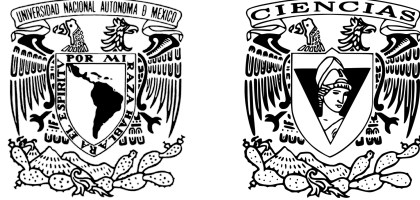


UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE CIENCIAS



Criptografía y Seguridad
Proyecto 02: Reporte

Sebastián Alamina Ramírez - 318685496

Camila Alexandra Cruz Miranda - 316084707

Carlos Alberto Desiderio Castillo - 312183839

Trabajo presentado como parte del curso de **Criptografía y Seguridad**, impartido por el profesor **Manuel Díaz Díaz** durante el semestre 2023-1 en la Facultad de Ciencias, UNAM.

Fecha de entrega: **miércoles 9 de noviembre del 2022.**

Especificación general: Utilizando las herramientas vistas en clase (whois, nslookup, traceroute y nmap), elaborar un breve reporte escrito con capturas de pantalla referente al flujo de escaneo de vulnerabilidades.

1. Para **whois**, incluir una captura de pantalla que muestre la siguiente información de algún dominio: fecha de creación, fecha de expiración, datos de contacto del administrador y direcciones IP de los DNS.

Whois Record for Nintendo.com

— Domain Profile


Registrant	Nintendo Nintendo
Registrant Org	Nintendo of America Inc.
Registrant Country	us
Registrar	CSC CORPORATE DOMAINS, INC. CSC Corporate Domains, Inc. IANA ID: 299 URL: www.cscprotectsbrands.com,http://cscdbs.com Whois Server: whois.corporatedomains.com domainabuse@cscglobal.com (p) 18887802723
Registrar Status	clientTransferProhibited, serverDeleteProhibited, serverTransferProhibited, serverUpdateProhibited
Dates	10,164 days old Created on 1995-01-10 Expires on 2024-01-09 Updated on 2020-10-20
Name Servers	NS-1047.AWSDNS-02.ORG (has 68,831 domains) NS-1908.AWSDNS-46.CO.UK (has 241 domains) NS-431.AWSDNS-53.COM (has 1,551 domains) NS-983.AWSDNS-58.NET (has 11 domains)
Tech Contact	Nintendo DNS Administration Nintendo of America Inc. 4600 150th Ave. N.E., Redmond, WA, 98052, us netadmin@noa.nintendo.com (p) 14258822040 (f) 14258823585
IP Address	146.75.42.132 - 2,745 other sites hosted on this server
IP Location	 - Vastra Gotalands Lan - Goteborg - Fastly Inc.

Figure 1: Whois nintendo.com

En la captura podemos ver en el apartado **Dates** las fechas de creación y expiración, en **Tech Contact** los datos de contacto del administrador y la dirección IP en **IP Address**.

2. Para **nslookup**, una captura de pantalla que muestre toda la información disponible (utilizando la opción `type`) de algún dominio: Nombre del host, dirección IP de los servidores DNS y demás detalles del servidor.

```
camila@Farore:~$ nslookup
> set type=ns
> redhat.com
Server:      1.1.1.1
Address:     1.1.1.1#53

Non-authoritative answer:
redhat.com   nameserver = a10-65.akam.net.
redhat.com   nameserver = a28-64.akam.net.
redhat.com   nameserver = a13-66.akam.net.
redhat.com   nameserver = a9-65.akam.net.
redhat.com   nameserver = a16-67.akam.net.
redhat.com   nameserver = a1-68.akam.net.

Authoritative answers can be found from:
> server a10-65.akam.net
Default server: a10-65.akam.net
Address: 96.7.50.65#53
> set type=a
> redhat.com
Server:      a10-65.akam.net
Address:     96.7.50.65#53

Name:   redhat.com
Address: 52.200.142.250
Name:   redhat.com
Address: 34.235.198.240
> set type=mx
> redhat.com
Server:      a10-65.akam.net
Address:     96.7.50.65#53

redhat.com   mail exchanger = 10 us-smtp-inbound-2.mimecast.com.
redhat.com   mail exchanger = 10 us-smtp-inbound-1.mimecast.com.
> 
```

Figure 2: nslookup redhat.com

Aquí podemos ver información de **redhat.com** como su nombre, sus direcciones IP: 52.200.142.250 / 34.235.198.240 e información de sus correos utilizando uno de los servidores que encontramos con `set type=ns`.

3. Para **tracert**, una captura de pantalla que muestre el trazado de ruta hacia el un servidor DNS (dominio cualquiera) y obtener información de algún servidor por donde viaja la comunicación con la herramienta **nslookup**. Se muestra el

```
Traza a la dirección amazon.com.mx [52.94.225.241]
sobre un máximo de 30 saltos:

 1  300 ms    2 ms    3 ms    192.168.1.254
 2   21 ms    19 ms    20 ms    dsl-servicio-l200.uninet.net.mx [200.38.193.226]
 3   61 ms    61 ms    61 ms    bb-la-grand-10-ae0_0.uninet.net.mx [189.246.220.97]
 4   *        *        *        Tiempo de espera agotado para esta solicitud.
 5  118 ms    116 ms    101 ms    150.222.234.31
 6   88 ms    198 ms    88 ms    54.239.102.232
 7   *        *        *        Tiempo de espera agotado para esta solicitud.
 8   90 ms    74 ms    76 ms    15.230.16.62
 9   *        *        *        Tiempo de espera agotado para esta solicitud.
10  *        *        *        Tiempo de espera agotado para esta solicitud.
11  *        *        *        Tiempo de espera agotado para esta solicitud.
12  *        *        *        Tiempo de espera agotado para esta solicitud.
13  *        *        *        Tiempo de espera agotado para esta solicitud.
14 128 ms    128 ms    127 ms    52.93.28.90
15  *        *        *        Tiempo de espera agotado para esta solicitud.
16  *        *        *        Tiempo de espera agotado para esta solicitud.
17  *        *        *        Tiempo de espera agotado para esta solicitud.
18  *        *        *        Tiempo de espera agotado para esta solicitud.
19  *        *        *        Tiempo de espera agotado para esta solicitud.
20  *        *        *        Tiempo de espera agotado para esta solicitud.
21  *        *        *        Tiempo de espera agotado para esta solicitud.
22  *        *        *        Tiempo de espera agotado para esta solicitud.
23  *        *        *        Tiempo de espera agotado para esta solicitud.
24  *        *        *        Tiempo de espera agotado para esta solicitud.
25 170 ms    202 ms    203 ms    52.94.225.241

Traza completa.
```

Figure 3: tracert amazon.com.mx

trazado de ruta hacia el dominio **amazon.com.mx**, para después mostrar información sobre el segundo servidor de la ruta trazada (**dsl-servicio-l200.uninet.net.mx**), usando **nslookup**.

```
> dsl-servicio-l200.uninet.net.mx
Servidor:  2806-1050-ffff-0004-0000-0000-0000-000e
Address:  2806:1050:ffff:4::e

Respuesta no autoritativa:
Nombre:  dsl-servicio-l200.uninet.net.mx
Address:  200.38.193.226

> set type=ns
>
> dsl-servicio-l200.uninet.net.mx
Servidor:  2806-1050-ffff-0004-0000-0000-0000-000e
Address:  2806:1050:ffff:4::e

uninet.net.mx
    primary name server = dnsadm-interno.uninet.net.mx
    responsible mail addr = adm-dns.reduno.com.mx
    serial = 10511
    refresh = 14400 (4 hours)
    retry = 3600 (1 hour)
    expire = 604800 (7 days)
    default TTL = 900 (15 mins)
```

Figure 4: nslookup dsl-servicio-l200.uninet.net.mx

Información que se pudo obtener con **nslookup**, para el servidor **dsl-servicio-l200.uninet.net.mx**.

4. Utilizar **nmap** para mostrar:

- (a) Barrido de red.

```
root@carlos-VirtualBox:/home/carlos# nmap 10.0.2.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-08 19:53 CST
Nmap scan report for _gateway (10.0.2.2)
Host is up (0.015s latency).
Not shown: 994 filtered ports
PORT      STATE SERVICE
135/tcp    open  msrpc
445/tcp    open  microsoft-ds
3306/tcp   open  mysql
5357/tcp   open  wsapi
5432/tcp   open  postgresql
6646/tcp   open  unknown
MAC Address: 52:54:00:12:35:02 (QEMU virtual NIC)

Nmap scan report for 10.0.2.3
Host is up (0.015s latency).
Not shown: 994 filtered ports
PORT      STATE SERVICE
135/tcp    open  msrpc
445/tcp    open  microsoft-ds
3306/tcp   open  mysql
5357/tcp   open  wsapi
5432/tcp   open  postgresql
6646/tcp   open  unknown
MAC Address: 52:54:00:12:35:03 (QEMU virtual NIC)
```

```
Nmap scan report for 10.0.2.4
Host is up (0.014s latency).
Not shown: 994 filtered ports
PORT      STATE SERVICE
135/tcp    open  msrpc
445/tcp    open  microsoft-ds
3306/tcp   open  mysql
5357/tcp   open  wsapi
5432/tcp   open  postgresql
6646/tcp   open  unknown
MAC Address: 52:54:00:12:35:04 (QEMU virtual NIC)

Nmap scan report for carlos-VirtualBox (10.0.2.15)
Host is up (0.0000080s latency).
All 1000 scanned ports on carlos-VirtualBox (10.0.2.15) are closed

Nmap done: 256 IP addresses (4 hosts up) scanned in 10.87 seconds
```

Figure 5: nmap: Barrido de red (Network sweep)

(b) Escaneo de puertos TCP SYN.

```
root@carlos-VirtualBox:/home/carlos# nmap -sS 10.0.2.4
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-08 20:00 CST
Nmap scan report for 10.0.2.4
Host is up (0.0068s latency).
Not shown: 994 filtered ports
PORT      STATE SERVICE
135/tcp    open  msrpc
445/tcp    open  microsoft-ds
3306/tcp   open  mysql
5357/tcp   open  wsapi
5432/tcp   open  postgresql
6646/tcp   open  unknown
MAC Address: 52:54:00:12:35:04 (QEMU virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 4.48 seconds
root@carlos-VirtualBox:/home/carlos#
```

Figure 6: nmap: Puertos TCP SYN

(c) Escaneo de puertos UDP.

```
root@carlos-VirtualBox:/home/carlos# nmap -sU 10.0.2.4
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-08 20:02 CST
Nmap scan report for 10.0.2.4
Host is up (0.00092s latency).
Not shown: 990 filtered ports
PORT      STATE SERVICE
67/udp    open|filtered dhcps
69/udp    open|filtered tftp
137/udp    open|filtered netbios-ns
500/udp    open|filtered isakmp
1900/udp   open|filtered upnp
3702/udp   open|filtered ws-discovery
4500/udp   open|filtered nat-t-ike
5050/udp   open|filtered mmcc
5353/udp   open|filtered zeroconf
5355/udp   open|filtered llmnr
MAC Address: 52:54:00:12:35:04 (QEMU virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 54.37 seconds
root@carlos-VirtualBox:/home/carlos#
```

Figure 7: nmap: Puertos UDP

(d) Determinar el Sistema Operativo del objetivo.

No se pudo determinar con certeza el sistema operativo del sistema objetivo, a pesar que se hizo uso de **nmap -O -o--osscan-guess**, para tratar de determinar de una forma mas agresiva el sistema operativo del sistema, los resultados fueron los siguientes:

```

root@carlos-VirtualBox:/home/carlos# nmap -O 10.0.2.4
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-08 20:23 CST
Nmap scan report for 10.0.2.4
Host is up (0.0027s latency).
Not shown: 994 filtered ports
PORT      STATE SERVICE
135/tcp    open  msrpc
445/tcp    open  microsoft-ds
3306/tcp   open  mysql
5357/tcp   open  wsdapi
5432/tcp   open  postgresql
6646/tcp   open  unknown
MAC Address: 52:54:00:12:35:04 (QEMU virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1
open and 1 closed port
Device type: general purpose|bridge|printer
Running (JUST GUESSING): QEMU (98%), Oracle Virtualbox (97%), Samsung embedded
(89%), Dell embedded (88%), Wind River VxWorks (88%), Xerox embedded (88%)
OS CPE: cpe:/a:qemu:qemu cpe:/o:oracle:virtualbox cpe:/h:samsung:clp-315w cpe:/
h:dell:1815dn cpe:/o:windriver:vxworks cpe:/h:xerox:workcentre_4150
Aggressive OS guesses: QEMU user mode network gateway (98%), Oracle Virtualbox
(97%), Samsung CLP-315W printer (89%), Dell 1815dn printer (88%), VxWorks (88%)
, Xerox WorkCentre 4150 printer (88%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

```

Figure 8: nmap: Determinación del sistema operativo

```

root@carlos-VirtualBox:/home/carlos# nmap -O --osscan-guess 10.0.2.4
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-08 20:21 CST
Nmap scan report for 10.0.2.4
Host is up (0.0030s latency).
Not shown: 994 filtered ports
PORT      STATE SERVICE
135/tcp    open  msrpc
445/tcp    open  microsoft-ds
3306/tcp   open  mysql
5357/tcp   open  wsdapi
5432/tcp   open  postgresql
6646/tcp   open  unknown
MAC Address: 52:54:00:12:35:04 (QEMU virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1
open and 1 closed port
Device type: general purpose|bridge|printer
Running (JUST GUESSING): QEMU (98%), Oracle Virtualbox (97%), Samsung embedded
(89%), Dell embedded (88%), Wind River VxWorks (88%), Xerox embedded (88%)
OS CPE: cpe:/a:qemu:qemu cpe:/o:oracle:virtualbox cpe:/h:samsung:clp-315w cpe:/
h:dell:1815dn cpe:/o:windriver:vxworks cpe:/h:xerox:workcentre_4150
Aggressive OS guesses: QEMU user mode network gateway (98%), Oracle Virtualbox
(97%), Samsung CLP-315W printer (89%), Dell 1815dn printer (88%), VxWorks (88%)
, Xerox WorkCentre 4150 printer (88%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

```

Figure 9: nmap: Determinación del sistema operativo con --osscan-guess

- (e) Determinar servicios y versiones de puertos abiertos.

```
root@carlos-VirtualBox:/home/carlos# nmap -sV 10.0.2.4
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-08 20:26 CST
Nmap scan report for 10.0.2.4
Host is up (0.0057s latency).
Not shown: 994 filtered ports
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
445/tcp    open  microsoft-ds?
3306/tcp   open  mysql?
5357/tcp   open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5432/tcp   open  postgresql?
6646/tcp   open  unknown
1 service unrecognized despite returning data. If you know the service/version,
please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi
?new-service :
```

Figure 10: nmap: servicios y versiones de puertos abiertos.

- (f) Evaluar reglas de firewall y determinar si hay puertos filtrados con TCP ACK

```
root@carlos-VirtualBox:/home/carlos# nmap -sA 10.0.2.4
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-08 20:41 CST
Nmap scan report for 10.0.2.4
Host is up (0.0015s latency).
All 1000 scanned ports on 10.0.2.4 are unfiltered
MAC Address: 52:54:00:12:35:04 (QEMU virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.62 seconds
```

Figure 11: nmap: reglas de firewall y puertos filtrados.

- (g) Investigar las categorías **NSE**, describir brevemente cada categoría NSE de nmap, así como mostrar el uso de cada una en equipo objetivo de tu red local:

- **auth**: Scripts NSE que se usan para la autenticación de usuario, en el sistema de destino, Las secuencias de comandos que utilizan ataques de fuerza bruta para determinar las credenciales se colocan en la categoría brute.

```
root@carlos-VirtualBox:/home/carlos# nmap --script auth 10.0.2.4
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-08 22:22 CST
Nmap scan report for 10.0.2.4
Host is up (0.0085s latency).
Not shown: 994 filtered ports
PORT      STATE SERVICE
135/tcp    open  msrpc
445/tcp    open  microsoft-ds
3306/tcp   open  mysql
5357/tcp   open  wsdaapi
5432/tcp   open  postgresql
6646/tcp   open  unknown
MAC Address: 52:54:00:12:35:04 (QEMU virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 7.77 seconds
```

Figure 12: nmap: script de categoría auth

- **broadcast:** Categoría de scripts que sirven para obtener información de la red, usando peticiones de transmisión, normalmente detectan hosts que no aparecen en la línea de comandos mediante la difusión en la red local.

```

root@carlos-VirtualBox:/home/carlos# nmap --script broadcast 10.0.2.4
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-08 22:24 CST
too short
Pre-scan script results:
| broadcast-dhcp-discover:
|   Response 1 of 1:
|     IP Offered: 10.0.2.16
|     Subnet Mask: 255.255.255.0
|     Router: 10.0.2.2
|     Domain Name Server: 192.168.1.254
|_   Server Identifier: 10.0.2.2
|_ eap-info: please specify an interface with -e
Nmap scan report for 10.0.2.4
Host is up (0.0059s latency).
Not shown: 994 filtered ports
PORT      STATE SERVICE
135/tcp    open  msrpc
445/tcp    open  microsoft-ds
3306/tcp   open  mysql
5357/tcp   open  wsddapi
5432/tcp   open  postgresql
6646/tcp   open  unknown
MAC Address: 52:54:00:12:35:04 (QEMU virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 46.41 seconds

```

Figure 13: nmap: script de categoría broadcast.

- **brute:** Son scripts que utilizan ataques de fuerza bruta para adivinar las credenciales de autenticación de un servidor remoto.

```

root@carlos-VirtualBox:/home/carlos# nmap --script brute 10.0.2.4
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-08 22:26 CST
Nmap scan report for 10.0.2.4
Host is up (0.011s latency).
Not shown: 994 filtered ports
PORT      STATE SERVICE
135/tcp    open  msrpc
445/tcp    open  microsoft-ds
3306/tcp   open  mysql
| mysql-brute:
|   Accounts: No valid accounts found
|_  Statistics: Performed 50009 guesses in 158 seconds, average tps: 325.0
| mysql-enum:
|   Valid usernames:
|     root:<empty> - Valid credentials
|     netadmin:<empty> - Valid credentials
|     guest:<empty> - Valid credentials
|     user:<empty> - Valid credentials
|     web:<empty> - Valid credentials
|     sysadmin:<empty> - Valid credentials
|     administrator:<empty> - Valid credentials
|     webadmin:<empty> - Valid credentials
|     admin:<empty> - Valid credentials
|     test:<empty> - Valid credentials
|_  Statistics: Performed 10 guesses in 1 seconds, average tps: 10.0
5357/tcp   open  wsddapi
5432/tcp   open  postgresql

```

Figure 14: nmap: script de categoría brute.

- **default:** Se utilizan para el escaneo de scripts, estos scripts son el conjunto predeterminado y se ejecutan cuando se usan las opciones -sC o -A, en lugar de enumerar los scripts con --script.

```

root@carlos-VirtualBox:/home/carlos# nmap -sC 10.0.2.4
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-08 22:32 CST
Nmap scan report for 10.0.2.4
Host is up (0.0090s latency).
Not shown: 994 filtered ports
PORT      STATE SERVICE
135/tcp    open  msrpc
445/tcp    open  microsoft-ds
3306/tcp   open  mysql
|_ mysql-info:
|   Protocol: 10
|   Version: 8.0.28
|   Thread ID: 50162
|   Capabilities flags: 65535
|   Some Capabilities: SupportsCompression, ODBCClient, ConnectWithDatabase, Support41Auth, Speaks41ProtocolOld, SupportsTransactions, IgnoreSpaceBeforeParenthesis, FoundRows, LongColumnFlag, InteractiveClient, SwitchToSSLAfterHandshake, LongPassword, IgnoreSigpipes, Speaks41ProtocolNew, SupportsLoadDataLocal, DontAllowDatabaseTableColumn, SupportsMultipleResults, SupportsAuthPlugins, SupportsMultipleStatements
|   Status: Autocommit
|   Salt: \x06E&\x12[E\x12yd5&\x03\x0C\x19C{%uD
|_ Auth Plugin Name: caching_sha2_password
5357/tcp   open  wsddapi
5432/tcp   open  postgresql
6646/tcp   open  unknown
MAC Address: 52:54:00:12:35:04 (QEMU virtual NIC)
Host script results:

```

Figure 15: nmap: script de categoría default.

- **discovery:** Son scripts usados para el descubrimiento de hosts y servicios. Intentan descubrir activamente más sobre la red consultando registros públicos, dispositivos habilitados para SNMP, servicios de directorio y similares.

```

root@carlos-VirtualBox:/home/carlos# nmap --script discovery 10.0.2.4
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-08 22:36 CST
too short
Pre-scan script results:
|_ targets-asn:
|_ targets-asn.asn is a mandatory parameter
Nmap scan report for 10.0.2.4
Host is up (0.0050s latency).
Not shown: 994 filtered ports
PORT      STATE SERVICE
135/tcp    open  msrpc
445/tcp    open  microsoft-ds
|_ smb-enum-services: ERROR: Script execution failed (use -d to debug)
3306/tcp   open  mysql
|_ banner: J\x00\x00\x00\x00A8.0.28\x00\xF7\xC3\x00\x00bXGT-[7;\x00\xFF\...
|_ mysql-info:
|   Protocol: 10
|   Version: 8.0.28
|   Thread ID: 50166
|   Capabilities flags: 65535
|   Some Capabilities: Support41Auth, ODBCClient, DontAllowDatabaseTableColumn, Speaks41ProtocolOld, ConnectWithDatabase, SupportsTransactions, SupportsCompression, InteractiveClient, SupportsLoadDataLocal, IgnoreSigpipes, LongColumnFlag, SwitchToSSLAfterHandshake, Speaks41ProtocolNew, FoundRows, IgnoreSpaceBeforeParenthesis, LongPassword, SupportsAuthPlugins, SupportsMultipleStatements, SupportsMultipleResults

```

Figure 16: nmap: script de categoría discovery.

- **dos:** Son scripts relacionados con ataques de denegación de servicio, algunos usos son para probar la vulnerabilidad a un método de denegación de servicio, estas pruebas a veces bloquean servicios vulnerables.

```

root@carlos-VirtualBox:/home/carlos# nmap --script broadcast --script-args=newt
argets 10.0.2.4
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-08 22:56 CST
too short
Pre-scan script results:
| broadcast-dhcp-discover:
|   Response 1 of 1:
|     IP Offered: 10.0.2.16
|     Subnet Mask: 255.255.255.0
|     Router: 10.0.2.2
|     Domain Name Server: 192.168.1.254
|     Server Identifier: 10.0.2.2
|_ eap-info: please specify an interface with -e
Nmap scan report for 10.0.2.4
Host is up (0.013s latency).
Not shown: 994 filtered ports
PORT      STATE SERVICE
135/tcp    open  msrpc
445/tcp    open  microsoft-ds
3306/tcp   open  mysql
5357/tcp   open  wsdapl
5432/tcp   open  postgresql
6646/tcp   open  unknown
MAC Address: 52:54:00:12:35:04 (QEMU virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 46.67 seconds
root@carlos-VirtualBox:/home/carlos#

```

Figure 17: nmap: script de categoría dos.

- **exploit:** Son scripts tienen como objetivo explotar activamente alguna vulnerabilidad de seguridad del sistema objetivo.

```

root@carlos-VirtualBox:/home/carlos# nmap -sV --script=afp-path-vuln 10.0.2.4
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-08 23:03 CST
Nmap scan report for 10.0.2.4
Host is up (0.0086s latency).
Not shown: 994 filtered ports
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
445/tcp    open  microsoft-ds?
3306/tcp   open  mysql?
| fingerprint-strings:
|   DNSStatusRequestTCP:
|     8.0.28
|     1[:Y2=
|     caching_sha2_password
|     #08501Got packets out of order
|   DNSVersionBindReqTCP:
|     8.0.28
|     ^|]2Rg{
|     caching_sha2_password
|     #08501Got packets out of order
|   GenericLines:
|     8.0.28
|     1KF[50>gr
|     caching_sha2_password
|     #08501Got packets out of order
|   GetRequest:
|     8.0.28
|     l;hsY
|     caching_sha2_password

```

Figure 18: nmap: script de categoría exploit.

- **external:** Son scripts que dependen de un servicio de terceros, los scripts de esta categoría pueden enviar datos a una base de datos de terceros u otro recurso de red.

```

root@carlos-VirtualBox:/home/carlos# nmap -sn 10.0.2.4 --script dns-blacklist
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-08 23:18 CST
Nmap scan report for 10.0.2.4
Host is up (0.00036s latency).
MAC Address: 52:54:00:12:35:04 (QEMU virtual NIC)

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

Nmap done: 1 IP address (1 host up) scanned in 12.99 seconds

```

Figure 19: nmap: script de categoría external.

- **fuzzer:** Son scripts NSE enfocados en fuzzing, esta categoría contiene scripts que están diseñados para enviar al software del servidor campos aleatorios o inesperados en cada paquete.

```

root@carlos-VirtualBox:/home/carlos# nmap --script http-form-fuzzer --script-args 'http-form-fuzzer.targets={1={path=/},2={path=/register.html}}' -p 80 10.0.2.4
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-08 23:31 CST
Nmap scan report for 10.0.2.4
Host is up (0.00031s latency).

PORT      STATE      SERVICE
80/tcp    filtered  http
MAC Address: 52:54:00:12:35:04 (QEMU virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.89 seconds

```

Figure 20: nmap: script de categoría fuzzer.

- **intrusive:** Son una categoría para scripts que pueden bloquear algo o generar mucho ruido en la red, el uso de estos scripts genera el riesgo de que bloqueen el sistema de destino, consuman recursos significativos en el host de destino o que el sistema los perciba como maliciosos.

```

root@carlos-VirtualBox:/home/carlos# nmap -p 8009 10.0.2.4 --script ajp-brute
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-08 23:33 CST
Nmap scan report for 10.0.2.4
Host is up (0.00029s latency).

PORT      STATE      SERVICE
8009/tcp  filtered  ajp13
MAC Address: 52:54:00:12:35:04 (QEMU virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.91 seconds

```

Figure 21: nmap: script de categoría intrusive.

- **malware:** Son scripts que prueban si la plataforma de destino está infectada por malware, se usan para la detección de este.

```
root@carlos-VirtualBox:/home/carlos# nmap -sn -PN --script=dns-zeustracker 10.0.2.4
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-09 00:11 CST
Nmap scan report for 10.0.2.4
Host is up.

Nmap done: 1 IP address (1 host up) scanned in 0.54 seconds
```

Figure 22: nmap: script de categoría malware.

- **safe:** Son scripts que no fueron diseñados para bloquear servicios, usar grandes cantidades de ancho de banda de la red u otros recursos, o explotar agujeros de seguridad, es decir son scripts que se consideran seguros en todas las situaciones.

```
root@carlos-VirtualBox:/home/carlos# nmap -sU -p 8611,8612 --script bjnp-discover 10.0.2.4
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-08 23:37 CST
Nmap scan report for 10.0.2.4
Host is up (0.00058s latency).

PORT      STATE      SERVICE
8611/udp   filtered   canon-bjnp1
8612/udp   filtered   canon-bjnp2
MAC Address: 52:54:00:12:35:04 (QEMU virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.75 seconds
```

Figure 23: nmap: script de categoría safe.

- **version:** Los scripts de esta categoría son una extensión de la función de detección avanzada de versiones. Se seleccionan para ejecutarse solo si se solicitó la detección de versión (-sV).

```
root@carlos-VirtualBox:/home/carlos# nmap --script bacnet-info -sU -p 47808 10.0.2.4
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-08 23:57 CST
Nmap scan report for 10.0.2.4
Host is up (0.00049s latency).

PORT      STATE      SERVICE
47808/udp   filtered   bacnet
MAC Address: 52:54:00:12:35:04 (QEMU virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.68 seconds
```

Figure 24: nmap: script de categoría version.

- **vuln:** Estos scripts verifican vulnerabilidades específicas conocidas y, en general, solo informan los resultados si se encuentran. Están relacionados con la detección y explotación de vulnerabilidades de seguridad.

```

root@carlos-VirtualBox:/home/carlos# nmap --script=broadcast-avahi-dos 10.0.2.4
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-08 23:43 CST
Nmap scan report for 10.0.2.4
Host is up (0.0066s latency).
Not shown: 994 filtered ports
PORT      STATE SERVICE
135/tcp   open  msrpc
445/tcp   open  microsoft-ds
3306/tcp   open  mysql
5357/tcp   open  wsapi
5432/tcp   open  postgresql
6646/tcp   open  unknown
MAC Address: 52:54:00:12:35:04 (QEMU virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 14.71 seconds
root@carlos-VirtualBox:/home/carlos#

```

Figure 25: nmap: script de categoría vuln.

- (h) ¿Qué es un **exploit**?. Con base en el inciso e) y g) buscar un exploit en la red que comprometa al sistema objetivo con las versiones vulnerables halladas (solo buscar el exploit, no es necesario ejecutarlo).

Un **exploit** es cuando se conoce alguna vulnerabilidad o falla de seguridad de un sistema, y se usan algún script que se aprovecha de esto, para poder explotar más dicha falla o vulnerabilidad.

Al escanear las vulnerabilidades de nuestro sistema, encontramos la siguiente vulnerabilidad de tipo **dos**:

```

Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
|_http-slowloris: false
443/tcp    open  https
|_http-slowloris:
|   Probably vulnerable:
|   the DoS attack took +2s
|   with 1 concurrent connections
|   and 0 sent queries
|_ Monitoring thread couldn't communicate with the server. This is probably due to max
clients exhaustion or something similar but not due to slowloris attack.

Nmap done: 1 IP address (1 host up) scanned in 1913.96 seconds

```

Figure 26: nmap: Vulnerabilidad encontrada.

para explotarla se haría uso del siguiente script: **nmap --script smb-vuln-cve2009-3103.nse -p445 <host>**, que se usa para ataques de tipo **dos**.