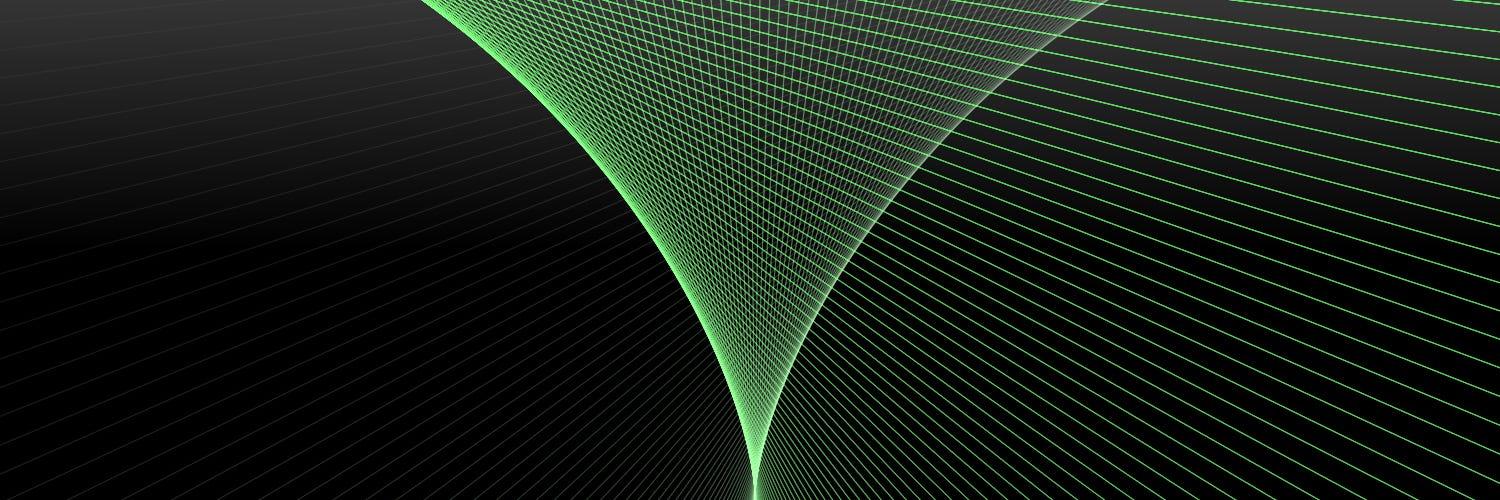
# Understanding the Basics of Network Scanning using Nmap

Intervenant : Ludvin Gatse/ OPENCYBERAI

 Nmap (Zenmap is the official Nmap GUI) is a free, open-source(license) utility for network exploration and security auditing.

Nmap is the most popular network-scanning utility, that most of security professionals use during security assessments. It supports various types of network-scanning techniques. During security assessment, you will be asked to perform network scanning using Nmap. Therefore, as a professional ethical hacker or a penetration tester, you will need to be confortable with Nmap to perform a network scan.

### Objectives:

* Scan a whole Subnet.
* Trace all the sent and received packets.
* Perform a slow comprehensive scan.
* Create a new profile to perform a Null Scan.
* Scan TCP and UDP ports.
* Analyze hosts details and their topology.
* Scanning Techniques:
  + TCP Connect Scan
  + Xmas Scan
  + ACK Flag Scan
  + UDP Scan
  + IDLE Scan
* Avoiding Scanning Detection

### Requirements:

* Windows server 2012 machine.
* Windows 10 machine.
* Ubuntu [Metasploitable](https://information.rapid7.com/download-metasploitable-2017.html) machine.
* Kali Linux machine.
* Make sure to [configure](https://www.techrepublic.com/article/how-to-create-multiple-nat-networks-in-virtualbox/) properly the network topology on your virtual environment.

**Note** #0: Since this lab is exclusive on scanning networks, you don't need to download these specifics machines. Since you have any virtual machine to scan (besides the Kali), you good to go.

**Note** #1: You can use whatever Nmap version you prefer. Personally I prefer the CLI version instead of the GUI, is more adaptable to workflow and have a more solid learning curve.

## Scan a whole Subnet

Open the Terminal window and type nmap -h to list all the commands available. Since Nmap have so many options, you can use this [cheat sheet](https://nmapcookbook.blogspot.com/2010/02/nmap-cheat-sheet.html), [[2]](https://www.stationx.net/nmap-cheat-sheet/) to view some examples.

nmap -O <IP Range>

The option -O is related to Operating System Detection.

To specify the IP range you can use two methods:

**Wildcard**: nmap -O 10.0.2.\*

**Subnet notation:** nmap -O 10.0.2.1/24

Both do the same, with little differentiations, like the subnet notation is a little bit more faster than wildcard.

**Run this scan and check out the results.**

The Nmap scans the entire network and displays information for all the hosts, along with open ports, device type, details of OS, and so on.

## Trace all the Sent and Received Packets

**Select** one host that you scanned

nmap --packet-trace 10.0.2.23

By issuing the --packet-trace command, Nmap sends some packets to the intended machine and receives packets in response to the sent packets. It prints a summary of every packet it sends and receives.

The output below show the packets **sent from host to target** and packets **received from target to host**.

...

SENT (4.1431s) TCP 10.0.2.15:35962 > 10.0.2.23:3005 S ttl=43 id=22968 iplen=44 seq=1965204224 win=1024 <mss 1460>

SENT (4.1433s) TCP 10.0.2.15:35962 > 10.0.2.23:4000 S ttl=39 id=51710 iplen=44 seq=1965204224 win=1024 <mss 1460>

SENT (4.1434s) TCP 10.0.2.15:35962 > 10.0.2.23:1503 S ttl=53 id=146 iplen=44 seq=1965204224 win=1024 <mss 1460>

SENT (4.1435s) TCP 10.0.2.15:35962 > 10.0.2.23:1761 S ttl=56 id=27951 iplen=44 seq=1965204224 win=1024 <mss 1460>

...



Note in the bottom of the output also is shown the open TCP ports:

PORT STATE SERVICE

53/tcp open domain

80/tcp open http

88/tcp open kerberos-sec

135/tcp open msrpc

139/tcp open netbios-ssn

389/tcp open ldap

443/tcp open https

445/tcp open microsoft-ds

...

## Identifying Services with TCP Null Scan

nmap -sN -T4 -A <Target IP address>

-sN: TCP Null Scan.

`-T4`: Timing: (4)Aggressive mode speeds scans up by making the assumption that you are on a reasonably fast and reliable network.

`-A`: Enables OS detection, version detection, script scanning, and traceroute

By issuing this command, Nmap sends TCP packets with none of the TCP flags set in the packet. If the scans returns an RST packet, it means the port is closed; If nothing is returned, the port is either filtered or open.

...

53/tcp open domain ISC BIND 9.4.2

| dns-nsid:

|\_ bind.version: 9.4.2

80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)

|\_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2

|\_http-title: Metasploitable2 - Linux

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 tcpwrapped

1099/tcp open java-rmi 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

...



As shown above, we can se the piece of the output of the scan, performed on the Metasploitable Linux. Later we can check the versions and type of services running on the open ports. This type of information is very valuable because we can search for vulnerabilities, flaws and so on.

# Scanning Techniques

Nmap comes with various inbuilt scripts that can be employed during a scan process in an attempt to find the open ports and services running on the ports.

Summary of scans that will be performed:

1. **TCP Connect Scan** uses a normal TCP connection to determine if a port is available.
2. **Xmas Scan** involves sending TCP segments with the all flags sent in the packet header, generating packets that are illegal according to RFC 793.
3. **ACK Flag Scan** involves sending ACK probe packet with random sequence number.
4. **UDP Scan** involves sending a generic UDP packet to the target.
5. **IDLE Scan** involves sending spoofed packets to a target.

## 1. TCP Connect Scan

This is scan is the most basic of TCP scanning. The connect() system call provided by your OS is used to open a connection to every interesting port on the machine. If the port is listening, connect() will succed, otherwise the port is not reachable. One strong advantage to this technique is that you don't need any special privileges.

Perform a TCP scan with a normal timing (-T3):

nmap -sT -T3 -A <Target IP address>

-sT: TCP connect port scan (Default without root privilege).

The scan result includes all the open ports, OS Fingerprint result, nbstat result, smb-os-discovery results, smb version, and so on.

## 2. Xmas Scan

Xmas Scan sends a TCP frame to a remote device with PSH, URG, and FIN flags set. FIN scans only with OS TCP/IP developed according to RFC 793. The current version of MS Windows is not supported.

**Note: The next scan will be on a Firewall-enabled machine (i.e., Windows Server 2012).**

nmap -sX -T4 <Target IP address>

-sX: Sets the FIN, PSH, and URG flags, lighting the packet up like a Christmas tree

Nmap scan report for 10.0.2.23

Host is up (0.00040s latency).

All 1000 scanned ports on 10.0.2.23 are open|filtered

MAC Address: 11:22:33:44:55:66 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 21.64 seconds



Nmap returns a result stating that the all ports are **opened/filtered, which means a firewall has been configured on the target machine.**

**Next, turn off the Firewall on the target machine.**

## 3. ACK Flag Scan

The ACK scan never locates an open port. It only provides a "filtered" or "unfiltered" disposition, because it never connects to an application to confirm an "open" state.

This scan initiates ACK scan and displays the port disposition, as show below:

nmap -sA -v -T4 <Target IP address>

Initiating ARP Ping Scan at 13:18

Scanning 10.0.2.23 [1 port]

Completed ARP Ping Scan at 13:18, 0.04s elapsed (1 total hosts)

Initiating Parallel DNS resolution of 1 host. at 13:18

Completed Parallel DNS resolution of 1 host. at 13:18, 0.05s elapsed

Initiating ACK Scan at 13:18

Scanning 10.0.2.23 [1000 ports]

Completed ACK Scan at 13:18, 1.26s elapsed (1000 total ports)

Nmap scan report for 10.0.2.23

Host is up (0.00029s latency).

All 1000 scanned ports on 10.0.2.23 are unfiltered

MAC Address: 11:22:33:44:55:66 (Oracle VirtualBox virtual NIC)

Read data files from: /usr/bin/../share/nmap

Nmap done: 1 IP address (1 host up) scanned in 1.51 seconds

Raw packets sent: 1060 (42.388KB) | Rcvd: 1001 (40.028KB)



Attackers send an ACK probe packet with a random sequence number.

* No response means the port is filtered.
* Unfiltered response means the port is closed.

## 4. UDP Scan

UDP scanning is performed to find any UDP ports on the target machine. If have any to determine their state (Open/Closed).

nmap -sU -T5 <Target IP address>

...

Not shown: 986 open|filtered ports

PORT STATE SERVICE

123/udp open ntp

137/udp open netbios-ns

389/udp open ldap

445/udp closed microsoft-ds

688/udp closed realm-rusd

1001/udp closed unknown

1901/udp closed fjicl-tep-a

8001/udp closed vcom-tunnel

16674/udp closed unknown

18818/udp closed unknown

28973/udp closed unknown

30656/udp closed unknown

31109/udp closed unknown

57172/udp open unknown

...

## 5. IDLE Scan

IDLE scan is an advanced scan method that performs a truly blind TCP port scan of the target (meaning no packets are sent to the target from your real IP address). Instead, a unique side-channel attack exploits predictable IP fragmentation ID sequence generation on the zombie host to glean information about the open ports on the target.

In this example the zombie will be Windows Server 2012 machine and the target Windows 10 machine using port number 80 (or any port which you want to test).

nmap -Pn -p 80 -sI <IP address of the zombie> <Target IP address>

Idle scan using zombie 10.0.2.37 (10.0.2.37:80); Class: Incremental

Nmap scan report for 10.0.2.23

Host is up (0.0069s latency).

PORT STATE SERVICE

80/tcp open http

MAC Address: 22:44:11:55:66:77 Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.08 seconds



IDLE scan can be tricky for the first-timers, I recommend try and test out in your own way. I recommend this [link](https://gbhackers.com/idle-zombie-scan-nmap/) for any missing information about it.

## Ping Sweep

Ping sweep is a method that can establish a range of IP addresses which map to live hosts.

Now instead of checking for individual systems, we will check for all the systems alive in the network by performing a ping sweep.

-sP: Perform a Ping Only Scan

nmap -sP 10.0.2.\*

Nmap scan report for 10.0.2.1

Host is up (0.0011s latency).

MAC Address: 22:44:99:33:11:55 QEMU virtual NIC)

Nmap scan report for 10.0.2.2

Host is up (0.00084s latency).

MAC Address: 22:44:99:33:11:55 (QEMU virtual NIC)

Nmap scan report for 10.0.2.3

Host is up (0.00097s latency).

MAC Address: 11:22:33:44:55:66 (Oracle VirtualBox virtual NIC)

Nmap scan report for 10.0.2.22

Host is up (0.00075s latency).

MAC Address: 11:22:33:44:55:66 (Oracle VirtualBox virtual NIC)

Nmap scan report for 10.0.2.23

Host is up (0.00066s latency).

MAC Address: 11:22:33:44:55:66 (Oracle VirtualBox virtual NIC)

Nmap scan report for 10.0.2.37

Host is up (0.00051s latency).

MAC Address: 11:22:33:44:55:66 (Oracle VirtualBox virtual NIC)

Nmap scan report for 10.0.2.15

Host is up.

Nmap done: 256 IP addresses (7 hosts up) scanned in 2.29 seconds



Nmap scans the subnet and shows a list of alive systems as shown above. The result might vary in your lab environment.

# Avoiding Scanning Detection using Multiple Decoy IP Addresses

The Nmap command nmap -D RND:10 is the decoy option, that lets you scan using multiple decoy IP addresses.

Firewalls and IDS detect normal scanning attempts on the target network. However, you can use the IP address decoy technique to avoid detection.

**Before starting this lab, make sure that you have your Windows Firewall on the target turned on.**

## IP Fragmentation

Open a new Terminal window on Kali and enter the target IP address (Windows).

nmap -f <Target IP Address>

-f: Used to scan tiny fragment packets.

Nmap scan report for 10.0.2.23

Host is up (0.00074s latency).

Not shown: 979 filtered ports

PORT STATE SERVICE

53/tcp open domain

80/tcp open http

88/tcp open kerberos-sec

135/tcp open msrpc

139/tcp open netbios-ssn

389/tcp open ldap

443/tcp open https

445/tcp open microsoft-ds

464/tcp open kpasswd5

593/tcp open http-rpc-epmap

636/tcp open ldapssl

3268/tcp open globalcatLDAP

3269/tcp open globalcatLDAPssl

3389/tcp open ms-wbt-server

MAC Address: 11:22:33:44:55:66 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.72 seconds



When the Windows Firewall service is turned on, you can only see the ports opened as shown in the output above.

## Perform Maximum Transmission Unit

This command is used to transmit smaller packets instead of sending one complete packet at a time.

This scan is very similar to the previous one but with **Maximum Transmission Unit** (-mtu) and 8 bytes of packets.

nmap -mtu 8 <Target IP Address>

If everything works, the results should be identical to the previous one.

## Decoying IP address

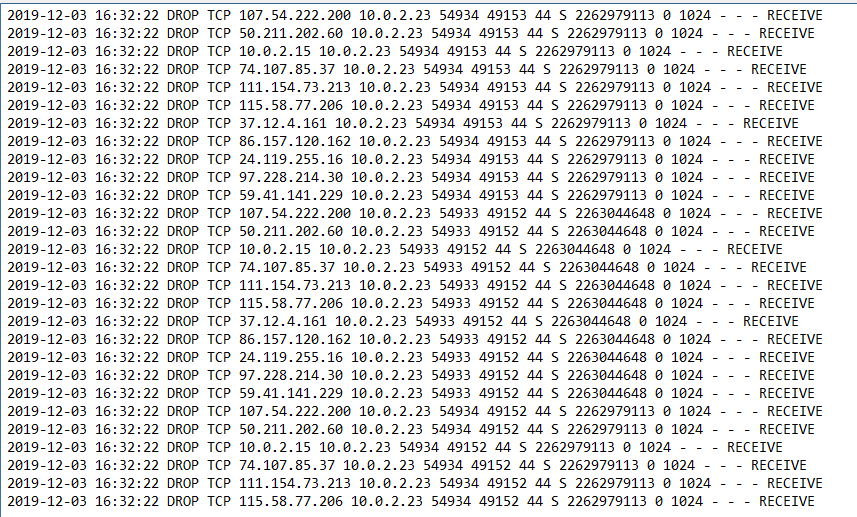
This command is used to scan multiple decoy IP addresses. Nmap will send multiple packets with different IP addresses, along with your attacker's IP address.

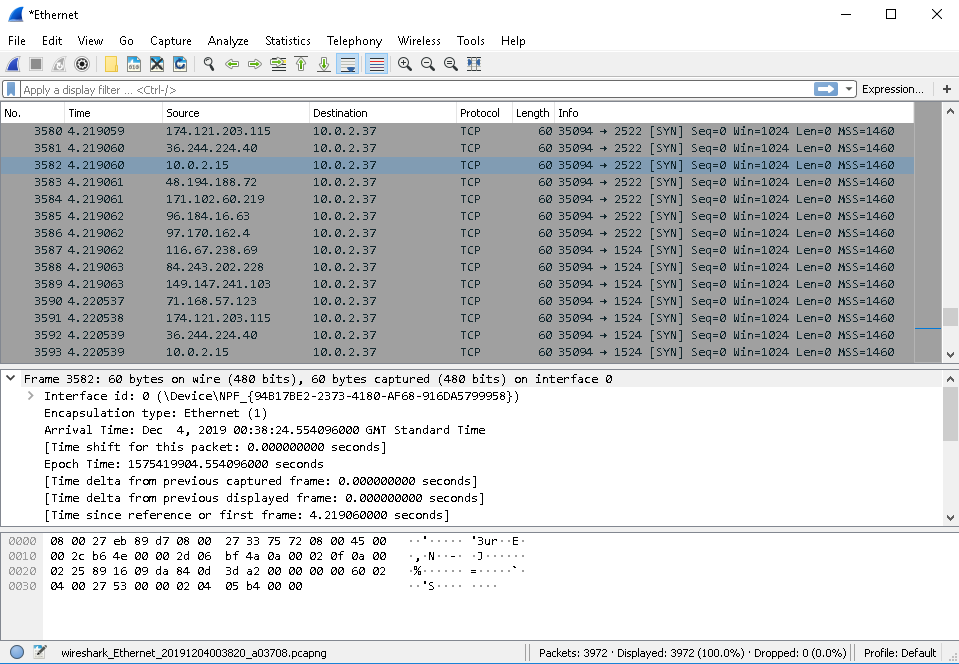
nmap -D RND:10 <Target IP Address>

Again, the output is the same as previous outputs but on the target view is very different.

Check the Logs on your Windows Server Firewall and analyze the last scan performed. You also can analyze this information with Wireshark turned on.

Both shows multiple IP addresses along with your real attacker IP address.

 *Windows Firewall Log: Decoyed IP Address*

 *Wireshark: Decoyed IP Address*

**In conclusion**: Nmap is a very powerful tool for network scanning / network security assessments. Basically the must-have tool on your belt when we talk about Network Security, Ethical Hacking or Pentesting.

Useful links:

* [Official Documentation](https://nmap.org/docs.html)
* [Cheat Sheet with Pro Tips](https://hackertarget.com/nmap-cheatsheet-a-quick-reference-guide/)
* [Cheat Sheet](https://nmapcookbook.blogspot.com/2010/02/nmap-cheat-sheet.html)
* [Cheat Sheet 2](https://www.stationx.net/nmap-cheat-sheet/)
* [Zenmap presets](https://www.securesolutions.no/zenmap-preset-scans/)
* [Bypassing Firewall Rules](https://nmap.org/book/firewall-subversion.html)