Infrastructure

Port Scanning with NMAP Commands

Scan All TCP Ports with Range

We can specify the port range with the -p option. As we know TCP port numbers are between 0 and 65535 . We will use -p0-65535 as an option in order to scan all TCP ports. We do not specify the TCP protocol because the default protocol for Nmap port scan is TCP.

```
$ nmap -p0-65535 192.168.122.1
```

Faster Scan For All Ports

If we are scanning all ports this will take a lot of time. If the situation is not critical we can use a faster scan with -T5 parameter. This is the fastest scan level for Nmap. This option can be used for UDP scans too.

```
$ nmap  -p0-65535 192.168.122.1 -T5
```

Scan All TCP Ports

Another way to specify all TCP ports is a dash. We can use -p- which is more practical then port range specification.

```
$ nmap -p- 192.168.122.1
```

Scan All UDP Ports with Range

Nmap uses TCP as the default protocol for the port scan. We should explicitly specify the UDP protocol for the UDP port scan. We will use the same port range specification used in TCP. We will use -sU for UDP protocol specification.

```
$ nmap -sU -p0-65535 192.168.122.1
```

Scan All UDP Ports

We can also scan all UDP ports by using the -sU option. We will use -p- to specify all ports easily. -p- express all ports from 0 to 65535. UDP scan is slow and takes some time to complete.

```
$ nmap -sU -p- 192.168.122.1
```

Scan All TCP UDP Ports

We can scan all UDP and TCP ports in a single command. We will use -sU for UDP and sT for TCP protocol. We will also specify the port range we want to scan which is all TCP and UDP ports that start from 0 to 65535. This will scan all 65535 ports of TCP and UDP for the specified remote host or IP address. Keep in mind that this will take some time because especially UDP scan is slow according to the TCP scan. We will also provide root privileges with the sudo command.

```
$ sudo nmap -sU -sT -p0-65535 192.168.122.1
```

Unique solution ID: #1023
Author: n/a
Last update: 2021-01-31 18:22