Information Gathering Tools-NMAP and ZenMAP

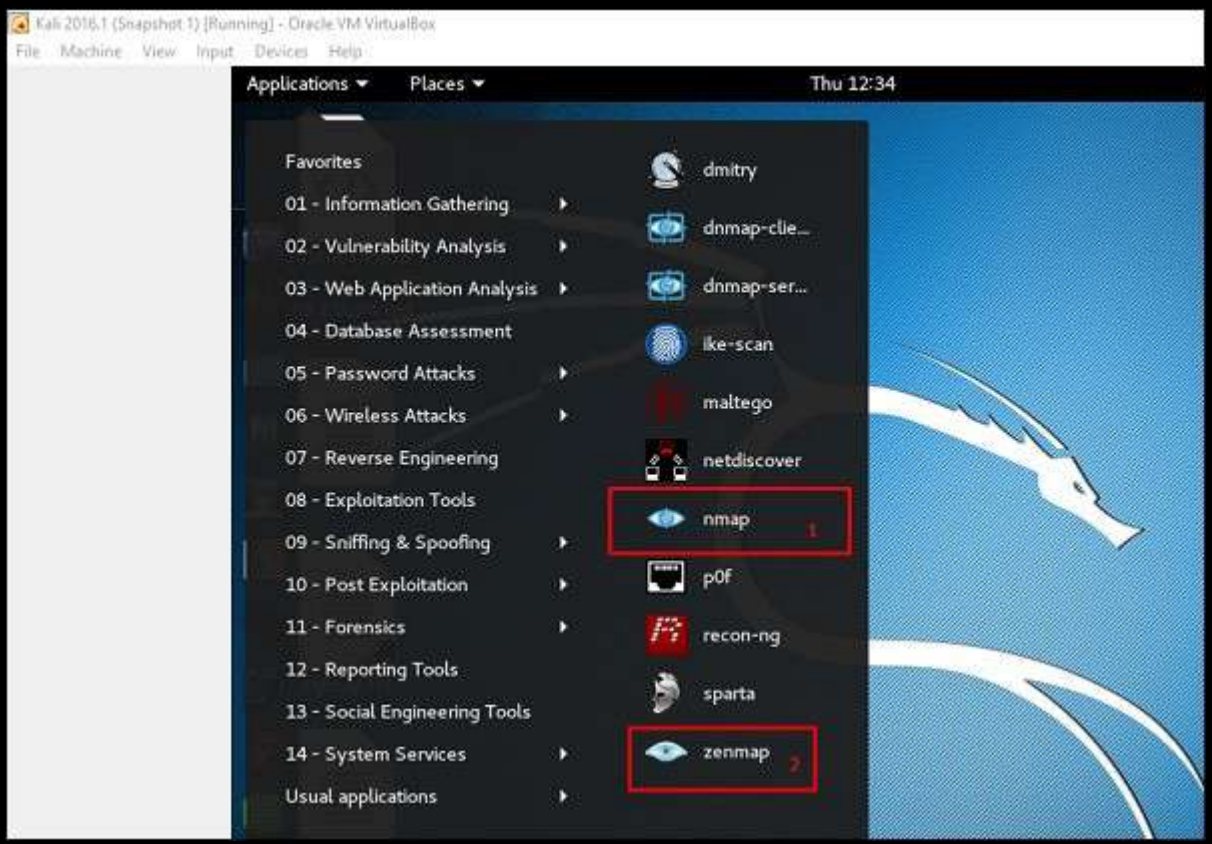
NMAP and ZenMAP are useful tools for the scanning phase of Ethical Hacking in Kali Linux. NMAP and ZenMAP are practically the same tool, however NMAP uses command line while ZenMAP has a GUI.

NMAP is a free utility tool for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.

NMAP uses raw IP packets in novel ways to determine which hosts are available on the network, what services (application name and version) those hosts are offering, which operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, etc.

Now, let's go step by step and learn how to use NMAP and ZenMAP.

Step 1 – To open, go to Applications → 01-Information Gathering → nmap or zenmap.

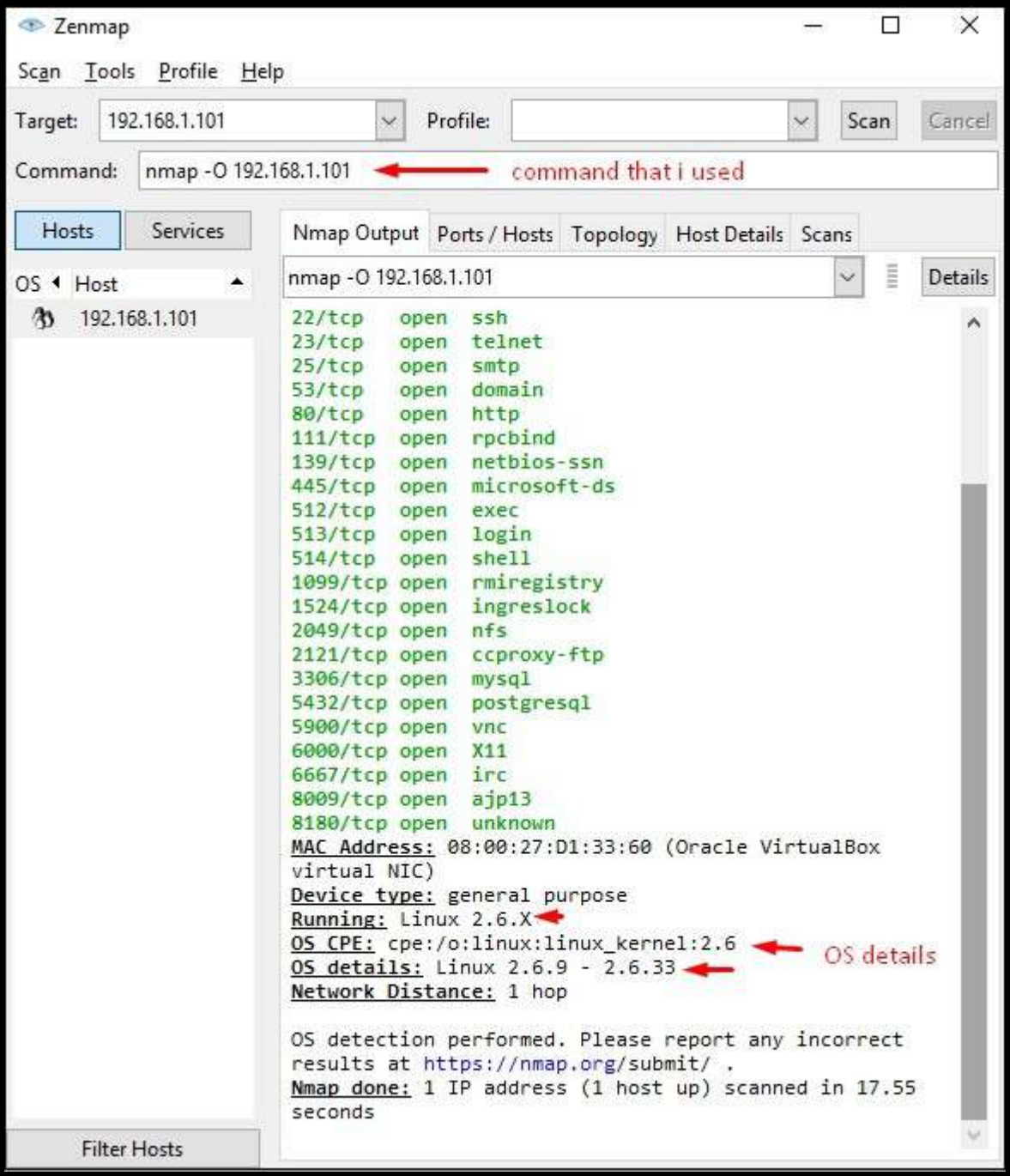


Step 2 – The next step is to detect the OS type/version of the target host. Based on the help indicated by NMAP, the parameter of OS type/version detection is variable "-O". For more information, use this link: https://nmap.org/book/man-os-detection.html

The command that we will use is –

```
nmap -O 192.168.1.101
```

The following screenshot shows where you need to type the above command to see the Nmap output –

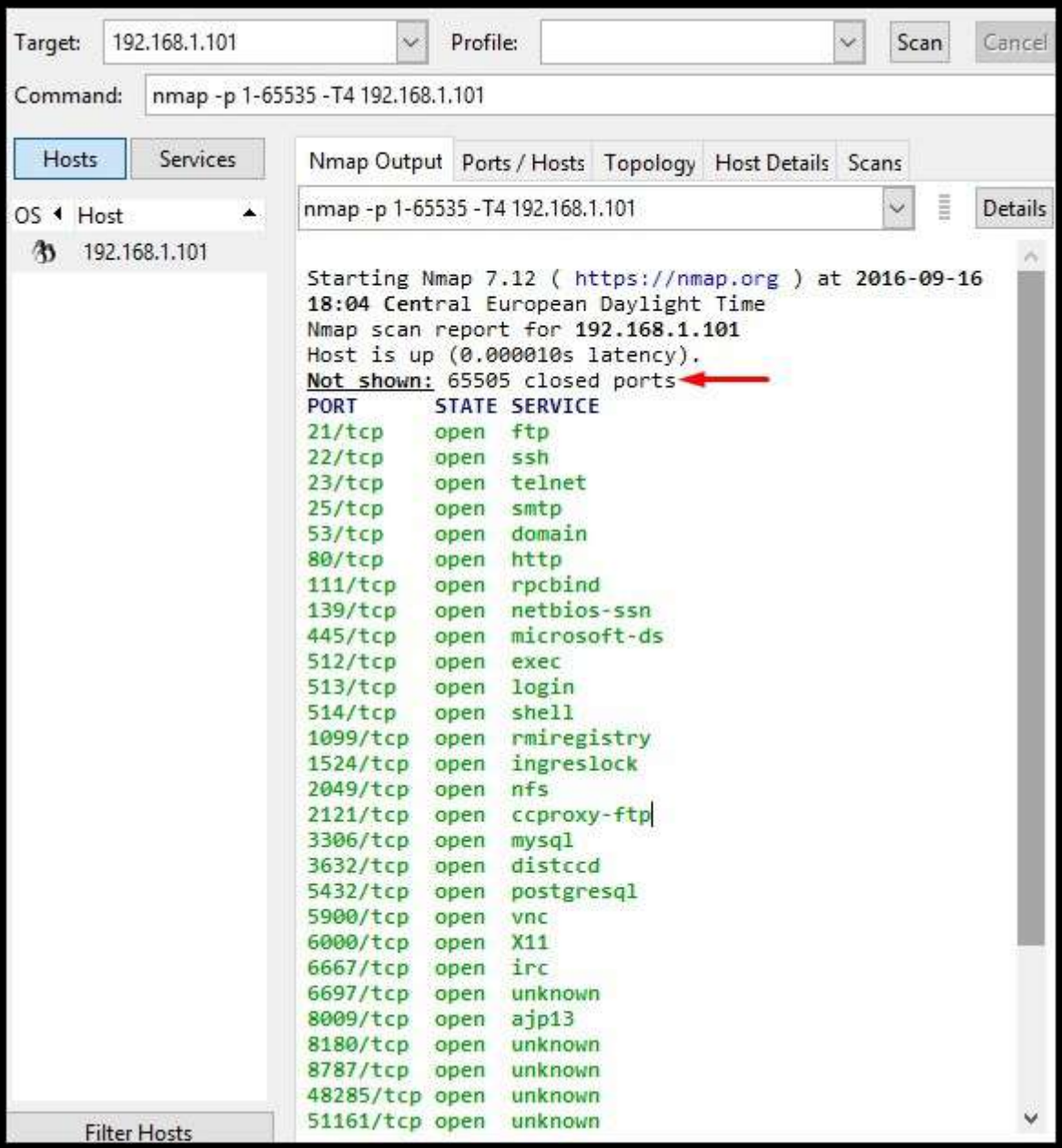


Step 3 – Next, open the TCP and UDP ports. To scan all the TCP ports based on NMAP, use the following command –

```
nmap -p 1-65535 -T4  192.168.1.101
```

Where the parameter "–p" indicates all the TCP ports that have to be scanned. In this case, we are scanning all the ports and "-T4" is the speed of scanning at which NMAP has to run.

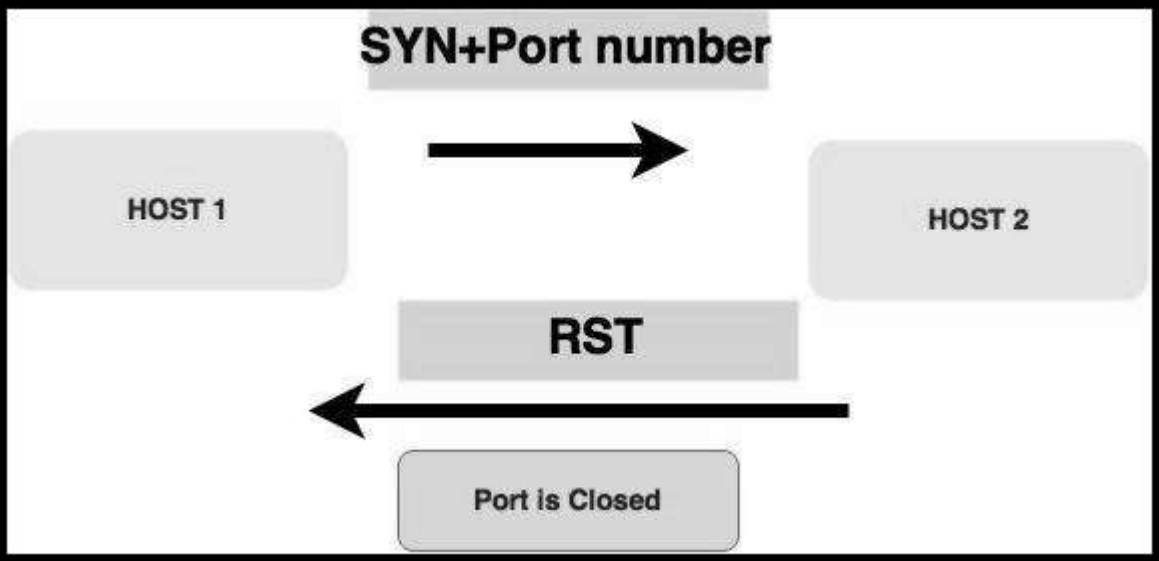
Following are the results. In green are all the TCP open ports and in red are all the closed ports. However, NMAP does not show as the list is too long.

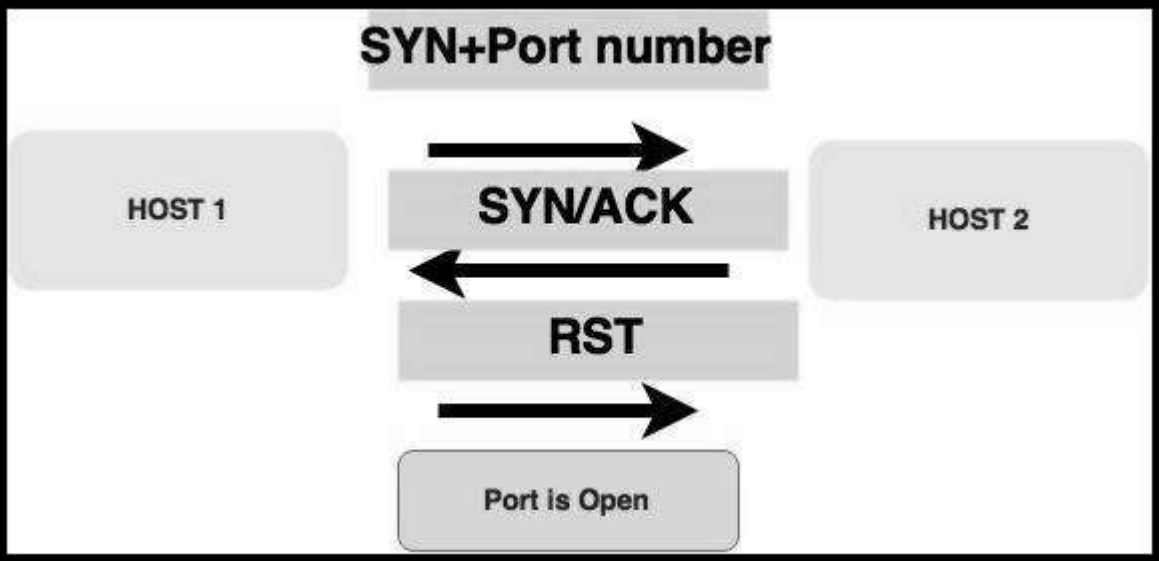


Stealth Scan

Stealth scan or SYN is also known as **half-open scan**, as it doesn't complete the TCP three-way handshake. A hacker sends a SYN packet to the target; if a SYN/ACK frame is received back, then

it's assumed the target would complete the connect and the port is listening. If an RST is received back from the target, then it is assumed the port isn't active or is closed.

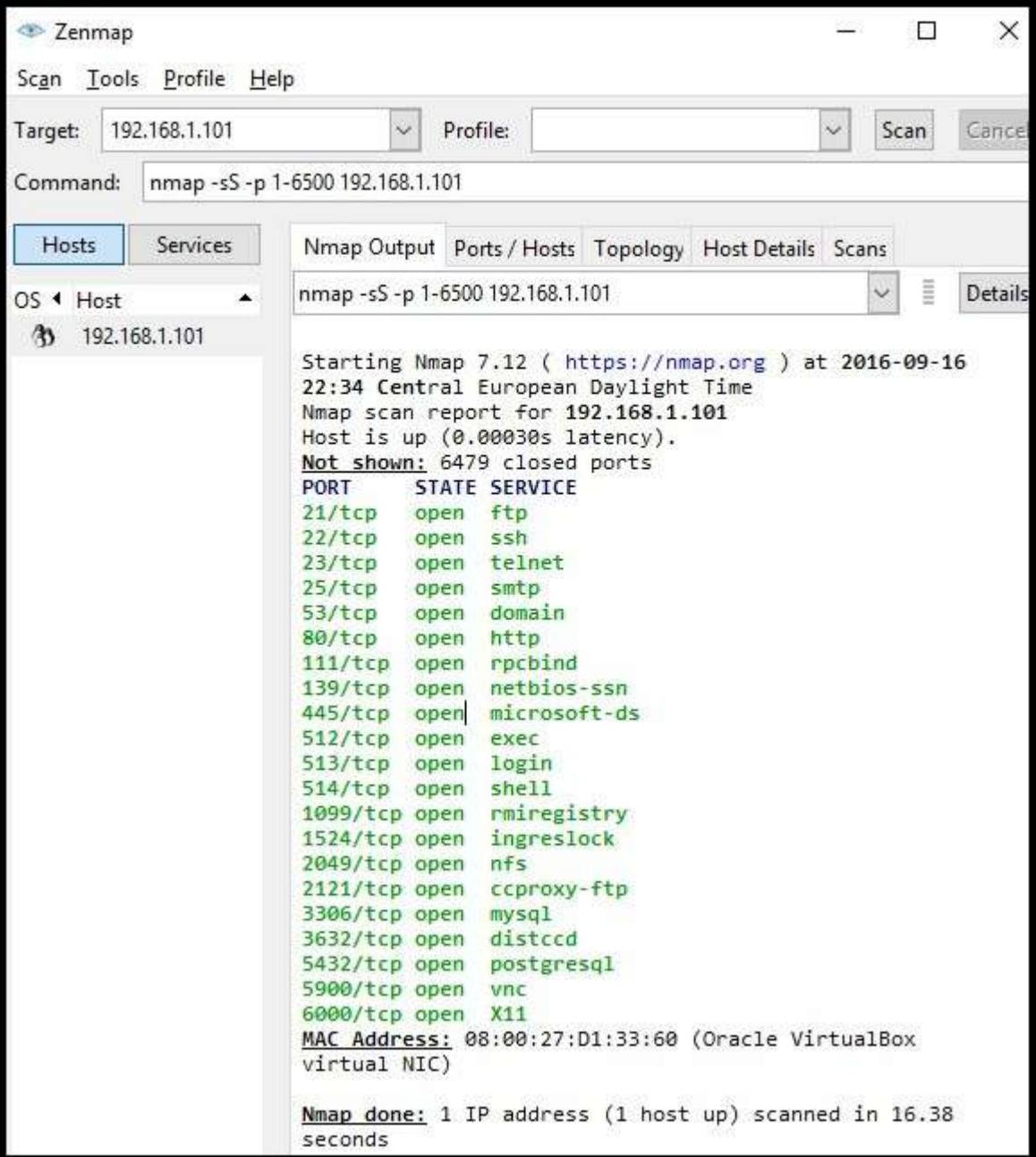




Now to see the SYN scan in practice, use the parameter –**sS** in NMAP. Following is the full command –

```
nmap -sS -T4 192.168.1.101
```

The following screenshot shows how to use this command –


Zenmap
Scan Tools Profile Help
Target: 192.168.1.101
Profile:
Scan
Command: nmap -sS -p 1-6500 192.168.1.101
Hosts
Services
OS Host
192.168.1.101
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -sS -p 1-6500 192.168.1.101
Details
Starting Nmap 7.12 (https://nmap.org) at 2016-09-16 22:34 Central European Daylight Time
Nmap scan report for 192.168.1.101
Host is up (0.00030s latency).
Not shown: 6479 closed ports
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
514/tcp open shell
1099/tcp open rmiregistry
1524/tcp open ingreslock
2049/tcp open nfs
2121/tcp open ccproxy-ftp
3306/tcp open mysql
3632/tcp open distccd
5432/tcp open postgresql
5900/tcp open vnc
6000/tcp open X11
MAC Address: 08:00:27:D1:33:60 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 16.38 seconds