# Introduction to Nmap

Nmap, short for "Network Mapper," is an open-source network exploration and security auditing tool. It's used to discover hosts, services, and other critical information on a network.

Nmap uses raw IP packets to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems they're running on, and what type of packet filters/firewalls are in use.

# Basic Scanning Techniques

## Basic host discovery

```
nmap -sn 192.168.1.0/24
```

This command performs a ping scan, also known as a "host discovery," to find live hosts within the specified IP range.

## Scan specific ports

```
nmap -p 80,443 192.168.1.1
```

Scans only specific ports (in this example, ports 80 and 443) on the specified IP address.

## Service version detection

```
nmap -sV 192.168.1.1
```

This command attempts to determine the service versions running on open ports. It's particularly useful for identifying software and its versions running on target systems.

# Advanced Scanning Techniques

## OS detection

```
nmap -O 192.168.1.1
```

Conducts OS detection to try and identify the operating system of the target host.

## Aggressive scan

```
nmap -A 192.168.1.1
```

The aggressive scan option enables various scan types including OS detection, service version detection, script scanning, and traceroute information.

# Output and Reporting

## Save output to a file

```
nmap -oN output.txt 192.168.1.1
```

Saves the scan results to a specified file in normal format (text).

## Output in XML format

```
nmap -oX output.xml 192.168.1.1
```

Saves the scan results in XML format, facilitating easy parsing by other tools for further analysis and reporting.

# Scripting and Automation

## Run a script against a target

```
nmap --script <script-name> 192.168.1.1
```

Executes a specific NSE (Nmap Scripting Engine) script designed to perform various tasks like vulnerability scanning, service enumeration, etc.

## Directory brute-force using NSE script

```
nmap --script=http-enum 192.168.1.1
```

Executes an NSE script focused on HTTP enumeration to discover directories and files on a web server.

# Timing and Performance

## Timing templates

```
nmap -T4 192.168.1.1
```

Sets the timing template to "aggressive" for faster scans. This might be more detectable but can provide quicker results.

## Scan multiple targets in a file

```
nmap -iL <targets.txt>
```

Reads a list of targets from a file and scans them. This can be useful for scanning multiple hosts in a single command.

Understanding these techniques allows for better utilization of Nmap's capabilities in a variety of scenarios.

Always remember to use Nmap responsibly, with proper authorization, and in compliance with the law and ethical standards.