Optimizing your scans

Scan Type Selection

While performing a scan, we have to choose the appropriate scan type based on our objectives and target environment. For example, we will use a SYN scan (`-sS`) for stealthier scanning while a TCP connect scan (`-sT`) for more reliable results.

Port Scanning Techniques

Instead of scanning all 65,535 ports, specify only the relevant port numbers or ranges using the `-p` option. This can significantly reduce scan times.

```
sudo nmap -p 80,22,443 IP

sudo nmap -p 21-100 IP
```

- If we dont specify any port option. Then nmap By default takes top 1000 most common ports.

```
sudo nmap IP
```

- If want to perform a all ports scan, scanning all 65,535 ports. We have to use -p- option.

```
sudo nmap -p- IP
```

- If we want to scan top 100 common ports, we can use the -F option.

```
sudo nmap -F IP
```

Timing and Performance Tuning

When running Nmap scans, there is a trade-off between speed and accuracy. Faster scans are less accurate, while slower scans provide more reliable results. Nmap provides various options to adjust the timing and performance to balance this trade-off based on our needs.

Timing Templates

Nmap has pre-defined timing templates from 0 (slowest) to 5 (fastest) that we can use with the `-T` option. For example, `-T4` is an aggressive scan, while `-T0` is a very slow, stealthy scan to evade firewalls and IDS.

The default timing template that nmap uses is -T3.

```
nmap -T0 IP

nmap -T5 IP
```

Parallelism

Nmap can scan multiple hosts in parallel. The `--min-parallelism` and `--max-parallelism` options control how many parallel probes Nmap sends at once. More parallelism speeds up scans but can overwhelm networks

Suppose you are dealing with a a large network with multiple hosts. Then we can use these techniques to parallelly scan each hosts in a short amount of time.

- **--min-parallelism** - This option sets the minimum number of parallel probes that Nmap will have outstanding at any time. Higher values increase parallelism and speed up scans, but can overwhelm networks.

```
nmap --min-parallelism 100 192.168.29.0/24
```

--max-parallelism - This option sets the maximum number of parallel probes across all hosts being scanned. It prevents Nmap from sending too many probes in parallel which could cause excessive network load.

```
nmap --max-parallelism 100 192.168.29.0/24
```

Host timeout

The `--host-timeout` option tells Nmap how long to wait for a host to respond before giving up and moving on. This is useful for slow networks or firewalls that rate-limit connections

```
nmap --host-timeout 5 192.168.29.0/24
```

Host Discovery Optimization

Suppose we have already discovered the live host on a network using the host discovery techniques we have learned earlier. Now while performing the port scans, we can skip the host discovery this time as we already know the live hosts.

This can be done using -Pn flag. We can also skip the DNS resolution using -n flag as we are already dealing with the IP address and no DNS lookup is required for that.

```
nmap -r -Pn IP
```

Output Formatting

While performing all the scans, we have to wait for the result to come back. Sometimes this is fast but sometimes it takes a lot of time. We can use the verbose mode to output real time information of our scans by proving -v flag.

It also works on intensity if we provide -vv it will give more result and with -vvv the maximum verbose output.

After performing so many scans, we do not to store the results somewhere so that we can review them later and add it to our penetration testing report. To do that, we have various nmap options.

The best output format to use is the -oA which gives us the output in all three major formats like text one, XML one and the greppable one.

```
nmap IP -oA nmap_result
```
