Date: 31-08-2020

NMAP – Information Gathering

Features of Nmap:

- Host discovery – Identifying hosts on a network. For example, listing the hosts that respond to TCP and/or ICMP requests or have a particular port open.
- Port scanning – Enumerating the open ports on target hosts.
- Version detection – Interrogating network services on remote devices to determine application name and version number.
- OS detection – Determining the operating system and hardware characteristics of network devices.
- Scriptable interaction with the target – using Nmap Scripting Engine (NSE) and Lua programming language.
- Nmap can provide further information on targets, including reverse DNS names, device types, and MAC addresses.

Typical uses of Nmap:

- Auditing the security of a device or firewall by identifying the network connections which can be made to, or through it.
- Identifying open ports on a target host in preparation for auditing.
- Network inventory, network mapping, maintenance and asset management.
- Auditing the security of a network by identifying new servers.
- Generating traffic to hosts on a network, response analysis and response time measurement.
- Finding and exploiting vulnerabilities in a network.

Syntax: nmap [<Scan Type> ...] [<Options>] {<target specification> }

Scan a single IP: This command scans a single IP on the network. If a threat hunter notices strange activity coming from an unfamiliar host, a single IP scan may be useful. Being able to quickly distinguish false positives from false negatives is critical for efficient network security. For example, a network attack might go unnoticed because too many false positives are triggering alerts, creating alert noise. The alert noise can potentially hide an attack from detection by creating a false negative. The noise also creates confusion and misdirection for the security analyst trying to determine if the attack is real or not. Using an intrusion detection system with an updated attack signature database will help distinguish false positives from false

negatives more efficiently. Also, it is important to remember that having too many false negatives can also cause problems. If the intrusion detection system misses an attack, no alerts are activated. This gives the security analyst the illusion that the network is safe and secure, which may not be the case. This is a major issue because an attack could be going on and nobody would be aware of it until it was too late:

nmap 10.30.151.151

Scan a host: This is the command to scan a single host. The information gained from this command can allow a hacker to quickly evaluate a high-value target on the network. Sometimes a hacker may be going after a specific host containing financial data records:

nmap www.google.com

Scan a range of IPs: This is the command to scan a range of IPs. Scanning a range of IPs is useful when trying to determine where a network attack may be occurring. Being able to scan multiple IPs also saves valuable time when tracing a network attack:

nmap 10.30.159.11-20

Scan a subnet: This command scans a subnet. Scanning a subnet will allow the scan to monitor multiple hosts. This command is useful when checking on multiple networks as well:

nmap 10.30.159.11/24

Nmap port selection

To utilize Nmap effectively, need to understand how to use the port selection options. The port selection options determine what ports will be scanned and whether the scan order is random or in a sequential order.

Scan a single port: This is the command to scan a single port. Some malware will consistently operate on a specific port on every host it infects. By knowing these ports, you can sometimes quickly determine what kind of malware you are dealing with. A single port scan would be useful in this situation:

nmap -p 80 10.30.151.151

Scan a range of ports: This is the command to scan a range of ports 1-100. The versatility of this command allows you to focus on specific ranges of ports:

nmap -p 1-1024 10.30.151.151

Scan 100 most common ports (fast): These are a number of different default scans. -f will scan the most common 100 ports used:

nmap -f 10.30.151.151

Scan all 65535 ports: This is the command to scan all ports. There are a total of 65,535 ports. A hacker will not usually employ this type of scan. Instead most hackers will initially use a scanning technique known as half-open scanning. The scan all ports command is better utilized by a threat hunter monitoring the network:

nmap -p- 10.30.151.151

Nmap port scan types

There are many different types of port scan that can be used with Nmap. It is important to know which type of port scan to use depending on your objective. For example, if you want to determine which TCP ports are active on a targeted host, run a TCP port scan. Hackers will often use various port scans to see if they can find a vulnerable open port to use as an attack vector.

Scan using TCP SYN scan (default): This command determines whether the port is listening. Using this command is a technique called half-open scanning. It is called **half-open scanning** because you don't establish a full TCP connection. Instead, you only send a SYN packet and wait for the response. If you receive a SYN/ACK response that means the port is listening:

nmap -sS 192.168.1.1

Scan using TCP connect: This is the command to scan using the TCP connect option. If a user does not have raw packet privileges, this is the command they will use:

nmap -sT 192.168.0.9

Privileged access is necessary to perform the default SYN scans. If privileges are not sufficient, a TCP connect scan will be used. A TCP connect scan needs a full TCP connection to be established, and is known to be a slower scan than SYN scans. Disregarding discovery is often required as many firewalls or hosts will not answer to ping, so it could be missed, unless you choose the -Pn parameter. Of course, this

can make the scan times much longer as you could end up sending scan probes to hosts that are not even there.

More Commands

Service and OS detection: Nmap is one of the most popular tools used for the enumeration of a targeted host. Nmap can use scans that provide the OS, version, and service detection for individual or multiple devices. Detection scans are critical to the enumeration process when conducting penetration testing of a network. It is important to know where vulnerable machines are located on the network so they can be fixed or replaced before they are attacked. Many attackers will use these scans to figure out what payloads would be most effective on a victim's device. The OS scan works by using the TCP/IP stack fingerprinting method. The services scan works by using the Nmap-service-probes database to enumerate details of services running on a targeted host.

Detect OS and Services: This is the command to scan and search for the OS (and the OS version) on a host. This command will provide valuable information for the enumeration phase of your network security assessment (if you only want to detect the operating system, type nmap -O 192.168.0.9):

nmap -A 192.168.0.9

Standard service detection: This is the command to scan for running service. Nmap contains a database of about 2,200 well-known services and associated ports. Examples of these services are HTTP (port 80), SMTP (port 25), DNS (port 53), and SSH (port 22):

nmap -sV 192.168.0.9

Nmap Basic Scan Commands:

Scan Type	Syntax	Example
TCP SYN Scan	-sS	nmap –sS 10.20.3.100
TCP Connect Scan	-sT	nmap –sT 10.20.3.100
Fin Scan	-sF	nmap –sF 10.20.3.100
XMAS Scan	-sX	nmap –sX 10.20.3.100
Null Scan	-sN	nmap –sN 10.20.3.100
Ping Scan	-sP	nmap –sP 10.20.3.100
Version Detection	-sV	nmap –sV 10.20.3.100
UDP Scan	-sU	nmap –sU 10.20.3.100
IP Protocol Scan	-sO	nmap –sO 10.20.3.100
ACK Scan	-sA	nmap –sA 10.20.3.100
Windows Scan	-sW	nmap –sW 10.20.3.100
List Scan	-sL	nmap –sL 10.20.3.100

More aggressive service detection: This is the command for an aggressive scan. Usually, experienced hackers will not use this command because it is noisy and leaves a large footprint on the network. Most black hat hackers prefer to run as silently as possible:

nmap -sV --version-intensity 5 192.168.0.9

Lighter banner-grabbing detection: This is the command for a light scan. A hacker will often use a light scan such as this to remain undetected. This scan is far less noisy than an aggressive scan. Running silently and staying undetected gives the hacker a major advantage while conducting enumeration of targeted hosts:

nmap -sV --version-intensity 0 192.168.0.9

Service and OS detection depend on different techniques to determine the operating system or service running on a certain port. A more aggressive service detection is useful if there are services running on unexpected ports, although the lighter version of the service will be much faster and leave less of a footprint. The lighter scan does not attempt to detect the service; it simply grabs the banner of the open service to determine what is running.

Nmap output formats

Save default output to file: This command saves the output of a scan. With Nmap, you can save the scan output in different formats:

nmap -oN outputfile.txt 192.168.0.12

Save in all formats: This command allows you to save in all formats. The default format can also be saved to a file using a file redirect command, or > file. Using the -oN option allows the results to be saved, but also allows them to be viewed in the terminal as the scan is being conducted:

nmap -oA outputfile 192.168.0.12

References:

1. https://nmap.org/book/man.html
2. https://www.networkcomputing.com/networking/nmap-tutorial-common-commands/520799832/page/0/1