﻿NMAP

﻿root@kali:~# nmap www.123easyinvite.com

Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-04 11:58 EDT

Nmap scan report for www.123easyinvite.com (18.168.216.191)

Host is up (0.022s latency).

rDNS record for 18.168.216.191: ec2-18-168-216-191.eu-west-2.compute.amazonaws.com

Not shown: 998 filtered ports

PORT STATE SERVICE

22/tcp open ssh

80/tcp open http

**TCP**

root@kali:~# sudo nmap -sT -p80,443,22 18.168.216.191

Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-04 12:02 EDT

Nmap scan report for ec2-18-168-216-191.eu-west-2.compute.amazonaws.com (18.168.216.191)

Host is up (0.00061s latency).

PORT STATE SERVICE

22/tcp filtered ssh

80/tcp filtered http

443/tcp filtered https

Nmap done: 1 IP address (1 host up) scanned in 1.29 seconds

**UDP**

﻿root@kali:~# sudo nmap -sU -p80,443,22 18.168.216.191

Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-04 12:06 EDT

Nmap scan report for ec2-18-168-216-191.eu-west-2.compute.amazonaws.com (18.168.216.191)

Host is up (0.00065s latency).

PORT STATE SERVICE

22/udp open|filtered ssh

80/udp open|filtered http

443/udp open|filtered https

Nmap done: 1 IP address (1 host up) scanned in 1.46 seconds

**OS**

﻿root@kali:~# sudo nmap -O 18.168.216.191

Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-04 12:12 EDT

Nmap scan report for ec2-18-168-216-191.eu-west-2.compute.amazonaws.com (18.168.216.191)

Host is up (0.10s latency).

Not shown: 998 filtered ports

PORT STATE SERVICE

22/tcp open ssh

80/tcp open http

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

Aggressive OS guesses: 2N Helios IP VoIP doorbell (98%), Grandstream GXP1105 VoIP phone (98%), Garmin Virb Elite action camera (94%), Advanced Illumination DCS-100E lighting controller (93%), Enlogic PDU (FreeRTOS/lwIP) (93%), Smart Mirage CX06 satellite receiver (93%), Ocean Signal E101V emergency beacon (FreeRTOS/lwIP) (93%), AzBox Bravissimo Twin satellite TV decoder (92%), Cognex DataMan 200 ID reader (lwIP TCP/IP stack) (92%), DTE Energy Bridge (lwIP stack) (92%)

No exact OS matches for host (test conditions non-ideal).

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

Nmap done: 1 IP address (1 host up) scanned in 18.20 seconds

**Host Key,Servertype**

﻿root@kali:~# sudo nmap -A 18.168.216.191

Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-04 12:16 EDT

Nmap scan report for ec2-18-168-216-191.eu-west-2.compute.amazonaws.com (18.168.216.191)

Host is up (0.026s latency).

Not shown: 998 filtered ports

PORT STATE SERVICE VERSION

22/tcp open tcpwrapped

| ssh-hostkey:

| 2048 27:bf:d1:ec:34:d9:26:cf:34:65:fc:7d:99:97:4e:76 (RSA)

| 256 ba:df:47:d1:e1:0e:5d:ea:43:d3:c5:e9:41:a8:38:fe (ECDSA)

|\_ 256 8c:68:d5:6d:47:fa:0f:72:f2:01:5b:28:f0:e9:59:1d (ED25519)

80/tcp open tcpwrapped

|\_http-server-header: Apache

|\_http-title: Your Thoughts

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

Device type: specialized|VoIP phone|webcam|general purpose

Running (JUST GUESSING): 2N embedded (93%), Grandstream embedded (92%), Garmin embedded (89%), Advanced Illumination embedded (85%), IBM OS/2 4.X (85%)

OS CPE: cpe:/h:2n:helios cpe:/h:grandstream:gxp1105 cpe:/h:garmin:virb\_elite cpe:/h:advanced\_illumination:dcs-100e cpe:/o:ibm:os2:4

Aggressive OS guesses: 2N Helios IP VoIP doorbell (93%), Grandstream GXP1105 VoIP phone (92%), Garmin Virb Elite action camera (89%), Advanced Illumination DCS-100E lighting controller (85%), IBM OS/2 Warp 2.0 (85%)

No exact OS matches for host (test conditions non-ideal).

Network Distance: 1 hop

TRACEROUTE (using port 80/tcp)

HOP RTT ADDRESS

1 0.22 ms ec2-18-168-216-191.eu-west-2.compute.amazonaws.com (18.168.216.191)

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 35.78 seconds

**Vulnerability**

﻿root@kali:~# sudo nmap --script vuln 18.168.216.191

Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-04 12:22 EDT

Nmap scan report for ec2-18-168-216-191.eu-west-2.compute.amazonaws.com (18.168.216.191)

Host is up (0.028s latency).

Not shown: 998 filtered ports

PORT STATE SERVICE

22/tcp open ssh

80/tcp open http

|\_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)

| http-csrf:

| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=ec2-18-168-216-191.eu-west-2.compute.amazonaws.com

| Found the following possible CSRF vulnerabilities:

|

| Path: http://ec2-18-168-216-191.eu-west-2.compute.amazonaws.com:80/add

| Form id: thoughtmessage

|\_ Form action: /add

|\_http-dombased-xss: Couldn't find any DOM based XSS.

|\_http-stored-xss: Couldn't find any stored XSS vulnerabilities.

|\_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)

Nmap done: 1 IP address (1 host up) scanned in 82.37 seconds