Nmap

Enumeration

- Most critical part of all.
  - Goal: To identify all possible ways we could attack a target
- This phase aims to improve our knowledge and understanding of the technologies, how they work and learn to deal with new information.
- More information, easier to find vectors of attack.

Enumeration

- When scanning, we look for two possibilities
  - Functions that allow us to interact with the target or provide additional information
  - Information that provides us with even more important information
- Most of the information comes from misconfigurations.

Enumeration

- More tools doesn’t mean success.
- Invest couple hours learning about the services
- Manual enumeration is critical.
  - Tools simplify and accelerate

Intro to Nmap

- Network Mapper is an open-source network analysis and security auditing tool
- Designed to scan networks and identify which available hosts.
- Offers scanning capabilities that can determine firewalls, IDS etc.

Use Cases

- Audit the security aspects of networks
- Simulate penetration tests
- Check firewall and IDS settings and configurations
- Types of possible connections
- Network mapping
- Response analysis
- Identify open ports
- Vulnerability assessment

Nmap Architecture

- Host discovery
- Port scanning
- Service enumeration and detection
- OS detection
- Nmap Scripting Engine

Syntax

- nmap <scan types> <options> <target>
  - nmap -sS -p- 192.168.1.56

Scan Techniques

- Offers many different scanning techniques

```
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
```

Things to know

- TCP-SYN scan (sS) is default
  - If our target reply with SYN-ACK, it means the port is open
  - If reply with RST, it means the port is closed
  - If no reply, it is deemed filtered.

Example

```
shivamaharjan[/root]$ sudo nmap -sS localhost

Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-11 22:50 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000010s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
5432/tcp open  postgresql
5901/tcp open  vnc-1

Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds
```

Host Discovery

- To start a internal penetration test, getting an overview of systems online are necessary.
- nmap <ip range> -sn -oA <filename to store>
  - nmap 196.168.56.0/24 -sn -oA hostDiscovery
    - 196.168.56.0/24 target network range
    - -sn: disables port scanning
    - -oA hostDiscovery: saves the result in all formats with name hostDiscovery

Scan IP List

- List of IPs can also be scanned
- nmap -sn -iL <host list>
  - nmap -sn -iL host.lst
    - -iL host.lst: scans against targets in host.lst file

Scan Multiple IPs

- nmap -sn 10.10.10.11 10.10.10.50 10.10.10.60
  - Scans specified ips
- nmap -sn 10.10.10.10-20
  - Scans ip range from 10 - 20

Scan Single IP

- nmap -sn 10.10.10.13
- nmap -sn 10.10.10.14 --packet-trace
  - --packet-trace: shows all packets sent and received
- nmap -sn 10.10.10.14 --packet-trace -PE --disable-arp-ping
  - --disable-arp-ping: disables default arp request and reply method and uses ICMP protocol to determine if host is alive
  - -PE: to ensure ICMP packets are sent

Host and Port Scanning

- Things to keep in mind:
  - Open ports and its services
  - Service versions
  - Information that the services provided
  - Operating system

State of scanned port

- Open
  - Indicates that the connection to the scanned port has been established
- Closed
  - Packet we received back contains a RST flag
- Filtered
  - Cannot correctly identify if port is open or closed, as no response is returned
- Unfiltered
  - Can occur only during TCP-ACK scan indicating port is accessible but cannot determine whether the port is open or closed
- Open|Filtered
  - If we do not get any response, Nmap will set this state. It indicated the port might be behind firewall

Discovering Open TCP ports

- Default: scans 1000 ports with SYN scan when run as root
- Can define ports like -p 21,22,80, 139,145 or -p 21-145 or –top-ports=10
- To scan all ports -p-

Nmap – Trace the Packets

- sudo nmap <ip-address> -p 21 --packet-trace -n -Pn --disable-arp-ping
  - --packet-trace: shows all packets sent and received
  - -n: disables dns resolution
  - -Pn: deems host as alive, disables ICMP echo request
  - --disable-arp-ping: disables arp ping

Nmap – Connect Scan

- Connect scan uses three way handshake to determine if a port is open or closed
- Is useful since it shows accurate state of port
- Since it has no abnormal activities, is deemed most stealthy scan
- nmap <ip> -sT --reason
  - -sT: Tcp connect scan
  - --reason: states why a port is in particular state

Filtered Ports

- A port can be shown as filtered for various reasons
- Packets might be dropped or rejected
- If no response if received then is deemed filtered.

Discovering Open UDP ports

- Sometimes sys-admins forget to filter UDP ports.
- Since no three way handshake occurs, this sort of scan takes a bit longer time.
- sudo nmap <ip> -sU
- If ICMP response with error code 3 is received, we can verify that the port is closed.
- -sV option can be used to know more about the versions of the open port.
- More about Nmap on:
  - https://nmap.org/book/man-port-scanning-techniques.html

Saving the Results

- -oX: xml format, Xml output
- -oN: nmap format, Normal output
- -oG: gnamp format, grepable output
- -oA: all format
- sudo nmap -p- <ip> -oA nmap_result
  - -oA: specifies type of file format to store
  - nmap_result: filename to store the output to
- .xml file can be converted to html
  - xsltproc nmap_result.xml -o nmap_result.html
- More on:
  - https://nmap.org/book/output.html

Service Enumeration

- -sV: is used for service enumeration.
- sudo nmap -p- <ip> -sV --stats-every=5s
  - -sV: service version
  - --stats-every=5s: shows the progress of scan every 5s

Nmap Scripting Engine

- Possibility to check default scripts provided by Nmap Scripting Engine (NSE)
- 14 different categories can be found:
- auth, brute, default, discovery, dos, exploit, external, etc.
- More on:
  - https://nmap.org/nsedoc/index.html

Script

- Default Script
  - nmap <ip> -sC
- Specific Script Category
  - nmap 10.0.0.25 --script vuln
- Defined Scripts
  - Nmap 10.0.0.50 -p25 --script banner,smtp-commands

Scan

- Aggressive Scan
  - nmap -p- 192.168.56.52 -A
    - Performs os detection, service detection, traceroute and uses default scripts to scan network
- Vulnerability Scan
  - nmap -p25 192.168.56.45 --script vuln
    - Scan for default vulnerabilities using vuln category from NSE

Performance

- -T <1-5>: Aggressiveness of scan
- --min-parallelism <number>: minimum number of threads to run scan
- --initial-rtt-timeout <time>: initial timeout for packet to return, rtt is round trip time usually in ms. Eg: 100ms
- --max-rtt-timeout <time>: max time out for packet to return
- --min-rate <number>: min number of packets to be sent per second
- --max-rate <number>: max number of packets to be sent per second
- --max-retries <number>: max number of retries

THM

- https://tryhackme.com/room/nmap01