NMAP

Deep Dive

What is 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
  - **NMAP** is the most widely used scanning and enumeration tool on the planet.
    - **NMAP** can perform many different types of scans from simply identifying active machines to port scanning and enumeration. You can also configure NMAP to control the speed of the scan. The slower the scan, the less likely it will be you will be discovered.

What Can NMAP Do?

- 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

How To Use NMAP Effectively

- Scanning a Single System
- If you want to scan a single system, then you can use a simple command
  - nmap target
  - nmap target.com
  - nmap 192.168.1.1

Scanning An Entire Subnet

- nmap target/cdir
- nmap 192.168.1.1/24

Scanning Multiple Targets

- 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

NMAP

Deep Dive

Scanning a Range of IP Addresses but Not An Entire Subnet

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

Excluding Specific IP Addresses In A Scan

- There could be a scenario when you want to scan an entire network, but it is dangerous to scan one particular machine. So you can exclude that machines IP address
- In this scenario, use the Nmap command with the excluding parameter
    - nmap 192.168.1.1/24 – -exclude 192.168.1.1
        - There are other scanning techniques but these are the main ones.

Options When Starting NMAP

- Starting NMAP without any of the options runs a "regular" scan and provides all sorts of information for you.
    - To get really sneaky and act like a hacker, you'll need to learn the many option switches to use when starting NMAP from the command line.
        - You will find an endless sources of information online on these switches you can use.

Zenmap

- Zenmap is a gui version of NMAP
    - Zenmap is the Nmap security scanner graphical user interface and provides for hundreds of options. It lets users do things like save scans and compare them, view network topology maps, view displays of ports running on a host or all hosts on a network, and store scans in a searchable database.

Now The Warning

- There are definitely things you should not scan with NMAP. As a beginner, limit scans to your local network on VirtualBox or the approved link I will give you.
- Would you scan 129.51.0.0? This is an IP address at Patrick Air Force Base. Don't do it!. 129.63.0.0 (Johnson Space Center)The military network monitoring folks would not appreciate you snooping around
- 128.50.0.0 Department of Defense. These guys are nervous, stay away.
- There are many other IP addresses you should not scan if you want to stay out or prison.
- Google Ip addresses you should not scan but here's a good start
- https://www.hellboundhackers.org/articles/read-article.php?article_id=721

NMAP

Deep Dive

Types Of Nmap Scans

- Using NMAP to perform a TCP connect scan
    - This scan is considered the most basic and stable of all port scans because NMAP attempts to complete a 3 way handshake on each port specified in the NMAP command.
        - There are many types of NMAP scans, we will just highlight some of the popular ones here.

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 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

NMAP

Deep Dive

Idle Scan (-sI)

- This is an advanced scan that provides complete anonymity while scanning. Nmap doesn't send the packets from your real IP address—instead of generating the packets from the attacker machine, Nmap uses another host from the target network to
    - Here is a representation
    - nmap -sI zombie_host target_host
    - nmap -sI 192.168.1.6 192.168.1.1
        - The idle scan technique (as mentioned above) is used to discover the open ports on 192.168.1.1 while it uses the zombie_host (192.168.1.6) to communicate with the target host. So this is an ideal technique to scan a target computer anonymously.

OS Detection NMAP

- One of the most important features 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.

OS Detection

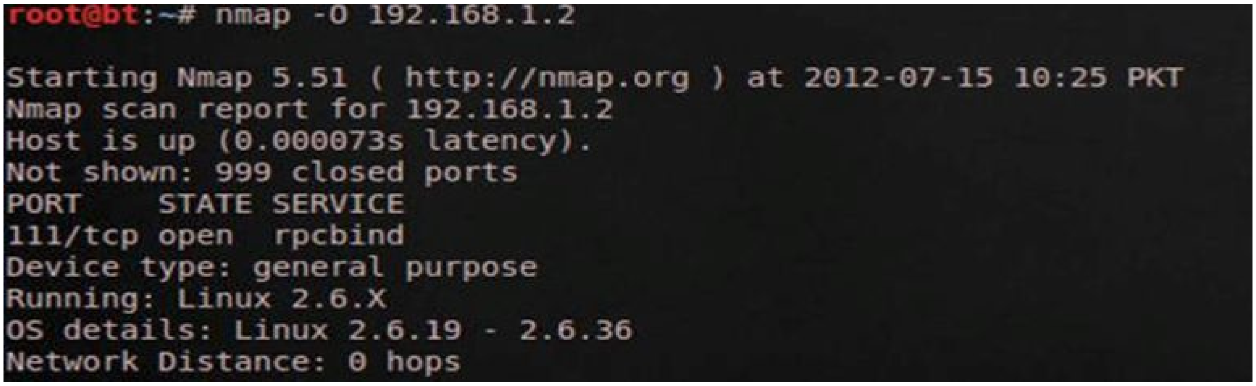
- Nmap has a database called nmap-os-db, the database contains information of more than 2,600 operating systems. Nmap sends TCP and UDP packets to the target machine and then it examines the response by comparing the result with the database. The Nmap operating system discovery technique is slightly slower then the scanning techniques because OS detection involves the process of finding open ports.

    -
      ```
      Initiating SYN Stealth Scan at 10:21
      Scanning localhost (127.0.0.1) [1000 ports]
      Discovered open port 111/tcp on 127.0.0.1
      Completed SYN Stealth Scan at 10:21, 0.08s elapsed (1000 total ports)
      Initiating OS detection (try #1) against localhost (127.0.0.1)
      Retrying OS detection (try #2) against localhost (127.0.0.1)
      ```
        - The example above clearly demonstrates that the Nmap first discovers the open ports, then it sends the packets to discover the remote operating system. The OS detection parameter is -O (capital O).

NMAP

Deep Dive

NMAP OS Scan Output



```
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
```

- Nmap OS fingerprinting technique discovers the:
- Device type (router, work station, and so on)
- Running (running operating system)
- OS details (the name and the version of OS)
- Network distance (the distance in hops between the target and attacker)