EXPERIMENT-10

10. Operating system Detection using N map.

Sometimes on a network it is beneficial to know the Operating System (OS) of a machine. Accessing a system is easier when you know the OS because you can specifically search the Internet for known security holes in the OS. Granted, security holes are usually patched quickly, but you need to know when a security hole exists.

Scanning your own network to detect the OS types can help you to see what a hacker will be able to see about your network.

Version detection and OS detection are two of the most popular features of Nmap. Nmap is known for having the most comprehensive OS and service fingerprint databases. Knowing the platform (OS) and the exact version of a service is highly valuable for people looking for security vulnerabilities or monitoring their networks for any unauthorized changes. Fingerprinting services may also reveal additional information about a target, such as available modules and specific protocol information.

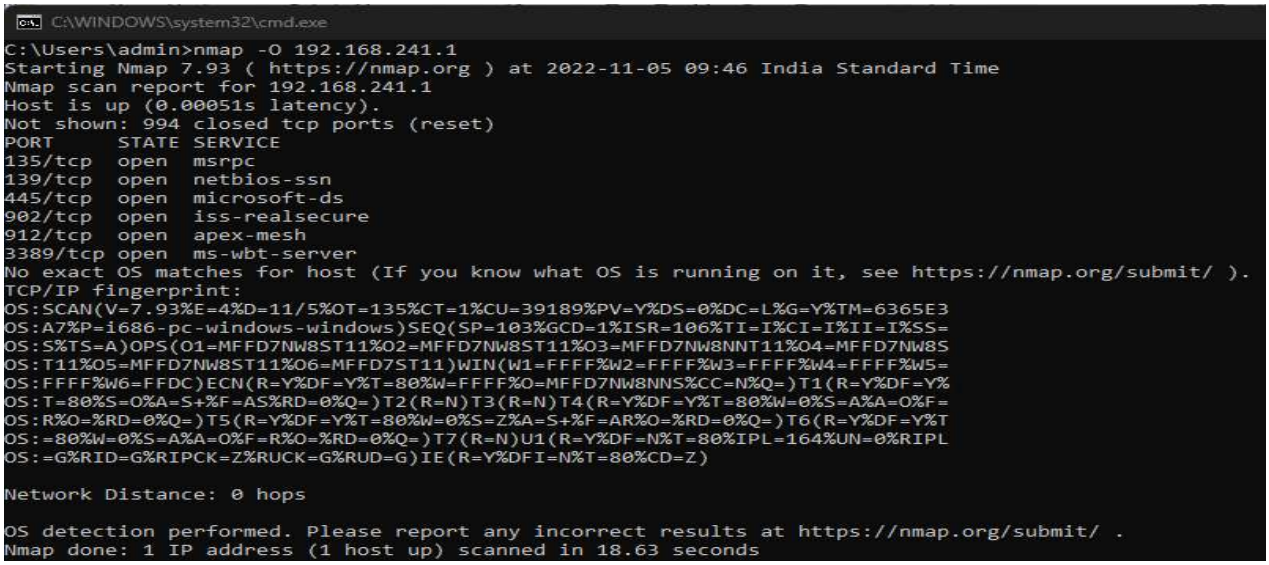
1. OS Scanning

OS scanning is one of the most powerful features of Nmap. When using this type of scan, Nmap sends TCP and UDP packets to a particular port, and then analyzes its response. It compares this response to a database of 2600 operating systems, and returns information on the OS (and version) of a host.

To run an OS scan, use the following command:

nmap -O <IP_ADDRESS>

nmap -O 192.168.241.1



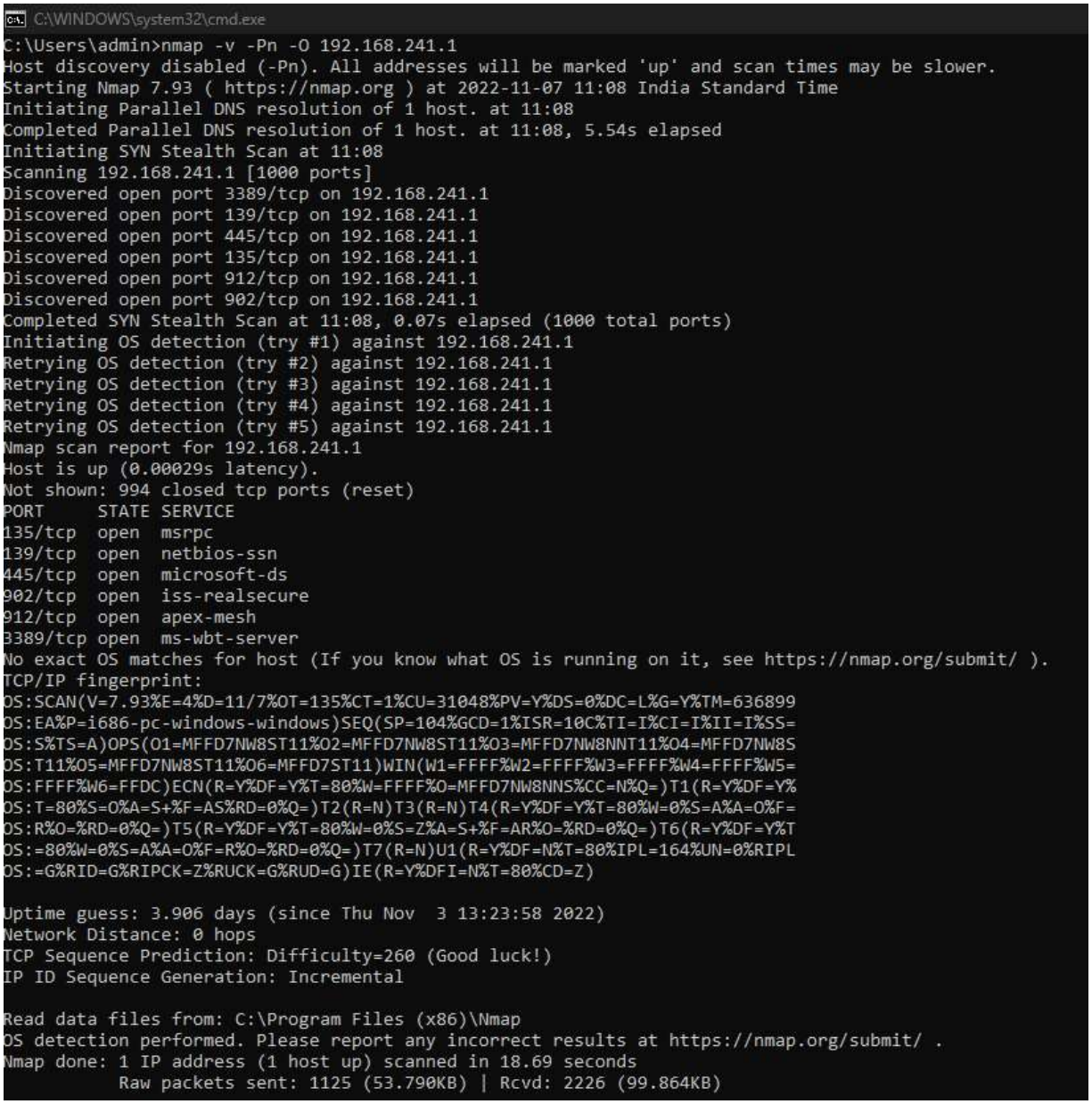
2. NMAP OS Detection Command

Now we need to run the actual command to perform an OS Detection. If you have read any of the other of my NMAP articles then it is best not to perform a PING. To skip the PING we use the parameter '-Pn'. To see the extra information we may require you should use the '-v' parameter for adding verbosity. Specifically to get the OS Detection the parameter '-O' is needed.

nmap -v -Pn -O [IP_ADDRESS]

For the command to complete properly and perform the TCP SYN Scan you need to perform the command as ROOT. In my case, I will perform the scan on one system only and not the whole network so the command would be:

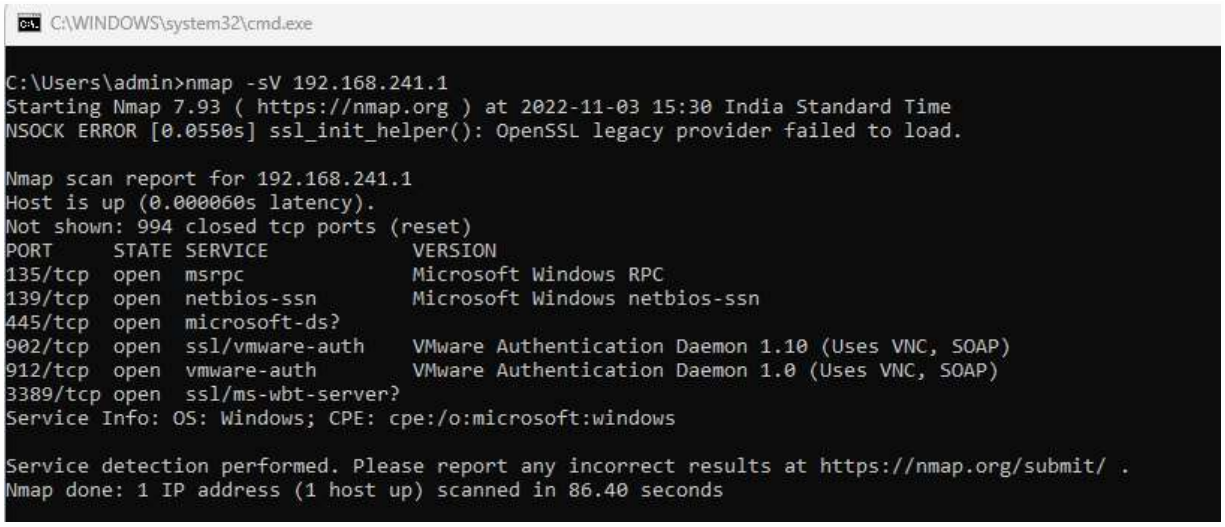
nmap -v -Pn -O 192.168.241.1



3. To enable service detection, add the Nmap option -sV to your port scan command:

nmap -sV Ip_Address

Nmap -sV 192.168.241.1



4. You can often guess just by determining what ports are open, but the most efficient tool is the venerable nmap utility. Using the -O (OS detection) and -sV (check ports to determine service/version info) flags, you get a complete report.

Nmap -O -sV [IP_ADDRESS]

Under the covers, nmap is running through a set of heuristics to determine what OS is most likely, based on what ports are open and unique “fingerprinting” of the device’s IP stack. nmap maintains a database of over 2,000 IP fingerprints. Different operating systems will set different values for things like initial TTL, max segment size, window scaling value, etc. and by analyzing packets, nmap can make an educated guess of what kind of OS is running.

It’s not 100% and nmap lacks the ability to say For Example Like “this is definitely Windows Server 2012 with Service Pack 2 applied” or “this is definitely Debian 9 and not Debian 10” because operating systems in the same family often use the same IP stack. But it is often an excellent start towards identification.

Nmap -O -sV 192.168.241.1

Standard service detection

This is the command to scan for running service. Nmap contains a database of about 2,200 well-known services and associated ports. Examples of these services are HTTP (port 80), SMTP (port 25), DNS (port 53), and SSH (port 22):

```
C:\Users\admin>nmap -O -sV 192.168.241.1
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-03 15:44 India Standard Time
NSOCK ERROR [0.2440s] ssl_init_helper(): OpenSSL legacy provider failed to load.

Nmap scan report for 192.168.241.1
Host is up (0.00067s latency).
Not shown: 994 closed tcp ports (reset)
PORT     STATE SERVICE            VERSION
135/tcp  open  msrpc              Microsoft Windows RPC
139/tcp  open  netbios-ssn        Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
902/tcp  open  ssl/vmware-auth    VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
912/tcp  open  vmware-auth        VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
3389/tcp open  ssl/ms-wbt-server?
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.93%E=4%D=11/3%OT=135%CT=1%CU=42049%PV=Y%DS=0%DC=L%G=Y%TM=636394
OS:EE%P=i686-pc-windows-windows)SEQ(SP=103%GCD=1%ISR=10B%TI=I%CI=I%II=I%SS=
OS:S%TS=A)OPS(O1=MFFD7NW8ST11%O2=MFFD7NW8ST11%O3=MFFD7NW8NNT11%O4=MFFD7NW8S
OS:T11%O5=MFFD7NW8ST11%O6=MFFD7ST11)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=
OS:FFFF%W6=FFDC)ECN(R=Y%DF=Y%T=80%W=FFFF%O=MFFD7NW8NNS%CC=N%Q=)T1(R=Y%DF=Y%
OS:T=80%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=
OS:R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T
OS:=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T7(R=N)U1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL
OS:=G%RID=G%RIPCK=Z%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=80%CD=Z)

Network Distance: 0 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 99.17 seconds
```