Cisco router of switch

IP 172.16.85.253

Starting Nmap 7.70 ( https://nmap.org ) at 2019-06-14 10:48 CEST

NSE: Loaded 148 scripts for scanning.

NSE: Script Pre-scanning.

Initiating NSE at 10:48

Completed NSE at 10:48, 0.00s elapsed

Initiating NSE at 10:48

Completed NSE at 10:48, 0.00s elapsed

Initiating Ping Scan at 10:48

Scanning 172.16.85.253 [4 ports]

Completed Ping Scan at 10:48, 0.24s elapsed (1 total hosts)

Initiating Parallel DNS resolution of 1 host. at 10:48

Completed Parallel DNS resolution of 1 host. at 10:48, 0.00s elapsed

Initiating SYN Stealth Scan at 10:48

Scanning 172.16.85.253 [1000 ports]

Discovered open port 80/tcp on 172.16.85.253

Discovered open port 443/tcp on 172.16.85.253

Discovered open port 22/tcp on 172.16.85.253

Increasing send delay for 172.16.85.253 from 0 to 5 due to 35 out of 86 dropped probes since last increase.

Increasing send delay for 172.16.85.253 from 5 to 10 due to 159 out of 396 dropped probes since last increase.

Warning: 172.16.85.253 giving up on port because retransmission cap hit (6).

Completed SYN Stealth Scan at 10:49, 23.30s elapsed (1000 total ports)

Initiating Service scan at 10:49

Scanning 3 services on 172.16.85.253

Completed Service scan at 10:49, 14.04s elapsed (3 services on 1 host)

Initiating OS detection (try #1) against 172.16.85.253

Retrying OS detection (try #2) against 172.16.85.253

adjust\_timeouts2: packet supposedly had rtt of -375579 microseconds.  Ignoring time.

adjust\_timeouts2: packet supposedly had rtt of -375579 microseconds.  Ignoring time.

adjust\_timeouts2: packet supposedly had rtt of -1221006 microseconds.  Ignoring time.

adjust\_timeouts2: packet supposedly had rtt of -1221006 microseconds.  Ignoring time.

WARNING: OS didn't match until try #2

Initiating Traceroute at 10:49

Completed Traceroute at 10:49, 0.02s elapsed

Initiating Parallel DNS resolution of 2 hosts. at 10:49

Completed Parallel DNS resolution of 2 hosts. at 10:49, 0.00s elapsed

NSE: Script scanning 172.16.85.253.

Initiating NSE at 10:49

Completed NSE at 10:50, 90.14s elapsed

Initiating NSE at 10:50

Completed NSE at 10:51, 1.01s elapsed

Nmap scan report for 172.16.85.253

Host is up (0.0028s latency).

Not shown: 997 closed ports

PORT    STATE SERVICE    VERSION

22/tcp  open  ssh        Cisco SSH 1.25 (protocol 2.0)

80/tcp  open  http       Cisco IOS http config

| http-auth:

| HTTP/1.1 401 Unauthorized\x0D

|\_  Basic realm=level\_15\_access

| http-methods:

|\_  Supported Methods: POST

|\_http-server-header: cisco-IOS

|\_http-title: Site doesn't have a title.

443/tcp open  ssl/https?

|\_ssl-date: 1993-04-05T22:10:22+00:00; -26y69d10h39m07s from scanner time.

OS details: Cisco 2950, 2960, 3550, 3560, 3750, or 4500 switch or 6500 router (IOS 12.1 - 15.0); or Adaptive Security Appliance firewall

Network Distance: 2 hops

TCP Sequence Prediction: Difficulty=262 (Good luck!)

IP ID Sequence Generation: Randomized

Service Info: OS: IOS; CPE: cpe:/o:cisco:ios

Host script results:

|\_clock-skew: mean: -9565d10h39m07s, deviation: 0s, median: -9565d10h39m07s

TRACEROUTE (using port 587/tcp)

HOP RTT     ADDRESS

1   2.82 ms \_gateway (172.16.83.254)

2   4.14 ms 172.16.85.253

NSE: Script Post-scanning.

Initiating NSE at 10:51

Completed NSE at 10:51, 0.00s elapsed

Initiating NSE at 10:51

Completed NSE at 10:51, 0.00s elapsed

Read data files from: /usr/bin/../share/nmap

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 136.17 seconds

           Raw packets sent: 3093 (141.612KB) | Rcvd: 5198 (224.288KB)