TryHackMe – Nmap

Walkthrough

Contents

[Nmap 2](#_Toc146820653)

[Vulnerability Scan 2](#_Toc146820654)

[TCP/UDP/SYN 2](#_Toc146820655)

[NULL/FIN/XMAS 2](#_Toc146820656)

[ICMP Scan 2](#_Toc146820657)

[UDP Port 2](#_Toc146820658)

[Xmas Scan 2](#_Toc146820659)

[Nmap Scripting Engine (NSE) 2](#_Toc146820660)

[Args 2](#_Toc146820661)

[Script Location 3](#_Toc146820662)

[Firewall Evasion 3](#_Toc146820663)

[Determine if firewall exists 3](#_Toc146820664)

[Verbosity 3](#_Toc146820665)

# Nmap

## Vulnerability Scan

**Use the following**: --script vuln\*

## TCP/UDP/SYN

1. -sT
2. -sU
3. -sS (requires sudo)

## NULL/FIN/XMAS

1. -sN
2. -sF
3. -sX

## ICMP Scan

This is used to perform a ping sweep to identify hosts.

**Usage**: nmap -sn <ip-address>

## UDP Port

Due to the lack of ACK UDP is more difficult and slow to scan. When a packet is sent to open UDP port, there should be no response. When this happens NMAP refers to port as open|filtered. In other words it suspects its open, but could be firewalled.

**Best Practice**: nmap -sU –top-ports 20 <target>

## Xmas Scan

It is used to attempt to evade firewall detection.

## Nmap Scripting Engine (NSE)

**Safe** – Wont affect target.

**Intrusive** – Not safe (may affect target).

**Vuln** – Scan for vulnerabilities.

**Exploit** – Attempt to exploit a vulnerability.

**Auth** – Attempt to bypass authentication for running services (log into ftp anon).

**Brute** – Attempt to brute force credentials for running services.

**Discovery** – Attempt to query running services for further info about networks (snmp).

**Note**: You can run multiple scripts by using a comma to separate each script.

### Args

Sometimes a script may require arguments. This can be done by adding –script-args <arg>.

Example: nmap -p 80 –script http-put –script-args http-put.url=’/dav/shell.php’, http-put.file=’./shell.php’.

You can find more information on the nmap.org website.

## Script Location

**Directory**: /usr/share/nmap/scripts

## Firewall Evasion

Use the flag -Pn to prevent pinging the host. Another flag to use is -f, which will fragment the packets (can use –mtu <number to further control packet size, this must be multiples of 8). You can also add –scan-delay <time>ms to modify the delay between packets sent.

### Determine if firewall exists

Use the flag –badsum which will generate an invalid checksum for packets. Any real tcp/ip stack would drop this packet. However, firewalls will respond automatically without bothering to check the checksum of the packet. This can tell you the presence of a firewall/IDS.

## Verbosity

It is very good practice to always use -vv when performing nmap scans. This will ensure you can see what is actually happening. If -vv is too much, then at least -v is necessary.