NMAP Cheatsheet

Basic Usage:

- Scan a single tarrget: **nmap [target]**
- Scan multiple targets: **nmap -sT [target]**

Scanning Techniques:

- Basic scan: **nmap -sP [target]**
- TCP SYN Scan: **nmap -sS [target]**
- TCP Connect Scan: **nmap -sT [target]**
- UDP Scan: **nmap -sU [target]**
- Comprehensive Scan: **nmap -sC [target]**
- All Ports Scan: **nmap -p [target]**
- OS Detection: **nmap -O [target]**

Output Options:

- Save results to a file: **nmap -oN output.txt [target]**
- Save results in XML format: **nmap -oX output.xml [target]**
- Verbose output: **nmap -v [target]**

Port Specification:

- Scan specific port(s): **nmap -p [port(s)] [target] (example nmap -p 80,443 [target])**
- Scan port ranges: **nmap -p [port-range] [target] (example nmap -p 1-100 [target])**

Timing and Performance:

- Faster scan (may be less accurate): **nmap -T4 [target]**
- Slower scan (more thorough): **nmap -T2 [target]**

Service Version Detection:

- Enable service version detection: **nmap -sV [target]**
- Aggressive service version: **nmap -A [target]**

Scripting Engine:

- Run Nmap scripts: **nmap --script [script-name] [target]**
- List available scripts: **ls /usr/share/nmap/scripts/**

Firewall Evasion:

- Fragment packets: **nmap -f [target]**
- Use decoy addresses: **nmap -D [decoy1,decoy2,me] [target]**

Operating System Detection:

- Detect OS and services: **nmap -A [target]**

Other Options:

- Specify source IP address: **nmap -S [source-IP] [target]**
- Disable DNS resolution: **nmap -n [target]**

Remember to replace **[target]** with the target IP address or hostname, and adjust the options to suit your scanning needs. Nmap provides a wide range of options and capabilities, so this cheat sheet covers some of the most used commands.

You can refer to the Nmap manual (**man nmap**) for more detailed information and options.