

# **Certified Ethical Hacking With Penetration Testing**

## **CEHWPT**

LABS Course

CEHWPT LAB4 Working With NMAP

Prepared by Eng. Khaled Gamo

15-6-2019

## LAB4 working with NMAP

Network Mapped (Nmap) is a network scanning and host detection tool that is very useful during several steps of penetration testing. Nmap is not limited to merely gathering information and enumeration, but it is also powerful utility that can be used as a vulnerability detector or a security scanner. So Nmap is a multipurpose tool, and it can be run on many different operating systems including Windows, Linux, BSD, and Mac. Nmap is a very powerful utility that can be used to:

- Detect the live host on the network (host discovery)
- Detect the open ports on the host (port discovery or enumeration)
- Detect the software and the version to the respective port (service discovery)
- Detect the operating system, hardware address, and the software version
- Detect the vulnerability and security holes (Nmap scripts)

### Part 1 scanning target using nmap

In this exercise we will use the metaspilotable machine as victim and kali Linux as attacker machine both systems connected as virtual hosts. We don't know the IP address of the victim machine so we will use netdiscover tools

Command: `netdiscover -i eth0 -r 192.168.56.0/24`

This will scan the connected subnet

```
Currently scanning: Finished! | Screen View: Unique Hosts
10 Captured ARP Req/Rep packets, from 4 hosts. Total size: 600
```

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
192.168.56.101	08:00:27:3a:08:39	1	60	PCS Systemtechnik GmbH
192.168.56.103	0a:00:27:00:00:14	2	120	Unknown vendor
192.168.56.104	08:00:27:54:3e:01	4	240	PCS Systemtechnik GmbH
192.168.56.105	08:00:27:cb:df:f5	3	180	PCS Systemtechnik GmbH

First we will scan the target using command **nmap 192.168.56.105**

The result show us the open ports without showing the version.

```
root@kali:~# nmap 192.168.56.105
Starting Nmap 7.70 ( https://nmap.org ) at 2019-06-18 15:30 EET
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using
Nmap scan report for 192.168.56.105
Host is up (0.00053s latency).
Not shown: 977 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
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:CB:DF:F5 (Oracle VirtualBox virtual NIC)
```

Then we will use the command **nmap -sV 192.168.56.105**

It's how as the open ports & service with the version.

```
Starting Nmap 7.70 ( https://nmap.org ) at 2019-06-18 15:33 EET
mass dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with
Stats: 0:00:06 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 47.83% done; ETC: 15:33 (0:00:07 remaining)
Nmap scan report for 192.168.56.105
Host is up (0.00077s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login        OpenBSD or Solaris rlogind
514/tcp   open  shell        Netkit rshd
1099/tcp  open  rmiregistry  GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:CB:DF:F5 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, localhost, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Let us try command **nmap -O 192.168.56.105**

```
Nmap scan report for 192.168.56.105
Host is up (0.0011s latency).
Not shown: 977 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
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:CB:DF:F5 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
```

We can detect the exposed netbios service using command **nmap -sV -v -p 137,445 192.168.56.105**

```
root@kali:~# nmap -sV -v -p 139,445 192.168.56.105
Starting Nmap 7.70 ( https://nmap.org ) at 2019-06-18 15:48 EET
NSE: Loaded 43 scripts for scanning.
Initiating ARP Ping Scan at 15:48
Scanning 192.168.56.105 [1 port]
Completed ARP Ping Scan at 15:48, 0.00s elapsed (1 total hosts)
mass dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns
Initiating SYN Stealth Scan at 15:48
Scanning 192.168.56.105 [2 ports]
Discovered open port 445/tcp on 192.168.56.105
Discovered open port 139/tcp on 192.168.56.105
Completed SYN Stealth Scan at 15:48, 0.00s elapsed (2 total ports)
Initiating Service scan at 15:48
Scanning 2 services on 192.168.56.105
Completed Service scan at 15:48, 11.02s elapsed (2 services on 1 host)
NSE: Script scanning 192.168.56.105.
Initiating NSE at 15:48
Completed NSE at 15:48, 0.02s elapsed
Initiating NSE at 15:48
Completed NSE at 15:48, 0.00s elapsed
Nmap scan report for 192.168.56.105
Host is up (0.00038s latency).

PORT      STATE SERVICE      VERSION
139/tcp    open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp    open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
MAC Address: 08:00:27:CB:DF:F5 (Oracle VirtualBox virtual NIC)
```

We can use nmap script nbstat.nse to find Netbios name

```
root@kali:~# nmap -sU --script nbstat.nse -p 137 192.168.56.105
Starting Nmap 7.70 ( https://nmap.org ) at 2019-06-18 15:43 EET
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-d
Nmap scan report for 192.168.56.105
Host is up (0.00079s latency).

PORT      STATE SERVICE
137/udp   open  netbios-ns
MAC Address: 08:00:27:CB:DF:F5 (Oracle VirtualBox virtual NIC)

Host script results:
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
```

## Part 2 Explaining the nmap commands

Step1: How to use nmap

```
# nmap target.com
```

```
# nmap 192.168.1.1
```

If you want to scan the entire subnet, then the command is

```
nmap target/CDIR
```

```
# nmap 192.168.1.1/24
```

It is very easy to scan a multiple targets, all you need to do is to separate each target via space:

```
nmap target target1 target2
```

```
# nmap 192.168.1.1 192.168.1.8
```

Let's suppose you want to scan a range of IP addresses, but not the entire subnet. In this scenario, use this command:

```
nmap target-100
```

```
# nmap 192.168.1.1-100
```

Let suppose you have a list of a target machines. You can make Nmap scan for the entire list:

```
# nmap -iL target.txt
```

Make sure to put the file on the same directory

In some cases we need to scan the entire subnet but not a specific IP addresses because it might be dangerous for us. In this scenario, use the Nmap command with the excluding parameter:

```
# nmap 192.168.1.1/24 --exclude 192.168.1.1
```

If you have a file that contains the list of IP addresses that you want to exclude, then you can call the file in the exclude parameter:

```
# nmap 192.168.1.1/24 --exclude file target.txt
```

If you want to scan a specific port on the target machines (for example, if you want to scan the HTTP, FTP, and Telnet port only on the target computer), then you can use the Nmap command with the relevant parameter:

```
# nmap -p80,21,23 192.168.1.1
```

 It scan the target for port number 80,21 and 23.

## Nmap Scanning Techniques

There are so many scanning techniques available on Nmap, so in this section, we will discuss the most popular scanning technique in detail.

### TCP SYN Scan (-sS)

It is a basic scan, and it is also called half-open scanning because this technique allows Nmap to get information from the remote host without the complete TCP handshake process, Nmap sends SYN packets to the destination, but it does not create any sessions, As a result, the target computer can't create any log of the interaction because no session was initiated, making this feature an advantage of the TCP SYN scan.

```
# nmap -sS 192.168.1.1
```

### **TCP connect() scan (-sT)**

This is the default scanning technique used, if and only if the SYN scan is not an option, because the SYN scan requires root privilege. Unlike the TCP SYN scan, it completes the normal TCP three way handshake process and requires the system to call connect(), which is a part of the operating system. Keep in mind that this technique is only applicable to find out the TCP ports, not the UDP ports.

```
# nmap -sT 192.168.1.1
```

### **UDP Scan (-sU)**

As the name suggests, this technique is used to find an open UDP port of the target machine. It does not require any SYN packet to be sent because it is targeting the UDP ports. But we can make the scanning more effective by using -sS along with -sU. UDP scans send the UDP packets to the target machine, and waits for a response—if an error message arrives saying the ICMP is unreachable, then it means that the port is closed; but if it gets an appropriate response, then it means that the port is open.

```
# nmap -sU 192.168.1.1
```

### **FIN Scan (-sF)**



Sometimes a normal TCP SYN scan is not the best solution because of the firewall. IDS and IPS scans might be deployed on the target machine, but a firewall will usually block the SYN packets. A FIN scan sends the packet only set with a FIN flag, so it is not required to complete the TCP handshaking.

```
root@bt:~# nmap -sF 192.168.1.8
```

Starting Nmap 5.51 ( <http://nmap.org> ) at 2012-07-08 19:21 PKT

Nmap scan report for 192.168.1.8

Host is up (0.000026s latency).

Not shown: 999 closed ports

PORT STATE SERVICE

111/tcp open|filtered rpcbind

The target computer is not able to create a log of this scan (again, an advantage of FIN). Just like a FIN scan, we can perform an xmas scan (-sX) and Null scan (-sN). The idea is same but there is a difference between each type of scan. For example, the FIN scan sends the packets containing only the FIN flag, where as the Null scan does not send any bit on the packet, and the xmas sends FIN, PSH, and URG flags.

Ping Scan (-sP)



Ping scanning is unlike the other scan techniques because it is only used to find out whether the host is alive or not, it is not used to discover open ports. Ping scans require root access s ICMP packets can be sent, but if the user does not have administrator privilege, then the ping scan uses connect() call.

```
# nmap -sP 192.168.1.1
```

### **Version Detection (-sV)**

Version detection is the right technique that is used to find out what software version is running on the target computer and on the respective ports. It is unlike the other scanning techniques because it is not used to detect the open ports, but it requires the information from open ports to detect the software version. In the first step of this scan technique, version detection uses the TCP SYN scan to find out which ports are open.

### **OS Detection Nmap**

One of the most important feature that Nmap has is the ability to detect remote operating systems and software. It is very helpful during a penetration test to know about the operating system and the software used by the remote computer because you can easily predict the known vulnerabilities from this information.

Nmap has a database called nmap-os-db, the database contains information of more than 2,600 operating systems. Nmap sends TCP and UDP packets to the target machine and then it examines the response by comparing the result with the database. The Nmap

operating system discovery technique is slightly slower than scanning techniques because OS detection involves process of finding open ports.

```
root@bt:~# nmap -O 192.168.1.2

Starting Nmap 5.51 ( http://nmap.org ) at 2012-07-15 10:25 PKT
Nmap scan report for 192.168.1.2
Host is up (0.000073s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
111/tcp   open  rpcbind
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.19 - 2.6.36
Network Distance: 0 hops
```

Suppose that the target machine has a firewall, IDS, and IPS all enabled. You can use the command `-PN` to ensure that you do not ping to find the remote operating system. The `-PN` tells Nmap not to ping the remote computer, since sometimes firewalls block the request.

```
# nmap -O -PN 192.168.1.1/24
```

The command informs the sender every host on the network is alive so there is no need to send a ping request as well. In short, it bypasses the ping request and goes on to discover the operating system.

The Nmap OS detection technique works on the basis of an open and closed port. If Nmap fails to discover the open and closed port, then it gives the error:

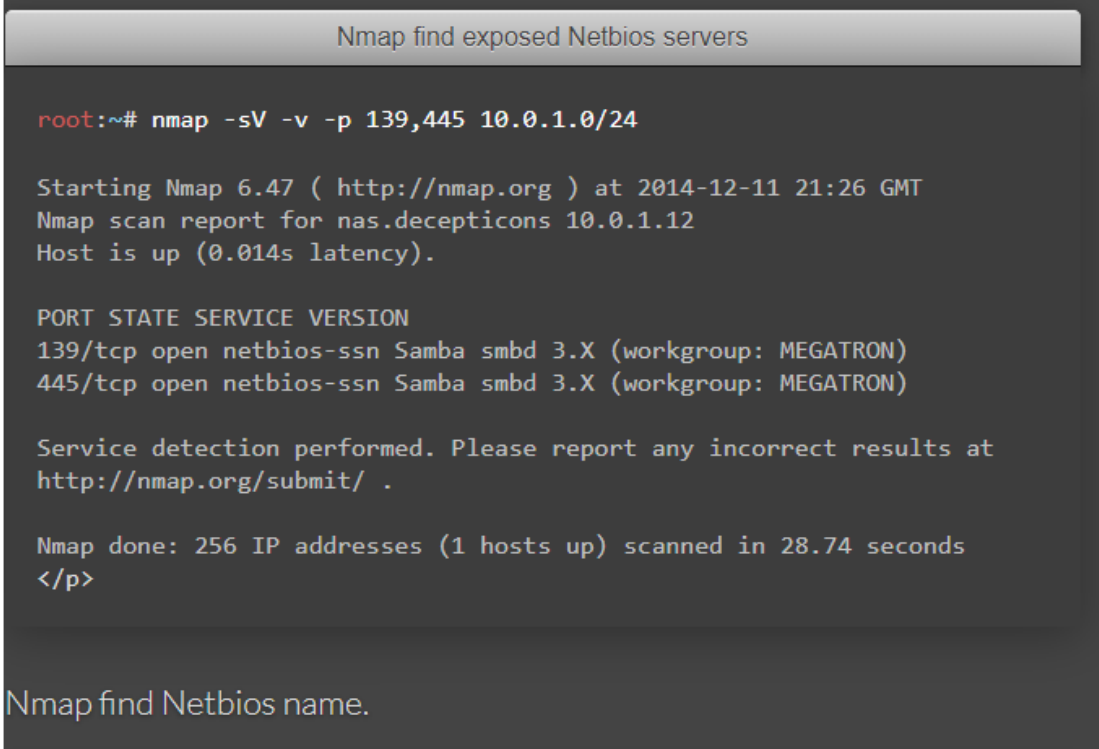
### NMAP Cheat-sheet

As a reference I highly recommend to use the following link

<https://highon.coffee/blog/nmap-cheat-sheet/>

## Nmap Enumeration Examples

Detect all exposed Netbios servers on the subnet.



```
Nmap find exposed Netbios servers

root:~# nmap -sV -v -p 139,445 10.0.1.0/24

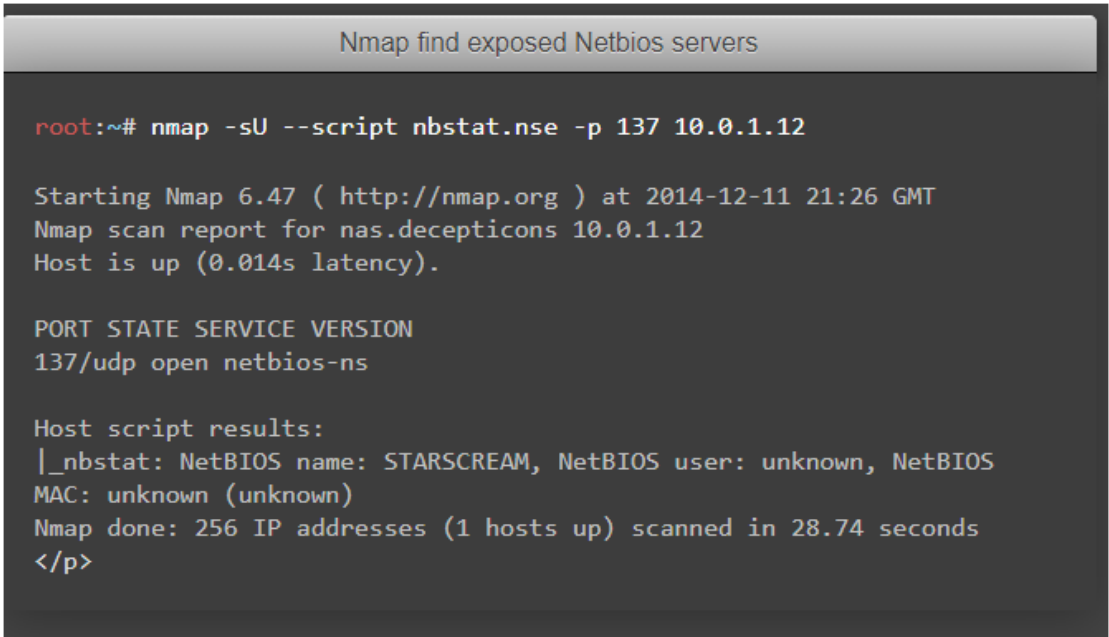
Starting Nmap 6.47 ( http://nmap.org ) at 2014-12-11 21:26 GMT
Nmap scan report for nas.decepticons 10.0.1.12
Host is up (0.014s latency).

PORT STATE SERVICE VERSION
139/tcp open netbios-ssn Samba smbd 3.X (workgroup: MEGATRON)
445/tcp open netbios-ssn Samba smbd 3.X (workgroup: MEGATRON)

Service detection performed. Please report any incorrect results at
http://nmap.org/submit/ .

Nmap done: 256 IP addresses (1 hosts up) scanned in 28.74 seconds
</p>
```

## Nmap find Netbios name



```
Nmap find exposed Netbios servers

root:~# nmap -sU --script nbstat.nse -p 137 10.0.1.12

Starting Nmap 6.47 ( http://nmap.org ) at 2014-12-11 21:26 GMT
Nmap scan report for nas.decepticons 10.0.1.12
Host is up (0.014s latency).

PORT STATE SERVICE VERSION
137/udp open netbios-ns

Host script results:
|_nbstat: NetBIOS name: STARSCREAM, NetBIOS user: unknown, NetBIOS
MAC: unknown (unknown)
Nmap done: 256 IP addresses (1 hosts up) scanned in 28.74 seconds
</p>
```

Check if Netbios servers are vulnerable to MS08-067

## Nmap check MS08-067

```
root:~#  
nmap --script-args=unsafe=1 --script smb-check-vulns.nse -p 445  
10.0.0.1  
  
Nmap scan report for ie6winxp.decepticons (10.0.1.1)  
Host is up (0.00026s latency).  
PORT STATE SERVICE  
445/tcp open microsoft-ds  
Host script results:  
| smb-check-vulns:  
| MS08-067: VULNERABLE  
| Conficker: Likely CLEAN  
| regsvc DoS: NOT VULNERABLE  
| SMBv2 DoS (CVE-2009-3103): NOT VULNERABLE  
|_ MS07-029: NO SERVICE (the Dns Server RPC service is inactive)  
Nmap done: 1 IP address (1 host up) scanned in 5.45 seconds  
</p>
```

The information gathered during the enumeration indicates the target is vulnerable to MS08-067, exploitation will confirm if it's vulnerable to MS08-067.