Common Nmap Scans

The UDP scan (-sU) can also be used in conjunction with a TCP SYN scan (-sS) option to build a more complete picture of our target:

```
kali@kali:~$ sudo nmap -sS -sU 10.11.1.115
```

When performing a network sweep with Nmap using the -sn option, the host discovery process consists of more than just sending an ICMP echo request. Several other probes are used in addition to the ICMP request. Nmap also sends a TCP SYN packet to port 443, a TCP ACK packet to port 80, and an ICMP timestamp request to verify if a host is available or not. `kali@kali:~$ nmap -sn 10.11.1.1-254`

We can also sweep for specific TCP or UDP ports across the network, probing for common services and ports, in an attempt to locate systems that may be useful, or otherwise have known vulnerabilities. This scan tends to be more accurate than a ping sweep:

```
nmap -p 80 10.11.1.1-254 -oG web-sweep.txt
```

To save time and network resources, we can also scan multiple IPs, probing for a short list of common ports. For example, let's conduct a TCP connect scan for the top twenty TCP ports with the –top-ports option and enable OS version detection, script scanning, and traceroute with -A:

```
kali@kali:~$ nmap -sT -A --top-ports=20 10.11.1.1-254 -oG top-port-sweep.txt
```

nmap OS fingerprint scan:

```
kali@kali:~$ sudo nmap -O 10.11.1.220
```

We can also identify services running on specific ports by inspecting service banners (-sV) and running various OS and service enumeration scripts (–A) against the target:

```
kali@kali:~$ nmap -sV -sT -A 10.11.1.220
```

Nmap script example:

```
kali@kali:~$ nmap --script-help dns-zone-transfer
Requests a zone transfer (AXFR) from a DNS server.
The script sends an AXFR query to a DNS server. The domain to query is
determined by examining the name given on the command line, the DNS
server's hostname, or it can be specified with the
<code>dns-zone-transfer.domain</code> script argument.

kali@kali:~$ nmap --script=dns-zone-transfer -p 53 ns2.megacorpone.com
```

Quick TCP Scan

```
-sC -sV -vv -oA quick 10.10.10.10
```

Quick UDP Scan

```
nmap -sU -sV -vv -oA quick_udp 10.10.10.10
```

Full TCP Scan

```
nmap -sC -sV -p- -vv -oA full 10.10.10.10
```