Nmap Target Selection

Scan a single IP	`nmap 192.168.1.1`
Scan a host	`nmap www.testhostname.com`
Scan a range of IPs	`nmap 192.168.1.1-20`
Scan a subnet	`nmap 192.168.1.0/24`
Scan targets from a text file	`nmap -iL list-of-ips.txt`

These are all default scans, which will scan 1000 TCP ports. Host discovery will take place.

Nmap Port Selection

Scan a single Port	`nmap -p 22 192.168.1.1`
Scan a range of ports	`nmap -p 1-100 192.168.1.1`
Scan 100 most common ports (Fast)	`nmap -F 192.168.1.1`
Scan all 65535 ports	`nmap -p- 192.168.1.1`

Nmap Port Scan types

Scan using TCP connect	`nmap -sT 192.168.1.1`
Scan using TCP SYN scan (default)	`nmap -sS 192.168.1.1`
Scan UDP ports	`nmap -sU -p 123,161,162 192.168.1.1`
Scan selected ports - ignore discovery	`nmap -Pn -F 192.168.1.1`

Privileged access is required to perform the default SYN scans. If privileges are insufficient a TCP connect scan will be used. A TCP connect requires a full TCP connection to be established and therefore is a slower scan. Ignoring discovery is often required as many firewalls or hosts will not respond to PING, so could be missed unless you select the -Pn parameter. Of course this can make scan times much longer as you could end up sending scan probes to hosts that are not there.

Take a look at the Nmap Tutorial for a detailed look at the scan process.

Service and OS Detection

Detect OS and Services	nmap -A 192.168.1.1
Standard service detection	nmap -sV 192.168.1.1
More aggressive Service Detection	nmap -sV --version-intensity 5 192.168.1.1
Lighter banner grabbing detection	nmap -sV --version-intensity 0 192.168.1.1

Service and OS detection rely on different methods to determine the operating system or service running on a particular port. The more aggressive service detection is often helpful if there are services running on unusual ports. On the other hand the lighter version of the service will be much faster as it does not really attempt to detect the service simply grabbing the banner of the open service.

Nmap Output Formats

Save default output to file	nmap -oN outputfile.txt 192.168.1.1
Save results as XML	nmap -oX outputfile.xml 192.168.1.1
Save results in a format for grep	nmap -oG outputfile.txt 192.168.1.1
Save in all formats	nmap -oA outputfile 192.168.1.1

The default format could also be saved to a file using a simple file redirect command > file. Using the -oN option allows the results to be saved but also can be monitored in the terminal as the scan is under way.