Miguel Estevez

2017-0200

Usando nmap

nmap es un programa de codigo abierto que sirve para efectuar rastreo de puertos escrito originalmente por Gordon Lyon.Se usa para evaluar la seguridad de sistemas informáticos, así como para descubrir servicios o servidores en una red informatica, para ello Nmap envía unos paquetes definidos a otros equipos y analiza sus respuestas.

Para esta practica se tomo las paginas "corrotos.com.do" y "plataformavirtual.pucmm.edu.do"

```
sudo nmap -A corrotos.com.do
```

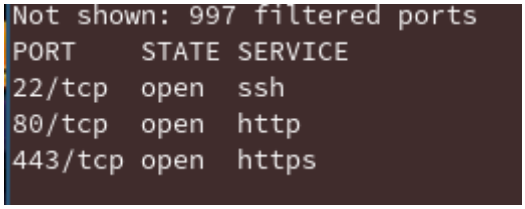
```
[miguelarch@miguelArch ~]$ sudo nmap -A www.corotos.com.do
[sudo] password for miguelarch:
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-18 17:38 AST
Nmap scan report for www.corotos.com.do (52.209.208.123)
Host is up (0.13s latency).
Other addresses for www.corotos.com.do (not scanned): 63.32.19.46 54.76.236.250
rDNS record for 52.209.208.123: ec2-52-209-208-123.eu-west-1.compute.amazonaws.com
Not shown: 998 filtered ports
PORT    STATE SERVICE  VERSION
80/tcp  open  http     OpenResty web app server
|_http-server-header: openresty
|_http-title: Did not follow redirect to https://www.corotos.com.do/
443/tcp open  ssl/http OpenResty web app server
| http-robots.txt: 6 disallowed entries
|_/ /graphql /messaging /api /tacoweb /tacomw
|_http-server-header: openresty
|_http-title: 429 Too Many Requests
| ssl-cert: Subject: commonName=*.cnt-tech.io
| Subject Alternative Name: DNS:*.cnt-tech.io, DNS:corotos.com.do, DNS:cnt-tech.io, DNS:tayara.tn, DNS:*.corotos.com.do, DNS:*.tayara.t
n
| Not valid before: 2020-09-19T00:00:00
|_Not valid after:  2021-10-19T12:00:00
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|   h2
|_  http/1.1
| tls-nextprotoneg:
|   h2
|_  http/1.1
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
```

```
Device type: general purpose|PBX
Running (JUST GUESSING): Linux 3.X (88%), Vodavi embedded (87%)
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/h:vodavi:xts-ip
Aggressive OS guesses: Linux 3.10 - 3.13 (88%), Vodavi XTS-IP PBX (87%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 30 hops

TRACEROUTE (using port 443/tcp)
HOP RTT       ADDRESS
1   3.35 ms   10.0.0.1
2   3.91 ms   pri-202-b3.codetel.net.do (196.3.74.202)
3   7.73 ms   172.23.235.249
4   32.69 ms  atl-b24-link.telia.net (62.115.183.242)
5   43.89 ms  ash-bb2-link.telia.net (62.115.125.129)
6   ...
7   120.71 ms ldn-bb3-link.telia.net (62.115.113.21)
8   123.45 ms ldn-b2-link.telia.net (62.115.122.189)
9   121.33 ms a100-ic-328653-ldn-b4.c.telia.net (80.239.195.89)
10  129.77 ms 52.95.61.200
11  126.32 ms 52.95.61.113
12  ...
13  132.49 ms 52.93.128.154
14  ... 29
30  132.24 ms ec2-52-209-208-123.eu-west-1.compute.amazonaws.com (52.209.208.123)

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 41.71 seconds
```

la cual al parecer esta montanda en la plataforma aws en un ec2 ya que su dns era **ec2-52-209-208-123.eu-west-1.compute.amazonaws.com**. Tambien se puede observar que los mas problable es que tenga como SO alguna distribucion de linux y los puertos que estan abiertos son: **80/TCP (http) y 443/TCP (https)**. Los cuales son los comunes para un servidor para una pagina web. En su caso solo tiene una host arriba y al parecer esta montado en openresty.

PVA

En este caso los servicios abiertos son:



Entonces como vi que ssh estaba abierto trate de entrar con un usuario: root y contraseña: root.

```
[miguelarch@miguelArch ~]$ ssh root@plataformavirtual.pucmm.edu.do
The authenticity of host 'plataformavirtual.pucmm.edu.do (190.113.74.4)' can't be established.
ECDSA key fingerprint is SHA256:bJaQS7/n1kKKehATS3Cbla9jeWPRmqv5znT5Ux8fzr0.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'plataformavirtual.pucmm.edu.do' (ECDSA) to the list of known hosts.
root@plataformavirtual.pucmm.edu.do: Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
```

entonces vi que pedia una llave publica entonces decidi no seguir.

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-18 18:54 AST
Nmap scan report for plataformavirtual.pucmm.edu.do (190.113.74.4)
Host is up (0.12s latency).
Not shown: 997 filtered ports
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 41:f8:b9:e0:a1:0a:62:7e:3c:8e:f3:58:8d:e7:a7:61 (RSA)
|   256 8d:c2:ea:9e:f0:94:5b:a1:42:68:44:9b:2a:34:b8:16 (ECDSA)
|_  256 e5:d7:fe:56:e6:37:4f:96:f2:cf:d1:cc:42:be:c9:02 (ED25519)
80/tcp  open  http     Apache httpd 2.4.6 ((CentOS) OpenSSL/1.0.2k-fips PHP/7.4.9)
|_http-auth: ERROR: Script execution failed (use -d to debug)
|_http-cookie-flags: ERROR: Script execution failed (use -d to debug)
|_http-favicon: ERROR: Script execution failed (use -d to debug)
|_http-generator: ERROR: Script execution failed (use -d to debug)
|_http-ls: ERROR: Script execution failed (use -d to debug)
|_http-ntlm-info: ERROR: Script execution failed (use -d to debug)
|_http-server-header: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.9
|_http-title: ERROR: Script execution failed (use -d to debug)
443/tcp open  ssl/http Apache httpd 2.4.6 ((CentOS) OpenSSL/1.0.2k-fips PHP/7.4.9)
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.9
|_http-title: PUCMM - Plataforma Virtual de Aprendizaje
| ssl-cert: Subject: commonName=*.pucmm.edu.do/organizationName=Pontificia Universidad Cat\xC3\xB3lica Madre y Maest
ra/countryName=DO
| Subject Alternative Name: DNS:*.pucmm.edu.do, DNS:campusvirtual.pucmm.edu.do, DNS:pucmm.edu.do
| Not valid before: 2020-07-30T00:00:00
|_Not valid after:  2021-08-13T12:00:00
|_ssl-date: TLS randomness does not represent time
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4.9
OS details: Linux 3.10 - 3.16, Linux 4.9
Network Distance: 9 hops

TRACEROUTE (using port 443/tcp)
HOP RTT       ADDRESS
1   143.55 ms 10.0.0.1
2   143.73 ms pri-202-b3.codetel.net.do (196.3.74.202)
3   143.97 ms 172.23.235.249
4   143.99 ms atl-b24-link.telia.net (62.115.183.242)
5   84.58 ms  mai-b1-link.telia.net (62.115.113.49)
6   183.00 ms asurnet-ic-339478-mai-b3.c.telia.net (62.115.12.17)
7   183.20 ms 69.79.100.77
8   183.22 ms 69.79.100.77
9   234.84 ms 190.113.74.4

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 36.44 seconds
```

Al analizar lo que me daba el nmap vi que esta montado en un servidor **apache** en **centos**. Al parecer esta plataforma esta hosteada por la misma universidad ya que el dns es ***.pucmm.edu.do**.