NMAP

CHEAT-SHEET

Goverdhan Pandey

Table of Contents

Introduction to Nmap

Nmap is a free and open-source network security scanner. It is used to discover hosts and services on a network, as well as to gather information about those hosts and services. Nmap can be used for a variety of purposes, including network inventory, security auditing, and penetration testing.

Target Selection

Nmap can scan a single host, a range of hosts, or a subnet. To scan a single host, use the following command:

```
Code snippet
nmap 192.168.1.1
```

To scan a range of hosts, use the following command:

```
Code snippet
nmap 192.168.1.1-10
```

To scan a subnet, use the following command:

```
Code snippet
nmap 192.168.1.0/24
```

Port Selection

By default, Nmap scans the 1,000 most popular ports. You can specify a different range of ports to scan using the `-p` flag. For example, to scan the ports 22, 80, and 443, you would use the following command:

```
Code snippet
```

```
nmap -p 22,80,443 192.168.1.1
```

You can also scan all 65,535 ports by using the `-p-` flag.

Scan Types

Nmap supports a variety of scan types. The default scan type is a TCP SYN scan. This type of scan is relatively fast and stealthy. Other scan types include:

- TCP connect scan
- UDP scan
- ICMP echo scan
- FIN scan
- Xmas scan
- NULL scan

Service and Operating System Detection

Nmap can detect the services and operating systems running on a host. This information can be useful for security auditing and penetration testing. To detect services, Nmap uses a database of known services. To detect operating systems, Nmap uses a variety of methods, including fingerprinting.

Output Formats

Nmap can output its results in a variety of formats, including:

- Text
- XML

- HTML
- CSV
- Markdown

The output format can be specified using the `-o` flag.

NSE Scripting

Nmap NSE (Nmap Scripting Engine) is a library of scripts that can be used to extend Nmap's functionality. NSE scripts can be used for a variety of purposes, including:

- Port scanning
- Service detection
- Operating system detection
- Vulnerability detection
- Intrusion detection

NSE scripts can be loaded into Nmap using the `-sC` flag.

Firewall / IDS Evasion and Spoofing

Nmap can be configured to evade firewalls and IDS systems. This can be done by using a variety of techniques, such as:

- Using stealth scan types
- Spoofing the source IP address
- Using random source ports

Helpful Nmap Output Examples

Here are some helpful examples of Nmap output:

- `Host is up (0.000007s latency).` This line indicates that the host is up and running.
- `PORT STATE SERVICE` This line indicates that the port is open and the service running on it is identified.
- `OS: Linux 2.6.32-431.11.1.el6.x86_64 (CentOS)` This line indicates the operating system running on the host.

Miscellaneous Nmap Flags

Here are some miscellaneous Nmap flags that you may find useful:

- `-T4` This flag specifies a faster scan.
- `-A` This flag enables all Nmap's OS detection capabilities.
- `-v` This flag increases the verbosity of Nmap's output.
- `-d` This flag enables debug output.

Other Useful Nmap Commands

Here are some other useful Nmap commands:

- `nmap --help` This command displays a list

Frequently Asked Questions

- What is the difference between a TCP SYN scan and a TCP connect scan?

A TCP SYN scan is a stealthier scan type than a TCP connect scan. A

TCP SYN scan does not actually establish a full TCP connection with the target host. Instead, it sends a SYN packet and waits for a response. If the target host responds with a SYN-ACK packet, then the port is considered to be open. A TCP connect scan, on the other hand, does establish a full TCP connection with the target host. This makes it a less stealthy scan type, but it also allows Nmap to gather more information about the target host, such as the service running on the port.

- How do I scan a range of ports with Nmap?

You can scan a range of ports with Nmap by using the `-p` flag. For example, to scan the ports 22, 80, and 443, you would use the following command:

```
Code snippet
nmap -p 22,80,443 192.168.1.1
```

You can also scan all 65,535 ports by using the `-p-` flag.

- How do I detect the operating system running on a host with Nmap?

Nmap can detect the operating system running on a host by using a variety of methods, including fingerprinting. Fingerprinting is the process of identifying a host's operating system by sending it a series of packets and observing the responses. Nmap uses a database of known operating system fingerprints to identify the operating system running on a host.

- How do I use NSE scripts with Nmap?

NSE scripts can be loaded into Nmap using the `-sC` flag. For example, to load the `http-vuln-cve2017-5638` NSE script, you would use the following command:

```
Code snippet
nmap -sC http-vuln-cve2017-5638 192.168.1.1
```

This script will scan the target host for the Heartbleed vulnerability.

- How do I evade firewalls and IDS systems with Nmap?

There are a number of ways to evade firewalls and IDS systems with Nmap. One way is to use stealth scan types, such as the TCP SYN scan. Another way is to spoof the source IP address of your Nmap scans. You can also use random source ports to make it more difficult for firewalls and IDS systems to detect your scans.

Conclusion

This cheat sheet has covered the basics of Nmap. For more information, please refer to the Nmap documentation: https://nmap.org/docs.html

Follow :

Linkedin : https://www.linkedin.com/in/goverdhankumar/
Github : https://github.com/wh04m1i
https://linktr.ee/g0v3rdh4n