NMAP

Usages

OS Detection

> *sudo nmap -O -v 192.168.1.236*

```
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-30 17:40 EST
Initiating ARP Ping Scan at 17:40
Scanning 192.168.1.236 [1 port]
Completed ARP Ping Scan at 17:40, 0.34s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 17:40
Completed Parallel DNS resolution of 1 host. at 17:40, 0.17s elapsed
Initiating SYN Stealth Scan at 17:40
Scanning 192.168.1.236 [1000 ports]
Stats: 0:00:06 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 1.50% done; ETC: 17:47 (0:06:34 remaining)
SYN Stealth Scan Timing: About 11.50% done; ETC: 17:45 (0:04:45 remaining)
SYN Stealth Scan Timing: About 21.00% done; ETC: 17:45 (0:04:16 remaining)
SYN Stealth Scan Timing: About 30.50% done; ETC: 17:45 (0:03:43 remaining)
SYN Stealth Scan Timing: About 39.55% done; ETC: 17:46 (0:03:17 remaining)
SYN Stealth Scan Timing: About 49.05% done; ETC: 17:45 (0:02:45 remaining)
SYN Stealth Scan Timing: About 58.50% done; ETC: 17:45 (0:02:14 remaining)
SYN Stealth Scan Timing: About 67.55% done; ETC: 17:45 (0:01:45 remaining)
SYN Stealth Scan Timing: About 77.05% done; ETC: 17:45 (0:01:14 remaining)
SYN Stealth Scan Timing: About 86.55% done; ETC: 17:45 (0:00:44 remaining)
Completed SYN Stealth Scan at 17:45, 323.61s elapsed (1000 total ports)
Initiating OS detection (try #1) against 192.168.1.236
Retrying OS detection (try #2) against 192.168.1.236
Nmap scan report for 192.168.1.236
Host is up (0.32s latency).
All 1000 scanned ports on 192.168.1.236 are filtered
MAC Address: 34:2F:BD:28:86:A5 (Nintendo)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```