nmap

> Network exploration tool and security / port scanner.
> Some features only activate when Nmap is run with privileges.

- Try to determine whether the specified hosts are up and what are their names:

```
nmap -sn {{ip_or_hostname}} {{optional_another_address}}
```

- Like above, but also run a default 1000-port TCP scan if host seems up:

```
nmap {{ip_or_hostname}} {{optional_another_address}}
```

- Also enable scripts, service detection, OS fingerprinting and traceroute:

```
nmap -A {{address_or_addresses}}
```

- Assume good network connection and speed up execution:

```
nmap -T4 {{address_or_addresses}}
```

- Scan a specific list of ports (use -p- for all ports 1-65535):

```
nmap -p {{port1,port2,...,portN}} {{address_or_addresses}}
```

- Perform TCP and UDP scanning (use -sU for UDP only, -sZ for SCTP, -sO for IP):

```
nmap -sSU {{address_or_addresses}}
```

- Perform TLS cipher scan against a host to determine supported ciphers and SSL/TLS protocols:

```
nmap --script ssl-enum-ciphers {{address_or_addresses}} -p 443
```