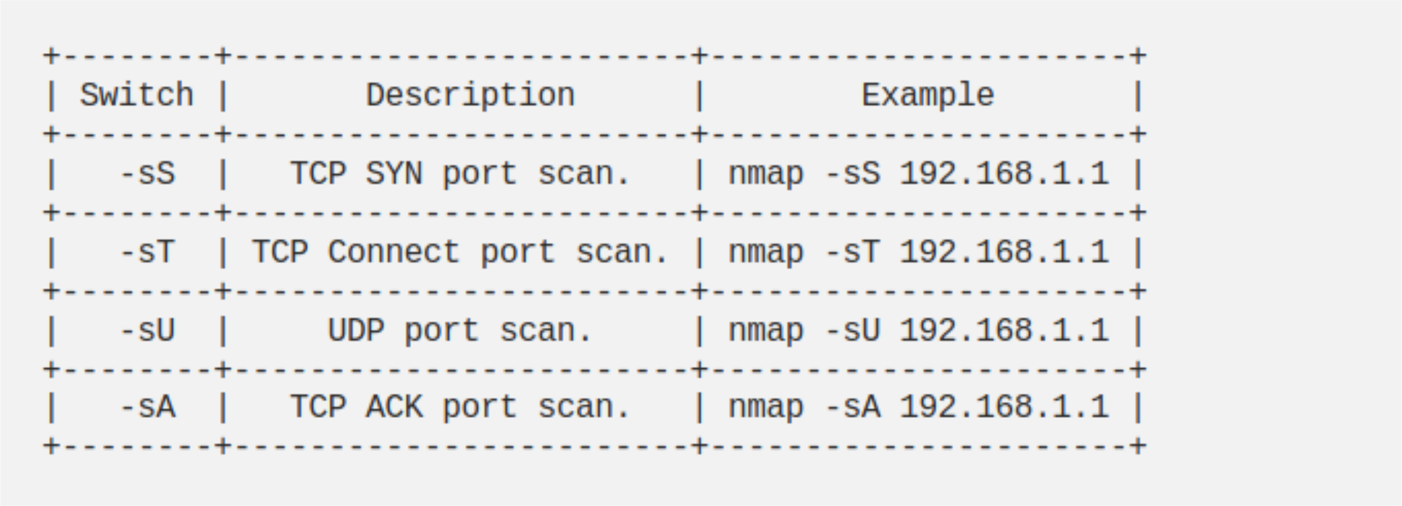
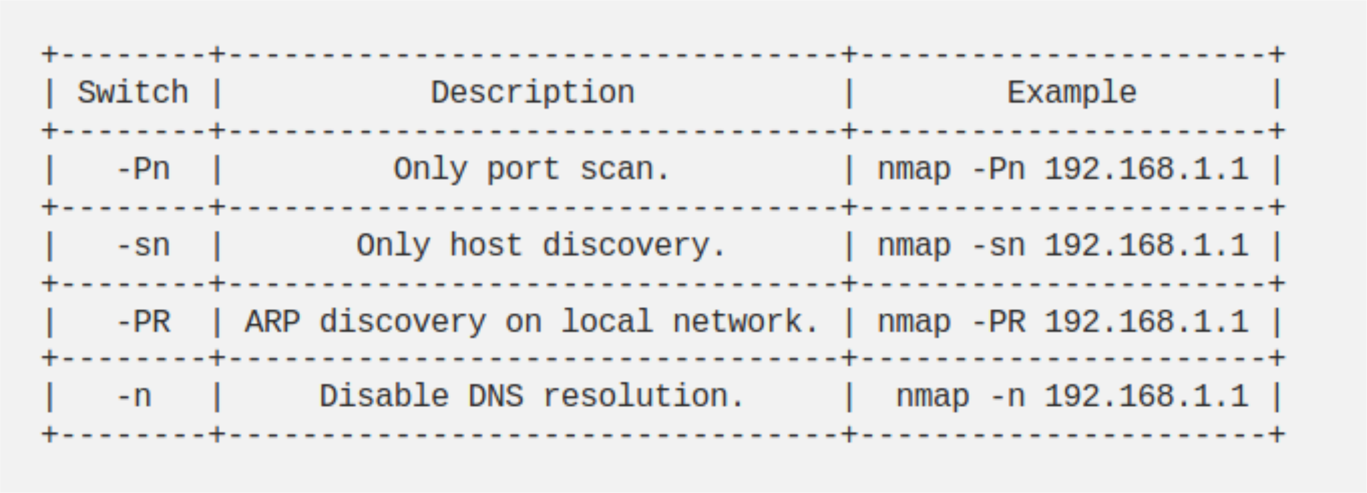
Scan Techniques



```
+--------+------------------------+----------------------+
| Switch |      Description       |       Example        |
+--------+------------------------+----------------------+
|  -sS   |   TCP SYN port scan.   | nmap -sS 192.168.1.1 |
+--------+------------------------+----------------------+
|  -sT   | TCP Connect port scan. | nmap -sT 192.168.1.1 |
+--------+------------------------+----------------------+
|  -sU   |     UDP port scan.     | nmap -sU 192.168.1.1 |
+--------+------------------------+----------------------+
|  -sA   |   TCP ACK port scan.   | nmap -sA 192.168.1.1 |
+--------+------------------------+----------------------+
```

Host Discovery



```
+--------+---------------------------------+----------------------+
| Switch |           Description           |       Example        |
+--------+---------------------------------+----------------------+
|  -Pn   |         Only port scan.         | nmap -Pn 192.168.1.1 |
+--------+---------------------------------+----------------------+
|  -sn   |      Only host discovery.       | nmap -sn 192.168.1.1 |
+--------+---------------------------------+----------------------+
|  -PR   | ARP discovery on local network. | nmap -PR 192.168.1.1 |
+--------+---------------------------------+----------------------+
|  -n    |     Disable DNS resolution.     |  nmap -n 192.168.1.1 |
+--------+---------------------------------+----------------------+
```

Port Specification

```
+--------+---------------------------+---------------------------+
| Switch |        Description        |          Example          |
+--------+---------------------------+---------------------------+
|   -p   |    Port or port range.    | nmap -p 22-80 192.168.1.1 |
+--------+---------------------------+---------------------------+
|   -p-  |      Scan all ports.      |    nmap -p- 192.168.1.1   |
+--------+---------------------------+---------------------------+
|   -F   | Fast port scan. (top 100) |    nmap -F 192.168.1.1    |
+--------+---------------------------+---------------------------+
```

Service and Version Detection

```
+--------+---------------------------------+----------------------+
| Switch |           Description           |        Example       |
+--------+---------------------------------+----------------------+
|   -sV  | Detect the version of services. | nmap -sV 192.168.1.1 |
+--------+---------------------------------+----------------------+
|   -A   |      Enable OS detection,       |  nmap -A 192.168.1.1 |
|        |       version detection,        |                      |
|        | script scanning and traceroute. |                      |
+--------+---------------------------------+----------------------+
```

OS Detection

```
+--------+-------------------------------+---------------------+
| Switch |          Description          |       Example       |
+--------+-------------------------------+---------------------+
|   -O   |       Identify OS using       | nmap -O 192.168.1.1 |
|        | TCP/IP strack fingerprinting. |                     |
+--------+-------------------------------+---------------------+
```

Timing and Performance

```
+--------+----------------------------------+----------------------+
| Switch |           Description            |       Example        |
+--------+----------------------------------+----------------------+
|   -T0  |       Paranoid IDS evasion.      | nmap -T0 192.168.1.1 |
+--------+----------------------------------+----------------------+
|   -T1  |        Sneaky IDS evasion.       | nmap -T1 192.168.1.1 |
+--------+----------------------------------+----------------------+
|   -T2  |        Polite IDS evasion.       | nmap -T2 192.168.1.1 |
|        |     (requires less bandwidth)    |                      |
+--------+----------------------------------+----------------------+
|   -T3  |   Normal IDS evasion. (default)  | nmap -T3 192.168.1.1 |
+--------+----------------------------------+----------------------+
|   -T4  |      Aggressive speed scan.      | nmap -T4 192.168.1.1 |
|        |      (requires fast network)     |                      |
+--------+----------------------------------+----------------------+
|   -T5  |        Insane speed scan.        | nmap -T5 192.168.1.1 |
|        | (requires massive network speed) |                      |
+--------+----------------------------------+----------------------+
```

NSE Scripts

```
+-----------------+------------------------+----------------------+
|      Switch     |       Description      |        Example       |
+-----------------+------------------------+----------------------+
|       -sC       |  Default script scan.  | nmap -sC 192.168.1.1 |
+-----------------+------------------------+----------------------+
| --script banner | Specify single script. | nmap --script banner |
|                 |    (banner grabbing)   |      192.168.1.1     |
+-----------------+------------------------+----------------------+
```

Firewall / IDS Evasion

```
+--------+-------------------------------+------------------------+
| Switch |          Description          |         Example        |
+--------+-------------------------------+------------------------+
|   -f   |   Use fragmented IP packets.  |   nmap -f 192.168.1.1  |
|        |    (packet filter evasion)    |                        |
+--------+-------------------------------+------------------------+
|   -D   |          Decoy scan.          |   nmap -D 192.168.1.1  |
|        |      (spoofed source IPs)     |                        |
+--------+-------------------------------+------------------------+
|   -g   | Use given source port number. | nmap -g 22 192.168.1.1 |
+--------+-------------------------------+------------------------+
```