Nmap

Introduction

Nmap= network mapper

Nmap is a free and open source tool that many hackers keep handy in their tool belts. It's often our first weapon of choice as recon is very important and we can't know what to investigate if we don't even know what ports are open on our server.

Ports

When i talk about ports, i can talk about both UDP and TCP ports. There is a big difference between these two protocols but to keep it simple, TCP packages always give a confirmation making it so that every package surely gets delivers. This takes time as the server has to wait for the confirmation for every single package. UDP tries to get rid of that by simply sending the packages and not waiting for confirmation.

TCP is often used in applications where it's very important all packages get delivered in the exact order. For example if you download a file, that will probably be done in the TCP protocol whereas a youtube video will probably be sent through a port via UDP.

I keep talking about everything but Nmap it seems but to understand what it does, we need to understand these basic concepts first. It's really important to know there are 65,535 ports that a server can have in use.

Status of the ports

These ports can have different statuses, just like ports in real life. They can be opened which is pretty self explanatory, it would be like an open gate where all the foot traffic would be allowed to go through as long as they follow the protocol that is bound to that port.

Open

Every open port is going to form a risk in terms of attackers like us. We are trying to find open ports so we can possible find out what is running on that ports (For example a webserver or ssh) and then possibly try to find an exploit for it. Our biggest attack surface is going to be web in most cases which will be running on port 80 and/or 443. Don't be fooled though, webservers can be configured to run on any port and both on the TCP/UDP protocols. More on this later in the "flags" chapter.

Closed

A closed port is pretty useless to us as hackers, we can access it but there is nothing running it, basically an empty pit that we can stuff too.

Filtered

A filtered port is mostly a mystery to us. How Nmap works is it sends a probe to a port and waits for a reply but in case of a filtered port, a package filter is preventing our probe from reaching our target. These ports are very frustrating to an attacked because they provide very little information.

Others

There are some other statuses as well but they are less prevalent while pentesting and can be found in the Nmap documentation or the help pages.

- Unfiltered
- open|filtered

- closed|filtered

https://nmap.org/book/man-port-scanning-basics.html

Basic nmap scan

If we combine all this we can execute several useful nmap commands. Right now we have the basics ready where we can scan an IP adres or website(As these URLs also resolve to an IP, they can also be scanned but be mindful of things like loadbalancers here).

```
nmap 10.10.10.10
```

Show me your secrets

Knowing whether or not a port is open or closed is ofcourse useful information but what we really need to know is what software is listening on that port. This is where nmap starts to get interesting because we can work with flags.

```
nmap -sV 10.10.10.10
```

When we add the -sV flag, Nmap will automatically try to grab the banners wherever possible. Every application that runs on a network port broadcasts a banner unless the administrators disabled it. Nmap will also try to grab the version of the software running to give you a better overview of where to look and how to exploit it possibly. We can use this data and go to exploit-db to find our exploit and execute a PoC.

```
nmap -sV --version-intensity 9 10.10.10.10
```

If we add the --version-intensity flag, we can make Nmap's version identifying probes either more or less likely to identify the correct version of software but ofcourse a higher level of intensity will take a lot longer.

Scripting the night away

Nmap also comes with a bunch of pre-installed scripts that you can run. By default it will not run these scripts but if we add the -sV flag, Nmap will execute the scripts that match the port it's found. For example if it finds port 80 and then it will run all the scripts it has available for a webserver.

```
nmap -sC 10.10.10.10
```

Expanding our scans

By default nmap will scan only the top 1000 most popular post but there are so many more. It will also just scan UDP ports by default. If we want to add TCP we need to add another flag as well.

```
nmap -p- 10.10.10.10
```

```
nmap -sU 10.10.10.10
```

```
nmap -sT -p- 10.10.10.10
```