MODULE no:- 3

**Scanning and Enumeration**

What is Network?

A computer network is a group of computer that use a of common communication protocols over digital interconnections for the purpose of sharing resources.

A network consists of two or more computer that are linked in order to share resources, exchanges files, or allow electronic communication.

**What is the Ip address?**

It stands for internet protocol. It is the logical address of the computer and is used to uniquely locate a computer connected via a network.

An Ip address is a unique address that identifies a device on the internet or a local network.

**What is MAC address?**

It stand for Media Access Control . MAC is physical address of network device or computer which is globally unique.

Before we had seen footprinting where hacker or intruder collect as much as information he can , on the be-half of that information hacker start scanning work to gain in depth information .

In scanning phase, an attacker develops an attack strategy .

There are types of scanning, through of this we also gather information

**Port Scanning:-**

We find the live ports which are open, also know what os is running, version detail. we also connect with TCP and UDP ports and try to see remote login ports or vulnerable ports .

**Network Scanning:-**

Network scanning is a procedure in which attackers find the live Host and secutiy of network.

**Vulnerability scanning:-**

Vulnerability scanning is the process or way of checking the system , whether it is vulnerable or not by identifying its vulnerabilities.

**CVSS and CVE**

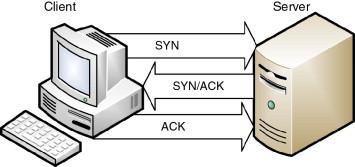
* **CVSS - Common Vulnerability Scoring System** [[+]](https://nvd.nist.gov/vuln-metrics/cvss)
  + Places numerical score based on severity

**CVE – Common Vulnerabilities and Exposures** [[+]](https://cve.mitre.org/)

* Is a list of publicly disclosed vulnerabilities and exposures that is maintained by MITRE.
* **NVD - National Vulnerability Database** [[+]](https://nvd.nist.gov/)
  + is a database, maintained by NIST, that is fully synchronized with the MITRE CVE list; US Gov. vulnerabilities repository.

***Before going to scan TCP lets understand the connection of TCP how it build***

**TCP three way handshake**:- Three way connection is for connecting with full duplex and maintain the reliable connection



This is how tcp connection built

**Perform Host Discovery** :-

Host discovery is the process of identifying active HOST in the target network.

Tool is nmap :- command : nmap -sn [ ip]

┌──(root㉿kali)-[~]

└─# nmap -sn -PE 192.168.1.242

Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-28 02:16 EDT

Nmap scan report for 192.168.1.242 (192.168.1.242)

Host is up (0.00063s latency).

MAC Address: 08:00:27:99:B1:5F (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds

Another tool is Angry Ip scanner

Sources :- <https://angryip.org/download/>

**Advance ip scanner**

Source :- <https://www.advanced-ip-scanner.com/>

Zenmap is GUI version of nmap

**Perform OS discovery**

OS detection is process of kowing os of machine.

Tool :- **nmap** -O [ip]

This can clear the os of the machine

**Netcat** ;

command :- nc [ip] (ipconfig)

result will clarify the os

**PING scan**

Command :- ping [ip]

Ttl value of result declare th os of machine

Source: https://subinsb.com/default-device-ttl-values/

**Scanning Methodology**

* **Check for live systems** - Ping or other type of way to determine live hosts
* **Check for open ports** - Once you know live host IPs, scan them for listening ports

**Tools**:- Nmap : command :- nmap -p- [ip]

* **Scan beyond IDS** - If needed, use methods to scan beyond the detection systems; evade IDS using proxies, spoofing, fragmented packets and so on.

Here we don’t do hacking our work is to just scan the network or system to check wheather it is configured correctly or not.If we are successful in scanning the Target machine ports with various techniques then IDS and Firewall need to take care of .

* **Perform banner grabbing** - Grab from servers as well as perform OS fingerprinting (versions of the running services)

**Tool:- Nmap and Netcat**.

* **Scan for vulnerabilities** - Use tools to look at the vulnerabilities of open systems
* **Draw network diagrams** - Shows logical and physical pathways into networks

It is way to explain the relationship of component

* **Use proxies** - Obscures efforts to keep you hidden
* **Pentest Report** - Document everything that you find

## **Identifying Targets**

* The easiest way to scan for live systems is through ICMP.(Internet control message protocol)

**Ping scanning tools**

* **Nmap**
  + **nmap -sn 192.168.1.0/24**
* **hping3**
  + **hping -1 10.0.0.x --rand-dest -I eth0**
    - -1 --> ICMP mode
    - --rand-dest --> random destionation address mode
    - -I <interface> --> network interface name

hping3 -1 192.168.1.40

HPING 192.168.1.40 (eth0 192.168.1.40): icmp mode set, 28 headers + 0 data bytes

len=46 ip=192.168.1.40 ttl=127 id=24 icmp\_seq=0 rtt=7.7 ms

len=46 ip=192.168.1.40 ttl=127 id=25 icmp\_seq=1 rtt=8.9 ms

len=46 ip=192.168.1.40 ttl=127 id=26 icmp\_seq=2 rtt=5.3 ms

len=46 ip=192.168.1.40 ttl=127 id=27 icmp\_seq=3 rtt=4.3 ms

len=46 ip=192.168.1.40 ttl=127 id=28 icmp\_seq=4 rtt=48.2 ms

^C

--- 192.168.1.40 hping statistic ---

6 packets transmitted, 5 packets received, 17% packet loss

round-trip min/avg/max = 4.3/14.9/48.2 ms

command :- hping3 -F -U -P [ip] [port no ]

if port is closed it will gives RST response

* **Angry IP Scanner -** Angry IP scanner is a very fast IP address and port scanner.
* **Advanced IP Scanner -**  It will allow you to quickly detect all network computers and obtain access to them

**OvErView of NMAP**

# Nmap is a [network scanner](https://en.wikipedia.org/wiki/Network_scanner) created by [Gordon Lyon](https://en.wikipedia.org/wiki/Gordon_Lyon)

**Lua** language is used in Nmap in development.

# **Nmap Scan Types:**

Default nmap website is there for student for just practice purpose

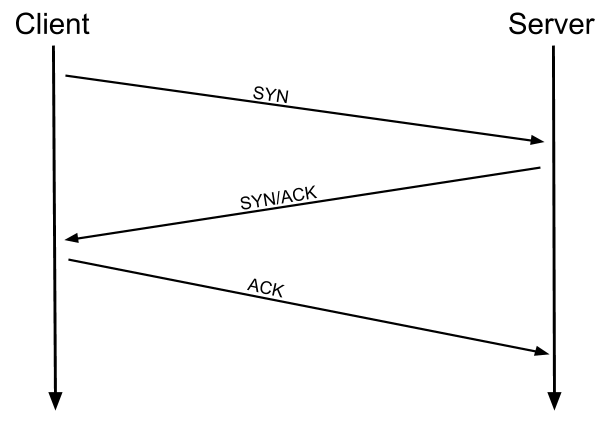
Scanme.nmap.org

**All connection will be shown practically in wireshark**

### **Full connection scan**

TCP connect or full open scan. The first two steps (SYN and SYN/ACK) are exactly the same as with a SYN scan. Then, instead of aborting the half-open connection with a RST packet, krad acknowledges the SYN/ACK with its own ACK packet, completing the connection.

* Full connection and then tears down with RST.
* Easiest to detect, but most reliable
* **nmap -sT <target IP>**

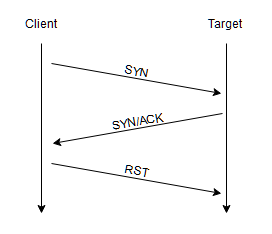


### **Stealth Scan**

Half-open scan or SYN scan - only SYN packets sent. Responses same as full.

* Useful for hiding efforts and evading firewalls
* **nmap -sS <target IP>**

**(practically in wireshark)**



### **TCP ACK scan / flag probe** - multiple methods

* TTL version - if TTL of RST packet < 64, port is open
* Window version - if the Window on the RST packet is anything other than 0, port open
* **Can be used to check filtering. If ACK is sent and no response, stateful firewall present.**
* **nmap -sA <target IP>** *(ACK scan)*
* **nmap -sW <target IP>** *(Window scan)*

This scan is different than the others discussed so far in that it never determines open (or even open|filtered) ports. It is used to map out firewall rulesets, determining whether they are stateful or not and which ports are filtered.

Types of TCP flag:

Null - set null bit value 0

Fin - it inform session had completed

Push - It push syn packet

Urgent - It set the syn packet at high priority

Syn - Synchronise

Ack - Acknowlodgement

Rst - Reset flag

### **NULL, FIN and Xmas Scan**

* **Open gives no response. Closed gives RSTttl64**
* **nmap -sN <target IP>** *(Null scan) -* it is more stealthier than -sS scan
* **nmap -sF <target IP>** *(FIN scan) -*  It is used to identify the port is open is closed. when we get port is filtered, we don,t know port is closed or open.

command:- nmap -sF $ip -p (filtered\_port) –-reason

-if we get rstttl64, means port is closed

* **Xmas Scan** - Sets the FIN, PSH, and URG flags, lighting the packet up like a Christmas tree.
  + Responses are same as Inverse TCP scan
  + Do not work against Windows machines
  + **nmap -sX <target IP>**

**The key advantage to these scan types (NULL, FIN or Xmas scan) is that they can sneak through certain non-stateful firewalls and packet filtering routers.**

How Nmap interprets responses to a NULL, FIN, or Xmas scan probe

| **Probe Response** | **Assigned State** |
| --- | --- |
| No response received (even after retransmissions) | open|filtered |
| TCP RST packet | closed |
| ICMP unreachable error (type 3, code 1, 2, 3, 9, 10, or 13) | filtered |

### **IDLE Scan**

uses a third party to check if a port is open

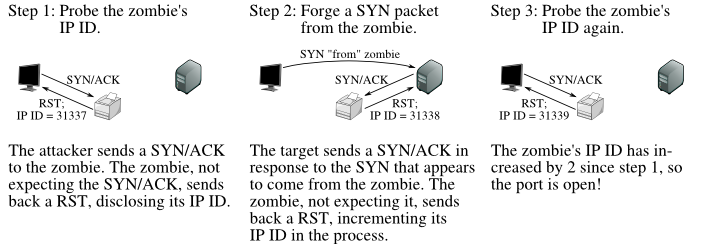
* Looks at the IPID to see if there is a response
* Only works if third party isn't transmitting data
* Sends a request to the third party to check IPID id; then sends a spoofed packet to the target with a return of the third party; sends a request to the third party again to check if IPID increased.
  + IPID increase of 1 indicates port closed
  + IPID increase of 2 indicates port open
  + IPID increase of anything greater indicates the third party was not idle
* **nmap -sI <zombie host> <target IP>**

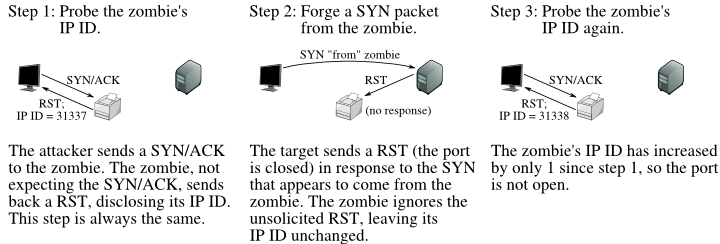
**condition for IDLE scan :-**

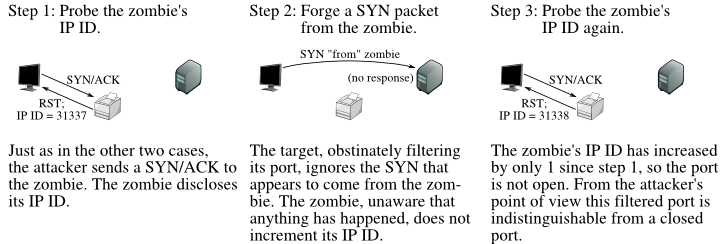
First system should reply SYN/ACK with reset

System should not generate traffic(silent pc)

System should allow incremental IPID







**Spoofing**

* **Decoy:**
  + **nmap -D <spoofed IP> <target>**
  + **nmap -D RND:(No) <target>**

**at RND we can set no so it will do scanning with random different Ip**

-Pn

Basically this flag say through nmap that I don’ want to ping the port I know that port is live , just send me the port detail.

### UDP Scan

Most popular services run over the TCP, but there are many common services that also uses UDP: **DNS (53), SMTP (25), DHCP (67), NTP (123), NetBIOS-ssn (137), etc.**

* **nmap -sU <target>**

You also can specify which UDP port:

* **nmap -sU -p U:53, 123 <target>**

Also you can fire up both TCP and UDP scan with port specification:

* **nmap -sU -sS -p U:53,123 T:80,443 <target>**

## List of Switches

| **Switch** | **Description** |
| --- | --- |
| -sA | ACK scan |
| -sF | FIN scan |
| -sI | IDLE scan |
| -sL | DNS scan (list scan) |
| -sN | NULL scan |
| -sO | Protocol scan (tests which IP protocols respond) |
| -sP or -sn | Ping scan |
| -sR | RPC scan |
| -sS | SYN scan |
| -sT | TCP connect scan |
| -sW | Window scan |
| -sX | XMAS scan |
| -A | OS detection, version detection, script scanning and traceroute |
| -sV | Determine only service/version info |
| -PI | ICMP ping |
| -Pn | No ping |
| -Po | No ping |
| -PS | SYN ping |
| -PT | TCP ping |
| -oN | Normal output |
| -oX | XML output |
| -n | Never do DNS resolution/Always resolve |
| -f | --mtu : fragment packets (optionally w/given MTU) |
| -D | IP address Decoy: <decoy1,decoy2[,ME],...>: Cloak a scan with decoys |
| -T0 through -T2 | Serial scans. T0 is slowest |
| -T3 through -T5 | Parallel scans. T3 is slowest |
| -F | Fast mode - Scan fewer ports than the default scan |

## **Service and Version Detection**

| **Switch** | **Example** | **Description** |
| --- | --- | --- |
| -sV | nmap 192.168.1.1 -sV | Attempts to determine the version of the service running on port |

## **OS Detection**

| **Switch** | **Example** | **Description** |
| --- | --- | --- |
| -O | nmap 192.168.1.1 -O | Remote OS detection using TCP/IP stack fingerprinting |

## **NSE Scripts**

NSE stands for Nmap Scripting Engine, and it’s basically a digital library of Nmap scripts that helps to enhance the default Nmap features and report the results in a traditional Nmap output.

One of the best things about NSE is its ability to let users write and share their own scripts, so you’re not limited to relying on the Nmap default NSE scripts. [[+]](https://nmap.org/nsedoc/)

| **Switch** | **Example** | **Description** |
| --- | --- | --- |
| -sC | nmap 192.168.1.1 -sC | Scan with default NSE scripts. Considered useful for discovery and safe |

## **Banner Grabbing**

*Banner grabbing can be used to get information about OS or specific server info (such as web server, mail server, etc.)*

* **Active** - sending specially crafted packets and comparing responses to determine OS
* **Passive** - reading error messages, sniffing traffic or looking at page extensions

*In banner grabbing server leak the info what type of technology is running , which type of os , what content is there etc*

* **Netcat** can be used to banner grab:
  + nc <IP address or FQDN> <port number>

**Example of Banner grabbing on netcat - extracting request HTTP header**

1. nc command with target IP address and port 80
2. Issue the GET / HTTP/1.0 (this GET request will send to the web server).
3. **The server responded with some interesting information:**

nc 192.168.63.143 80

GET / HTTP/1.0

HTTP/1.1 200 OK

Date: Sun, 12 Aug 2018 13:36:59 GMT

Server: Apache/2.2.8 (Ubuntu) DAV/2 🡨 ( os & version are leaked by server)

X-Powered-By: PHP/5.2.4-2ubuntu5.10

Content-Length: 891

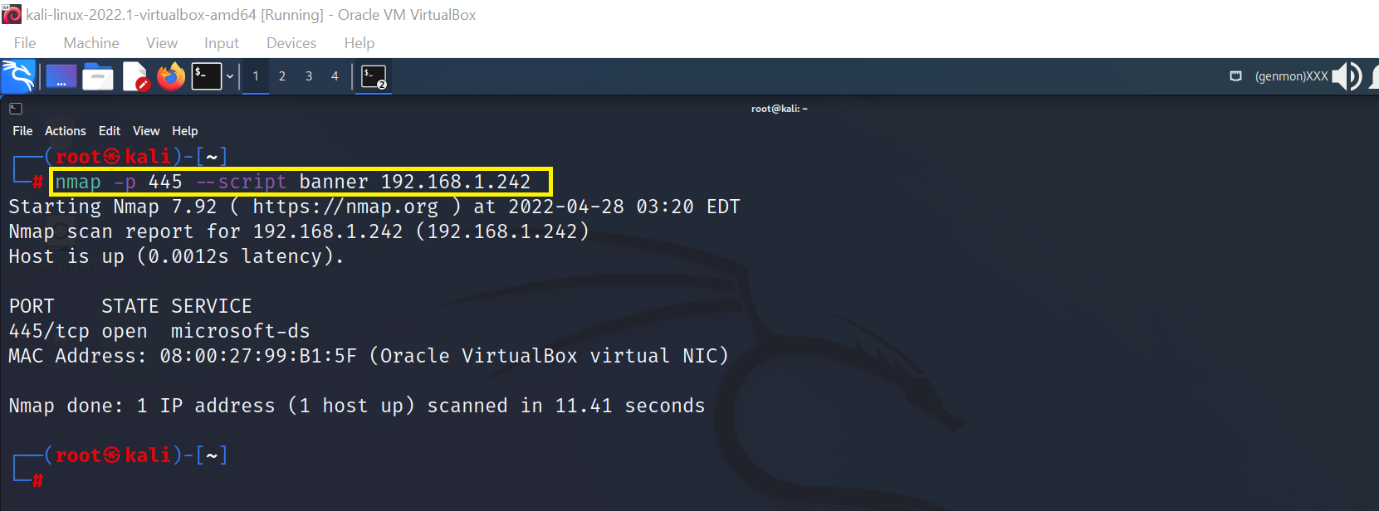
Connection: close

Content-Type: text/html

Another tool is nmap , in this tool we have grabbing script

**Command :-**

nmap -p [ports no] --script=banner [target IP]



**Dimitry :**

Command :- dmitry -b [ip]

**Metasploit**

This tool is very famous and very powerfull tool , we can do everything with this tool

Command :- msfconsole

auxiliary/scanner/portscan/tcp 🡨 this is a port scanner

it will scan all tcp ports like nmap

and nmap also come with prebuilt with Metasploit

### Port Numbers

* **Internet Assigned Numbers Authority** (IANA) - maintains Service Name and Transport Protocol Port Number Registry which lists all port number reservations
* Ranges
  + **Well-known ports** - 0 - 1023
  + **Registered ports** - 1024 - 49,151
  + **Dynamic ports** - 49,152 - 65,535

| **Port Number** | **Protocol** | **Transport Protocol** |
| --- | --- | --- |
| 20/21 | FTP | TCP |
| 22 | SSH | TCP |
| 23 | Telnet | TCP |
| 25 | SMTP | TCP |
| 53 | DNS | TCP/UDP |
| 67 | DHCP | UDP |
| 69 | TFTP | UDP |
| 80 | HTTP | TCP |
| 110 | POP3 | TCP |
| 135 | RPC | TCP |
| 137-139 | NetBIOS | TCP/UDP |
| 143 | IMAP | TCP |
| 161/162 | SNMP | UDP |
| 389 | LDAP | TCP/UDP |
| 443 | HTTPS | TCP |
| 445 | SMB | TCP |
| 514 | SYSLOG | UDP |