How to Use NMAP (1) on a Security Test

NMAP is a standard TCP/UDP port scanning tool. It allows us to identify open and closed ports on a target system. It supports a number of scanning techniques and allows to scan all ports or specific ports. It also allows us to identify the operating system that is running on the target system. To perform a simple scan against a machine, with the most common TCP ports we can do the following:

```
$ nmap www.merimetso.net
```

Please note that run these scans you must be root. The following scan will scan all TCP ports on the target system `192.168.2.12`. When performing a scan, it is important to disable ICMP host discovery. The reason for this is that Microsoft windows systems block ICMP traffic.

```
$ sudo nmap -Pn -sT -sV -O -p 0-65535 192.168.2.12
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-08 15:31 EDT
Nmap scan report for 192.168.2.13
Host is up (0.0012s latency).
Not shown: 65522 closed tcp ports (conn-refused)
PORT      STATE SERVICE  VERSION
53/tcp    open  domain      ISC BIND 9.9.5-3ubuntu0.19 (Ubuntu Linux)
111/tcp   open  rpcbind     2-4 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: DMZ)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: DMZ)
2049/tcp  open  nfs_acl     2-3 (RPC #100227)
38541/tcp open  nlockmgr    1-4 (RPC #100021)
47736/tcp open  mountd      1-3 (RPC #100005)
59573/tcp open  status      1 (RPC #100024)
Service Info: Host: NS01; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

This scan performs a TCP Connect scan (`-sT`), on each open port it performs banner grabbing (`-sV`), then it performs operating systems finger printing (`-O`). It also scans all TCP ports (`-p 0-65335`). It is often useful to make use of CIDR address when performing a scan. So, to scan every TCP on a class C network we would perform the following

```
$ sudo nmap -Pn -sT -sV -O -p 0-65535 192.168.2.0/24
```

The following scan will scan all TCP ports on the target system `192.168.2.12`. This scan performs a UDP scan (`-sU`) on all UDP ports (`-p 0-65535`).

```
$ sudo nmap -Pn -sU -p 0-65535 192.168.2.12
```

We can configure NMAP to perform a number of other useful functions when.

- Perform a TCP connect scan on a class C network on all ports
    - **`nmap -Pn -sT -p 0-65535 192.168.2.0/24`**
- Write all output to a file as normal output.
    - **`nmap -Pn -sT -oN output.txt -p 0-65535 192.168.2.12`**
- Perform an TCP Connect (`-sT`) Scan every port **(`-p 0-65535`)** for every address in the input file (`-iL input.txt`) and write it to an output file (`-oN output.txt`) as standard text
    - **`nmap -Pn -sT -oN output.txt -iL input.txt -p 0-65535`**

NMAP supports a number of other TCP scanning methods such as

```
-sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
-sN/sF/sX: TCP Null, FIN, and Xmas scans
```