Reporte Nmap

Emiliano Galeana Araujo
César Eduardo Jardines Mendoza
César Gustavo Sánchez de la Rosa

May 2020

1. Nmap

```
»»»» $  nmap --version

Nmap version 7.01 ( https://nmap.org )
Platform: x86_64-pc-linux-gnu
Compiled with: liblua-5.2.4 openssl-1.0.2g libpcre-8.38 libpcap-1.7.4 nmap-libdnet-1.12 ipv6
Compiled without:
Available nsock engines: epoll poll select
```

La versión que se está usando es 7.01, estamos ejecutando esta herramienta en un sistema operativo GNU/Linux, específicamente Linux Mint. Se ejecutó el comando en la terminal **ip a**, aunque también con **ifconfig** se puede obtener la IP del equipo pero dicen que ya es un comando viejo y muy pronto obsoleto. La ip obtenida es la **192.168.0.106**.

```
»»»» $  ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens38: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:58:a7:59 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.106/24 brd 192.168.0.255 scope global dynamic ens38
       valid_lft 5010sec preferred_lft 5010sec
    inet6 fe80::a5cf:53a2:f6f6:e81e/64 scope link
       valid_lft forever preferred_lft forever
```

Es una IP privada que nos la esta ofreciendo un enrutador o algún dispositivo que este haciendo el modo NAT, lo que nos hace sospechar que en este segmento de red hay más equipos conectados, en los siguientes escaneos podrémos averiguar más.

2. Barrido de Red
   Se ejecutó el comando nmap -sP **192.168.0.0/24**, sabemos que tiene

máscara 24 por la información que nos da el comando **ip a**. Esto con la finalidad de ver la ip de todos los dispositivos conectados a la red.

```
»»»» $  nmap -sP 192.168.0.0/24

Starting Nmap 7.01 ( https://nmap.org ) at 2020-05-25 21:22 CDT
Nmap scan report for 192.168.0.1
Host is up (0.028s latency).
Nmap scan report for 192.168.0.100
Host is up (0.025s latency).
Nmap scan report for 192.168.0.101
Host is up (0.021s latency).
Nmap scan report for 192.168.0.103
Host is up (0.010s latency).
Nmap scan report for 192.168.0.106
Host is up (0.017s latency).
Nmap done: 256 IP addresses (5 hosts up) scanned in 3.57 seconds
```

Otra manera de averiguar que la ip de los dispositivos conectados es lanzando un **ping** a todo el segmento y áquellos que respondan están conectados. **Ojo** aquellos que no respondan no necesariamente no están conectados, puede que no tengan habilitado el ping. El siguiente comando muestra como se puede hacer un barrido a la red con el comando **ping** desde una línea de comando.

```
Se puede hace un redescubrimiento de dispositivos mediante ping, solo viendo que dispositivos estan respondiendo

@virtual ~/security
»»»» $  for i in `seq 0 255 ; do echo "192.168.0.$i" && ping -w 1 -c 1 192.168.0.$i | tr \\n ' ' | awk '/1 received/ {print "\tSuccess! ""\t"$2}'; done
```

Después de haber realizado el barrido de red, seleccionamos un equipo para las siguientes pruebas.

3. Escaneo de puertos TCP

En nuestro caso seleccionamos la IP **192.168.0.101** para los siguientes escaneos.

Para hacer un escaneo de puertos TCP se usa el parámetro **-sS** como muestra la imágen.

```
»»»» $  sudo nmap -sS 192.168.0.101 -oX analisis-maquina.xml --webxml

Starting Nmap 7.01 ( https://nmap.org ) at 2020-05-25 21:31 CDT
Nmap scan report for 192.168.0.101
Host is up (0.023s latency).
Not shown: 993 filtered ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
902/tcp  open  iss-realsecure
912/tcp  open  apex-mesh
5357/tcp open  wsdapi
MAC Address: B4:6D:83:2B:70:91 (Intel Corporate)

Nmap done: 1 IP address (1 host up) scanned in 38.59 seconds
```

Hay que aclarar que también agregamos el parámetro **-oX some-name.xml** –**webxml** que quiere decir "guarda la salida en el formato de hojas de estilo compatible con webxml", el documento creado lo podemos abrir con firefox y se muestra de la siguiente manera:

Nmap Scan Report - Scanned at Mon May 25 21:31:14 2020

Scan Summary | 192.168.0.101

Scan Summary

Nmap 7.01 was initiated at Mon May 25 21:31:14 2020 with these arguments:
nmap -sS -oX analisis-maquina.xml --webxml 192.168.0.101

Verbosity: 0; Debug level 0

Nmap done at Mon May 25 21:31:52 2020; 1 IP address (1 host up) scanned in 38.59 seconds

192.168.0.101

Address

- 192.168.0.101 (ipv4)
- B4:6D:83:2B:70:91 - Intel Corporate (mac)

Ports

The 993 ports scanned but not shown below are in state: **filtered**

- 993 ports replied with: **no-responses**

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
135	tcp	open	msrpc	syn-ack			
139	tcp	open	netbios-ssn	syn-ack			
443	tcp	open	https	syn-ack			
445	tcp	open	microsoft-ds	syn-ack			
902	tcp	open	iss-realsecure	syn-ack			
912	tcp	open	apex-mesh	syn-ack			
5357	tcp	open	wsdapi	syn-ack			

4. Escaneo de puertos UDP

Para saber si tiene puertos **UDP** se usa el parámetro **-sU**. De la siguiente manera y de igual forma guardamos la salida. Se recomienda guardar la salida cuando se hacen escaneos para reportes y cuándo son muy tardados, con la finalidad de no repetir el escaneo y desperdiciar tiempo.

```
»»»» $  sudo nmap -sU 192.168.0.101 -oX upd.xml --webxml

Starting Nmap 7.01 ( https://nmap.org ) at 2020-05-25 21:48 CDT
Nmap scan report for 192.168.0.101
Host is up (0.0066s latency).
Not shown: 999 open|filtered ports
PORT    STATE SERVICE
137/udp open  netbios-ns
MAC Address: B4:6D:83:2B:70:91 (Intel Corporate)

Nmap done: 1 IP address (1 host up) scanned in 14.72 seconds
```

Ports

The 999 ports scanned but not shown below are in state: **open|filtered**

- 999 ports replied with: **no-responses**

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
137	udp	open	netbios-ns	udp-response			

5. Servicios y Versiones

   Para hacer un escaneo de Servicios y Versiones hay que poner como parámetro **-sV**, de igual manera guardamos la salida estándar en un archivo y se ve de la siguiente manera:

Nmap Scan Report - Scanned at Mon May 25 21:35:47 2020

Scan Summary | 192.168.0.101

Scan Summary

Nmap 7.01 was initiated at Mon May 25 21:35:47 2020 with these arguments:
nmap -sV -O -oX servicioaYversiones.xml --webxml 192.168.0.101

Verbosity: 0; Debug level 0

Nmap done at Mon May 25 21:38:43 2020; 1 IP address (1 host up) scanned in 176.79 seconds

192.168.0.101

Address

- 192.168.0.101 (ipv4)
- B4:6D:83:2B:70:91 - Intel Corporate (mac)

Ports

The 993 ports scanned but not shown below are in state: **filtered**

- 993 ports replied with: **no-responses**

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
135	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		
139	tcp	open	netbios-ssn	syn-ack	Microsoft Windows 98 netbios-ssn		
443	tcp	open	https	syn-ack			
445	tcp	open	microsoft-ds	syn-ack			
902	tcp	open	vmware-auth	syn-ack	VMware Authentication Daemon	1.10	Uses VNC, SOAP
912	tcp	open	vmware-auth	syn-ack	VMware Authentication Daemon	1.0	Uses VNC, SOAP
5357	tcp	open	http	syn-ack	Microsoft HTTPAPI httpd	2.0	SSDP/UPnP

Remote Operating System Detection

- Used port: **135/tcp (open)**
- OS match: **Microsoft Windows XP SP2 (87%)**
- OS match: **Microsoft Windows 7 (85%)**
- OS match: **Microsoft Windows Server 2008 SP1 or Windows Server 2008 R2 (85%)**

   Hay otro parámetro en nuestra línea de comandos que explicaremos adelante.

6. Sistema Operativo

   El parámetro **-O** que se muestra en la imagen anterior es para saber que tipo de sistema operativo tiene el dispositivo.

```
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows XP|7|2008 (87%)
OS CPE: cpe:/o:microsoft:windows_xp::sp2 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2
Aggressive OS guesses: Microsoft Windows XP SP2 (87%), Microsoft Windows 7 (85%), Microsoft Windows Server 2008 SP1 or Windows Server 2008 R2 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OSs: Windows, Windows 98; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_98

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 176.79 seconds
```

Esto lo podemos medio saber mediante el comando **ping**, ya que el **Time To Live** que devuelve el dispositivo al que le hacemos ping tiene un valor. Por lo regular los dispositivos Windows tienen un **ttl** de 128 y los sistemas GNU/Linux de 64.

A continuación se muestra el **ttl** de un sistema windows.

```
64 bytes from 192.168.0.103: icmp_seq=1 ttl=128 time=1.94 ms
64 bytes from 192.168.0.103: icmp_seq=2 ttl=128 time=1.25 ms
64 bytes from 192.168.0.103: icmp_seq=3 ttl=128 time=1.45 ms
```

Mientras que un sistema con linux es algo así:

```
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.203 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.154 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.303 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.142 ms
```

Con **ping** solo podríamos imaginarnos que sistema operativo es, pero **nmap** nos puede dar más información como se observo en la primera imágen de este punto.

7. Vulnerabilidades

   Para hacer un escaneo de vulnerabilidades se usa el parámetro –**script vuln**, de igual manera guardamos la salida estandar y nuestro objetivo es **192.168.0.101**

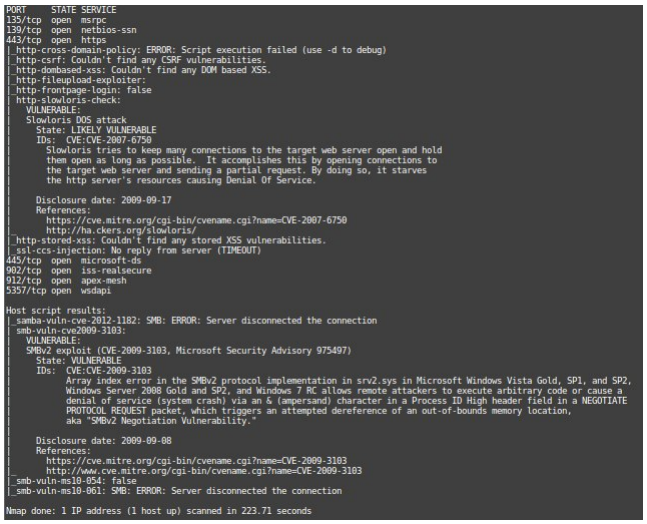
   Esta opción que tiene nmap nos permite saber que tipo de vulnerabilidades conocidas es susceptible el equipo al que le hicimos el análisis.

Scan Summary

Nmap 7.01 was initiated at Mon May 25 22:08:38 2020 with these arguments:
nmap --script vuln -oX vulnerabilidades.xml --webxml 192.168.0.101

Verbosity: 0; Debug level 0

Nmap done at Mon May 25 22:12:51 2020; 1 IP address (1 host up) scanned in 252.70 seconds



8. Exploit

   De acuerdo con el **NICCS** un exploit es una técnica para violar la seguridad de una red o sistema de información en violación de la política de seguridad.

   Uno podría decir que es un ataque a un sistema informático, especialmente uno que aprovecha una vulnerabilidad particular que el sistema ofrece a los intrusos. Pero todos los exploits se pueden clasificar de distinta manera, dependiendo de la forma en que trabajen. Hay exploits de día Cero, "Zero Day" porque es una vulnerabilidad crítica donde hasta ese momento el proveedor o desarrollador no la conocía, entre otros tipos de exploits.

9. Referencias

   https://niccs.us-cert.gov/about-niccs/cybersecurity-glossaryE

1 README RSA

Para compilar el programa: `javac RSA.java`

Para correr el programa se requiere de tres pasos, los cuales describimos a continuación:

1. `java RSA -k` Esto es para obtener las llaves. El orden es:
   (a) N
   (b) D
   (c) E

2. `java RSA -e "MENSAJE" N E`, una vez hecho el paso anterior, le pasamos el mensaje entre comillas, luego los números que la ejecución anterior nos dio, estos son N, E. Ejemplo: `java RSA "Hola Mundo" 123124123 12421`. El resultado de esto, es una cadena con el mensaje cifrado.

3. `java RSA -d "MENSAJE CIFRADO" N D`, lo mismo que en el paso anterior, escribimos el mensaje cifrado entre comillas y le pasamos los números que recibimos de la primera ejecución del programa. Ejemplo: `java "13%-14%2" N D` Y esto nos va a regresar el mensaje descifrado.