Universidad Nacional Autónoma de México

Facultad de Ciencias

Criptografía y Seguridad

Proyecto 2

Criptosistema RSA

Profesor:

Manuel Díaz Díaz

Integrantes:

Lázaro Pérez David Jonathan

Licona Gómez Aldo Daniel

Marín Parra José Guadalupe de Jesús

Índice

1. Herramientas de Seguridad **3**
1.1. WHOIS . . . 3
1.2. NSLOOKUP . . . 5
1.3. TRACEROUTE . . . 8
1.4. NMAP . . . 9

2. Categorías NSE **12**
2.1. Categorías . . . 12

3. Referencias **19**
3.1. Bibliografía . . . 19

1. Herramientas de Seguridad

1.1. WHOIS

Whois es una herramienta que nos permite ver la información técnica y los datos de registro de los titulares del dominio registrado.

Veamos el funcionamiento de esta herramienta en facebook.com

```
→  ~ whois facebook.com
   Domain Name: FACEBOOK.COM
   Registry Domain ID: 2320948_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.registrarsafe.com
   Registrar URL: http://www.registrarsafe.com
   Updated Date: 2022-01-26T16:45:06Z
   Creation Date: 1997-03-29T05:00:00Z
   Registry Expiry Date: 2031-03-30T04:00:00Z
   Registrar: RegistrarSafe, LLC
   Registrar IANA ID: 3237
   Registrar Abuse Contact Email: abusecomplaints@registrarsafe.com
   Registrar Abuse Contact Phone: +1-650-308-7004
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
   Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
   Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
   Name Server: A.NS.FACEBOOK.COM
   Name Server: B.NS.FACEBOOK.COM
   Name Server: C.NS.FACEBOOK.COM
   Name Server: D.NS.FACEBOOK.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2022-10-25T19:46:58Z <<<
```

En el primer apartado nos muestra datos como la fecha de creación, fecha de expiración y datos de contacto.

```
The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.
Domain Name: FACEBOOK.COM
Registry Domain ID: 2320948_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.registrarsafe.com
Registrar URL: https://www.registrarsafe.com
Updated Date: 2022-01-26T16:45:06Z
Creation Date: 1997-03-29T05:00:00Z
Registrar Registration Expiration Date: 2031-03-30T04:00:00Z
Registrar: RegistrarSafe, LLC
Registrar IANA ID: 3237
Registrar Abuse Contact Email: abusecomplaints@registrarsafe.com
Registrar Abuse Contact Phone: +1.6503087004
Domain Status: serverUpdateProhibited https://www.icann.org/epp#serverUpdateProhibited
Domain Status: clientDeleteProhibited https://www.icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://www.icann.org/epp#clientTransferProhibited
Domain Status: serverDeleteProhibited https://www.icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited https://www.icann.org/epp#serverTransferProhibited
Domain Status: clientUpdateProhibited https://www.icann.org/epp#clientUpdateProhibited
Registry Registrant ID:
Registrant Name: Domain Admin
Registrant Organization: Meta Platforms, Inc.
Registrant Street: 1601 Willow Rd
Registrant City: Menlo Park
Registrant State/Province: CA
Registrant Postal Code: 94025
Registrant Country: US
Registrant Phone: +1.6505434800
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: domain@fb.com
Registry Admin ID:
Admin Name: Domain Admin
Admin Organization: Meta Platforms, Inc.
Admin Street: 1601 Willow Rd
Admin City: Menlo Park
Admin State/Province: CA
Admin Postal Code: 94025
Admin Country: US
Admin Phone: +1.6505434800
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: domain@fb.com
Registry Tech ID:
Tech Name: Domain Admin
Tech Organization: Meta Platforms, Inc.
Tech Street: 1601 Willow Rd
Tech City: Menlo Park
Tech State/Province: CA
Tech Postal Code: 94025
Tech Country: US
Tech Phone: +1.6505434800
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: domain@fb.com
Name Server: C.NS.FACEBOOK.COM
Name Server: B.NS.FACEBOOK.COM
Name Server: A.NS.FACEBOOK.COM
Name Server: D.NS.FACEBOOK.COM
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2022-10-25T19:46:49Z <<<
```

En el segundo apartado relevante nos aparecen datos como las direcciones de los dominios así como más datos de contacto y direcciones.

1.2. NSLOOKUP

Nslookup es una herramienta que nos permite encontrar la dirección IP de un determinado equipo o realizar una búsqueda inversa, es decir, encontrar el nombre del dominio dada una dirección IP.

Veamos el funcionamiento de esta herramienta en google.com

```
→  ~ nslookup -type=any google.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   google.com
Address: 2607:f8b0:4012:817::200e
google.com      nameserver = ns3.google.com.
google.com      nameserver = ns1.google.com.
google.com      nameserver = ns4.google.com.
google.com      nameserver = ns2.google.com.
google.com
        origin = ns1.google.com
        mail addr = dns-admin.google.com
        serial = 483332882
        refresh = 900
        retry = 900
        expire = 1800
        minimum = 60
Name:   google.com
Address: 142.251.34.142
google.com      rdata_65 = 1 . alpn="h2,h3"

Authoritative answers can be found from:
ns4.google.com  internet address = 216.239.38.10
ns2.google.com  internet address = 216.239.34.10
ns3.google.com  internet address = 216.239.36.10
ns1.google.com  internet address = 216.239.32.10
```

-type=any hace una búsqueda de cualquier registro, es decir, podemos ver todos los registros DNS disponibles.

```
→  ~ nslookup -type=soa google.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
google.com
        origin = ns1.google.com
        mail addr = dns-admin.google.com
        serial = 483625360
        refresh = 900
        retry = 900
        expire = 1800
        minimum = 60

Authoritative answers can be found from:
```

-type=soa hace una búsqueda de un registro, es decir, el registro SOA (start of authority) o inicio de autoridad en español proporciona la información autorizada sobre el dominio.

```
→  ~ nslookup -type=ns google.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
google.com      nameserver = ns4.google.com.
google.com      nameserver = ns2.google.com.
google.com      nameserver = ns3.google.com.
google.com      nameserver = ns1.google.com.

Authoritative answers can be found from:
ns4.google.com  internet address = 216.239.38.10
ns2.google.com  internet address = 216.239.34.10
ns3.google.com  internet address = 216.239.36.10
ns1.google.com  internet address = 216.239.32.10
```

-type=ns hace una búsqueda de un registro ns, es decir, ns (name server) asigna un nombre de dominio a una lista de servidores DNS autorizados para ese dominio.

```
→  ~ nslookup -type=a google.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   google.com
Address: 142.251.34.142
```

-type=a hace una búsqueda de un registro, es decir, podemos ver todos los registros DNS disponibles de uno en particular.

```
→  ~ nslookup -type=mx google.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
google.com      mail exchanger = 10 smtp.google.com.

Authoritative answers can be found from:
```

-type=mx hace una búsqueda de un registro mx (mail exchange), es decir, asigna un nombre de dominio a una lista de servidores de intercambio de correo para ese dominio.

```
→  ~ nslookup -type=txt google.com
;; Truncated, retrying in TCP mode.
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
google.com      text = "google-site-verification=TV9-DBe4R80X4v0M4U_bd_J9cpOJM0nikft0jAgjmsQ"
google.com      text = "atlassian-domain-verification=5YjTmWmjI92ewqkx2oXmBaD60Td9zWon9r6eakvHX6B77zzkFQto8PQ9QsKnbf4I"
google.com      text = "google-site-verification=wD8N7i1JTNTkezJ49swvWW48f8_9xveREV4oB-0Hf5o"
google.com      text = "apple-domain-verification=30afIBcvSuDV2PLX"
google.com      text = "MS=E4A68B9AB2BB9670BCE15412F62916164C0B20BB"
google.com      text = "onetrust-domain-verification=de01ed21f2fa4d8781cbc3ffb89cf4ef"
google.com      text = "facebook-domain-verification=22rm551cu4k0ab0bxsw536tlds4h95"
google.com      text = "docusign=1b0a6754-49b1-4db5-8540-d2c12664b289"
google.com      text = "v=spf1 include:_spf.google.com ~all"
google.com      text = "globalsign-smime-dv=CDYX+XFHUw2wml6/Gb8+59BsH31KzUr6c1l2BPvqKX8="
google.com      text = "webexdomainverification.8YX6G=6e6922db-e3e6-4a36-904e-a805c28087fa"
google.com      text = "docusign=05958488-4752-4ef2-95eb-aa7ba8a3bd0e"

Authoritative answers can be found from:
```

-type=txt hace una búsqueda de un registro txt, es decir, podemos encontrar todos los registros txt configurados para este dominio.

1.3. TRACEROUTE

Traceroute es una herramienta que nos ayuda a seguir ciertos paquetes de datos, con los resultados que nos ofrece esta herramienta, nosotros podemos diagnosticar qué estaciones han enviado los paquetes dado un destino previsto y dónde hay dificultades.

Veamos el funcionamiento de esta herramienta en youtube.com

```
→  ~ traceroute youtube.com
traceroute to youtube.com (142.251.34.174), 30 hops max, 60 byte packets
 1  _gateway (192.168.1.1)  0.270 ms  64.843 ms  64.837 ms
 2  192.168.0.1 (192.168.0.1)  2.149 ms  3.274 ms  3.928 ms
 3  10.43.192.1 (10.43.192.1)  32.490 ms  32.931 ms  33.213 ms
 4  10.3.70.62 (10.3.70.62)  29.476 ms  39.418 ms  39.745 ms
 5  * * *
 6  10.100.17.137 (10.100.17.137)  42.303 ms  16.716 ms  21.542 ms
 7  10.100.17.13 (10.100.17.13)  22.352 ms  29.264 ms  30.317 ms
 8  customer-189-216-5-6.cablevision.net.mx (189.216.5.6)  27.434 ms  28.344 ms  28.678 ms
 9  90.189-204-152.bestelclientes.com.mx (189.204.152.90)  41.455 ms  42.310 ms  42.552 ms
10  72.14.219.36 (72.14.219.36)  52.452 ms  59.435 ms  36.644 ms
11  * * *
12  142.251.78.196 (142.251.78.196)  34.589 ms 108.170.254.1 (108.170.254.1)  35.152 ms 142.250.211.200 (142.250.211.200)  45.861 ms
13  142.251.78.191 (142.251.78.191)  42.315 ms 142.251.78.193 (142.251.78.193)  42.837 ms  43.642 ms
14  108.170.226.127 (108.170.226.127)  43.929 ms 142.251.69.47 (142.251.69.47)  51.197 ms 108.170.226.127 (108.170.226.127)  44.168 ms
15  qro02s26-in-f14.1e100.net (142.251.34.174)  41.161 ms 74.125.243.33 (74.125.243.33)  44.625 ms  44.821 ms
```

En donde la primera columna nos muestra el número de saltos, la segunda nos muestra la dirección de tal salto, después de eso veremos tres espacios con algunos ms en cada uno los cuales corresponden al tiempo de tres paquetes lanzados por esta herramienta.

Ahora veamos la información de la primera ip (192.168.1.1) en nslookup.

```
→  ~ nslookup 192.168.1.1
1.1.168.192.in-addr.arpa        name = _gateway.
```

Donde solo nos muestra la dirección y el nombre.

1.4. NMAP

Nmap es una herramienta que nos permite analizar rápidamente grandes redes con el objetivo de obtener información importante de éstas.

Veamos el funcionamiento de esta herramienta en nuestra ip.

1. Barrido de red.
   Solución.

```
→  ~ nmap -sP 192.168.2.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-25 15:50 CDT
Nmap scan report for 192.168.2.100
Host is up (0.063s latency).
Nmap done: 256 IP addresses (1 host up) scanned in 10.27 seconds
```

Detectamos los equipos en la red, observamos que solo hay un host activo (192.168.2.100).

2. Escaneo de puertos TCP SYN.
   Solución.

```
root@josemp366:/home/jose# nmap -sS 192.168.2.100
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-25 17:06 CDT
Nmap scan report for 192.168.2.100
Host is up (0.18s latency).
Not shown: 984 closed ports
PORT     STATE    SERVICE
20/tcp   filtered ftp-data
21/tcp   open     ftp
22/tcp   filtered ssh
23/tcp   filtered telnet
37/tcp   open     time
111/tcp  filtered rpcbind
2126/tcp open     pktcable-cops
3918/tcp open     pktcablemmcops
6000/tcp filtered X11
6001/tcp filtered X11:1
6002/tcp filtered X11:2
6003/tcp filtered X11:3
6004/tcp filtered X11:4
6006/tcp filtered X11:6
6009/tcp filtered X11:9
6059/tcp filtered X11:59

Nmap done: 1 IP address (1 host up) scanned in 30.38 seconds
```

Observamos todos los puertos de nuestro host.

3. Escaneo de puertos UDP.
   Solución.

```
root@josemp366:/home/jose# nmap -sU 192.168.2.100
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-25 17:07 CDT
Nmap scan report for 192.168.2.100
Host is up (0.018s latency).
Not shown: 990 closed ports
PORT      STATE         SERVICE
37/udp    open|filtered time
67/udp    open|filtered dhcps
69/udp    open|filtered tftp
111/udp   open|filtered rpcbind
161/udp   open          snmp
162/udp   open|filtered snmptrap
1813/udp  open|filtered radacct
9876/udp  open|filtered sd
37602/udp open|filtered unknown
49174/udp open|filtered unknown

Nmap done: 1 IP address (1 host up) scanned in 1094.60 seconds
```

Posibles puertos UDP abiertos del host.

4. Determinar el Sistema Operativo del objetivo.
   Solución.

```
Not shown: 993 closed ports
PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   filtered ssh
23/tcp   filtered telnet
37/tcp   open     time
111/tcp  filtered rpcbind
2126/tcp open     pktcable-cops
3918/tcp open     pktcablemmcops
Device type: general purpose|WAP|media device|PBX|broadband router
Running (JUST GUESSING): Linux 2.6.X|2.4.X (96%), ZyXEL embedded (94%), Sony embedded (92%), Cisco
embedded (91%), Asus embedded (91%)
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:2.6.22 cpe:/o:linux:linux_kernel:2.
4.30 cpe:/o:sony:smp-n200 cpe:/o:linux:linux_kernel:2.4.18 cpe:/h:cisco:uc320 cpe:/h:asus:rt-ac66u
Aggressive OS guesses: Linux 2.6.9 - 2.6.27 (96%), Linux 2.6.27 - 2.6.28 (94%), ZyXEL Keenetic Giga
 WAP 2.04 - 2.05 (94%), Linux 2.6.22 - 2.6.36 (93%), Linux 2.6.8 - 2.6.30 (93%), Linux 2.6.37 (93%)
, Linux 2.6.11 (Auditor) (92%), Linux 2.6.5 (SUSE Enterprise Server 9) (92%), Tomato 1.28 (Linux 2.
6.22) (92%), Linux 2.6.22 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 54 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.29 seconds
```

Notamos que Linux es el posible sistema operativo de tal host.

5. Determinar servicios y versiones de puertos abiertos.
   Solución.

```
root@josemp366:/home/jose# nmap -sV 192.168.2.100
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-25 17:29 CDT
Nmap scan report for 192.168.2.100
Host is up (0.057s latency).
Not shown: 993 closed ports
PORT     STATE    SERVICE    VERSION
21/tcp   open     ftp        vsftpd 3.0.2
22/tcp   filtered ssh
23/tcp   filtered telnet
37/tcp   open     tcpwrapped
111/tcp  filtered rpcbind
2126/tcp open     cops       Common Open Policy Service (COPS) 1
3918/tcp open     cops       Common Open Policy Service (COPS) 1
Service Info: Host: CASA_C100G_IXTAPALUCA_9; OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 4.40 seconds
```

Observamos los puertos, servicios así como su versión en el host.

6. Evaluar reglas de firewall y determinar si hay puerto filtrados con TCP ACK.
   Solución.

```
root@josemp366:/home/jose# nmap -sA 192.168.2.100
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-25 17:30 CDT
Nmap scan report for 192.168.2.100
Host is up (0.062s latency).
Not shown: 997 unfiltered ports
PORT    STATE    SERVICE
22/tcp  filtered ssh
23/tcp  filtered telnet
111/tcp filtered rpcbind

Nmap done: 1 IP address (1 host up) scanned in 4.42 seconds
```

Nos muestra los puertos filtrados de tal host.

2. Categorías NSE

2.1. Categorías

7. Investigar las categorias **NSE**: *auth, broadcast, brute, default, discovery, dos, exploit, external, fuzzer, intrusive, malware, safe, version* y *vuln*. Describir brevemente cada categoría NSE de nmap, así como mostrar el uso de cada una en equipo objetivo de tu red local.

   Solución. NSE (Nmap Scripting Engine) o Motor de Secuencias de Comandos permite a Nmap realizar una gran variedad de tareas e informar los resultados.

   - **Auth.** Scripts que se ocupan de las credenciales de autenticación en el sistema de destino.
     Veamos un ejemplo de esta categoría en nuestra red (192.168.2.100).

```
→  ~ nmap --script auth --script-args=newtargets 192.168.2.100
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-07 15:00 CST
Nmap scan report for 192.168.2.100
Host is up (0.040s latency).
Not shown: 993 closed ports
PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   filtered ssh
23/tcp   filtered telnet
37/tcp   open     time
111/tcp  filtered rpcbind
2126/tcp open     pktcable-cops
3918/tcp open     pktcablemmcops

Nmap done: 1 IP address (1 host up) scanned in 4.19 seconds
```

   - **Broadcast.** Se encarga de detectar hosts que no aparecen en la línea de comando mediante la difusión en la red local.
     Veamos un ejemplo de esta categoría en nuestra red (192.168.2.100).

```
→  ~ nmap --script broadcast --script-args=newtargets 192.168.2.100
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-07 14:59 CST
Pre-scan script results:
| broadcast-upnp-info:
|   239.255.255.250
|       Server: ipos/7.0 UPnP/1.0 TL-WR940N/6.0
|_      Location: http://192.168.1.1:1900/igd.xml
Nmap scan report for 192.168.2.100
Host is up (0.017s latency).
Not shown: 993 closed ports
PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   filtered ssh
23/tcp   filtered telnet
37/tcp   open     time
111/tcp  filtered rpcbind
2126/tcp open     pktcable-cops
3918/tcp open     pktcablemmcops

Nmap done: 2 IP addresses (1 host up) scanned in 48.31 seconds
```

- **Brute.** Utiliza ataques de fuerza bruta para adivinar las credenciales de autenticación de un servidor remoto.

  Veamos un ejemplo de esta categoría en nuestra red (192.168.2.100).

```
→  ~ nmap --script brute --script-args=newtargets 192.168.2.100
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-07 15:17 CST
Nmap scan report for 192.168.2.100
Host is up (0.054s latency).
Not shown: 993 closed ports
PORT     STATE    SERVICE
21/tcp   open     ftp
| ftp-brute:
|   Accounts: No valid accounts found
|_  Statistics: Performed 9760 guesses in 600 seconds, average tps: 16.1
22/tcp   filtered ssh
23/tcp   filtered telnet
37/tcp   open     time
111/tcp  filtered rpcbind
2126/tcp open     pktcable-cops
3918/tcp open     pktcablemmcops

Nmap done: 1 IP address (1 host up) scanned in 607.92 seconds
```

- **Default.** Son scripts predeterminados cuando se usa $-sC$ o $-A$ en la línea de comandos.

  Veamos un ejemplo de esta categoría en nuestra red (192.168.2.100).

```
→  ~ nmap --script default --script-args=newtargets 192.168.2.100
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-07 15:08 CST
Nmap scan report for 192.168.2.100
Host is up (0.039s latency).
Not shown: 993 closed ports
PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   filtered ssh
23/tcp   filtered telnet
37/tcp   open     time
111/tcp  filtered rpcbind
2126/tcp open     pktcable-cops
3918/tcp open     pktcablemmcops

Nmap done: 1 IP address (1 host up) scanned in 13.86 seconds
```

- **Discovery.** Se utilizan para descubrir más sobre la red consultando registros públicos, dispositivos habilitados para SNMP, servicios de directorio y similares.

  Veamos un ejemplo de esta categoría en nuestra red (192.168.2.100).

```
→  ~ nmap --script discovery --script-args=newtargets 192.168.2.100
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-07 15:08 CST
Pre-scan script results:
| targets-asn:
|_  targets-asn.asn is a mandatory parameter
Nmap scan report for 192.168.2.100
Host is up (0.050s latency).
Not shown: 993 closed ports
PORT     STATE    SERVICE
21/tcp   open     ftp
| banner: 220 (vsFTPd 3.0.2)
22/tcp   filtered ssh
23/tcp   filtered telnet
37/tcp   open     time
111/tcp  filtered rpcbind
2126/tcp open     pktcable-cops
|_banner: \x10\x06\x80\x08\x00\x00\x00$\x00\x1C\x0B\x01CASA_C100G_IXTA...
3918/tcp open     pktcablemmcops
|_banner: \x10\x06\x80\x0A\x00\x00\x000\x00\x1C\x0B\x01CASA_C100G_IXTA...

Host script results:
|_dns-brute: Can't guess domain of "192.168.2.100"; use dns-brute.domain script argument.
|_fcrdns: FAIL (No PTR record)

Nmap done: 1 IP address (1 host up) scanned in 22.30 seconds
```

- **Dos.** Pueden provocar una denegación de servicio para probar la vulnerabilidad a un método de denegación de servicio.

  Veamos un ejemplo de esta categoría en nuestra red (192.168.2.100).

```
→  ~ nmap --script dos --script-args=newtargets 192.168.2.100
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-07 15:09 CST
Nmap scan report for 192.168.2.100
Host is up (0.038s latency).
Not shown: 993 closed ports
PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   filtered ssh
23/tcp   filtered telnet
37/tcp   open     time
111/tcp  filtered rpcbind
2126/tcp open     pktcable-cops
3918/tcp open     pktcablemmcops

Nmap done: 1 IP address (1 host up) scanned in 15.50 seconds
```

- **Exploit.** Explotan activamente alguna vulnerabilidad.
  Veamos un ejemplo de esta categoría en nuestra red (192.168.2.100).

```
→  ~ nmap --script exploit --script-args=newtargets 192.168.2.100
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-07 15:10 CST
Nmap scan report for 192.168.2.100
Host is up (0.022s latency).
Not shown: 993 closed ports
PORT     STATE    SERVICE
21/tcp   open     ftp
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
22/tcp   filtered ssh
23/tcp   filtered telnet
37/tcp   open     time
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
111/tcp  filtered rpcbind
2126/tcp open     pktcable-cops
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
3918/tcp open     pktcablemmcops
|_clamav-exec: ERROR: Script execution failed (use -d to debug)

Nmap done: 1 IP address (1 host up) scanned in 14.11 seconds
```

- **External.** Pueden enviar datos a una base de datos de terceros u otro recurso de red.
  Veamos un ejemplo de esta categoría en nuestra red (192.168.2.100).

```
→  ~ nmap --script external --script-args=newtargets 192.168.2.100
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-07 15:11 CST
Pre-scan script results:
| targets-asn:
|_  targets-asn.asn is a mandatory parameter
Nmap scan report for 192.168.2.100
Host is up (0.022s latency).
Not shown: 993 closed ports
PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   filtered ssh
23/tcp   filtered telnet
37/tcp   open     time
111/tcp  filtered rpcbind
2126/tcp open     pktcable-cops
3918/tcp open     pktcablemmcops

Host script results:
| dns-blacklist:
|   SPAM
|     l2.apews.org - FAIL
|_    list.quorum.to - FAIL

Nmap done: 1 IP address (1 host up) scanned in 17.50 seconds
```

- **Fuzzer.** Contiene scripts que están diseñados para enviar al software del servidor campos aleatorios o inesperados en cada paquete para encontrar errores y vulnerabilidades no descubiertos en el software, sin embargo, es un proceso lento que requiere mucho ancho de banda.

  Veamos un ejemplo de esta categoría en nuestra red (192.168.2.100).

```
→  ~ nmap --script fuzzer --script-args=newtargets 192.168.2.100
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-07 15:12 CST
Nmap scan report for 192.168.2.100
Host is up (0.033s latency).
Not shown: 993 closed ports
PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   filtered ssh
23/tcp   filtered telnet
37/tcp   open     time
111/tcp  filtered rpcbind
2126/tcp open     pktcable-cops
3918/tcp open     pktcablemmcops

Nmap done: 1 IP address (1 host up) scanned in 10.85 seconds
```

- **Intrusive.** Scrips cuyos riesgos de que bloqueen el sistema de destino, usen recursos significativos en el host de destino o que los usuarios del destino los perciban como maliciosos los administradores del sistema, son demasiado altos.

  Veamos un ejemplo de esta categoría en nuestra red (192.168.2.100).

```
→  ~ nmap --script intrusive --script-args=newtargets 192.168.2.100
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-07 15:12 CST
Nmap scan report for 192.168.2.100
Host is up (0.056s latency).
Not shown: 993 closed ports
PORT     STATE    SERVICE
21/tcp   open     ftp
| ftp-brute:
|   Accounts: No valid accounts found
|_  Statistics: Performed 9692 guesses in 601 seconds, average tps: 16.0
|_sslv2-drown:
22/tcp   filtered ssh
23/tcp   filtered telnet
37/tcp   open     time
111/tcp  filtered rpcbind
2126/tcp open     pktcable-cops
3918/tcp open     pktcablemmcops

Host script results:
|_dns-brute: Can't guess domain of "192.168.2.100"; use dns-brute.domain script argument.

Nmap done: 1 IP address (1 host up) scanned in 616.76 seconds
```

- **Malware.** Prueban si la plataforma de destino está infectada por malware o puertas traseras.
  Veamos un ejemplo de esta categoría en nuestra red (192.168.2.100).

```
→  ~ nmap --script malware --script-args=newtargets 192.168.2.100
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-07 15:14 CST
Nmap scan report for 192.168.2.100
Host is up (0.047s latency).
Not shown: 993 closed ports
PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   filtered ssh
23/tcp   filtered telnet
37/tcp   open     time
111/tcp  filtered rpcbind
2126/tcp open     pktcable-cops
3918/tcp open     pktcablemmcops

Nmap done: 1 IP address (1 host up) scanned in 7.62 seconds
```

- **Safe.** Secuencias de comandos que no fueron diseñadas para colapsar los servicios, usar grandes cantidades de ancho de banda de red u otros recursos, o explotar agujeros de seguridad.
  Veamos un ejemplo de esta categoría en nuestra red (192.168.2.100).

```
→  ~ nmap --script safe --script-args=newtargets 192.168.2.100
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-07 15:15 CST
Pre-scan script results:
| broadcast-upnp-info:
|   239.255.255.250
|       Server: ipos/7.0 UPnP/1.0 TL-WR940N/6.0
|_      Location: http://192.168.1.1:1900/igd.xml
| targets-asn:
|_  targets-asn.asn is a mandatory parameter
Nmap scan report for 192.168.2.100
Host is up (0.026s latency).
Not shown: 993 closed ports
PORT     STATE    SERVICE
21/tcp   open     ftp
|_banner: 220 (vsFTPd 3.0.2)
22/tcp   filtered ssh
23/tcp   filtered telnet
37/tcp   open     time
111/tcp  filtered rpcbind
2126/tcp open     pktcable-cops
|_banner: \x10\x06\x80\x08\x00\x00\x00$\x00\x1C\x0B\x01CASA_C100G_IXTA...
3918/tcp open     pktcablemmcops
|_banner: \x10\x06\x80\x0A\x00\x00\x000\x00\x1C\x0B\x01CASA_C100G_IXTA...

Host script results:
| dns-blacklist:
|   SPAM
|     l2.apews.org - FAIL
|_    list.quorum.to - FAIL
|_fcrdns: FAIL (No PTR record)
| unusual-port:
|_  WARNING: this script depends on Nmap's service/version detection (-sV)

Post-scan script results:
| reverse-index:
|   21/tcp: 192.168.2.100
|   37/tcp: 192.168.2.100
|   2126/tcp: 192.168.2.100
|_  3918/tcp: 192.168.2.100
Nmap done: 2 IP addresses (1 host up) scanned in 59.23 seconds
```

- **Version.** Son una extensión de la función de detección de versiones y no se pueden seleccionar de forma explícita.

  Veamos un ejemplo de esta categoría en nuestra red (192.168.2.100).

```
→  ~ nmap --script version --script-args=newtargets 192.168.2.100
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-07 15:15 CST
Nmap scan report for 192.168.2.100
Host is up (0.054s latency).
Not shown: 993 closed ports
PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   filtered ssh
23/tcp   filtered telnet
37/tcp   open     time
111/tcp  filtered rpcbind
2126/tcp open     pktcable-cops
3918/tcp open     pktcablemmcops

Nmap done: 1 IP address (1 host up) scanned in 10.65 seconds
```

- **Vuln.** Verifican vulnerabilidades específicas conocidas y, en general, solo informan los resultados si se encuentran.

  Veamos un ejemplo de esta categoría en nuestra red (192.168.2.100).

```
→  ~ nmap --script vuln --script-args=newtargets 192.168.2.100
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-07 15:16 CST
Nmap scan report for 192.168.2.100
Host is up (0.060s latency).
Not shown: 993 closed ports
PORT     STATE    SERVICE
21/tcp   open     ftp
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_sslv2-drown:
22/tcp   filtered ssh
23/tcp   filtered telnet
37/tcp   open     time
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
111/tcp  filtered rpcbind
2126/tcp open     pktcable-cops
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
3918/tcp open     pktcablemmcops
|_clamav-exec: ERROR: Script execution failed (use -d to debug)

Nmap done: 1 IP address (1 host up) scanned in 20.32 seconds
```

8. ¿Qué es un exploit? Con base en el punto 5 y 7 buscar un exploit en la red que comprometa al sistema objetivo con las versiones vulnerables halladas (solo buscar el exploit, no es necesario ejecutarlo).

   Solución. Un exploit es un programa informático, una parte de un software o una secuencia de comandos que se aprovecha de un error o vulnerabilidad para provocar un comportamiento no intencionado o imprevisto en un software, hardware o en cualquier dispositivo electrónico.

3. Referencias

3.1. Bibliografía

- McKay, D. (2020, julio 9). How to use the whois command on Linux. How-To Geek. https://www.howtogeek.com/680086/how-to-use-the-whois-command-on-linux/
- nslookup command in Linux with Examples. (2018, diciembre 20). GeeksforGeeks. https://www.geeksforgeeks.org/nslookup-command-in-linux-with-examples/
- traceroute command in Linux with Examples. (2019, febrero 18). GeeksforGeeks. https://www.geeksforgeeks.org/traceroute-command-in-linux-with-examples/
- Usage and Examples. (s/f). Nmap.org. Recuperado el 25 de octubre de 2022, de https://nmap.org/book/nse-usage.html