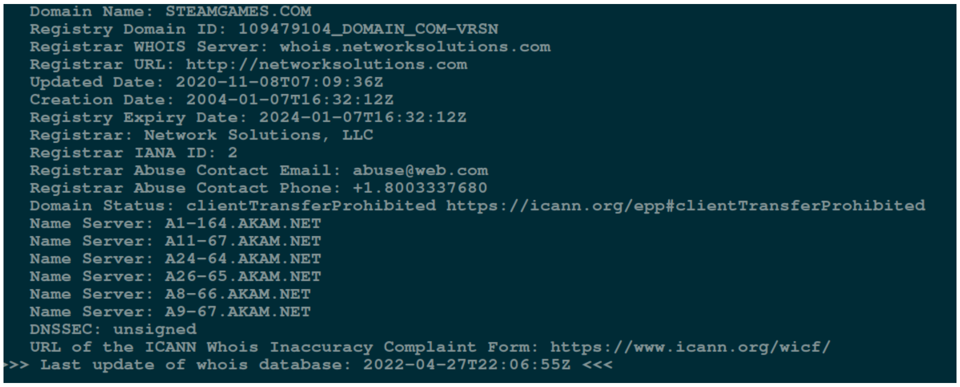
Criptografía y Seguridad 2022-2
Proyecto 02

Diego Dozal Magnani.
No de cuenta: 316032708
José Eduardo González Jasso.
No de cuenta: 316093837

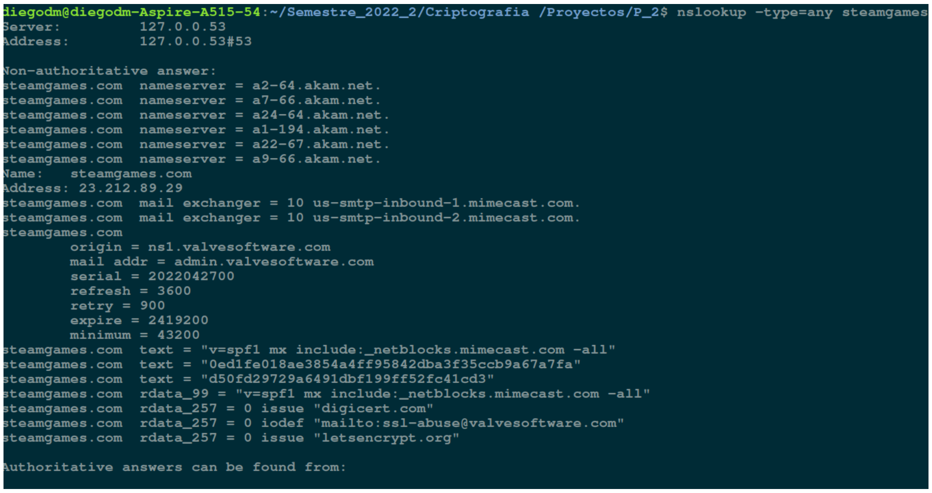
Mayo 2022

1. `whois`



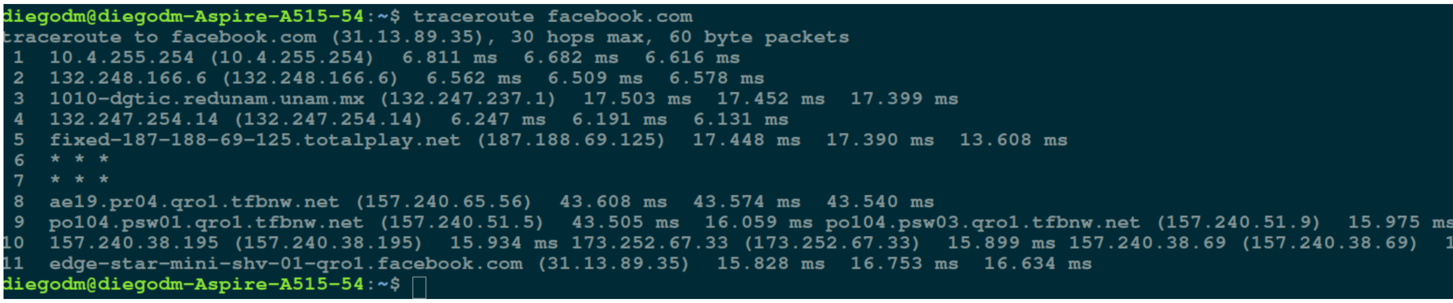
```
   Domain Name: STEAMGAMES.COM
   Registry Domain ID: 109479104_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.networksolutions.com
   Registrar URL: http://networksolutions.com
   Updated Date: 2020-11-08T07:09:36Z
   Creation Date: 2004-01-07T16:32:12Z
   Registry Expiry Date: 2024-01-07T16:32:12Z
   Registrar: Network Solutions, LLC
   Registrar IANA ID: 2
   Registrar Abuse Contact Email: abuse@web.com
   Registrar Abuse Contact Phone: +1.8003337680
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Name Server: A1-164.AKAM.NET
   Name Server: A11-67.AKAM.NET
   Name Server: A24-64.AKAM.NET
   Name Server: A26-65.AKAM.NET
   Name Server: A8-66.AKAM.NET
   Name Server: A9-67.AKAM.NET
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2022-04-27T22:06:55Z <<<
```

2. `nslookup`

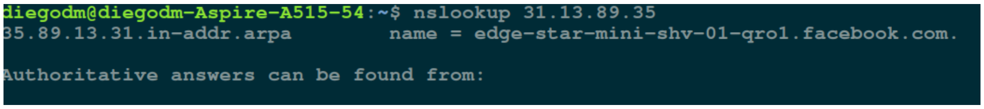


```
diegodm@diegodm-Aspire-A515-54:~/Semestre_2022_2/Criptografia /Proyectos/P_2$ nslookup -type=any steamgames
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
steamgames.com  nameserver = a2-64.akam.net.
steamgames.com  nameserver = a7-66.akam.net.
steamgames.com  nameserver = a24-64.akam.net.
steamgames.com  nameserver = a1-194.akam.net.
steamgames.com  nameserver = a22-67.akam.net.
steamgames.com  nameserver = a9-66.akam.net.
Name:   steamgames.com
Address: 23.212.89.29
steamgames.com  mail exchanger = 10 us-smtp-inbound-1.mimecast.com.
steamgames.com  mail exchanger = 10 us-smtp-inbound-2.mimecast.com.
steamgames.com
        origin = ns1.valvesoftware.com
        mail addr = admin.valvesoftware.com
        serial = 2022042700
        refresh = 3600
        retry = 900
        expire = 2419200
        minimum = 43200
steamgames.com  text = "v=spf1 mx include:_netblocks.mimecast.com -all"
steamgames.com  text = "0ed1fe018ae3854a4ff95842dba3f35ccb9a67a7fa"
steamgames.com  text = "d50fd29729a6491dbf199ff52fc41cd3"
steamgames.com  rdata_99 = "v=spf1 mx include:_netblocks.mimecast.com -all"
steamgames.com  rdata_257 = 0 issue "digicert.com"
steamgames.com  rdata_257 = 0 iodef "mailto:ssl-abuse@valvesoftware.com"
steamgames.com  rdata_257 = 0 issue "letsencrypt.org"

Authoritative answers can be found from:
```

3. traceroute



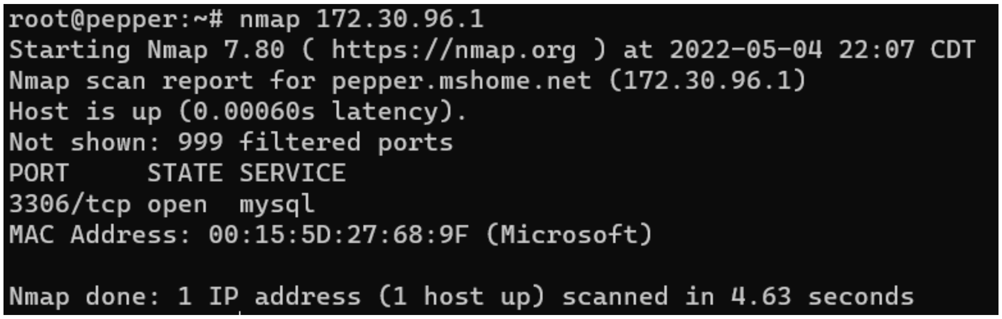
```
diegodm@diegodm-Aspire-A515-54:~$ traceroute facebook.com
traceroute to facebook.com (31.13.89.35), 30 hops max, 60 byte packets
 1  10.4.255.254 (10.4.255.254)  6.811 ms  6.682 ms  6.616 ms
 2  132.248.166.6 (132.248.166.6)  6.562 ms  6.509 ms  6.578 ms
 3  1010-dgtic.redunam.unam.mx (132.247.237.1)  17.503 ms  17.452 ms  17.399 ms
 4  132.247.254.14 (132.247.254.14)  6.247 ms  6.191 ms  6.131 ms
 5  fixed-187-188-69-125.totalplay.net (187.188.69.125)  17.448 ms  17.390 ms  13.608 ms
 6  * * *
 7  * * *
 8  ae19.pr04.qro1.tfbnw.net (157.240.65.56)  43.608 ms  43.574 ms  43.540 ms
 9  po104.psw01.qro1.tfbnw.net (157.240.51.5)  43.505 ms  16.059 ms po104.psw03.qro1.tfbnw.net (157.240.51.9)  15.975 ms
10  157.240.38.195 (157.240.38.195)  15.934 ms 173.252.67.33 (173.252.67.33)  15.899 ms 157.240.38.69 (157.240.38.69)  1
11  edge-star-mini-shv-01-qro1.facebook.com (31.13.89.35)  15.828 ms  16.753 ms  16.634 ms
diegodm@diegodm-Aspire-A515-54:~$ 
```



```
diegodm@diegodm-Aspire-A515-54:~$ nslookup 31.13.89.35
35.89.13.31.in-addr.arpa        name = edge-star-mini-shv-01-qro1.facebook.com.

Authoritative answers can be found from:
```

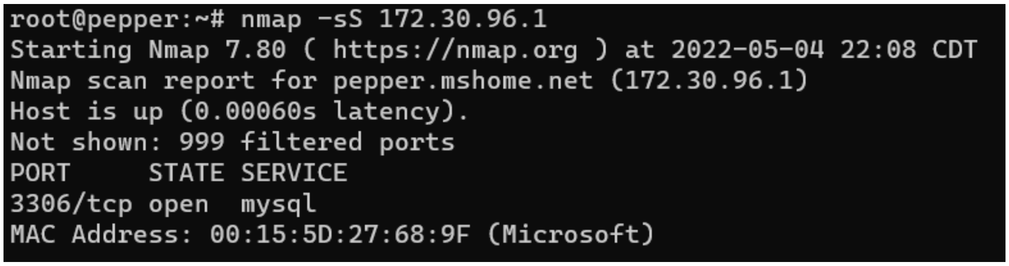
4. nmap

1 .



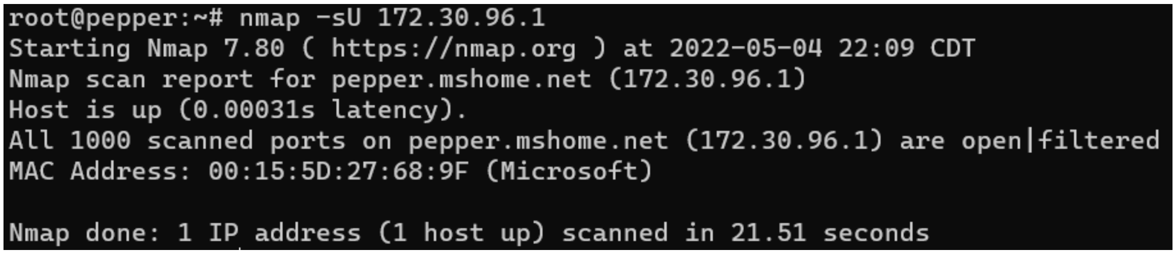
```
root@pepper:~# nmap 172.30.96.1
Starting Nmap 7.80 ( https://nmap.org ) at 2022-05-04 22:07 CDT
Nmap scan report for pepper.mshome.net (172.30.96.1)
Host is up (0.00060s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE
3306/tcp open  mysql
MAC Address: 00:15:5D:27:68:9F (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 4.63 seconds
```

2 .



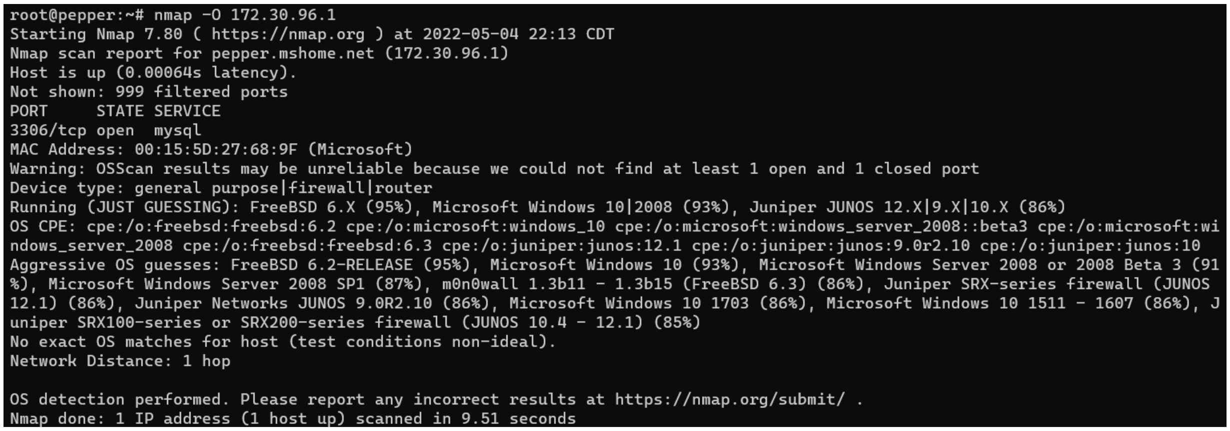
```
root@pepper:~# nmap -sS 172.30.96.1
Starting Nmap 7.80 ( https://nmap.org ) at 2022-05-04 22:08 CDT
Nmap scan report for pepper.mshome.net (172.30.96.1)
Host is up (0.00060s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE
3306/tcp open  mysql
MAC Address: 00:15:5D:27:68:9F (Microsoft)
```

3 .



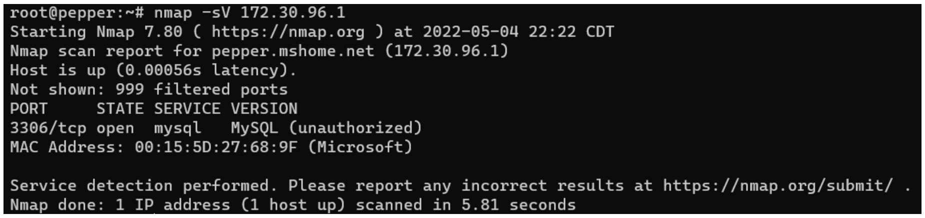
```
root@pepper:~# nmap -sU 172.30.96.1
Starting Nmap 7.80 ( https://nmap.org ) at 2022-05-04 22:09 CDT
Nmap scan report for pepper.mshome.net (172.30.96.1)
Host is up (0.00031s latency).
All 1000 scanned ports on pepper.mshome.net (172.30.96.1) are open|filtered
MAC Address: 00:15:5D:27:68:9F (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 21.51 seconds
```

4 .



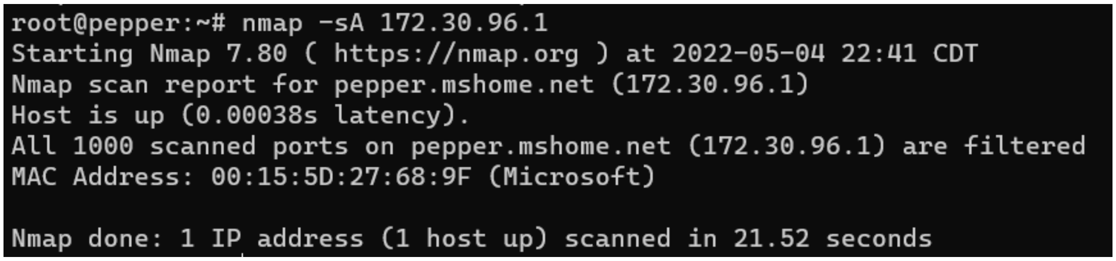
```
root@pepper:~# nmap -O 172.30.96.1
Starting Nmap 7.80 ( https://nmap.org ) at 2022-05-04 22:13 CDT
Nmap scan report for pepper.mshome.net (172.30.96.1)
Host is up (0.00064s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE
3306/tcp open  mysql
MAC Address: 00:15:5D:27:68:9F (Microsoft)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|firewall|router
Running (JUST GUESSING): FreeBSD 6.X (95%), Microsoft Windows 10|2008 (93%), Juniper JUNOS 12.X|9.X|10.X (86%)
OS CPE: cpe:/o:freebsd:freebsd:6.2 cpe:/o:microsoft:windows_10 cpe:/o:microsoft:windows_server_2008::beta3 cpe:/o:microsoft:wi
ndows_server_2008 cpe:/o:freebsd:freebsd:6.3 cpe:/o:juniper:junos:12.1 cpe:/o:juniper:junos:9.0r2.10 cpe:/o:juniper:junos:10
Aggressive OS guesses: FreeBSD 6.2-RELEASE (95%), Microsoft Windows 10 (93%), Microsoft Windows Server 2008 or 2008 Beta 3 (91
%), Microsoft Windows Server 2008 SP1 (87%), m0n0wall 1.3b11 - 1.3b15 (FreeBSD 6.3) (86%), Juniper SRX-series firewall (JUNOS
12.1) (86%), Juniper Networks JUNOS 9.0R2.10 (86%), Microsoft Windows 10 1703 (86%), Microsoft Windows 10 1511 - 1607 (86%), J
uniper SRX100-series or SRX200-series firewall (JUNOS 10.4 - 12.1) (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.51 seconds
```

5 .



```
root@pepper:~# nmap -sV 172.30.96.1
Starting Nmap 7.80 ( https://nmap.org ) at 2022-05-04 22:22 CDT
Nmap scan report for pepper.mshome.net (172.30.96.1)
Host is up (0.00056s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE VERSION
3306/tcp open  mysql   MySQL (unauthorized)
MAC Address: 00:15:5D:27:68:9F (Microsoft)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 5.81 seconds
```

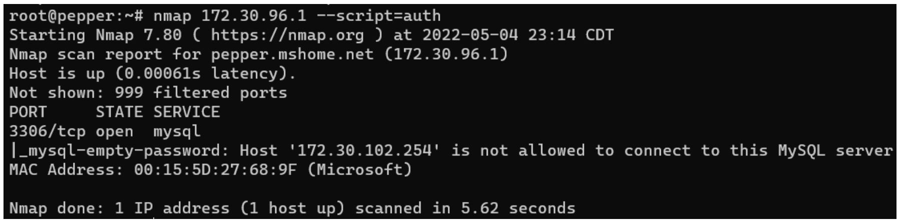
6 .



```
root@pepper:~# nmap -sA 172.30.96.1
Starting Nmap 7.80 ( https://nmap.org ) at 2022-05-04 22:41 CDT
Nmap scan report for pepper.mshome.net (172.30.96.1)
Host is up (0.00038s latency).
All 1000 scanned ports on pepper.mshome.net (172.30.96.1) are filtered
MAC Address: 00:15:5D:27:68:9F (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 21.52 seconds
```

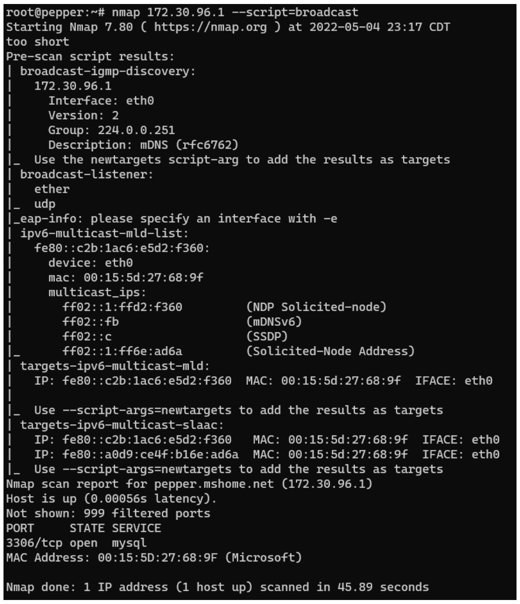
7 .

- **auth**. Estos scripts se ocupan de las credenciales de autenticación en el sistema de destino como: x11-access, ftp-anon y oracle-enum-users.



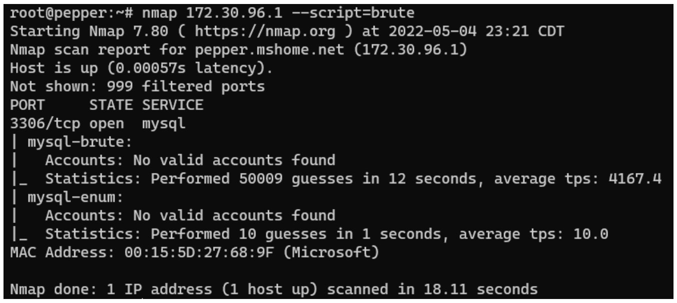
```
root@pepper:~# nmap 172.30.96.1 --script=auth
Starting Nmap 7.80 ( https://nmap.org ) at 2022-05-04 23:14 CDT
Nmap scan report for pepper.mshome.net (172.30.96.1)
Host is up (0.00061s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE
3306/tcp open  mysql
|_mysql-empty-password: Host '172.30.102.254' is not allowed to connect to this MySQL server
MAC Address: 00:15:5D:27:68:9F (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 5.62 seconds
```

- **broadcast**. Los scripts de esta categoría normalmente detectan hosts que no aparecen en la línea de comandos mediante la difusión en la red local.



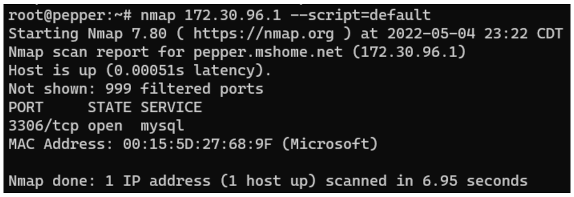
```
root@pepper:~# nmap 172.30.96.1 --script=broadcast
Starting Nmap 7.80 ( https://nmap.org ) at 2022-05-04 23:17 CDT
too short
Pre-scan script results:
| broadcast-igmp-discovery:
|   172.30.96.1
|     Interface: eth0
|     Version: 2
|     Group: 224.0.0.251
|     Description: mDNS (rfc6762)
|_  Use the newtargets script-arg to add the results as targets
| broadcast-listener:
|   ether
|_  udp
|_eap-info: please specify an interface with -e
| ipv6-multicast-mld-list:
|   fe80::c2b:1ac6:e5d2:f360:
|     device: eth0
|     mac: 00:15:5d:27:68:9f
|     multicast_ips:
|       ff02::1:ffd2:f360         (NDP Solicited-node)
|       ff02::fb                  (mDNSv6)
|       ff02::c                   (SSDP)
|_      ff02::1:ff6e:ad6a         (Solicited-Node Address)
| targets-ipv6-multicast-mld:
|   IP: fe80::c2b:1ac6:e5d2:f360  MAC: 00:15:5d:27:68:9f  IFACE: eth0
|
|_  Use --script-args=newtargets to add the results as targets
| targets-ipv6-multicast-slaac:
|   IP: fe80::c2b:1ac6:e5d2:f360   MAC: 00:15:5d:27:68:9f  IFACE: eth0
|   IP: fe80::a0d9:ce4f:b16e:ad6a  MAC: 00:15:5d:27:68:9f  IFACE: eth0
|_  Use --script-args=newtargets to add the results as targets
Nmap scan report for pepper.mshome.net (172.30.96.1)
Host is up (0.00056s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE
3306/tcp open  mysql
MAC Address: 00:15:5D:27:68:9F (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 45.89 seconds
```

- **brute**. Estos scripts se utilizan en ataques de fuerza bruta para adivinar las credenciales de autenticación de un servidor remoto.



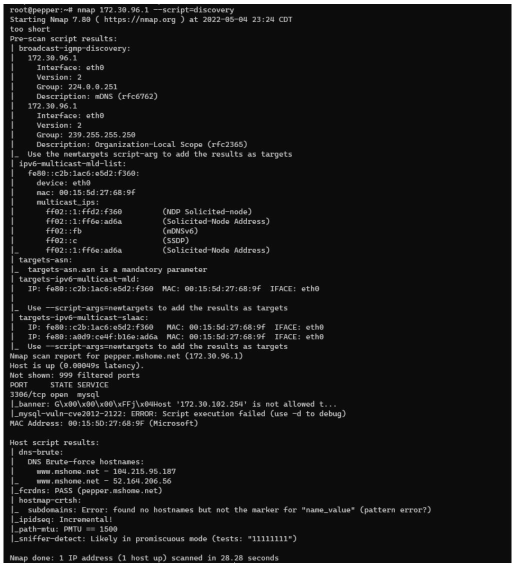
```
root@pepper:~# nmap 172.30.96.1 --script=brute
Starting Nmap 7.80 ( https://nmap.org ) at 2022-05-04 23:21 CDT
Nmap scan report for pepper.mshome.net (172.30.96.1)
Host is up (0.00057s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE
3306/tcp open  mysql
| mysql-brute:
|   Accounts: No valid accounts found
|_  Statistics: Performed 50009 guesses in 12 seconds, average tps: 4167.4
| mysql-enum:
|   Accounts: No valid accounts found
|_  Statistics: Performed 10 guesses in 1 seconds, average tps: 10.0
MAC Address: 00:15:5D:27:68:9F (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 18.11 seconds
```

- **default**. Son el conjunto predeterminado de scripts y se ejecutan cuando se usan las opciones -sC o -A en lugar de enumerar los scripts con la bandera –script. Para ser ejecutados se toman en cuenta diversos factores como: velocidad, utilidad, verbosidad, fiabilidad, intrusividad y privacidad.



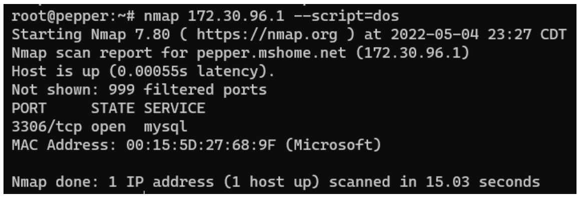
```
root@pepper:~# nmap 172.30.96.1 --script=default
Starting Nmap 7.80 ( https://nmap.org ) at 2022-05-04 23:22 CDT
Nmap scan report for pepper.mshome.net (172.30.96.1)
Host is up (0.00051s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE
3306/tcp open  mysql
MAC Address: 00:15:5D:27:68:9F (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 6.95 seconds
```

- discovery. Estos scripts intentan descubrir activamente más sobre la red consultando registros públicos, dispositivos habilitados para SNMP, servicios de directorio y similares.



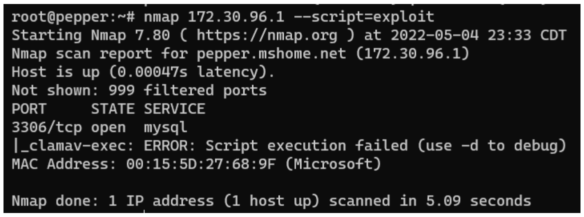
```
root@pepper:~# nmap 172.30.96.1 --script=discovery
Starting Nmap 7.80 ( https://nmap.org ) at 2022-05-04 23:24 CDT
too short
Pre-scan script results:
| broadcast-igmp-discovery:
|   172.30.96.1
|     Interface: eth0
|     Version: 2
|     Group: 224.0.0.251
|     Description: mDNS (rfc6762)
|   172.30.96.1
|     Interface: eth0
|     Version: 2
|     Group: 239.255.255.250
|     Description: Organization-Local Scope (rfc2365)
|_  Use the newtargets script-arg to add the results as targets
| ipv6-multicast-mld-list:
|   fe80::c2b:1ac6:e5d2:f360:
|     device: eth0
|     mac: 00:15:5d:27:68:9f
|     multicast_ips:
|       ff02::1:ffd2:f360         (NDP Solicited-node)
|       ff02::1:ff6e:ad6a         (Solicited-Node Address)
|       ff02::fb                  (mDNSv6)
|       ff02::c                   (SSDP)
|_      ff02::1:ff6e:ad6a         (Solicited-Node Address)
| targets-asn:
|_  targets-asn.asn is a mandatory parameter
| targets-ipv6-multicast-mld:
|   IP: fe80::c2b:1ac6:e5d2:f360  MAC: 00:15:5d:27:68:9f  IFACE: eth0
|
|_  Use --script-args=newtargets to add the results as targets
| targets-ipv6-multicast-slaac:
|   IP: fe80::c2b:1ac6:e5d2:f360   MAC: 00:15:5d:27:68:9f  IFACE: eth0
|   IP: fe80::a0d9:ce4f:b16e:ad6a  MAC: 00:15:5d:27:68:9f  IFACE: eth0
|_  Use --script-args=newtargets to add the results as targets
Nmap scan report for pepper.mshome.net (172.30.96.1)
Host is up (0.00049s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE
3306/tcp open  mysql
|_banner: G\x00\x00\x00\xFFj\x04Host '172.30.102.254' is not allowed t...
|_mysql-vuln-cve2012-2122: ERROR: Script execution failed (use -d to debug)
MAC Address: 00:15:5D:27:68:9F (Microsoft)

Host script results:
| dns-brute:
|   DNS Brute-force hostnames:
|     www.mshome.net - 104.215.95.187
|_    www.mshome.net - 52.164.206.56
|_fcrdns: PASS (pepper.mshome.net)
| hostmap-crtsh:
|_  subdomains: Error: found no hostnames but not the marker for "name_value" (pattern error?)
|_ipidseq: Incremental!
|_path-mtu: PMTU == 1500
|_sniffer-detect: Likely in promiscuous mode (tests: "11111111")

Nmap done: 1 IP address (1 host up) scanned in 28.28 seconds
```

- **dos**. Los scripts de esta categoría pueden provocar 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 por necesidad de probar una vulnerabilidad tradicional. Estas pruebas a veces bloquean servicios vulnerables.



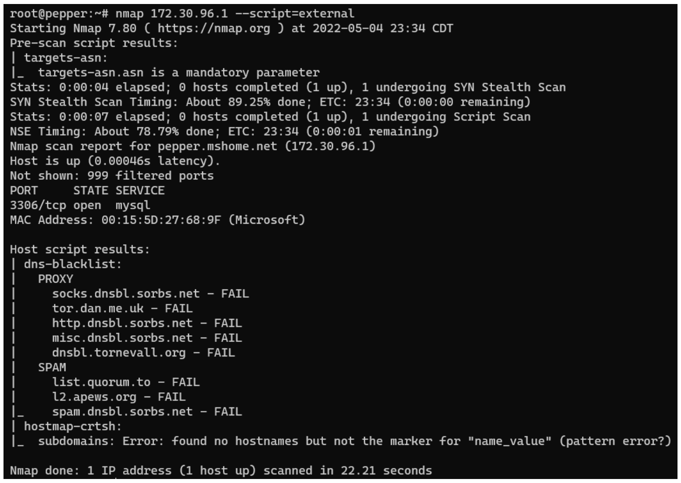
```
root@pepper:~# nmap 172.30.96.1 --script=dos
Starting Nmap 7.80 ( https://nmap.org ) at 2022-05-04 23:27 CDT
Nmap scan report for pepper.mshome.net (172.30.96.1)
Host is up (0.00055s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE
3306/tcp open  mysql
MAC Address: 00:15:5D:27:68:9F (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 15.03 seconds
```

- **exploit**. Estos scripts tienen como objetivo explotar activamente alguna vulnerabilidad.



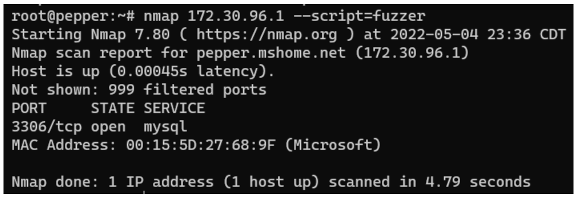
```
root@pepper:~# nmap 172.30.96.1 --script=exploit
Starting Nmap 7.80 ( https://nmap.org ) at 2022-05-04 23:33 CDT
Nmap scan report for pepper.mshome.net (172.30.96.1)
Host is up (0.00047s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE
3306/tcp open  mysql
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
MAC Address: 00:15:5D:27:68:9F (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 5.09 seconds
```

- **external**. Los scripts de esta categoría pueden enviar datos a una base de datos de terceros u otro recurso de red. 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.



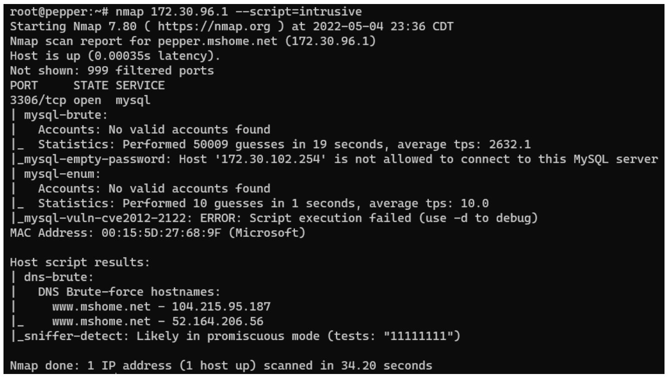
```
root@pepper:~# nmap 172.30.96.1 --script=external
Starting Nmap 7.80 ( https://nmap.org ) at 2022-05-04 23:34 CDT
Pre-scan script results:
| targets-asn:
|_  targets-asn.asn is a mandatory parameter
Stats: 0:00:04 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 89.25% done; ETC: 23:34 (0:00:00 remaining)
Stats: 0:00:07 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 78.79% done; ETC: 23:34 (0:00:01 remaining)
Nmap scan report for pepper.mshome.net (172.30.96.1)
Host is up (0.00046s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE
3306/tcp open  mysql
MAC Address: 00:15:5D:27:68:9F (Microsoft)

Host script results:
| dns-blacklist:
|   PROXY
|     socks.dnsbl.sorbs.net - FAIL
|     tor.dan.me.uk - FAIL
|     http.dnsbl.sorbs.net - FAIL
|     misc.dnsbl.sorbs.net - FAIL
|     dnsbl.tornevall.org - FAIL
|   SPAM
|     list.quorum.to - FAIL
|     l2.apews.org - FAIL
|_    spam.dnsbl.sorbs.net - FAIL
| hostmap-crtsh:
|_  subdomains: Error: found no hostnames but not the marker for "name_value" (pattern error?)

Nmap done: 1 IP address (1 host up) scanned in 22.21 seconds
```

- **fuzzer**. Esta categoría contiene scripts que están diseñados para enviar al software del servidor campos aleatorios o inesperados en cada paquete. Si bien esta técnica puede ser útil para encontrar errores y vulnerabilidades no descubiertos en el software, es un proceso lento y requiere mucho ancho de banda.



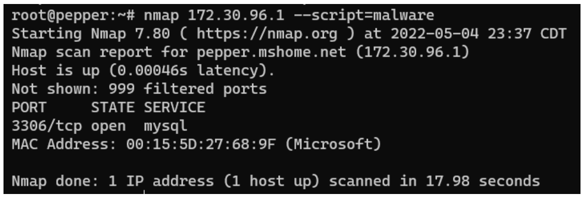
```
root@pepper:~# nmap 172.30.96.1 --script=fuzzer
Starting Nmap 7.80 ( https://nmap.org ) at 2022-05-04 23:36 CDT
Nmap scan report for pepper.mshome.net (172.30.96.1)
Host is up (0.00045s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE
3306/tcp open  mysql
MAC Address: 00:15:5D:27:68:9F (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 4.79 seconds
```

- **intrusive** . Estos son scripts que no se pueden clasificar en la categoría segura porque los riesgos son demasiado altos de que bloqueen el sistema de destino, consuman recursos significativos en el host de destino (como el ancho de banda o el tiempo de CPU) o que el sistema los perciba como maliciosos. administradores del sistema de destino.



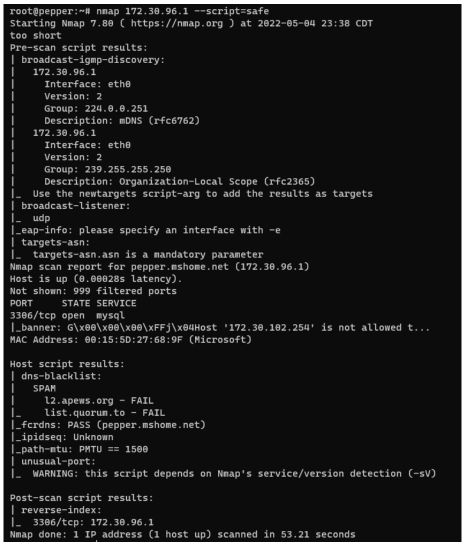
```
root@pepper:~# nmap 172.30.96.1 --script=intrusive
Starting Nmap 7.80 ( https://nmap.org ) at 2022-05-04 23:36 CDT
Nmap scan report for pepper.mshome.net (172.30.96.1)
Host is up (0.00035s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE
3306/tcp open  mysql
| mysql-brute:
|   Accounts: No valid accounts found
|_  Statistics: Performed 50009 guesses in 19 seconds, average tps: 2632.1
|_mysql-empty-password: Host '172.30.102.254' is not allowed to connect to this MySQL server
| mysql-enum:
|   Accounts: No valid accounts found
|_  Statistics: Performed 10 guesses in 1 seconds, average tps: 10.0
|_mysql-vuln-cve2012-2122: ERROR: Script execution failed (use -d to debug)
MAC Address: 00:15:5D:27:68:9F (Microsoft)

Host script results:
| dns-brute:
|   DNS Brute-force hostnames:
|     www.mshome.net - 104.215.95.187
|_    www.mshome.net - 52.164.206.56
|_sniffer-detect: Likely in promiscuous mode (tests: "11111111")

Nmap done: 1 IP address (1 host up) scanned in 34.20 seconds
```

- **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.



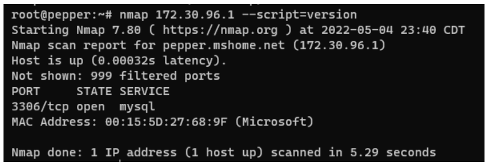
```
root@pepper:~# nmap 172.30.96.1 --script=malware
Starting Nmap 7.80 ( https://nmap.org ) at 2022-05-04 23:37 CDT
Nmap scan report for pepper.mshome.net (172.30.96.1)
Host is up (0.00046s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE
3306/tcp open  mysql
MAC Address: 00:15:5D:27:68:9F (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 17.98 seconds
```

- **safe** . Los 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 se clasifican como seguros. Es menos probable que ofendan a los administradores remotos, aunque (al igual que con todas las demás funciones de Nmap) no podemos garantizar que nunca causen reacciones adversas. La mayoría de estos realizan un descubrimiento de red general.



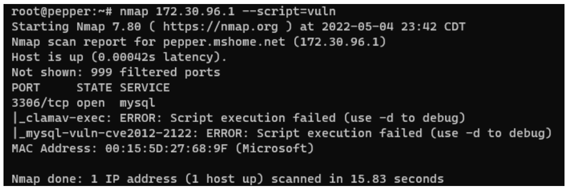
```
root@pepper:~# nmap 172.30.96.1 --script=safe
Starting Nmap 7.80 ( https://nmap.org ) at 2022-05-04 23:38 CDT
too short
Pre-scan script results:
| broadcast-igmp-discovery:
|   172.30.96.1
|     Interface: eth0
|     Version: 2
|     Group: 224.0.0.251
|     Description: mDNS (rfc6762)
|   172.30.96.1
|     Interface: eth0
|     Version: 2
|     Group: 239.255.255.250
|     Description: Organization-Local Scope (rfc2365)
|_  Use the newtargets script-arg to add the results as targets
| broadcast-listener:
|_  udp
|_eap-info: please specify an interface with -e
| targets-asn:
|_  targets-asn.asn is a mandatory parameter
Nmap scan report for pepper.mshome.net (172.30.96.1)
Host is up (0.00028s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE
3306/tcp open  mysql
|_banner: G\x00\x00\x00\xFFj\x04Host '172.30.102.254' is not allowed t...
MAC Address: 00:15:5D:27:68:9F (Microsoft)

Host script results:
| dns-blacklist:
|   SPAM
|     l2.apews.org - FAIL
|_    list.quorum.to - FAIL
|_fcrdns: PASS (pepper.mshome.net)
|_ipidseq: Unknown
|_path-mtu: PMTU == 1500
| unusual-port:
|_  WARNING: this script depends on Nmap's service/version detection (-sV)

Post-scan script results:
| reverse-index:
|_  3306/tcp: 172.30.96.1
Nmap done: 1 IP address (1 host up) scanned in 53.21 seconds
```

- **version** . Los scripts de esta categoría especial son una extensión de la función de detección de versiones y no se pueden seleccionar de forma explícita. Se seleccionan para ejecutarse solo si se solicitó la detección de versión (-sV). Su salida no se puede distinguir de la salida de detección de versión y no producen resultados de script de host o servicio.



```
root@pepper:~# nmap 172.30.96.1 --script=version
Starting Nmap 7.80 ( https://nmap.org ) at 2022-05-04 23:40 CDT
Nmap scan report for pepper.mshome.net (172.30.96.1)
Host is up (0.00032s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE
3306/tcp open  mysql
MAC Address: 00:15:5D:27:68:9F (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 5.29 seconds
```

- **vuln** . Estos scripts verifican vulnerabilidades específicas conocidas y, en general, solo informan los resultados si se encuentran.



```
root@pepper:~# nmap 172.30.96.1 --script=vuln
Starting Nmap 7.80 ( https://nmap.org ) at 2022-05-04 23:42 CDT
Nmap scan report for pepper.mshome.net (172.30.96.1)
Host is up (0.00042s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE
3306/tcp open  mysql
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_mysql-vuln-cve2012-2122: ERROR: Script execution failed (use -d to debug)
MAC Address: 00:15:5D:27:68:9F (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 15.83 seconds
```

8 . `Exploit` (del inglés exploit, ”explotar” o ‘aprovechar’) es un fragmento de software, fragmento de datos o secuencia de comandos y/o acciones, utilizada con el fin de aprovechar una vulnerabilidad de seguridad de un sistema de información para conseguir un comportamiento no deseado del mismo.
En la captura del punto 5 podemos observar que el único puerto disponible y que además está abierto es el 3306, por el cual accedemos al servicio de `mysql`. Un posible `Exploit` podría ser habilitar la conexción remota con el ordenador y controlar `mysql`.