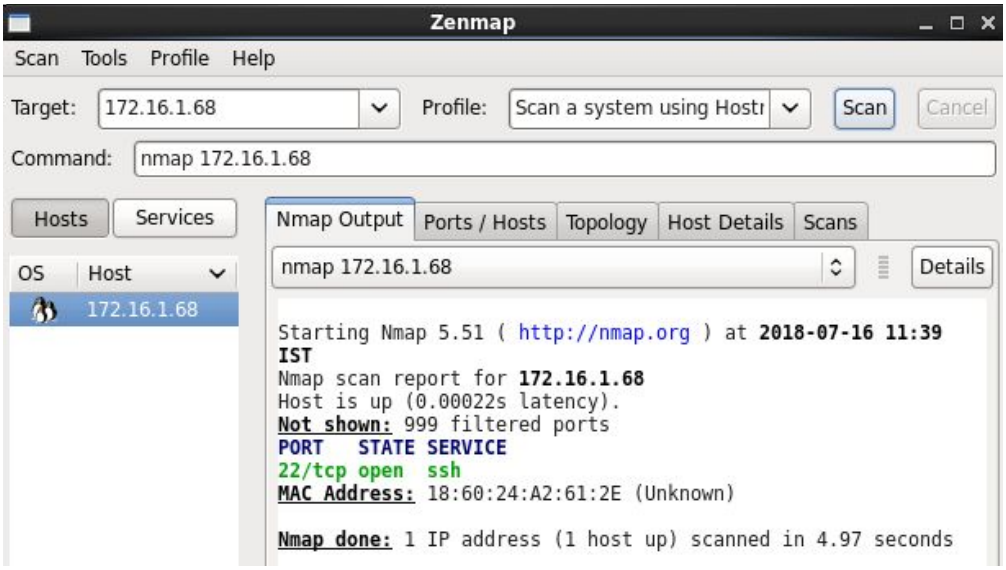
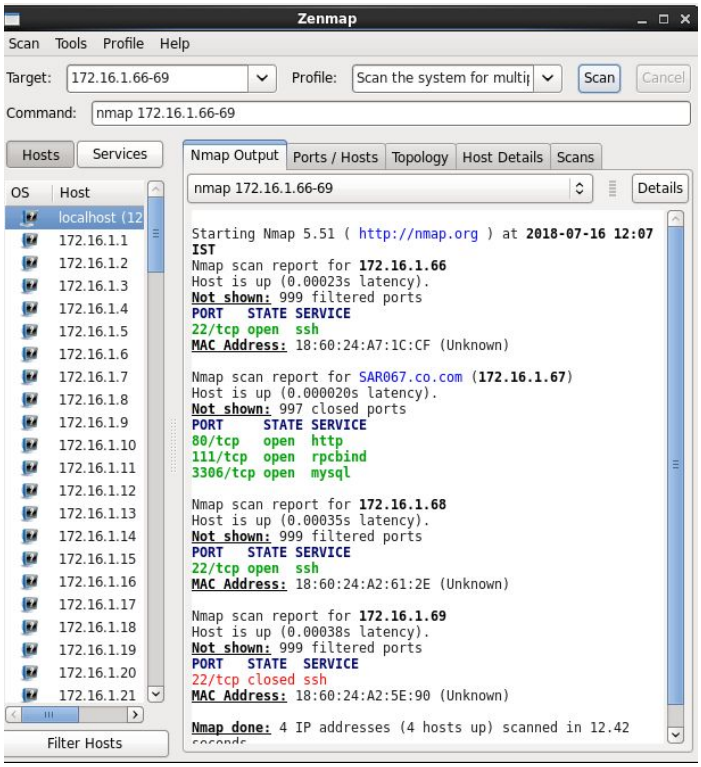
3.Perform Scan Using Zenmap

---

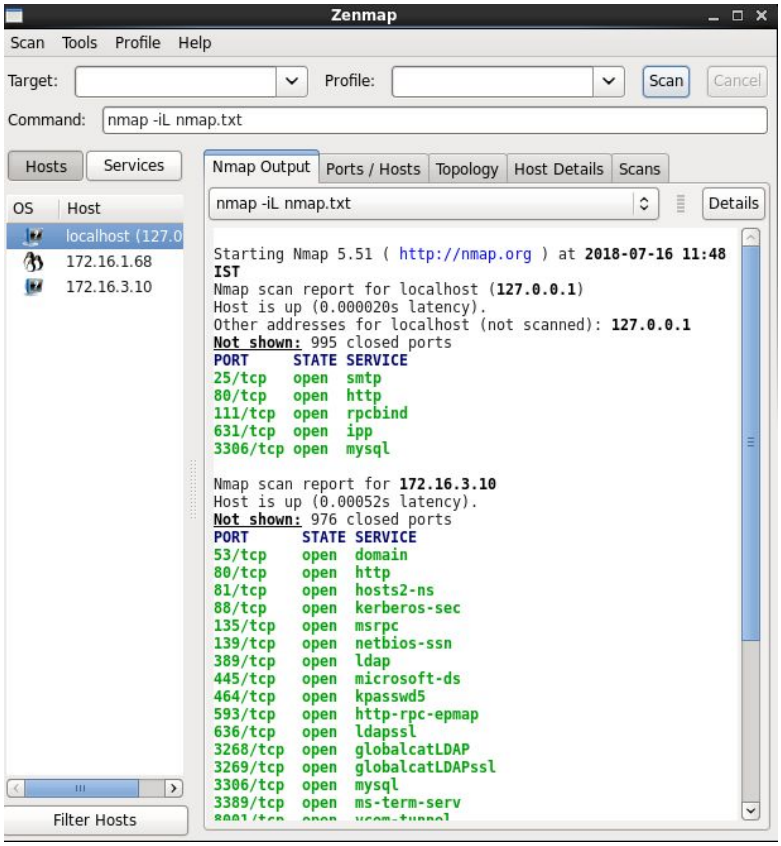
1) Scan a system using Hostname and IP address.



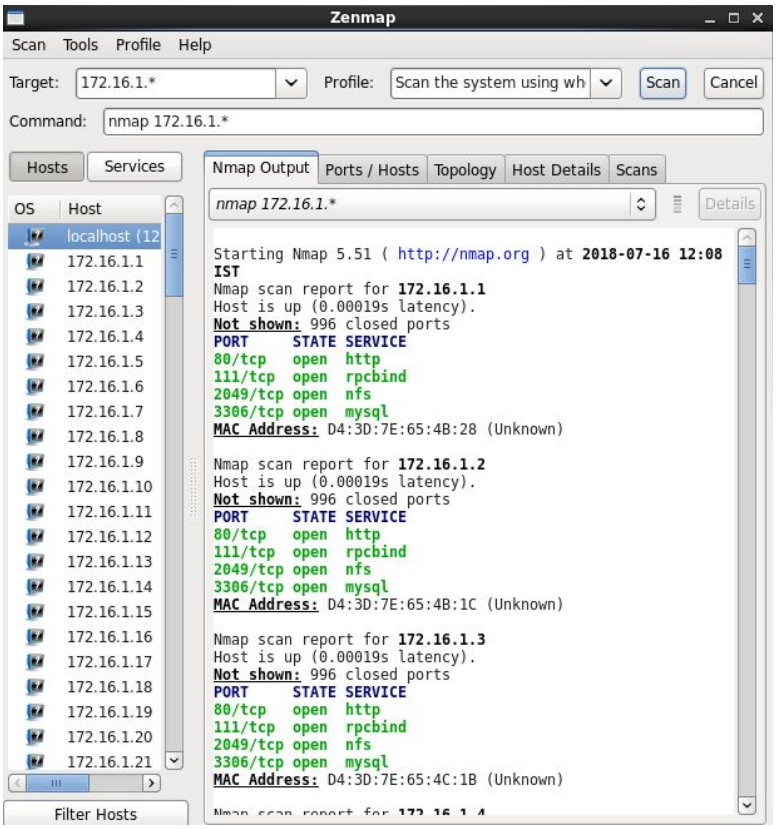
2) Scan the system for multiple host.



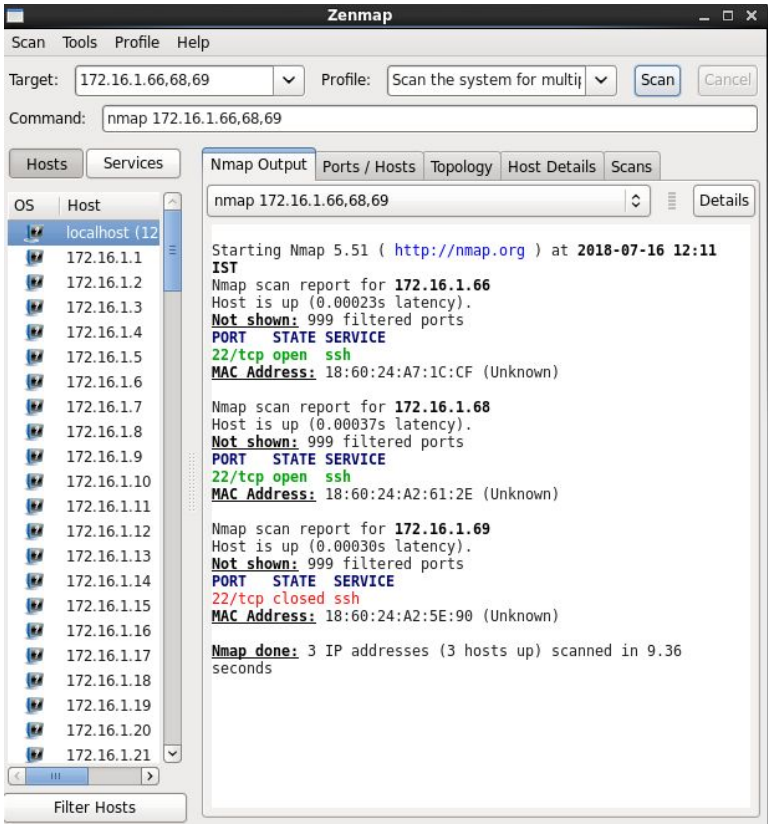
3) Scan the system for multiple host using file



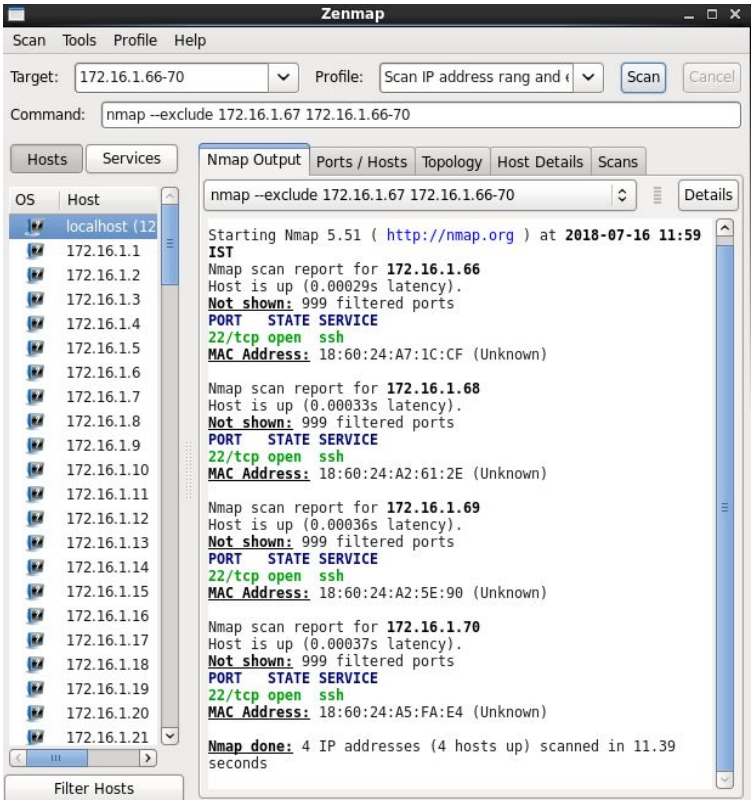
4) Scan the system using whole subnet mask.



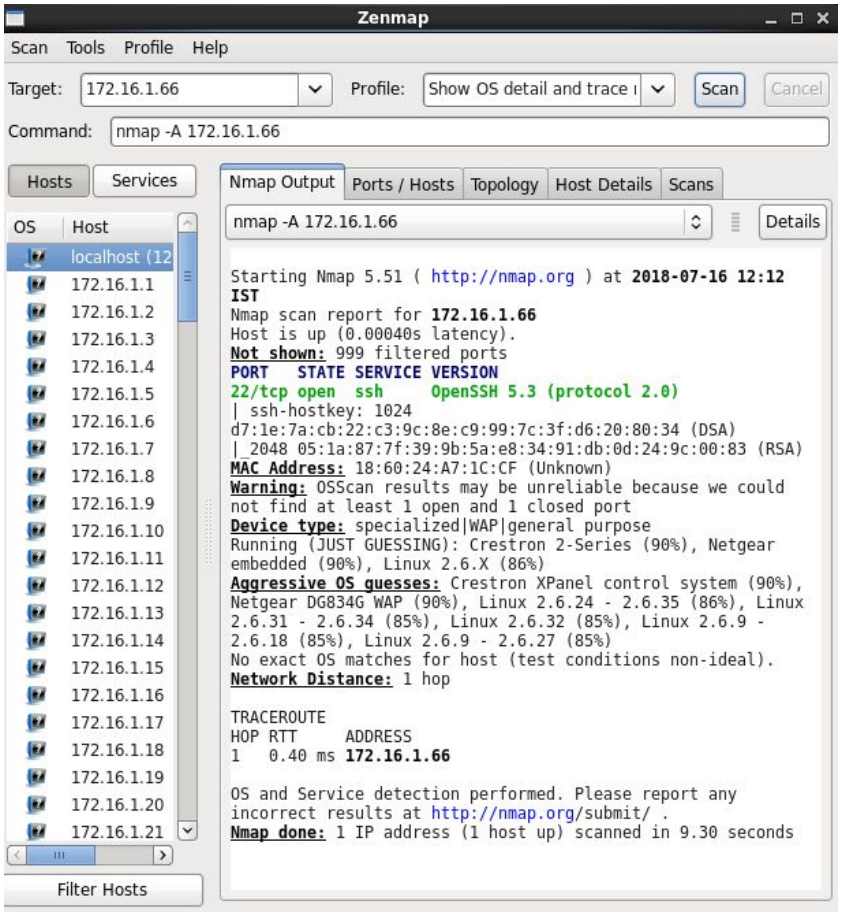
5) Scan the system for multiple system using last octet of IP address.



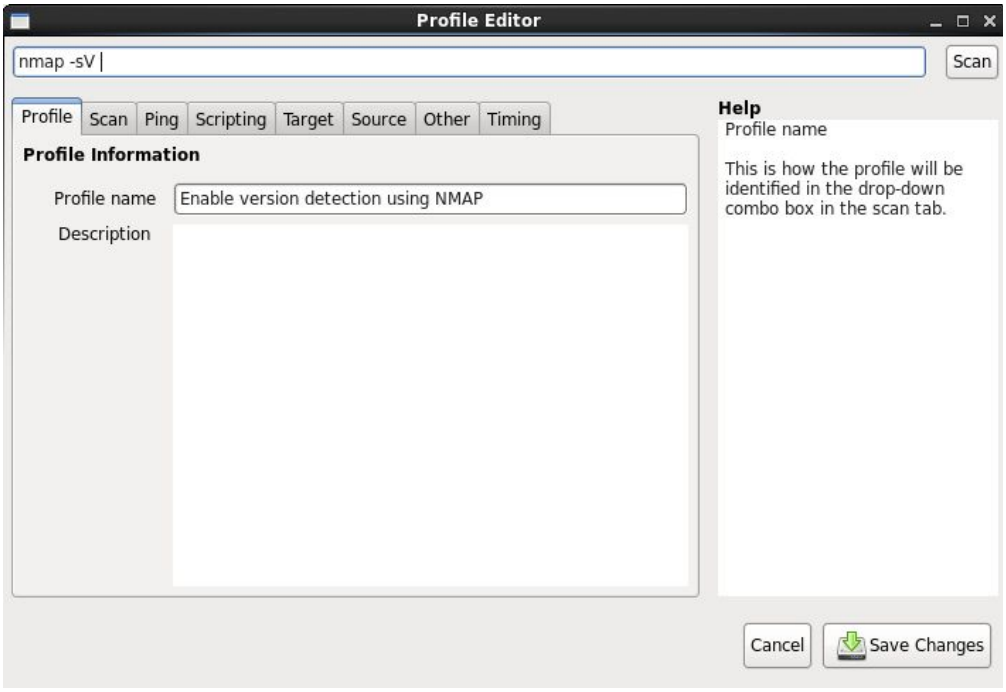
6) Scan IP address rang and excluding particular user

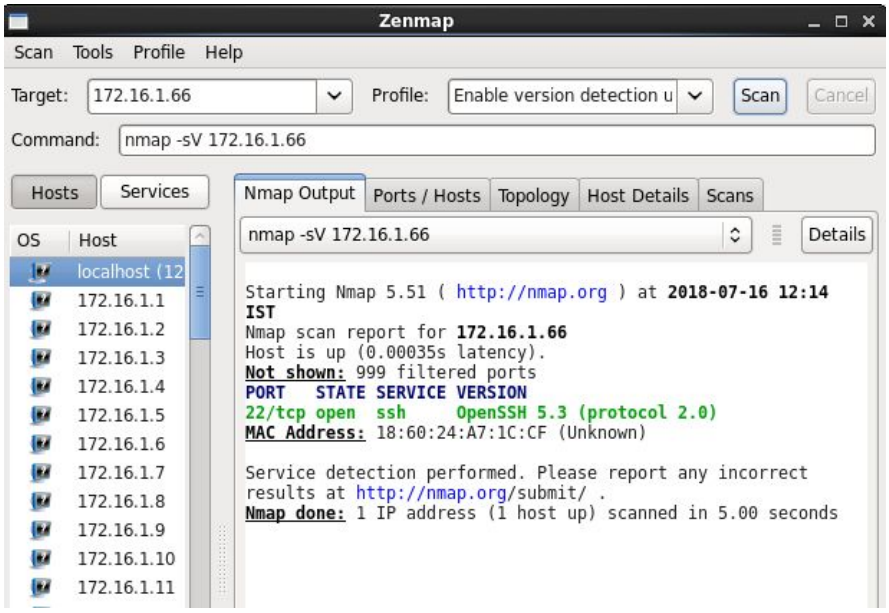


7) Show OS detail and trace route.

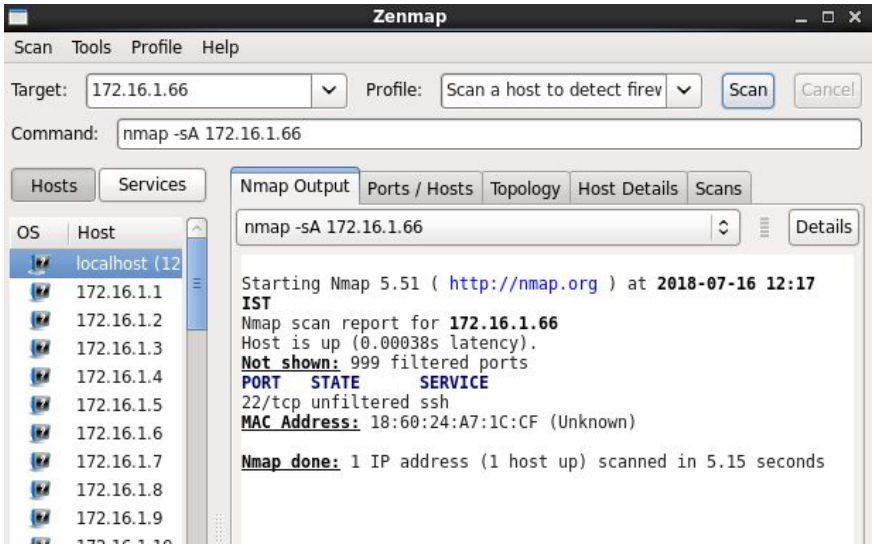


8) Enable version detection using NMAP.

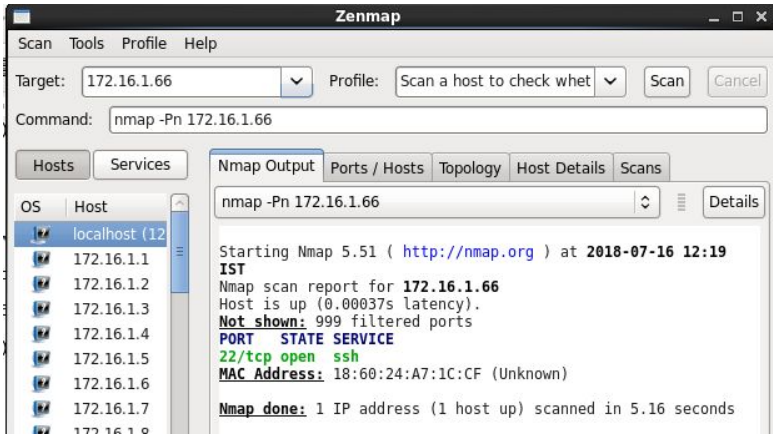




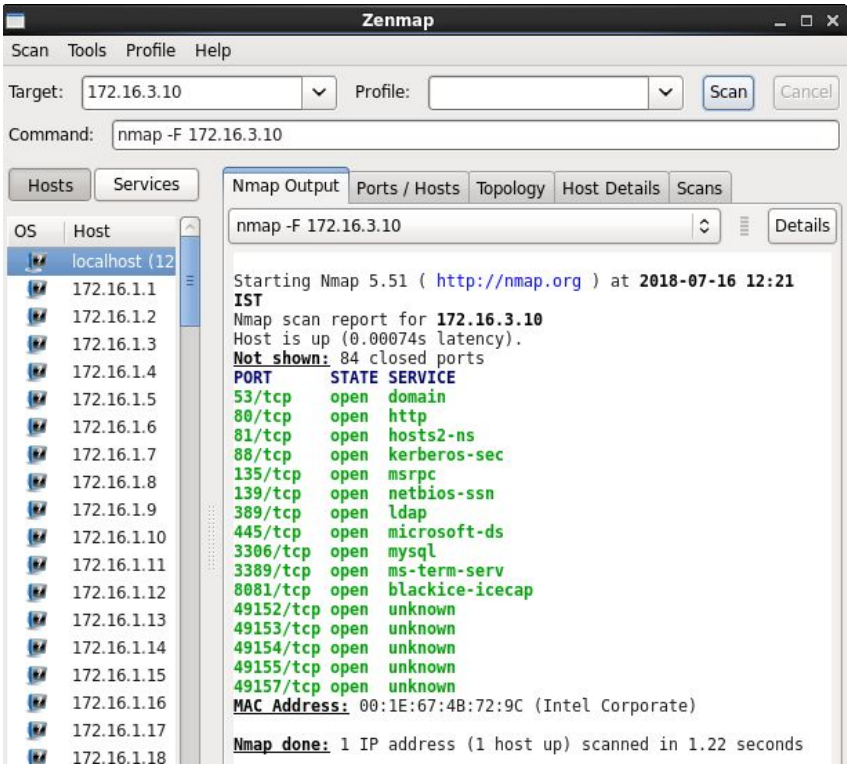
9) Scan a host to detect firewall.



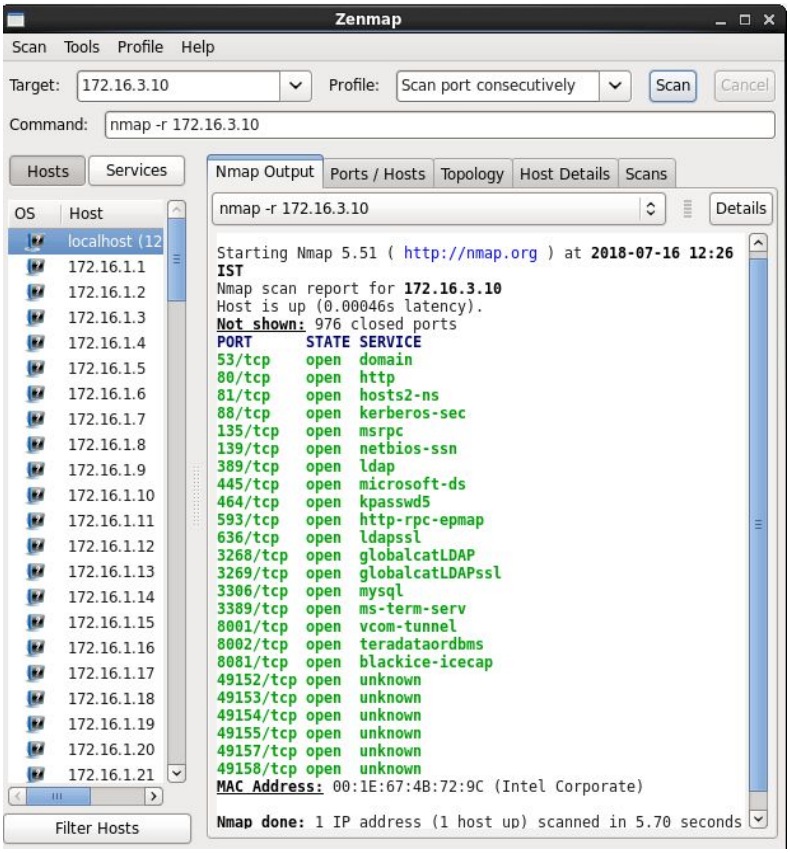
10) Scan a host to check whether its protected by a firewall or not



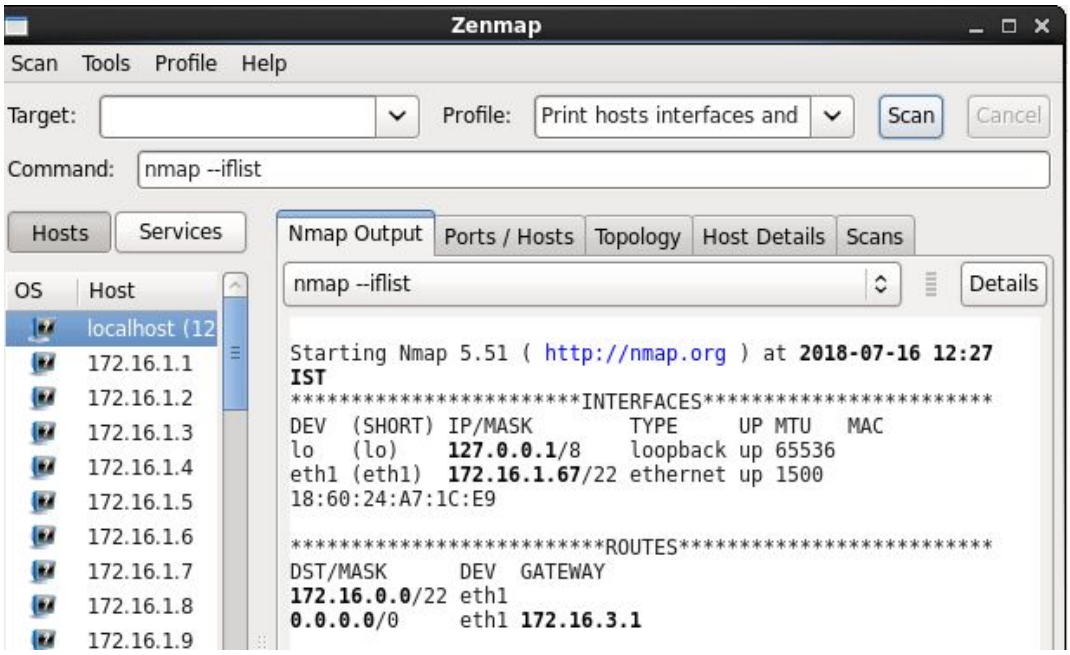
11) Perform fast scan using NMAP



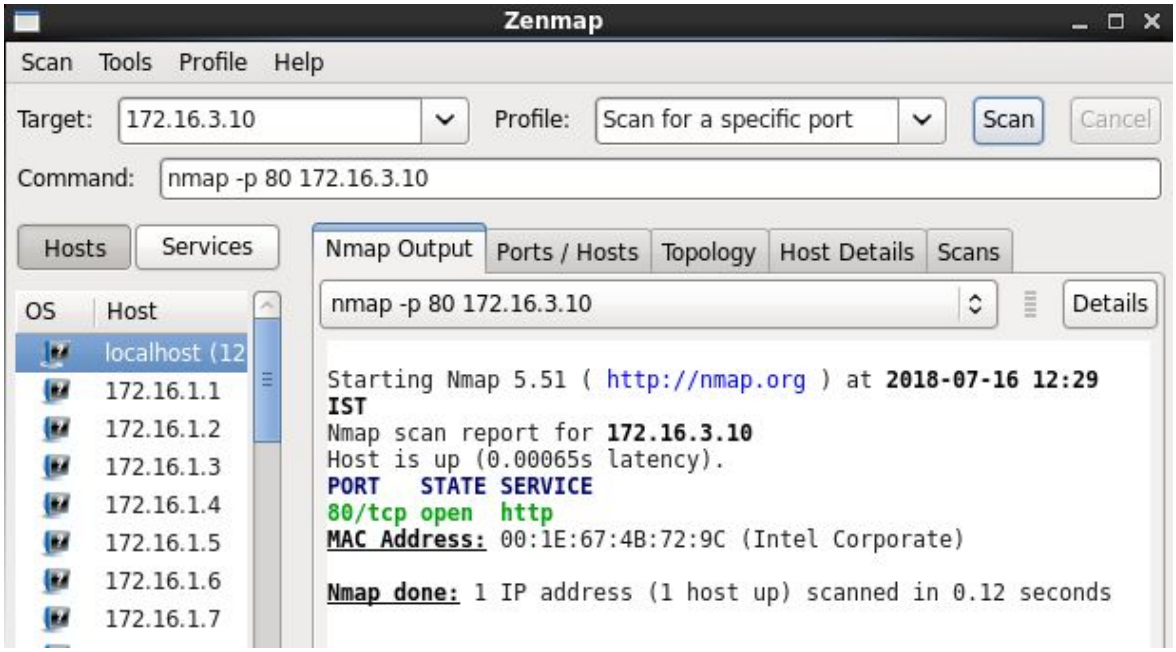
12) Scan port consecutively



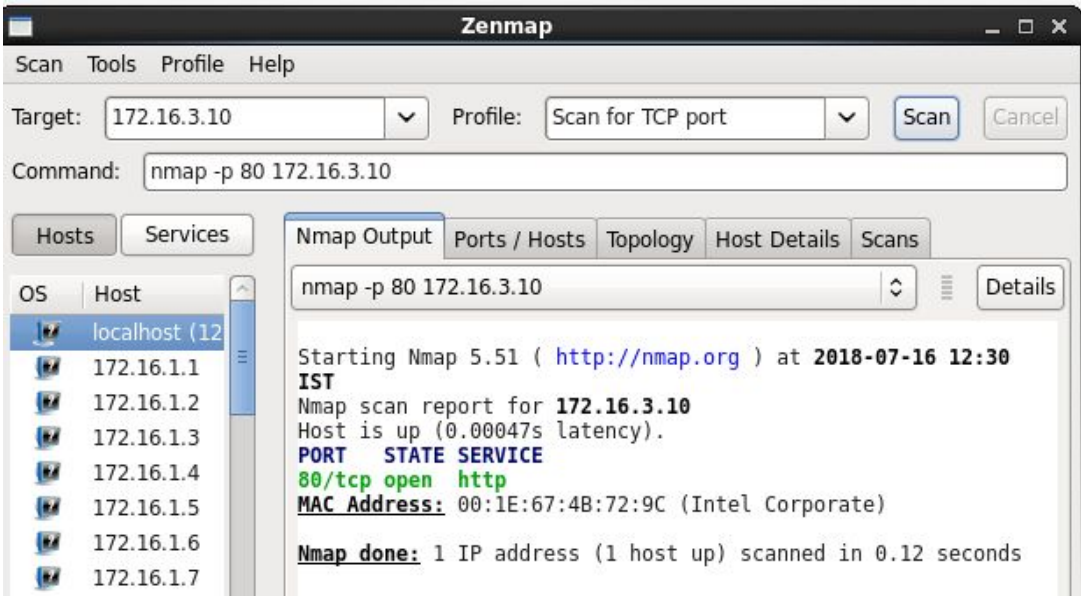
13) Print hosts interfaces and routes



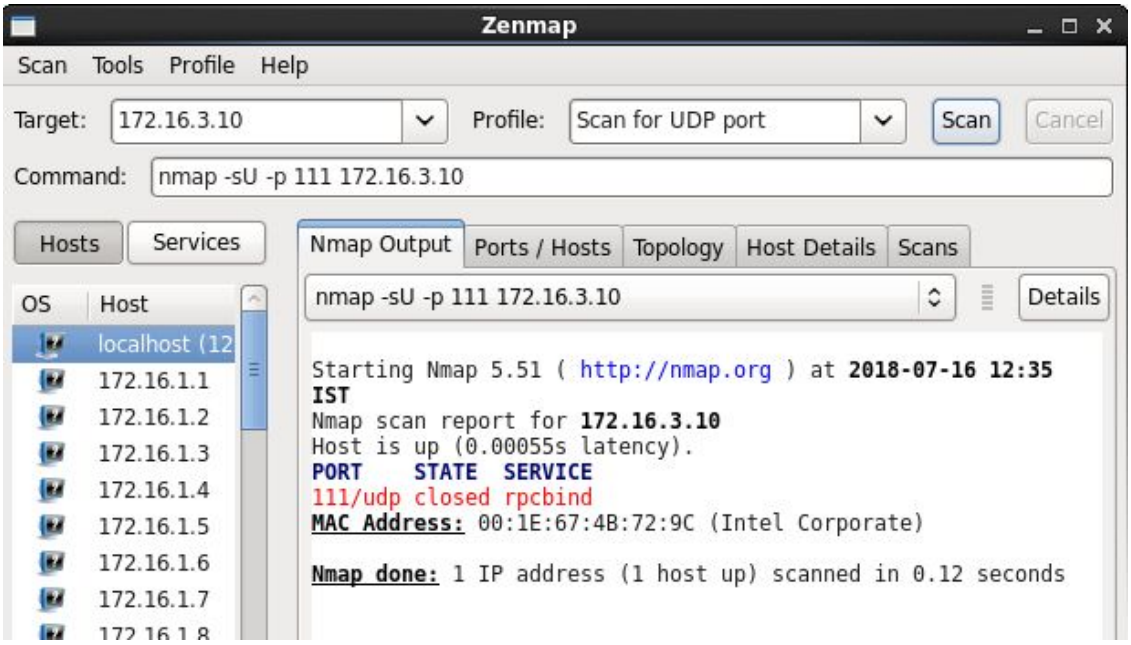
14) Scan for a specific port



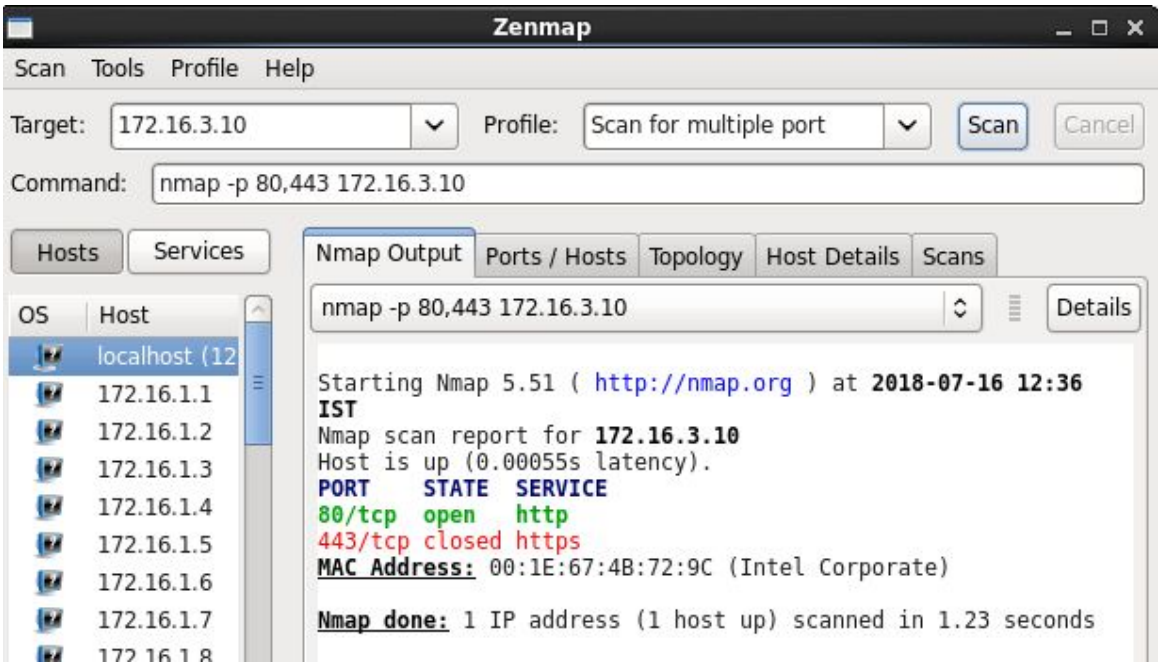
15) Scan for TCP port.



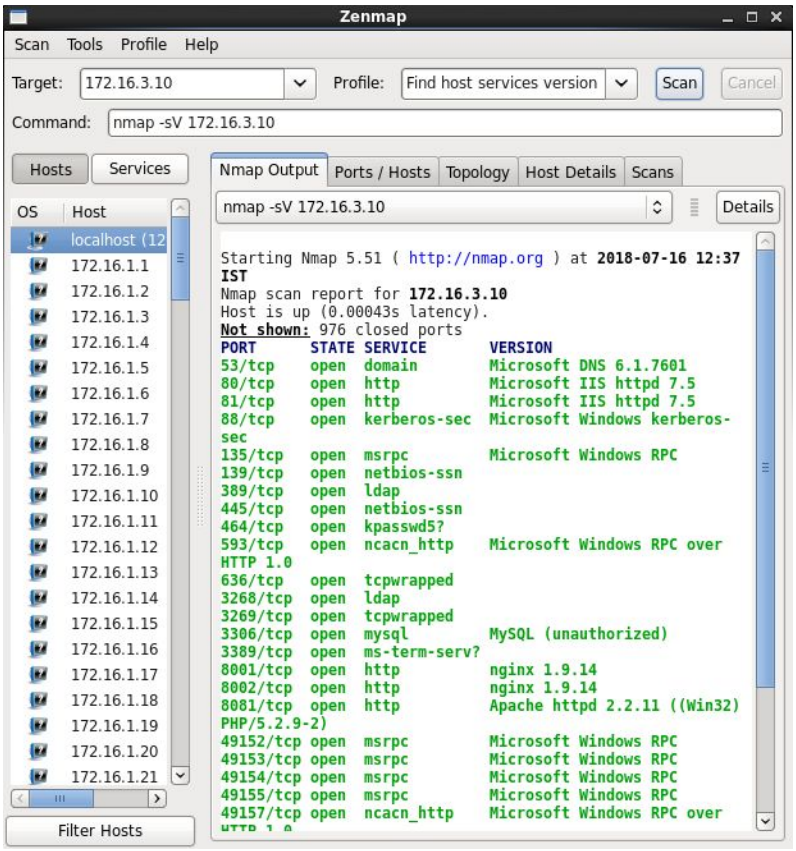
16) Scan for UDP port.



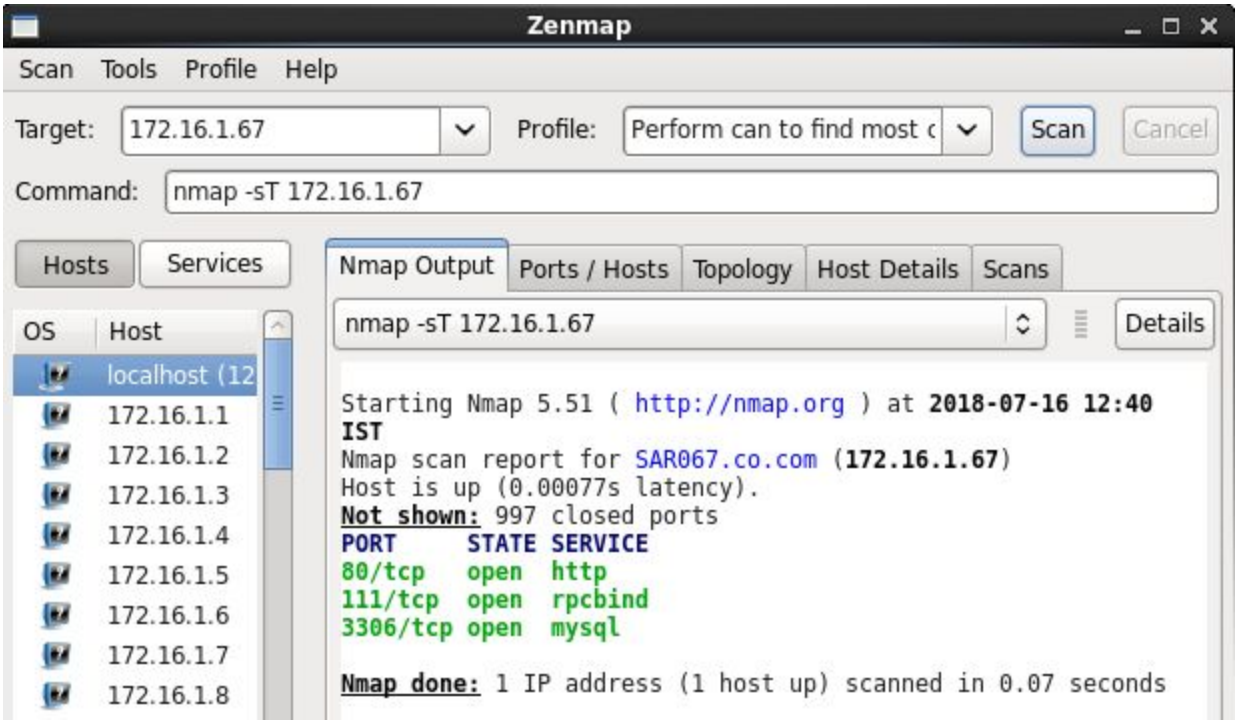
17) Scan for multiple port.



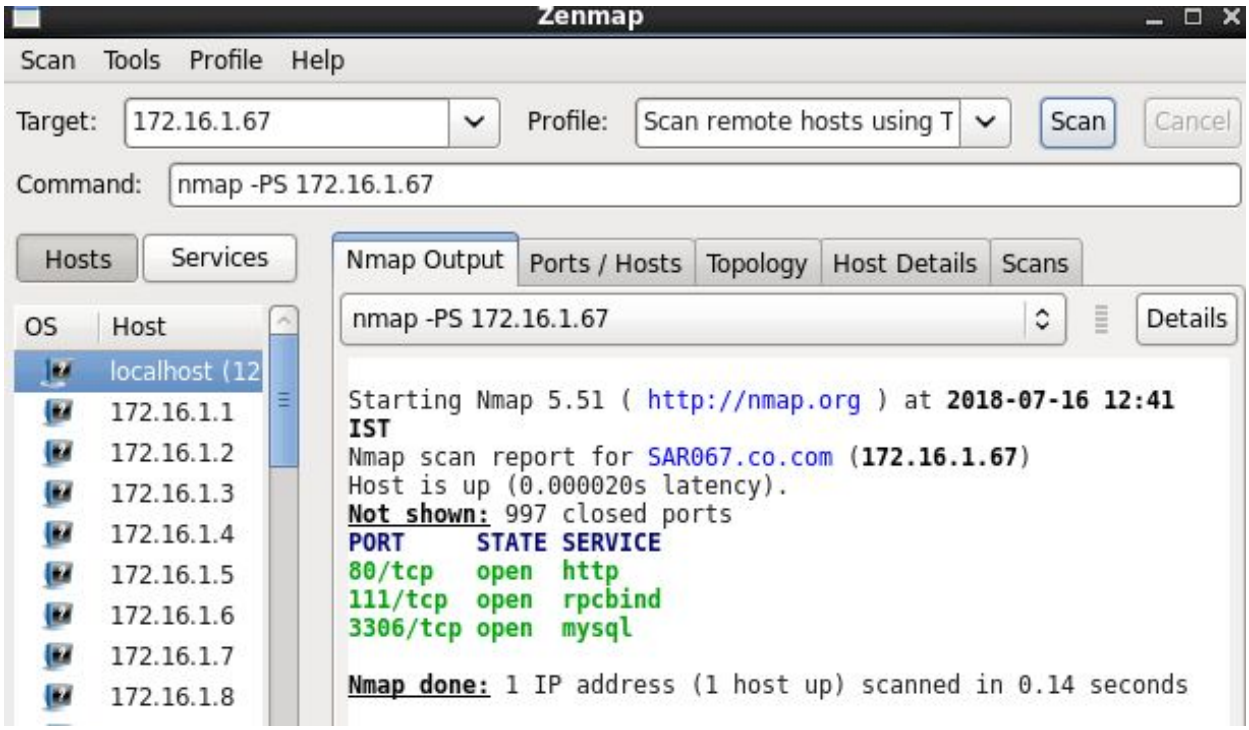
18) Find host services version no.



19) Perform can to find most commonly used ports using TCP syn.



20) Scan remote hosts using TCP ACK and TCP SYN.



4.TCP/UDP connectivity using Netcat

---

1. Write down the command to install NETCAT on CentOS.

Command: yum install netcat

2. Explain nc command with following options:

a) –v

Command: [root@SAR030 ~]# nc -v -z 172.16.1.30 22

Output :

Connection to 172.16.1.30 22 port [tcp/ssh] succeeded!
SSH -2.0-OpenSSH_5.3

b) –z

Command: [root@SAR030 ~]# nc -z 172.16.1.30 22

Output :

Connection to 172.16.1.30 22 port [tcp/ssh] succeeded!

c) **–w**

Command: [root@SAR030 ~]# nc -w 4 172.16.1.30 30

Output :

[root@SAR030 ~]# nc -w 0 172.16.1.30 30
[root@SAR030 ~]# nc -w 1.9 172.16.1.30 30
nc: timeout cannot be negative
[root@SAR030 ~]# nc -w 1 172.16.1.30 30

3. Perform a port scan using the TCP protocol. Show more verbose output than the default NETCAT setting, setup a timeout value of 5 seconds, and scan the port range 20 to 100. Write down the command along with output.

Command:

[root@SAR030 ~]# nc -v -w 5 172.16.1.30 20-100
nc: connect to 172.16.1.30 port 20 (tcp) failed: Connection refused
nc: connect to 172.16.1.30 port 21 (tcp) failed: Connection refused
Connection to 172.16.1.30 22 port [tcp/ssh] succeeded!
SSH-2.0-OpenSSH_5.3
nc: connect to 172.16.1.30 port 23 (tcp) failed: Connection refused
nc: connect to 172.16.1.30 port 24 (tcp) failed: Connection refused
nc: connect to 172.16.1.30 port 25 (tcp) failed: Connection refused
nc: connect to 172.16.1.30 port 26 (tcp) failed: Connection refused
nc: connect to 172.16.1.30 port 27 (tcp) failed: Connection refused
nc: connect to 172.16.1.30 port 28 (tcp) failed: Connection refused
nc: connect to 172.16.1.30 port 29 (tcp) failed: Connection refused
nc: connect to 172.16.1.30 port 30 (tcp) failed: Connection refused
nc: connect to 172.16.1.30 port 31 (tcp) failed: Connection refused
nc: connect to 172.16.1.30 port 32 (tcp) failed: Connection refused

```
nc: connect to 172.16.1.30 port 33 (tcp) failed: Connection refused
nc: connect to 172.16.1.30 port 34 (tcp) failed: Connection refused
nc: connect to 172.16.1.30 port 35 (tcp) failed: Connection refused
nc: connect to 172.16.1.30 port 36 (tcp) failed: Connection refused
nc: connect to 172.16.1.30 port 37 (tcp) failed: Connection refused
nc: connect to 172.16.1.30 port 38 (tcp) failed: Connection refused
nc: connect to 172.16.1.30 port 39 (tcp) failed: Connection refused
nc: connect to 172.16.1.30 port 40 (tcp) failed: Connection refused
nc: connect to 172.16.1.30 port 41 (tcp) failed: Connection refused
nc: connect to 172.16.1.30 port 42 (tcp) failed: Connection refused
nc: connect to 172.16.1.30 port 43 (tcp) failed: Connection refused
nc: connect to 172.16.1.30 port 44 (tcp) failed: Connection refused
nc: connect to 172.16.1.30 port 45 (tcp) failed: Connection refused
nc: connect to 172.16.1.30 port 46 (tcp) failed: Connection refused
nc: connect to 172.16.1.30 port 47 (tcp) failed: Connection refused
nc: connect to 172.16.1.30 port 48 (tcp) failed: Connection refused
nc: connect to 172.16.1.30 port 49 (tcp) failed: Connection refused
nc: connect to 172.16.1.30 port 50 (tcp) failed: Connection refused
nc: connect to 172.16.1.30 port 51 (tcp) failed: Connection refused
nc: connect to 172.16.1.30 port 52 (tcp) failed: Connection refused
nc: connect to 172.16.1.30 port 53 (tcp) failed: Connection refused
nc: connect to 172.16.1.30 port 54 (tcp) failed: Connection refused
nc: connect to 172.16.1.30 port 55 (tcp) failed: Connection refused
nc: connect to 172.16.1.30 port 56 (tcp) failed: Connection refused
nc: connect to 172.16.1.30 port 57 (tcp) failed: Connection refused
nc: connect to 172.16.1.30 port 58 (tcp) failed: Connection refused
nc: connect to 172.16.1.30 port 59 (tcp) failed: Connection refused
nc: connect to 172.16.1.30 port 60 (tcp) failed: Connection refused
nc: connect to 172.16.1.30 port 61 (tcp) failed: Connection refused
nc: connect to 172.16.1.30 port 62 (tcp) failed: Connection refused
nc: connect to 172.16.1.30 port 63 (tcp) failed: Connection refused
nc: connect to 172.16.1.30 port 64 (tcp) failed: Connection refused
nc: connect to 172.16.1.30 port 65 (tcp) failed: Connection refused
nc: connect to 172.16.1.30 port 66 (tcp) failed: Connection refused
nc: connect to 172.16.1.30 port 67 (tcp) failed: Connection refused
nc: connect to 172.16.1.30 port 68 (tcp) failed: Connection refused
nc: connect to 172.16.1.30 port 69 (tcp) failed: Connection refused
nc: connect to 172.16.1.30 port 70 (tcp) failed: Connection refused
nc: connect to 172.16.1.30 port 71 (tcp) failed: Connection refused
nc: connect to 172.16.1.30 port 72 (tcp) failed: Connection refused
nc: connect to 172.16.1.30 port 73 (tcp) failed: Connection refused
nc: connect to 172.16.1.30 port 74 (tcp) failed: Connection refused
nc: connect to 172.16.1.30 port 75 (tcp) failed: Connection refused
nc: connect to 172.16.1.30 port 76 (tcp) failed: Connection refused
nc: connect to 172.16.1.30 port 77 (tcp) failed: Connection refused
nc: connect to 172.16.1.30 port 78 (tcp) failed: Connection refused
nc: connect to 172.16.1.30 port 79 (tcp) failed: Connection refused
```

```
nc: connect to 172.16.1.30 port 80 (tcp) failed: Connection refused
nc: connect to 172.16.1.30 port 81 (tcp) failed: Connection refused
nc: connect to 172.16.1.30 port 82 (tcp) failed: Connection refused
nc: connect to 172.16.1.30 port 83 (tcp) failed: Connection refused
nc: connect to 172.16.1.30 port 84 (tcp) failed: Connection refused
nc: connect to 172.16.1.30 port 85 (tcp) failed: Connection refused
nc: connect to 172.16.1.30 port 86 (tcp) failed: Connection refused
nc: connect to 172.16.1.30 port 87 (tcp) failed: Connection refused
nc: connect to 172.16.1.30 port 88 (tcp) failed: Connection refused
nc: connect to 172.16.1.30 port 89 (tcp) failed: Connection refused
nc: connect to 172.16.1.30 port 90 (tcp) failed: Connection refused
nc: connect to 172.16.1.30 port 91 (tcp) failed: Connection refused
nc: connect to 172.16.1.30 port 92 (tcp) failed: Connection refused
nc: connect to 172.16.1.30 port 93 (tcp) failed: Connection refused
nc: connect to 172.16.1.30 port 94 (tcp) failed: Connection refused
nc: connect to 172.16.1.30 port 95 (tcp) failed: Connection refused
nc: connect to 172.16.1.30 port 96 (tcp) failed: Connection refused
nc: connect to 172.16.1.30 port 97 (tcp) failed: Connection refused
nc: connect to 172.16.1.30 port 98 (tcp) failed: Connection refused
nc: connect to 172.16.1.30 port 99 (tcp) failed: Connection refused
nc: connect to 172.16.1.30 port 100 (tcp) failed: Connection refused
```

4. Write down below what port numbers that were detected as Open

Port 22.

5. Perform the same task as Q.3 but use the UDP protocol instead of the TCP protocol. Write down the syntax used below.

Command: [root@SAR030 ~]# nc -v -u 172.16.1.30 20-100

Command: [root@SAR030 ~]# nc -u -z 172.16.1.29 100-120
Connection to 172.16.1.29 111 port [udp/ sunrpc] succeeded!

6. As you have seen in your previous tasks, scanning could be very noisy on a network. You will most likely be detected by any anomaly or intrusion detection devices. In order to do this smartly, you will slow down your scan and use an interval of 5 second between probe and you will randomize your port numbers as well. Write down the syntax below.

Command: [root@SAR030 ~]# nc -v -u -r -w 5 172.16.1.30 20-100

Command: [root@SAR030 ~]# nc -u -w 5 -z 172.16.1.29 100-120
Connection to 172.16.1.29 111 port [udp/ sunrpc] succeeded!

7. Using the ports that were identified in your TCP scan above, perform banner grabbing to see what could be the applications running on those ports. Do this for all of the TCP ports that were detected. Write your results below.

[root@SAR030]# nc 172.16.1.31 80
HEAD HTTP/1.0
HTTP/1.1 408 Request Timeout
Date: Fri, 03 Aug 2018 07:11:14 GMT
Server: Apache/2.4.6 (Centos) OpenSSL/1.0. le-fips mod auth assapi/1.4.0 mod fcgi
d/2.3.9 mod_nss/1.0.14 NSS/3.21 Basic ECC PHP/5.4.16 mod_wsgi/3.4 Python/2.7.5
Connection: close
Content-Type: text/html; charset=iso-8859-1

8. Establish a chatting mechanism using NETCAT commands (Pair wise activity).Be aware that ports like21, 80 might already be used. Pick a random port above 1024 for better results. Write down the commands used below.

Command:
Server
[root@SAR030 ~]# nc 172.16.1.30 3040
hi
hello

Client
[root@SAR029 ~]# nc -l 3040
hi
hello

9. Write the required commands to transfer a file from one machine to another using NETCAT.

Server :
[root@SAR030 ~]# nc -l 3040 > test.txt
[root@SAR030 ~]# cat test.txt

Client
[root@SAR029 ~] cat f1.txt | nc 172.16.1.31 3040