

Segundo Proyecto

Reporte

Criptografía y Seguridad



Universidad
Nacional
Autónoma
De
México

CARLOS CRUZ RANGEL

carloscruzrangel@ciencias.unam.mx

JOSÉ DEMIAN JIMÉNEZ SALGADO

josedemian@ciencias.unam.mx

VICTOR HUGO GALLEGOS MOTA

316160456@ciencias.unam.mx

INDICE

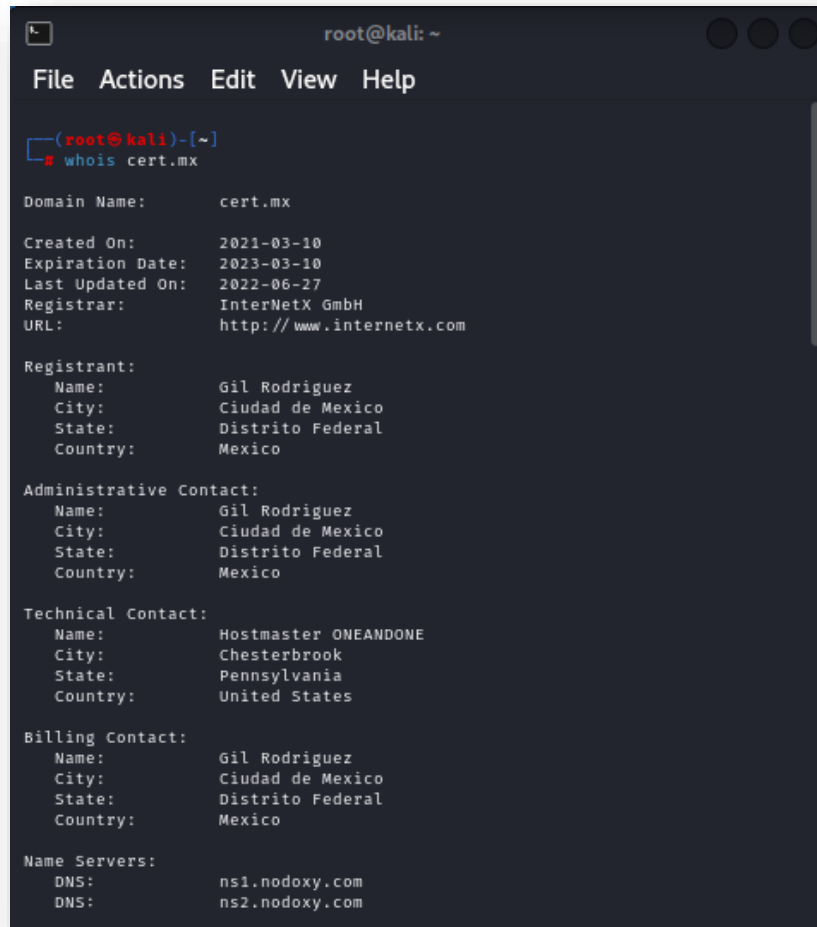
REPORTE	3
WHOIS	3
NSLOOKUP	3
TRACEROUTE	4
NMAP	5
1.- Barrido de red.	5
2.- Escaneo de puertos TCP SYN.	6
3.- Escaneo de puertos UDP.	6
4.- Determinar el Sistema Operativo del objetivo.	7
5.- Determinar servicios y versiones de puertos abiertos.	7
6.- Evaluar reglas de firewall y determinar si hay puerto filtrados con TCP ACK	8
7.- Investigar las categorías NSE:	8
• Auth	8
• Broadcast	9
• Brute	9
• Default	10
• Discovery	11
• Dos	13
• Exploit	13
• External	13
• Fuzzer	14
• Intrusive	14
• Malware	14
• Safe	15
• Version	16
• Vuln	17
8.- ¿Qué es un exploit?.	17

REPORTE

WHOIS

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.

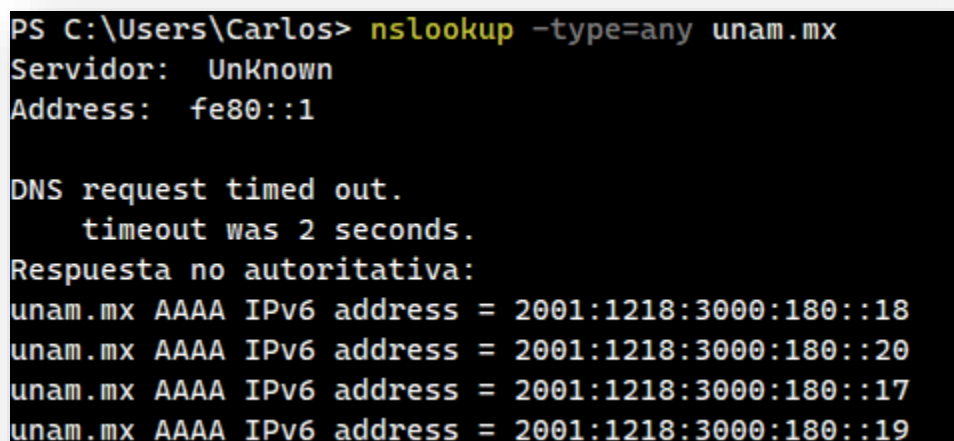
Ejecutamos whois desde la terminal de Kali Linux, esta función nos da los datos detallados del dominio, este caso de cert.mx



```
root@kali: ~  
File Actions Edit View Help  
(root@kali)-[~]  
# whois cert.mx  
  
Domain Name:      cert.mx  
  
Created On:       2021-03-10  
Expiration Date:  2023-03-10  
Last Updated On:  2022-06-27  
Registrar:       InterNetX GmbH  
URL:             http://www.internetx.com  
  
Registrant:  
  Name:           Gil Rodriguez  
  City:           Ciudad de Mexico  
  State:          Distrito Federal  
  Country:        Mexico  
  
Administrative Contact:  
  Name:           Gil Rodriguez  
  City:           Ciudad de Mexico  
  State:          Distrito Federal  
  Country:        Mexico  
  
Technical Contact:  
  Name:           Hostmaster ONEANDONE  
  City:           Chesterbrook  
  State:          Pennsylvania  
  Country:        United States  
  
Billing Contact:  
  Name:           Gil Rodriguez  
  City:           Ciudad de Mexico  
  State:          Distrito Federal  
  Country:        Mexico  
  
Name Servers:  
  DNS:            ns1.nodoxy.com  
  DNS:            ns2.nodoxy.com
```

NSLOOKUP

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.



```
PS C:\Users\Carlos> nslookup -type=any unam.mx  
Servidor:  UnKnown  
Address:   fe80::1  
  
DNS request timed out.  
  timeout was 2 seconds.  
Respuesta no autoritativa:  
unam.mx AAAA IPv6 address = 2001:1218:3000:180::18  
unam.mx AAAA IPv6 address = 2001:1218:3000:180::20  
unam.mx AAAA IPv6 address = 2001:1218:3000:180::17  
unam.mx AAAA IPv6 address = 2001:1218:3000:180::19
```

TRACEROUTE

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

```
(root@kali)-[~]
# traceroute sat.gob.mx
traceroute to sat.gob.mx (200.33.84.233), 30 hops max, 60 byte packets
 1  10.0.2.2 (10.0.2.2)  0.773 ms  0.881 ms  0.758 ms
 2  10.0.2.2 (10.0.2.2)  4.901 ms  5.686 ms  5.063 ms
```

07-RSA (Proyecto 2) - PresentaciLinux Whois Command Help andTraceroute visual - Rastree y map

gsuite.tools/es/traceroute

G Suite.Tools

Bookmark This Page

VERIFICADOR EMAILBÚSQUEDA DE DNSTRACEROUTEUBICACIÓN IPMI IPPINGAUDITORÍA SEOVELOCIDAD DE PÁGINA

traceroute to sat.gob.mx (200.33.84.233), 30 hops max

Hop	Host	IP	Time (ms)
1	dgw1-wan-uk-lon1.ipv4.upcloud.com	83.136.248.1	0.137ms
2	100.69.38.225	100.69.38.225	0.312ms
3	172.17.255.213	172.17.255.213	0.312ms
4	172.17.255.249	172.17.255.249	0.196ms
5	te0-3-1-4.rcr51.lon17.atlas.cogentco.com	149.11.141.9	0.520ms
6	be2971.ccr42.lon13.atlas.cogentco.com	154.54.39.81	1.195ms
7	be2490.ccr42.jfk02.atlas.cogentco.com	154.54.42.85	86.357ms
8	be2807.ccr42.dca01.atlas.cogentco.com	154.54.40.110	76.886ms
9	be2113.ccr42.atl01.atlas.cogentco.com	154.54.24.222	93.265ms
10	be2690.ccr42.iah01.atlas.cogentco.com	154.54.28.130	106.486ms
11	be2292.ccr21.sat01.atlas.cogentco.com	154.54.1.82	111.086ms
12	38.104.164.234	38.104.164.234	116.848ms
13	249.189-204-203.bestelclientes.com.mx	189.204.203.249	118.762ms
14	245.189-204-203.bestelclientes.com.mx	189.204.203.245	132.666ms
15	106.200-57-8.bestelclientes.com.mx	200.57.8.106	131.463ms
16	104.200-57-8.bestelclientes.com.mx	200.57.8.104	139.237ms
17	42.201-148-95.bestelclientes.com.mx	201.148.95.42	139.865ms
18	74.189-202-216.bestelclientes.com.mx	189.202.216.74	142.341ms
19	*	*	*

Escribe aquí para buscar

25°C

07:15 p. m.

04/11/2022

07-RSA (Proyecto 2) - PresentaciLinux Whois Command Help andTraceroute visual - Rastree y map

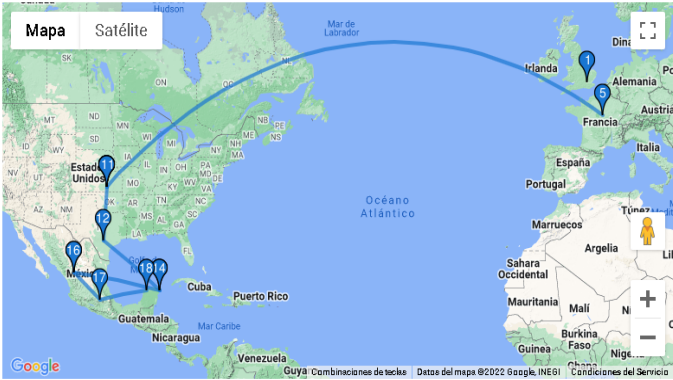
gsuite.tools/es/traceroute

G Suite.Tools

Bookmark This Page

VERIFICADOR EMAILBÚSQUEDA DE DNSTRACEROUTEUBICACIÓN IPMI IPPINGAUDITORÍA SEOVELOCIDAD DE PÁGINA

MapaSatélite



Google

traceroute to sat.gob.mx (200.33.84.233), 30 hops max

Hop	Host	IP	Time (ms)
1	dgw1-wan-uk-lon1.ipv4.upcloud.com	83.136.248.1	0.137ms
2	100.69.38.225	100.69.38.225	0.312ms
3	172.17.255.213	172.17.255.213	0.312ms
4	172.17.255.249	172.17.255.249	0.196ms
5	te0-3-1-4.rcr51.lon17.atlas.cogentco.com	149.11.141.9	0.520ms
6	be2971.ccr42.lon13.atlas.cogentco.com	154.54.39.81	1.195ms
7	be2490.ccr42.jfk02.atlas.cogentco.com	154.54.42.85	86.357ms
8	be2807.ccr42.dca01.atlas.cogentco.com	154.54.40.110	76.886ms
9	be2113.ccr42.atl01.atlas.cogentco.com	154.54.24.222	93.265ms
10	be2690.ccr42.iah01.atlas.cogentco.com	154.54.28.130	106.486ms
11	be2292.ccr21.sat01.atlas.cogentco.com	154.54.1.82	111.086ms
12	38.104.164.234	38.104.164.234	116.848ms
13	249.189-204-203.bestelclientes.com.mx	189.204.203.249	118.762ms
14	245.189-204-203.bestelclientes.com.mx	189.204.203.245	132.666ms
15	106.200-57-8.bestelclientes.com.mx	200.57.8.106	131.463ms
16	104.200-57-8.bestelclientes.com.mx	200.57.8.104	139.237ms
17	42.201-148-95.bestelclientes.com.mx	201.148.95.42	139.865ms
18	74.189-202-216.bestelclientes.com.mx	189.202.216.74	142.341ms
19	*	*	*

Escribe aquí para buscar

25°C

07:14 p. m.

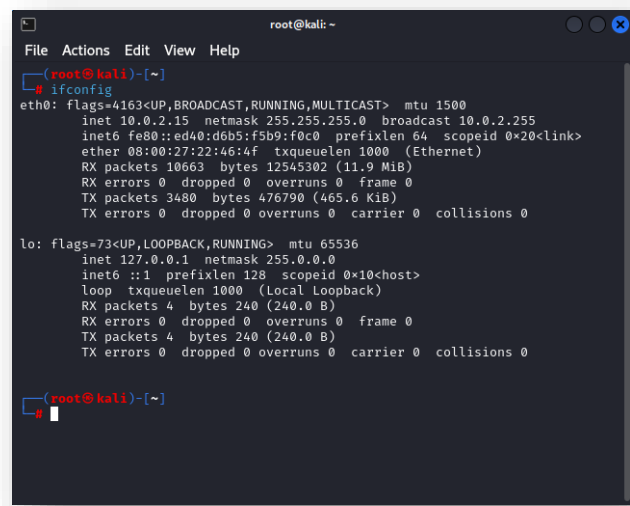
04/11/2022

NMAP

Utilizar nmap para mostrar:

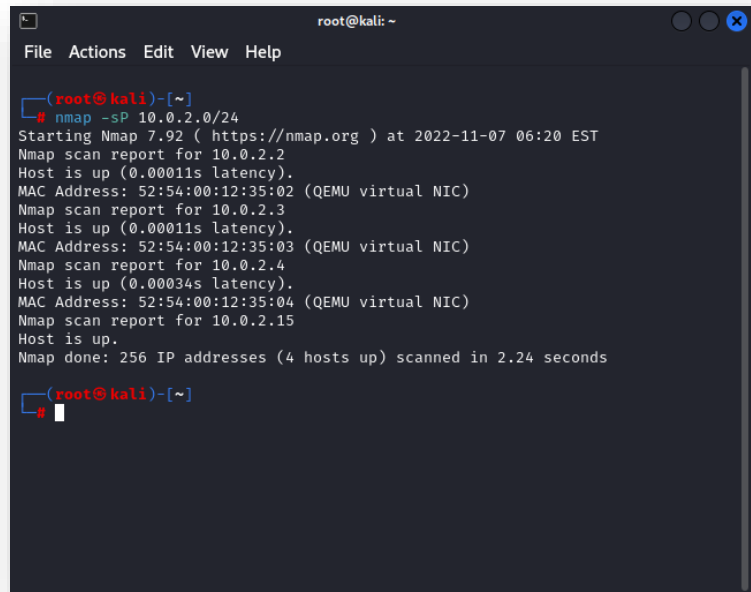
1.- Barrido de red.

Por medio de la herramienta ifconfig (incluida en el Sistema Operativo), detectaremos nuestra ip:



```
root@kali: ~  
File Actions Edit View Help  
(root@kali)-[~]  
└─$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255  
    inet6 fe80::ed40:d6b5:f5b9:f0c0 prefixlen 64 scopeid 0x20<link>  
    ether 08:00:27:22:46:4f txqueuelen 1000 (Ethernet)  
    RX packets 10663 bytes 12545302 (11.9 MiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 3480 bytes 476790 (465.6 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 4 bytes 240 (240.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 4 bytes 240 (240.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
(root@kali)-[~]  
└─$
```

Realizar un barrido de red (Network sweep) en el segmento de red que pertenecemos, para detectar equipos en la red, usamos el comando `nmap -sP 10.0.2.0/24`



```
root@kali: ~  
File Actions Edit View Help  
(root@kali)-[~]  
└─$ nmap -sP 10.0.2.0/24  
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-07 06:20 EST  
Nmap scan report for 10.0.2.2  
Host is up (0.00011s latency).  
MAC Address: 52:54:00:12:35:02 (QEMU virtual NIC)  
Nmap scan report for 10.0.2.3  
Host is up (0.00011s latency).  
MAC Address: 52:54:00:12:35:03 (QEMU virtual NIC)  
Nmap scan report for 10.0.2.4  
Host is up (0.00034s latency).  
MAC Address: 52:54:00:12:35:04 (QEMU virtual NIC)  
Nmap scan report for 10.0.2.15  
Host is up.  
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.24 seconds  
  
(root@kali)-[~]  
└─$
```

Y tomamos a 10.0.2.4 como objetivo

2.- Escaneo de puertos TCP SYN.

Hacer un escaneo de puertos TCP SYN para identificar los puertos abiertos comunes en el objetivo de evaluación. En la terminal se debe ingresar lo siguiente comando: `nmap -sS 10.0.2.4`

```
root@kali: ~
File Actions Edit View Help

(root@kali)-[~]
# nmap -sS 10.0.2.4
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-07 06:28 EST
Nmap scan report for 10.0.2.4
Host is up (0.010s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp    open  msrpc
445/tcp    open  microsoft-ds
3306/tcp    open  mysql
3389/tcp    open  ms-wbt-server
5357/tcp    open  wsddapi
MAC Address: 52:54:00:12:35:04 (QEMU virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 5.47 seconds

(root@kali)-[~]
#
```

3.- Escaneo de puertos UDP.

Para el escaneo de los puertos UDP usamos el comando `nmap -sU 10.0.2.4`

```
root@kali: ~
File Actions Edit View Help

(root@kali)-[~]
# nmap -sU 10.0.2.4
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-07 06:29 EST
Nmap scan report for 10.0.2.4
Host is up (0.0014s latency).
Not shown: 988 filtered udp ports (port-unreach)
PORT      STATE SERVICE
67/udp    open|filtered dhcpd
69/udp    open  tftp
123/udp    open|filtered ntp
137/udp    open|filtered netbios-ns
500/udp    open|filtered isakmp
1900/udp    open|filtered upnp
3389/udp    open|filtered ms-wbt-server
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 225.82 seconds

(root@kali)-[~]
#
```

4.- Determinar el Sistema Operativo del objetivo.

Se determina el el sistema operativo del equipo, este caso porque era una máquina virtual nos da como resultado QEMU

```
root@kali: ~
File Actions Edit View Help
(root@kali)-[~]
# nmap -O 10.0.2.4
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-07 06:39 EST
Nmap scan report for 10.0.2.4
Host is up (0.0075s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp    open  msrpc
445/tcp    open  microsoft-ds
3306/tcp    open  mysql
3389/tcp    open  ms-wbt-server
5357/tcp    open  wsddapi
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
Running: QEMU
OS CPE: cpe:/a:qemu:qemu
OS details: QEMU user mode network gateway
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.o
rg/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.36 seconds

(root@kali)-[~]
#
```

5.- Determinar servicios y versiones de puertos abiertos.

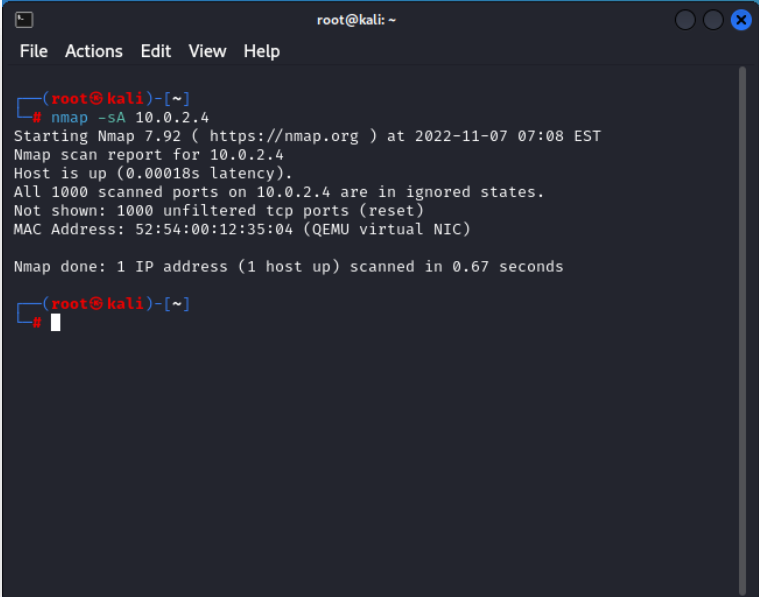
Usamos la técnica de Banner Grabbing o escaneo de versión, identificar el servicio y la versión correspondiente de los puertos abiertos. Usamos el siguiente comando `nmap -sV 10.0.2.4`

```
root@kali: ~
File Actions Edit View Help
(root@kali)-[~]
# nmap -sV 10.0.2.4
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-07 06:43 EST
Nmap scan report for 10.0.2.4
Host is up (0.0064s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
445/tcp    open  microsoft-ds?
3306/tcp    open  mysql        MySQL 8.0.29
3389/tcp    open  ms-wbt-server Microsoft Terminal Services
5357/tcp    open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
MAC Address: 52:54:00:12:35:04 (QEMU virtual NIC)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.38 seconds

(root@kali)-[~]
#
```

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

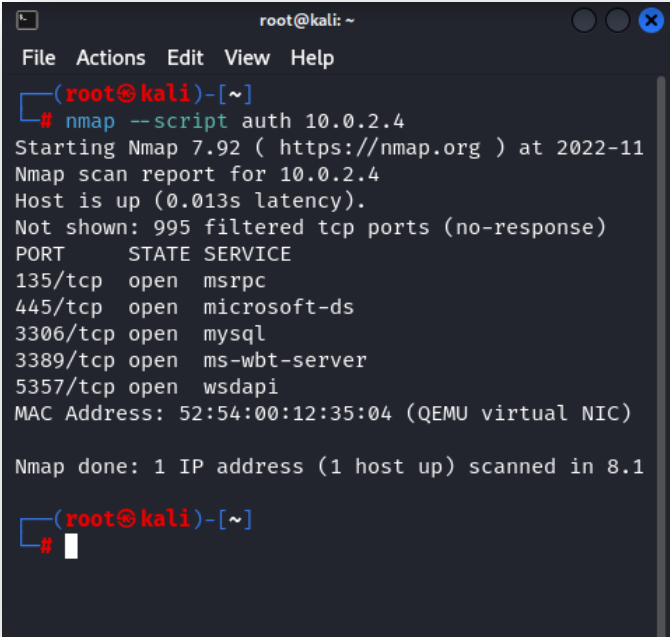


7.- Investigar las categorías NSE:

Describir brevemente cada categoría NSE de nmap, así como mostrar el uso de cada una en equipo objetivo de tu red local.

- Auth

Este tipo de script se encarga de las credenciales de autenticación o de eludir las credenciales de autenticación en el sistema de destino, estos no ocupan la “fuerza bruta”, estos últimos tienen su propia categoría. Tenemos algunos ejemplos de Auth como lo son: x11-access y ftp-anon.



- Broadcast

Este tipo realiza el descubrimiento de hosts no listados en la línea de comandos mediante el broadcasting en la red local.

Este usa el argumento de script newtargets para permitir que estos scripts añadan automáticamente los hosts que descubren a la scanning queue de Nmap.

```
root@kali: ~
File Actions Edit View Help

(root@kali)-[~]
# nmap --script broadcast 10.0.2.4
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-07 13:21 EST
Pre-scan script results:
|_eap-info: please specify an interface with -e
| broadcast-netbios-master-browser:
|_ip server domain
| broadcast-dhcp-discover:
|   Response 1 of 1:
|     Interface: eth0
|     IP Offered: 10.0.2.16
|     Subnet Mask: 255.255.255.0
|     Router: 10.0.2.2
|     Domain Name Server: 192.168.1.254
|     Domain Name: huawei.net
|     Server Identifier: 10.0.2.2
|_
Nmap scan report for 10.0.2.4
Host is up (0.0088s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp    open  msrpc
445/tcp    open  microsoft-ds
3306/tcp   open  mysql
3389/tcp   open  ms-wbt-server
5357/tcp   open  wsddapi
MAC Address: 52:54:00:12:35:04 (QEMU virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 46.15 seconds

(root@kali)-[~]
#
```

- Brute

Como su nombre lo dice, estos ocupan la fuerza bruta para obtener las credenciales de autenticación de un servidor remoto. Aquí algunos ejemplos de esto: http-brute y oracle-brute.

```
root@kali: ~
File Actions Edit View Help

(root@kali)-[~]
# nmap --script brute 10.0.2.4
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-07 13:33 EST
Nmap scan report for 10.0.2.4
Host is up (0.0073s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp    open  msrpc
445/tcp    open  microsoft-ds
3306/tcp   open  mysql
| 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
| mysql-brute:
|   Accounts: No valid accounts found
|_ Statistics: Performed 50009 guesses in 98 seconds, average tps: 507.9
3389/tcp   open  ms-wbt-server
5357/tcp   open  wsddapi
MAC Address: 52:54:00:12:35:04 (QEMU virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 103.15 seconds
```

● Default

Estos son los scripts que se ejecutan por defecto, Hay unos criterios que tiene que cumplir para poder pertenecer a esta categoría, pero no hay umbrales exactos para cada uno de estos criterios, y muchos de ellos son subjetivos. Todos estos factores se consideran en conjunto cuando se toma la decisión de tomar a un script y decir que pertenece a Default.

Los criterios a considerar son los siguientes:

1. **Velocidad:**
Debemos ser conscientes que un escaneo por defecto debe terminar rápidamente.
2. **Utilidad:**
Aquí el resultado del script influye, si podemos decir que el resultado es aprovechable y útil entonces puede ser candidato, mientras que si observamos que el resultado es todo lo contrario entonces no se deberá ejecutar por defecto.
3. **Consistencia:**
La salida de Nmap se utiliza para una gran variedad de propósitos y necesita ser legible y concisa. Un script que frecuentemente produce páginas llenas de salida no debería ser añadido a la categoría por defecto. Cuando no hay información importante que reportar, los scripts de NSE (particularmente los predeterminados) no deberían devolver nada. La comprobación de una vulnerabilidad oscura puede estar bien por defecto siempre que sólo produzca salida cuando se descubra esa vulnerabilidad.
4. **Fiabilidad:**
Muchos scripts utilizan la heurística y la coincidencia difusa de firmas para llegar a conclusiones sobre el host o servicio objetivo. Algunos ejemplos son sniffer-detect y sql-injection. Si el script se equivoca a menudo, no pertenece a la categoría por defecto donde puede confundir o engañar a los usuarios casuales. Los usuarios que especifican un script o categoría directamente son generalmente más avanzados y probablemente saben cómo funciona el script o al menos dónde encontrar su documentación.
5. **Intrusión**
Algunos scripts son muy intrusivos porque usan recursos significativos en el sistema remoto, es probable que colapsen el sistema o el servicio, o es probable que sean percibidos como un ataque por los administradores remotos. Cuanto más intrusivo es un script, menos adecuado es para la categoría por defecto. Los scripts por defecto también están casi siempre en la categoría de seguros, aunque ocasionalmente permitimos scripts intrusivos por defecto cuando sólo son ligeramente intrusivos y tienen buena puntuación en los otros factores.
6. **Privacidad**
Algunos scripts, especialmente los de la categoría externa descrita más adelante, divulgan información a terceros por su propia naturaleza. Por ejemplo, el script whois debe divulgar la dirección IP de destino a los registros whois regionales. También hemos considerado (y decidido no hacerlo) añadir scripts que comprueben las huellas digitales de las claves SSH y SSL de destino en las bases de datos de claves débiles de Internet. Cuanto más invasiva sea una secuencia de comandos en cuanto a la privacidad, menos adecuada será la inclusión de la categoría por defecto.

```
(root@kali)~# nmap --script=default 10.0.2.4
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-07 16:02 EST
Nmap scan report for 10.0.2.4
Host is up (0.0052s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp    open  msrpc
445/tcp    open  microsoft-ds
3306/tcp   open  mysql
|_ ssl-cert: Subject: commonName=MySQL_Server_8.0.29_Auto_Generated_Server_Certificate
|_ Not valid before: 2022-06-07T09:03:11
|_ Not valid after: 2022-06-04T09:03:11
|_ mysql-info:
|   Protocol: 10
|   Version: 8.0.29
|   Thread ID: 54927
|   Capabilities flags: 05535
|   Some Capabilities: SupportsLoadDataLocal, Speaks41ProtocolNew, ConnectWithDatabase, InteractiveClient, LongColumnFlag, SwitchToSSLAfterHandshake, LongPassword, SupportsTransactions, Speaks41ProtocolOld, IgnoreSpaceBeforeParenthesis, ODBCClient, Support41Auth, SupportsCompression, DontAllowDatabaseTableColumn, FoundRows, IgnoreSigpipes, SupportsMultipleStatements, SupportsAuthPlugins, SupportsMultipleResults
|   Status: Autocommit
|   Salt: ~c@a\x1D\x01B4gydTOuH1L*Vr
|_ Auth Plugin Name: caching_sha2_password
|_ ssl-date: TLS randomness does not represent time
3389/tcp   open  ms-wbt-server
|_ ssl-date: 2022-11-07T21:02:37+00:00; 0s from scanner time.
|_ rdp-ntlm-info:
|   Target_Name: EIFFELDELL
|   NetBIOS_Domain_Name: EIFFELDELL
|   NetBIOS_Computer_Name: EIFFELDELL
|   DNS_Domain_Name: EiffelDell
```

```
| Some Capabilities: SupportsLoadDataLocal, Speaks41ProtocolNew, ConnectWithDatabase, InteractiveClient, LongColumnFlag, SwitchToSSLAfterHandshake, LongPassword, SupportsTransactions, Speaks41ProtocolOld, IgnoreSpaceBeforeParenthesis, ODBCClient, Support41Auth, SupportsCompression, DontAllowDatabaseTableColumn, FoundRows, IgnoreSigpipes, SupportsMultipleStatements, SupportsAuthPlugins, SupportsMultipleResults
| Status: Autocommit
| Salt: ~c@a\x1D\x0184GydTOUh1*Vr
|_ Auth Plugin Name: caching_sha2_password
|_ ssl-date: TLS randomness does not represent time
3389/tcp open  ms-wbt-server
|_ ssl-date: 2022-11-07T21:02:37+00:00; 0s from scanner time.
| rdp-ntlm-info:
|   Target_Name: EIFFELDELL
|   NetBIOS_Domain_Name: EIFFELDELL
|   NetBIOS_Computer_Name: EIFFELDELL
|   DNS_Domain_Name: EiffelDell
|   DNS_Computer_Name: EiffelDell
|   Product_Version: 10.0.19041
|   System_Time: 2022-11-07T21:02:37+00:00
|_ ssl-cert: Subject: commonName=EiffelDell
| Not valid before: 2022-06-09T18:35:30
|_ Not valid after: 2022-12-09T18:35:30
5357/tcp open  wsdapi
MAC Address: 52:54:00:12:35:04 (QEMU virtual NIC)

Host script results:
| smb2-time:
|   date: 2022-11-07T21:02:38
|   start_date: N/A
|_ smb2-security-mode:
|   3.1.1:
|_ Message signing enabled but not required

Nmap done: 1 IP address (1 host up) scanned in 22.29 seconds

(root@kali)-[~]
```

● Discovery

Estos scripts intentan descubrir activamente más información sobre la red consultando registros públicos, dispositivos habilitados para SNMP, servicios de directorio y similares. Un ejemplo es html-title, este obtiene el título de la ruta raíz de los sitios web.

```
(root@kali)-[~]
# nmap --script-discovery 10.0.2.4
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-07 22:44 EST
Pre-scan script results:
|_ hostmap-robtext: *TEMPORARILY DISABLED* due to changes in Robtex's API. See https://www.robtext.com/api/
|_ http-robtext-shared-ns: *TEMPORARILY DISABLED* due to changes in Robtex's API. See https://www.robtext.com/api/
| targets-asn:
|   targets-asn.asn is a mandatory parameter
Nmap scan report for 10.0.2.4
Host is up (0.0061s latency).
Not shown: 995 filtered tcp ports (no-response)
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
|_ ssl-enum-ciphers:
|   TLSv1.2:
|     ciphers:
|       TLS_DHE_RSA_WITH_AES_128_CBC_SHA (dh 2048) - A
|       TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (dh 2048) - A
|       TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (dh 2048) - A
|       TLS_DHE_RSA_WITH_AES_256_CBC_SHA (dh 2048) - A
|       TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (dh 2048) - A
|       TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (dh 2048) - A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
```

```
|       TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - A
|       TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (rsa 2048) - A
|     compressors:
|       NULL
|     cipher preference: client
|   TLSv1.3:
|     ciphers:
|       TLS_AKE_WITH_AES_128_GCM_SHA256 (ecdh_x25519) - A
|       TLS_AKE_WITH_AES_256_GCM_SHA384 (ecdh_x25519) - A
|       TLS_AKE_WITH_CHACHA20_POLY1305_SHA256 (ecdh_x25519) - A
|     cipher preference: client
|     least strength: A
|_ ssl-date: TLS randomness does not represent time
| mysql-info:
|   Protocol: 10
|   Version: 8.0.29
|   Thread ID: 108099
|   Capabilities Flags: 65535
|   Some Capabilities: SwitchToSSLAfterHandshake, Support41Auth, ConnectWithDatabase, Speaks41ProtocolOld, LongPassword, SupportsTransactions, IgnoreSigpipes, SupportsLoadDataLocal, LongColumnFlag, IgnoreSpaceBeforeParenthesis, InteractiveClient, Speaks41ProtocolNew, FoundRows, SupportsCompression, ODBCClient, DontAllowDatabaseTableColumn, SupportsMultipleStatements, SupportsMultipleResults, SupportsAuthPlugins
|   Status: Autocommit
|   Salt: f\x10\x01\x16Xs\x00BNC/\x02
|   #hu1f
|   %
|_ Auth Plugin Name: caching_sha2_password
|_ ssl-cert: Subject: commonName=MySQL_Server_8.0.29_Auto_Generated_Server_Certificate
| Not valid before: 2022-06-07T09:03:11
|_ Not valid after: 2032-06-04T09:03:11
|_ banner: J\x00\x00\x00A8.0.29\x00D\xA6\x01\x00*nMRF\x0E>h\x00\xff ...
3389/tcp open  ms-wbt-server
|_ rdp-enum-encryption:
|   Security Layer
```

```
File Actions Edit View Help
| rdp-enum-encryption:
| Security layer
| CredSSP (NLA): SUCCESS
| CredSSP with Early User Auth: SUCCESS
|_ RDSTLS: SUCCESS
| ssl-cert: Subject: commonName=EiffelDell
| Not valid before: 2022-06-09T18:35:30
|_ Not valid after: 2022-12-09T18:35:30
| ssl-enum-ciphers:
| TLSv1.0:
|   ciphers:
|     TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|     TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|     TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
|     TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp384r1) - A
|     TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (ecdh_x25519) - A
|   compressors:
|     NULL
|   cipher preference: server
|   warnings:
|     64-bit block cipher 3DES vulnerable to SWEET32 attack
| TLSv1.1:
|   ciphers:
|     TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|     TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|     TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
|     TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp384r1) - A
|     TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (ecdh_x25519) - A
|   compressors:
|     NULL
|   cipher preference: server
|   warnings:
|     64-bit block cipher 3DES vulnerable to SWEET32 attack
| TLSv1.2:
|   ciphers:
```

```
|     64-bit block cipher 3DES vulnerable to SWEET32 attack
| TLSv1.2:
|   ciphers:
|     TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - A
|     TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - A
|     TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048) - A
|     TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048) - A
|     TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|     TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|     TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
|     TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp384r1) - A
|     TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (ecdh_x25519) - A
|     TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (dh 2048) - A
|     TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (dh 2048) - A
|     TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp384r1) - A
|     TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (ecdh_x25519) - A
|     TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp384r1) - A
|     TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (ecdh_x25519) - A
|   compressors:
|     NULL
|   cipher preference: server
|   warnings:
|     64-bit block cipher 3DES vulnerable to SWEET32 attack
|   least strength: C
|_ ssl-date: 2022-11-08T03:44:55+00:00; +1s from scanner time.
| rdp-ntlm-info:
| Target Name: EIFFELDELL
| NetBIOS_Domain_Name: EIFFELDELL
| NetBIOS_Computer_Name: EIFFELDELL
| DNS_Domain_Name: EiffelDell
| DNS_Computer_Name: EiffelDell
| Product_Versions: 10.0.19041
| System_Time: 2022-11-08T03:44:55+00:00
5357/tcp open  wsdaapi
MAC Address: 52:54:00:12:35:04 (QEMU virtual NIC)
```

```
Host script results:
| smb-protocols:
|   dialects:
|     2.0.2
|     2.1
|     3.0
|     3.0.2
|     3.1.1
|_ smb2-capabilities:
|   2.0.2:
|     Distributed File System
|   2.1:
|     Distributed File System
|     Leasing
|     Multi-credit operations
|   3.0:
|     Distributed File System
|     Leasing
|     Multi-credit operations
|   3.0.2:
|     Distributed File System
|     Leasing
|     Multi-credit operations
|   3.1.1:
|     Distributed File System
|     Leasing
|     Multi-credit operations
|_ fcrdns: FAIL (No PTR record)
|_ dns-brute: Can't guess domain of "10.0.2.4"; use dns-brute.domain script argument.
| smb2-time:
|   date: 2022-11-08T03:45:14
|   start_date: N/A
|_ path-mtu: PMTU = 1500
|_ ipidseq: ERROR: Script execution failed (use -d to debug)
```

```
| date: 2022-11-08T03:45:14
|_ start_date: N/A
|_ path-mtu: PMTU = 1500
|_ ipidseq: ERROR: Script execution failed (use -d to debug)
|_ sniffer-detect: Likely in promiscuous mode (tests: "11111111")
| qscan:
| PORT  FAMILY  MEAN (us)  STDDEV  LOSS (%)
| 135   0         3707.80    2018.88  0.0%
| 445   0         8360.60    8538.87  0.0%
| 3306  0         3468.60    1245.04  0.0%
| 3389  0         7591.70    7354.91  0.0%
|_ 5357  1         8667.10    8659.37  0.0%
| smb2-security-mode:
|   3.1.1:
|     Message signing enabled but not required
| smb-mbenum:
|_ ERROR: Failed to connect to browser service: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR
|_ msrpc-enum: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR
Nmap done: 1 IP address (1 host up) scanned in 76.13 seconds
```

- Dos

Pueden causar una denegación de servicio. A veces esto se hace para probar la vulnerabilidad a un método de denegación de servicio, pero más comúnmente es un efecto secundario no deseado pero necesario de las pruebas de una vulnerabilidad tradicional. Estas pruebas a veces bloquean los servicios vulnerables.

```
(root@kali)-[~]
# nmap --script broadcast --script-args=newtargets 10.0.2.4
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-07 15:52 EST
Pre-scan script results:
|_eap-info: please specify an interface with -e
| broadcast-netbios-master-browser:
|_ip server domain
| broadcast-dhcp-discover:
|   Response 1 of 1:
|     Interface: eth0
|     IP Offered: 10.0.2.16
|     Subnet Mask: 255.255.255.0
|     Router: 10.0.2.2
|     Domain Name Server: 192.168.1.254
|     Domain Name: huawei.net
|_   Server Identifier: 10.0.2.2
Nmap scan report for 10.0.2.4
Host is up (0.0079s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
3389/tcp  open  ms-wbt-server
5357/tcp  open  wsddapi
MAC Address: 52:54:00:12:35:04 (QEMU virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 45.62 seconds

(root@kali)-[~]
#
```

- Exploit

Estos scripts tienen como objetivo explotar activamente alguna vulnerabilidad.

```
(root@kali)-[~]
# nmap --script=exploit 10.0.2.4
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-07 23:09 EST
Nmap scan report for 10.0.2.4
Host is up (0.0079s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
3389/tcp  open  ms-wbt-server
5357/tcp  open  wsddapi
MAC Address: 52:54:00:12:35:04 (QEMU virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.31 seconds
```

- External

Los scripts de esta categoría pueden enviar datos a una base de datos de terceros u otro recurso de red. Un ejemplo de esto es whois-ip, que establece una conexión con los servidores whois para conocer la dirección del objetivo. Siempre existe la posibilidad de que los operadores de la base de datos de terceros registren cualquier cosa que les envíe, que en muchos casos incluirá su dirección IP y la dirección del objetivo. La mayoría de los scripts involucran tráfico estrictamente entre la computadora de escaneo y el cliente; cualquiera que no se coloca en esta categoría.

```
(root@kali)-[~]
# nmap --script external 10.0.2.4
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-07 15:25 EST
Pre-scan script results:
|_http-robtext-shared-ns: *TEMPORARILY DISABLED* due to changes in Robtex's API. See https://www.robtext.com/api/
|_hostmap-robtext: *TEMPORARILY DISABLED* due to changes in Robtex's API. See https://www.robtext.com/api/
|_targets-asn:
|   targets-asn.asn is a mandatory parameter
Nmap scan report for 10.0.2.4
Host is up (0.0079s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
3389/tcp  open  ms-wbt-server
5357/tcp  open  wsddapi
MAC Address: 52:54:00:12:35:04 (QEMU virtual NIC)

Host script results:
| dns-blacklist:
|   SPAM
|   12.apews.org - FAIL
|_   list.quorum.to - FAIL

Nmap done: 1 IP address (1 host up) scanned in 16.14 seconds
```

- Fuzzer

Esta categoría contiene scripts que están diseñados para enviar al software del servidor campos inesperados o aleatorios en cada paquete. Aunque esta técnica puede ser útil para encontrar bugs y vulnerabilidades no descubiertas en el software, es un proceso lento y que consume mucho ancho de banda. Un ejemplo de un script de esta categoría es dns-fuzz, que bombardea un servidor DNS con peticiones de dominio ligeramente defectuosas hasta que el servidor se bloquea o transcurre un límite de tiempo especificado por el usuario.

```
(root@kali)-[~]
# nmap --script fuzzer 10.0.2.4
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-08 03:02 EST
Nmap scan report for 10.0.2.4
Host is up (0.0083s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
5357/tcp  open  wsapi
MAC Address: 52:54:00:12:35:04 (QEMU virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 6.26 seconds

(root@kali)-[~]
#
```

- Intrusive

Se trata de scripts que no pueden clasificarse en la categoría de seguros porque los riesgos son demasiado altos como para que se bloquee el sistema de destino, se utilicen recursos significativos en el host de destino (como el ancho de banda o el tiempo de CPU), o sean percibidos como maliciosos por los administradores del sistema de destino. Algunos ejemplos son http-open-proxy (que intenta utilizar el servidor de destino como un proxy HTTP) y snmp-brute (que intenta adivinar la cadena de comunidad SNMP de un dispositivo enviando valores comunes como public, private y cisco). A menos que un script esté en la categoría de versión especial, debería ser categorizado como seguro o intrusivo.

- Malware

Estos scripts prueban si la plataforma de destino está infectada por malware o puertas traseras. Los ejemplos incluyen smtp-strangeport, que busca servidores SMTP que se ejecutan en números de puerto inusuales, y auth-spoof, que detecta demonios de suplantación de identidad que brindan una respuesta falsa incluso antes de recibir una consulta. Ambos comportamientos se asocian comúnmente con infecciones de malware.

```
(root@kali)-[~]
# nmap --script malware 10.0.2.4
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-07 15:14 EST
Nmap scan report for 10.0.2.4
Host is up (0.0074s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
3389/tcp  open  ms-wbt-server
5357/tcp  open  wsapi
MAC Address: 52:54:00:12:35:04 (QEMU virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 6.62 seconds
```


- Safe

Los scripts que no han sido diseñados para colapsar servicios, utilizar grandes cantidades de ancho de banda de red u otros recursos, o explotar agujeros de seguridad se clasifican como seguros. Es menos probable que ofendan a los administradores remotos, aunque (como con todas las demás funciones de Nmap) no podemos garantizar que no causen nunca reacciones adversas. La mayoría de ellas realizan un descubrimiento general de la red. Algunos ejemplos son ssh-hostkey (recupera una clave de host SSH) y html-title (toma el título de una página web). Los scripts en la categoría de versiones no están categorizados por seguridad, pero cualquier otro script que no esté en safe debe ser colocado en intrusive

```
root@kali: ~#
nmap --script safe 10.0.2.4
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-07 15:18 EST
Pre-scan script results:
|_ eap-info: please specify an interface with -e
|_ http-robtex-shared-ns: *TEMPORARILY DISABLED* due to changes in Robtex's API. See https://www.robtex.com/api/
|_ targets-asn:
|_   targets-asn.asn is a mandatory parameter
|_ hostmap-robtex: *TEMPORARILY DISABLED* due to changes in Robtex's API. See https://www.robtex.com/api/
|_ broadcast-dhcp-discover:
|   Response 1 of 1:
|     Interface: eth0
|     IP Offered: 10.0.2.16
|     Subnet Mask: 255.255.255.0
|     Router: 10.0.2.2
|     Domain Name Server: 192.168.1.254
|     Domain Name: huawei.net
|     Server Identifier: 10.0.2.2
|_ broadcast-netbios-master-browser:
|_ ip_server_domain
Nmap scan report for 10.0.2.4
Host is up (0.0074s latency).
Not shown: 995 filtered tcp ports (no-response)
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
|_ ssl-date: TLS randomness does not represent time
|_ mysql-info:
|   Protocol: 10
|   Version: 8.0.29
|   Thread ID: 54855
|   Capabilities flags: 65535
|   Some Capabilities: LongPassword, Support41Auth, IgnoreSpaceBeforeParenthesis, SupportsLoadDataLocal, LongColumnFlag, Speaks41ProtocolOld, Speaks41ProtocolNew, Do
```

```
|   Capabilities flags: 65535
|   Some Capabilities: LongPassword, Support41Auth, IgnoreSpaceBeforeParenthesis, SupportsLoadDataLocal, LongColumnFlag, Speaks41ProtocolOld, Speaks41ProtocolNew, Do
ntAllowDatabaseTableColumn, ConnectWithDatabase, IgnoreSignipes, SupportsTransactions, FoundRows, SwitchToSSLAfterHandshake, ODBCClient, SupportsCompression, Interac
tiveClient, SupportsMultipleStatements, SupportsAuthPlugins, SupportsMultipleResults
|   Status: Autocommit
|   Salt: .<z\x0B\x18\ 8*\x0E\x9L\x7Fj_n\x11"
|   Auth Plugin Name: caching_sha2_password
|_ ssl-cert: Subject: commonName=MySQL_Server_8.0.29_Auto_Generated_Server_Certificate
|_ Not valid before: 2022-06-07T09:03:11
|_ Not valid after: 2022-06-04T09:03:11
|_ banner: J\x00\x00\x00\x0A08.0.29*\x00H\xD6*\x00*\x00*\x13]offF7j3*\x00*\xFF\ ...
3389/tcp   open  ms-wbt-server
|_ rdp-enum-encryption:
|   Security layer
|   CredSSP (NLA): SUCCESS
|   CredSSP with Early User Auth: SUCCESS
|   RDSTLS: SUCCESS
|_ ssl-cert: Subject: commonName=EiffelDell
|_ Not valid before: 2022-06-09T18:35:30
|_ Not valid after: 2022-12-09T18:35:30
|_ rdp-ntlm-info:
|   Target_Name: EIFFELDELL
|   NetBIOS_Domain_Name: EIFFELDELL
|   NetBIOS_Computer_Name: EIFFELDELL
|   DNS_Domain_Name: EiffelDell
|   DNS_Computer_Name: EiffelDell
|   Product_Version: 10.0.19041
|   System_Time: 2022-11-07T20:19:29+00:00
|_ ssl-date: 2022-11-07T20:19:28+00:00; 0s from scanner time.
5357/tcp   open  wsddapi
MAC Address: 52:54:00:12:35:04 (QEMU virtual NIC)

Host script results:
|_ dns-blacklist:
|   SPAM
```

```
5357/tcp   open  wsddapi
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
|_ path-mtu: PMTU = 1500
|_ port-states:
|   tcp:
|     opens: 135,445,3306,3389,5357
|     filtered: 1,2,4,6,7,9,13,17,19,26,30,32,33,37,42-43,49,53,70,79-85,88-90,99-100,106,109-111,113,119,125,139,143-144,146,161,163,179,199,211-212,222,254-256,259
,264,280,301,306,311,340,366,389,406-407,416-417,425,427,443-444,458,464-465,481,497,500,512-515,524,541,543-545,548,554-555,563,587,593,616-617,625,631,636,646,648,
666-668,683,687,691,700,705,711,714,720,722,726,749,765,777,783,787,800-801,808,843,873,880,888,898,900-903,911-912,981,987,990,992-993,995,999-1002,1007,1009-1011,1
021-1100,1102,1104-1108,1110-1114,1117,1119,1121-1124,1126,1130-1132,1137-1138,1141,1145,1147-1149,1151-1152,1154,1163-1166,1169,1174-1175,1183,1185-1187,1192,1198-1
199,1201,1213,1216-1218,1233-1234,1236,1244,1247-1248,1259,1271-1272,1277,1287,1296,1300-1301,1309-1311,1322,1328,1334,1352,1417,1433-1434,1443,1455,1461,1494,1500-1
501,1503,1521,1524,1533,1556,1580,1583,1594,1600,1641,1658,1666,1687-1688,1700,1717-1721,1723,1755,1761,1782-1783,1801,1805,1812,1839-1840,1862-1864,1875,1900,1914,1
935,1947,1971-1972,1974,1984,1998-2010,2013,2020-2022,2030,2033-2035,2038,2040-2043,2045-2049,2065,2068,2099-2100,2103,2105-2107,2111,2119,2121,2126,2135,2144,2180-2
181,2170,2179,2190-2191,2195,2200,2222,2251,2260,2268,2301,2323,2366,2381-2383,2393-2394,2399,2401,2492,2500,2522,2525,2557,2601-2602,2604-2605,2607-2608,2630,2701-2
702,2710,2717-2718,2725,2800,2809,2811,2869,2875,2989-2910,2920,2967-2968,2998,3000-3001,3003,3005-3007,3011,3013,3017,3030-3031,3052,3071,3077,3128,3168,3211,3221,3
260-3261,3268-3269,3283,3300-3301,3322-3325,3333,3351,3367,3369-3372,3390,3404,3476,3493,3517,3527,3546,3551,3580,3659,3689-3690,3703,3737,3766,3784,3800-3801,3809,3
814,3826-3828,3851,3869,3871,3878,3880,3889,3905,3914,3918,3920,3945,3971,3986,3995,3998,4000-4006,4045,4111,4125-4126,4129,4224,4242,4279,4321,4343,4443-4446,4449,4
550,4567,4662,4848,4899-4900,4998,5000-5004,5009,5030,5033,5050-5051,5054,5060-5061,5080,5087,5100-5102,5120,5190,5200,5214,5221-5222,5225-5226,5269,5280,5298,5405,5
414,5431-5432,5440,5500,5510,5544,5550,5555,5560,5566,5631,5633,5666,5678-5679,5718,5730,5800-5802,5810-5811,5815,5822,5825,5850,5859,5862,5877,5900-5904,5906-5907,5
910-5911,5915,5922,5925,5950,5952,5959-5963,5987-5989,5998-6007,6009,6025,6059,6100-6101,6106,6112,6123,6129,6156,6346,6389,6502,6510,6543,6547,6565-6567,6580,6646,6
666-6669,6689,6692,6699,6779,6788-6789,6792,6839,6881,6901,6969,7000-7002,7004,7007,7019,7025,7070,7100,7103,7106,7200-7201,7402,7435,7443,7496,7512,7625,7627,7676,7
741,7777-7778,7800,7911,7920-7921,7937-7938,7999-8002,8007-8011,8021-8022,8031,8042,8045,8080-8090,8093,8099-8100,8100-8181,8192-8194,8200,8222,8254,8290-8292,8300,8
333,8383,8400,8402,8443,8500,8600,8649,8651-8652,8654,8701,8800,8873,8888,8899,8994,9000-9003,9009-9011,9040,9050,9071,9088-9081,9090-9091,9099-9103,9110-9111,9200,9
207,9220,9290,9415,9418,9435,9500,9502-9503,9535,9575,9593-9595,9618,9666,9876-9878,9898,9900,9917,9929,9943-9944,9968,9998-10004,10009-10010,10012,10024-10025,10082
,10180,10215,10243,10566,10616-10617,10621,10626,10628-10629,10778,11110-11111,11967,12000,12174,12265,12345,13456,13722,13782-13783,14000,14238,14441-14442,15000,15
002-15004,15660,15742,16000-16001,16012,16016,16018,16080,16113,16992-16993,17877,17988,18040,18101,18988,19101,19283,19315,19350,19780,19801,19842,20000,20005,20031
,20221-20222,20828,21571,22939,23502,24444,24800,25734-25735,26214,27000,27352-27353,27355-27356,27715,28201,30000,30718,30951,31038,31337,32768-32785,33354,33899,34
571-34573,35500,38292,40193,40911,41511,42510,44176,44442-44443,44501,45100,48080,49152-49161,49163,49165,49167,49175-49176,49400,49999-50003,50006,50300,50389,50500
,50636,50800,51103,51493,52673,52822,52848,52869,54045,54328,55055-55056,55555,55600,56737-56738,57294,57797,58080,60020,60443,61532,61900,62078,63331,64623,64680,65
```

```
,20221-20222,20828,21571,22939,23502,24444,24800,25734-25735,26214,27000,27352-27353,27355-27356,27715,28201,30000,30718,30951,31038,31337,32768-32785,33354,33899,34
571-34573,35500,38292,40193,40911,41511,42510,44176,44442-44443,44501,45100,48080,49152-49161,49163,49165,49167,49175-49176,49400,49999-50003,50006,50300,50389,50500
,50636,50800,51103,51493,52673,52822,52848,52869,54045,54328,55055-55056,55555,55600,56737-56738,57294,57797,58080,60020,60443,61532,61900,62078,63331,64623,64680,65
000,65129,65389
| smb-mbenum:
| _ ERROR: Failed to connect to browser service: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR
| _ fcrdns: FAIL (No PTR record)
| _ msrpc-enum: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR
| _ unusual-port:
| _ WARNING: this script depends on Nmap's service/version detection (-sV)
| _ smb-protocols:
| _ dialects:
| _ 2.0.2
| _ 2.1
| _ 3.0
| _ 3.0.2
| _ 3.1.1
| _ qscan:
| _ PORT FAMILY MEAN (us) STDDEV LOSS (%)
| _ 135 0 2496.10 905.83 0.0%
| _ 445 0 3450.40 3134.90 0.0%
| _ 3386 0 2232.20 869.36 0.0%
| _ 3389 0 2750.00 988.02 0.0%
| _ 5357 0 3863.20 3536.89 0.0%
| _ ipidseq: ERROR: Script execution failed (use -d to debug)
| _ smb2-capabilities:
| _ 2.0.2:
| _ Distributed File System
| _ 2.1:
| _ Distributed File System
| _ Leasing
| _ Multi-credit operations
| _ 3.0:
| _ Distributed File System
| _ Leasing
```

```
File Actions Edit View Help
| Distributed File System
| 2.1:
| Distributed File System
| Leasing
| Multi-credit operations
| 3.0:
| Distributed File System
| Leasing
| Multi-credit operations
| 3.0.2:
| Distributed File System
| Leasing
| Multi-credit operations
| 3.1.1:
| Distributed File System
| Leasing
| Multi-credit operations
| _ smb2-security-mode:
| _ 3.1.1:
| _ Message signing enabled but not required
| _ smb2-times:
| _ date: 2022-11-07T20:19:30
| _ start_date: N/A

Post-scan script results:
| reverse-index:
| 135/tcp: 10.0.2.4
| 445/tcp: 10.0.2.4
| 3386/tcp: 10.0.2.4
| 3389/tcp: 10.0.2.4
| 5357/tcp: 10.0.2.4
|
Nmap done: 1 IP address (1 host up) scanned in 87.89 seconds

(root@kali)-[~]
# ssssss
```

● Version

Los scripts de esta categoría especial son una extensión de la función de detección de versiones y no pueden seleccionarse explícitamente. Se seleccionan para ejecutarse sólo si se solicita la detección de versiones (-sV). Su salida no puede distinguirse de la salida de la detección de versiones y no producen resultados de scripts de servicio o de host. Algunos ejemplos son skypev2-version, pptp-version y iax2-version.

```
(root@kali)-[~]
# nmap -sV 10.0.2.4
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-08 03:18 EST
Nmap scan report for 10.0.2.4
Host is up (0.0079s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE          VERSION
135/tcp   open  msrpc            Microsoft Windows RPC
445/tcp   open  microsoft-ds?
3389/tcp  open  ms-wbt-server    Microsoft Terminal Services
5357/tcp  open  http             Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
MAC Address: 52:54:00:12:35:04 (QEMU virtual NIC)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.37 seconds

(root@kali)-[~]
#
```


- Vuln

Estos scripts comprueban vulnerabilidades específicas conocidas y generalmente sólo informan de los resultados si se encuentran. Algunos ejemplos son realvnc-auth-bypass y afp-path-vuln.

```
root@kali: ~
File Actions Edit View Help

(root@kali)-[~]
# nmap --script vuln 10.0.2.4
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-07 12:56 EST
Nmap scan report for 10.0.2.4
Host is up (0.0082s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp    open  msrpc
445/tcp    open  microsoft-ds
3306/tcp   open  mysql
3389/tcp   open  ms-wbt-server
5357/tcp   open  wsdapi
MAC Address: 52:54:00:12:35:04 (QEMU virtual NIC)

Host script results:
|_samba-vuln-cve-2012-1182: Could not negotiate a
connection:SMB: Failed to receive bytes: ERROR
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: Could not negotiate a connect
ion:SMB: Failed to receive bytes: ERROR

Nmap done: 1 IP address (1 host up) scanned in 48.
72 seconds

(root@kali)-[~]
#
```

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).

Un exploit es cualquier ataque que aprovecha las vulnerabilidades de las aplicaciones, las redes, los sistemas operativos o el hardware. Por lo general, los exploits toman la forma de un programa de software o una secuencia de código previsto para hacerse con el control de los ordenadores o robar datos de red.

No se hayo ninguna vulnerabilidad

```
(root@kali)-[~]
# nmap -sV --script=vuln 10.0.2.4
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-08 03:54 EST
Stats: 0:01:01 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.38% done; ETC: 03:55 (0:00:00 remaining)
Stats: 0:01:23 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.38% done; ETC: 03:55 (0:00:00 remaining)
Nmap scan report for 10.0.2.4
Host is up (0.0074s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
445/tcp    open  microsoft-ds?
3389/tcp   open  ms-wbt-server Microsoft Terminal Services
5357/tcp   open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
55555/tcp  open  tcpwrapped
MAC Address: 52:54:00:12:35:04 (QEMU virtual NIC)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR
|_samba-vuln-cve-2012-1182: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 158.74 seconds

(root@kali)-[~]
#
```