

Seguridad en Sistemas Operativos

PEC 2

Securizar servidores, análisis de puertos

Pablo Riutort Grande

12 de abril de 2020

1. Linux Server

Para este apartado se ha instalado y configurado software que utiliza algunos puertos de la máquina virtual:

- nginx: Para los puertos 22, 80 y 443
- CUPS: Utiliza el puerto 631
- FTP: Utiliza el puerto 21

```
1 apt update -y; apt install -y nginx openssh-server cups vsftpd ftp
```

Generamos un certificado autofirmado y configuramos nginx para que lo utilice [1], de esta forma podemos servir mediante nginx conexiones a través del puerto 443 (SSL).

a) nmap:

```
1 root@debian:~# nmap -sV localhost
2 Starting Nmap 7.70 ( https://nmap.org ) at 2020-04-05 22:23 CEST
3 Nmap scan report for localhost (127.0.0.1)
4 Host is up (0.000012s latency).
5 Other addresses for localhost (not scanned): ::1
6 Not shown: 995 closed ports
7 PORT      STATE SERVICE VERSION
8 21/tcp    open  ftp      vsftpd 3.0.3
9 22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
10 80/tcp    open  http     nginx 1.14.2
11 443/tcp   open  ssl/http nginx 1.14.2
12 631/tcp   open  ipp      CUPS 2.2
13 Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
14
15 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
16 Nmap done: 1 IP address (1 host up) scanned in 14.17 seconds
```

netstat:

```
1 root@debian:~# netstat --listening
2 Active Internet connections (only servers)
3 Proto Recv-Q Send-Q Local Address           Foreign Address         State
4 tcp        0      0 0.0.0.0:80             0.0.0.0:*               LISTEN
5 tcp        0      0 0.0.0.0:22             0.0.0.0:*               LISTEN
6 tcp        0      0 0.0.0.0:21             0.0.0.0:*               LISTEN
7 tcp        0      0 0.0.0.0:443            0.0.0.0:*               LISTEN
8 tcp6       0      0 :::80                 :::*                    LISTEN
9 tcp6       0      0 :::22                 :::*                    LISTEN
10 tcp6       0      0 :::21                 :::*                    LISTEN
11 tcp6       0      0 :::443                :::*                    LISTEN
12 tcp6       0      0 :::https              :::*                    LISTEN
13 udp        0      0 0.0.0.0:21             0.0.0.0:*               LISTEN
14 udp        0      0 0.0.0.0:mdns           0.0.0.0:*               LISTEN
15 udp        0      0 0.0.0.0:46806          0.0.0.0:*               LISTEN
16 udp        0      0 0.0.0.0:bootpc         0.0.0.0:*               LISTEN
17 udp6       0      0 :::mdns               :::*                    LISTEN
18 udp6       0      0 :::47332              :::*                    LISTEN
19 raw6       0      0 ::::ip6-icmp          :::*                    LISTEN
20 Active UNIX domain sockets (only servers)
21 Proto RefCnt Flags      Type       State      I-Node   Path
```

22	unix	2	[ACC]	STREAM	LISTENING	19784	/tmp/.ICE-unix/721
23	unix	2	[ACC]	STREAM	LISTENING	10499	/run/systemd/journal/stdout
24	unix	2	[ACC]	STREAM	LISTENING	17770	/tmp/.X11-unix/X0
25	unix	2	[ACC]	STREAM	LISTENING	19628	/tmp/ssh-kx6ERuyT0jOS/agent.680
26	unix	2	[ACC]	STREAM	LISTENING	17769	@/tmp/.X11-unix/X0
27	unix	2	[ACC]	SEQPACKET	LISTENING	10786	/run/udev/control
28	unix	2	[ACC]	STREAM	LISTENING	19783	@/tmp/.ICE-unix/721
29	unix	2	[ACC]	STREAM	LISTENING	17485	/run/NetworkManager/private-dhcp
30	unix	2	[ACC]	STREAM	LISTENING	14216	/var/run/dbus/system_bus_socket
31	unix	2	[ACC]	STREAM	LISTENING	14221	/run/cups/cups.sock
32	unix	2	[ACC]	STREAM	LISTENING	14225	/run/avahi-daemon/socket
33	unix	2	[ACC]	STREAM	LISTENING	19727	@/tmp/dbus-cLiJoZjMM2
34	unix	2	[ACC]	STREAM	LISTENING	19429	/run/user/0/systemd/private
35	unix	2	[ACC]	STREAM	LISTENING	19436	/run/user/0/gnupg/S.gpg-agent.browser
36	unix	2	[ACC]	STREAM	LISTENING	19439	/run/user/0/gnupg/S.dirmngr
37	unix	2	[ACC]	STREAM	LISTENING	10479	/run/systemd/private
38	unix	2	[ACC]	STREAM	LISTENING	19441	/run/user/0/gnupg/S.gpg-agent.ssh
39	unix	2	[ACC]	STREAM	LISTENING	19443	/run/user/0/gnupg/S.gpg-agent.extra
40	unix	2	[ACC]	STREAM	LISTENING	19445	/run/user/0/gnupg/S.gpg-agent
41	unix	2	[ACC]	STREAM	LISTENING	19447	/run/user/0/bus
42	unix	2	[ACC]	STREAM	LISTENING	10488	/run/systemd/fsck.progress

b) Los servicios que utilizan puertos que no son 22, 80 y 443 son ftp (21) y CUPS (631). Para deshabilitar estos procesos ejecutamos los comandos `systemctl stop` y `disable`:

```

1 root@debian:~# systemctl stop vsftpd
2 root@debian:~# systemctl disable vsftpd
3 Synchronizing state of vsftpd.service with SysV service script with /lib/systemd/systemd-sysv-
  install.
4 Executing: /lib/systemd/systemd-sysv-install disable vsftpd
5 Removed /etc/systemd/system/multi-user.target.wants/vsftpd.service.
6 root@debian:~# systemctl stop cups
7 root@debian:~# systemctl disable cups
8 Synchronizing state of cups.service with SysV service script with /lib/systemd/systemd-sysv-
  install.
9 Executing: /lib/systemd/systemd-sysv-install disable cups
10 Removed /etc/systemd/system/printer.target.wants/cups.service.
11 Removed /etc/systemd/system/multi-user.target.wants/cups.path.
12 Removed /etc/systemd/system/sockets.target.wants/cups.socket.
13 root@debian:~# systemctl stop cups-browsed
14 root@debian:~# systemctl disable cups-browsed
15 Synchronizing state of cups-browsed.service with SysV service script with /lib/systemd/systemd-
  sysv-install.
16 Executing: /lib/systemd/systemd-sysv-install disable cups-browsed
17 Removed /etc/systemd/system/multi-user.target.wants/cups-browsed.service.

```

En el caso de que quisiéramos actualizar los enlaces a los scripts de init para prevenir la ejecución al cambiar el nivel de ejecución podemos ejecutar [2]:

```

1 root@debian:~# update-rc.d vsftpd remove
2 root@debian:~# update-rc.d cups remove

```

Después de parar y deshabilitar los servicios relativos a ftp y CUPS reiniciamos. Al ejecutar nuevamente el comando `nmap` sobre `localhost` vemos que los únicos servicios en funcionamiento son los relativos a los puertos 22, 80 y 443.

```

1 root@debian:~# nmap -sV localhost
2 Starting Nmap 7.70 ( https://nmap.org ) at 2020-04-07 01:00 CEST
3 Nmap scan report for localhost (127.0.0.1)
4 Host is up (0.000021s latency).
5 Other addresses for localhost (not scanned): ::1
6 Not shown: 997 closed ports
7 PORT      STATE SERVICE VERSION
8 22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
9 80/tcp    open  http     nginx 1.14.2
10 443/tcp   open  ssl/http nginx 1.14.2
11 Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
12
13 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
14 Nmap done: 1 IP address (1 host up) scanned in 14.17 seconds

```

c) Primera prueba de ping desde host:

```

1 ~ $ ping 192.168.1.172
2 PING 192.168.1.172 (192.168.1.172) 56(84) bytes of data.
3 64 bytes from 192.168.1.172: icmp_seq=1 ttl=64 time=0.947 ms
4 64 bytes from 192.168.1.172: icmp_seq=2 ttl=64 time=0.559 ms
5 64 bytes from 192.168.1.172: icmp_seq=3 ttl=64 time=0.580 ms
6 ^C
7 --- 192.168.1.172 ping statistics ---
8 3 packets transmitted, 3 received, 0% packet loss, time 2015ms
9 rtt min/avg/max/mdev = 0.559/0.695/0.947/0.179 ms

```

Las máquinas pueden verse y hay respuesta con ping. Ahora deshabilitamos el ping de la máquina virtual con los comandos: [3]

```
1 echo 1 > /proc/sys/net/ipv4/icmp_echo_ignore_all
2 echo "net.ipv4.icmp_echo_ignore_all = 1" >> /etc/sysctl.conf
3 sysctl -p
```

Reiniciamos la máquina, realizamos nuevamente el ping y vemos que no recibimos ningún paquete de vuelta:

```
1 ~ $ ping 192.168.1.172
2 PING 192.168.1.172 (192.168.1.172) 56(84) bytes of data.
3 ^C
4 --- 192.168.1.172 ping statistics ---
5 3 packets transmitted, 0 received, 100% packet loss, time 2051ms
```

d) A continuación se muestra el proceso por el cual logramos una Shell desde el Grub: [4]

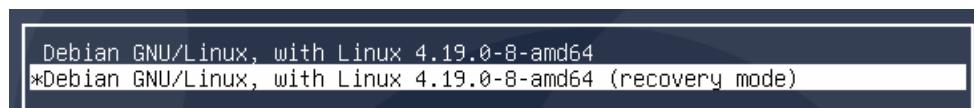


Figura 1: Entramos a través del grub en *recovery mode*

```
You are in rescue mode. After logging in, type "journalctl -xb" to view
system logs, "systemctl reboot" to reboot, "systemctl default" or "exit"
to boot into default mode.
Give root password for maintenance
(or press Control-D to continue): _
```

Figura 2: Introducimos la contraseña de *root*

```
root@debian:/# cat /proc/sys/net/ipv4/icmp_echo_ignore_all
1
root@debian:/# echo 0 > /proc/sys/net/ipv4/icmp_echo_ignore_all
root@debian:/# cat /proc/sys/net/ipv4/icmp_echo_ignore_all
0
root@debian:/#
```

Figura 3: Tenemos una shell en modo root. Ejecutamos algunos cambios

```
root@debian:/# touch i_am_root
root@debian:/# ls
bin  etc      initrd.img
boot home    initrd.img.old
dev  i_am_root lib
```

Figura 4: Creamos archivos en la raíz

```
root@debian:/# ls
bin  home      lib      lost+found  proc  srv  var
boot i_am_root  lib32    media       root  sys  vmlin
dev  initrd.img lib64    mnt         run   tmp  vmlin
etc  initrd.img.old libx32  opt         sbin  usr
root@debian:/# cat /proc/sys/net/ipv4/icmp_echo_ignore_all
1
```

Figura 5: Una vez dentro del sistema vemos que los cambios son persistentes

- e) 1. Generamos una password segura con el comando **grub-mkpasswd-pbkdf2**
2. Añadimos al archivo **/etc/grub.d/00_header**:

```
1 cat << EOF
2 set superusers="root"
3 password_pbkdf2 root <password generado en paso anterior>
4 EOF
```

3. Ejecutamos el comando **update-grub2**
4. Reiniciamos

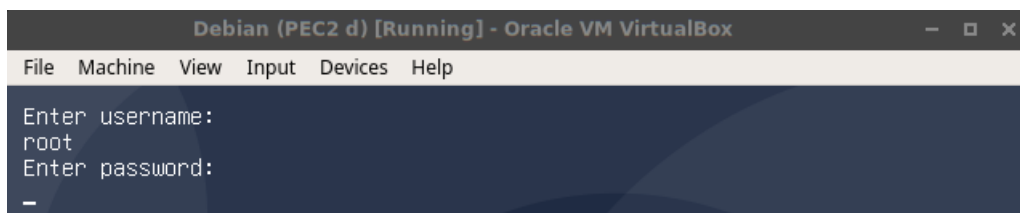


Figura 6: Grub protegido por usuario y contraseña [5]

2. Windows Server

- f) Microsoft Compliance Toolkit es un conjunto de herramientas que permite a un administrador gestionar los objetos de políticas de grupo (*Group Policy Objects* o *GPO*). Mediante esta herramienta se pueden comparar estos objetos con los recomendados por Microsoft u otras bases de políticas; se pueden editar, guardar y aplicar a través del Active Directory o individualmente [6].

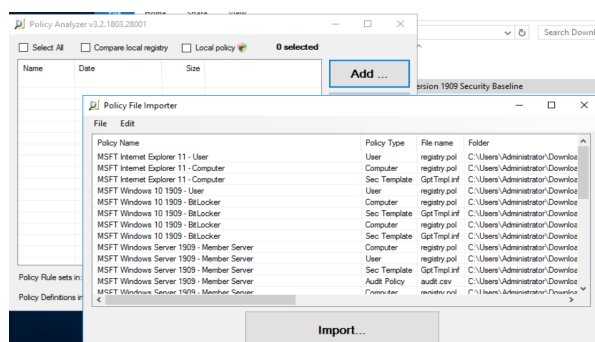


Figura 7: Para importar las GPOs ejecutamos el programa de PolicyAnalyzer y añadimos las políticas que se encuentran en “Windows 10 Version 1909 and Windows ServerVersion 1909 Security Baseline/GPOs”

Para hacer una copia de seguridad de las políticas locales ejecutamos la herramienta de Group Policy Management Console con el comando `gpmc.msc`, seleccionamos `Forest: uoc.local > Domains > View > Options > Table location: Group Policy Objects`.

Seleccionamos el dominio `uoc.local > Group Policy Objects` y con click derecho tendremos la opción de `Back Up All...` y seleccionamos un directorio donde guardar los GPOs [7]. Finalmente, ejecutamos la herramienta Policy Analyzer nuevamente para importarlas.

La herramienta de Policy Analyzer nos permite comparar las GPOs de Baseline con las importadas del entorno local y existen una serie de configuraciones **conflictivas**:

- *Credential Validation*: Permite revisar eventos generados por validación de credenciales. No especificado en la política local.
- *LsaCfgFlags*: Especifica si la seguridad basada en virtualización está habilitada. No especificada en local.
- *SeDenyNetworkLogonRight*: Deniega el acceso al ordenador desde la red. No especificada en local.
- *SeEnableDelegationPrivilege*: Permite a las cuentas de usuario confiables para la delegación.
- *SeInteractiveLogonRight*: Permite el login de manera local. Existen discrepancias entre los flags de la política de baseline y los de la local.
- *SeNetworkLogonRight*: Permite el acceso al ordenador desde la red. Los flags de baseline son distintos a los de la política local.

```

g) PS C:\Users\Administrator> netstat -ab -p TCP
2
3 Active Connections
4
5 Proto Local Address Foreign Address State
6 TCP 0.0.0.0:80 U0C1:0 LISTENING
7 Can not obtain ownership information
8 TCP 0.0.0.0:88 U0C1:0 LISTENING
9 [lsass.exe]
10 TCP 0.0.0.0:135 U0C1:0 LISTENING
11 RpcSs
12 [svchost.exe]
13 TCP 0.0.0.0:389 U0C1:0 LISTENING
14 [lsass.exe]
15 TCP 0.0.0.0:445 U0C1:0 LISTENING
16 Can not obtain ownership information
17 TCP 0.0.0.0:464 U0C1:0 LISTENING
18 [lsass.exe]
19 TCP 0.0.0.0:593 U0C1:0 LISTENING
20 RpcEptMapper
21 [svchost.exe]
22 TCP 0.0.0.0:636 U0C1:0 LISTENING
23 [lsass.exe]
24 TCP 0.0.0.0:3268 U0C1:0 LISTENING
25 [lsass.exe]
26 TCP 0.0.0.0:3269 U0C1:0 LISTENING
27 [lsass.exe]
28 TCP 0.0.0.0:5985 U0C1:0 LISTENING
29 Can not obtain ownership information
30 TCP 0.0.0.0:9389 U0C1:0 LISTENING
31 [Microsoft.ActiveDirectory.WebServices.exe]
32 TCP 0.0.0.0:47001 U0C1:0 LISTENING
33 Can not obtain ownership information
34 TCP 0.0.0.0:49664 U0C1:0 LISTENING
35 Can not obtain ownership information
36 TCP 0.0.0.0:49665 U0C1:0 LISTENING
37 EventLog
38 [svchost.exe]
39 TCP 0.0.0.0:49666 U0C1:0 LISTENING
40 Schedule
41 [svchost.exe]
42 TCP 0.0.0.0:49667 U0C1:0 LISTENING
43 [lsass.exe]
44 TCP 0.0.0.0:49669 U0C1:0 LISTENING
45 [lsass.exe]
46 TCP 0.0.0.0:49670 U0C1:0 LISTENING
47 [lsass.exe]
48 TCP 0.0.0.0:49672 U0C1:0 LISTENING
49 [spoolsv.exe]
50 TCP 0.0.0.0:49675 U0C1:0 LISTENING
51 Can not obtain ownership information
52 TCP 0.0.0.0:49686 U0C1:0 LISTENING
53 [dns.exe]
54 TCP 0.0.0.0:58996 U0C1:0 LISTENING
55 [DFSRs.exe]
56 TCP 127.0.0.1:53 U0C1:0 LISTENING
57 [dns.exe]
58 TCP 192.168.1.174:53 U0C1:0 LISTENING
59 [dns.exe]
60 TCP 192.168.1.174:139 U0C1:0 LISTENING
61 Can not obtain ownership information
62 TCP 192.168.1.174:58975 40.67.254.36:https ESTABLISHED
63 [Explorer.EXE]
64 TCP 192.168.1.174:58981 51.124.78.146:https TIME_WAIT
65 TCP 192.168.1.174:58982 40.67.254.36:https ESTABLISHED
66 ProfSvc
67 [svchost.exe]
68 TCP 192.168.1.174:58983 51.124.78.146:https TIME_WAIT
69 TCP 192.168.1.174:58985 40.77.226.250:https TIME_WAIT
70 TCP 192.168.1.174:58987 51.124.78.146:https ESTABLISHED
71 UsoSvc
72 [svchost.exe]
73 TCP 192.168.1.174:58988 40.77.226.250:https TIME_WAIT
74 TCP 192.168.1.174:58989 13.74.179.117:https TIME_WAIT
75 TCP 192.168.1.174:59001 20.36.218.70:https ESTABLISHED
76 wuauserv
77 [svchost.exe]

```

Todos los servicios listados son, en cierta medida, necesarios para el correcto funcionamiento del sistema. Quizá los procesos Explorer.EXE y DSFRs.exe son los más prescindibles en nuestro contexto puesto que el primero se trata

del Explorador de archivos de Windows y el segundo permite la sincronización de ficheros entre múltiples servidores de la red local o WAN.

El proceso que utiliza el TCP/88 es el lsass.exe, es el proceso de autenticación de seguridad local de Microsoft, autentica la identificación de un usuario y la aplicación de políticas de seguridad. Al intentar matar el proceso la máquina se reinicia automáticamente así que, en principio, no parece que se pueda desactivar.

- h) Nmap funciona conectándose a cada puerto e intenta obtener información del tipo de servicio que está tras el puerto. Debido a su funcionamiento se trata de un proceso más lento y no puede mostrar el ID del proceso que se encuentra usando el puerto ya que se encuentra al otro lado de la máquina. Netstat obtiene la información del Sistema Operativo a través del kernel. Puede sacar un listado de puertos que están en uso y obtener también el ID del proceso que lo está usando.

Tiene sentido usar nmap cuando se desea saber información de un sistema remoto, de los puertos que tenga abiertos y de los servicios escuchando en cada puerto. Se puede optar por usar netstat cuando se quiere saber qué proceso está usando cada puerto en la máquina local e incluso estadísticas de conexiones de red [13].

```
Starting Nmap 7.60 ( https://nmap.org ) at 2020-04-11 18:56 CEST
Nmap scan report for 192.168.1.174
Host is up (0.00066s latency).
Not shown: 988 filtered ports
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
Nmap done: 1 IP address (1 host up) scanned in 4.56 seconds
```

Figura 8: Nmap desde Linux para ver los puertos en escucha en el equipo de Windows

- i) Para instalar un servidor web con estas características primero debemos crear un certificado que nos permita utilizar HTTPS [14].
1. Ejecutamos la aplicación de Internet Information Services (ISS) Manager.
 2. Seleccionamos nuestro servidor UOC1 y Server Certificates bajo el área de ISS.
 3. Aparecerá la opción de crear un certificado en el panel derecho. Lo seleccionamos.
 4. Aparecerá una nueva ventana donde debemos asignar un nombre a nuestro certificado y un sitio donde guardarlo (Personal, Web Hosting).
 5. Volvemos al panel izquierdo y seleccionamos UOC1 > Sites > Default Web Site y en el área derecha de la ventana nos aparecerá la opción de Bindings. La seleccionamos.
 6. Añadimos un nuevo binding de tipo HTTPS, puerto 443 y certificado anteriormente creado.
 7. Añadimos otro binding que sea el del puerto 8080 de la misma forma.
 8. Hacemos click en Restart en la sección de Manage Website.

Para que el Web Server acepte conexiones al mismo site por el puerto 8080:

1. Abrimos el programa Windows Firewall with Advanced Security.
2. Seleccionamos en el panel izquierdo Inbound rules y en el derecho New Rule.
3. Especificamos que esta regla es sobre un puerto y le especificamos el 8080 en el siguiente menú.
4. Especificamos que debe permitir la conexión y finalmente le asignamos un nombre.

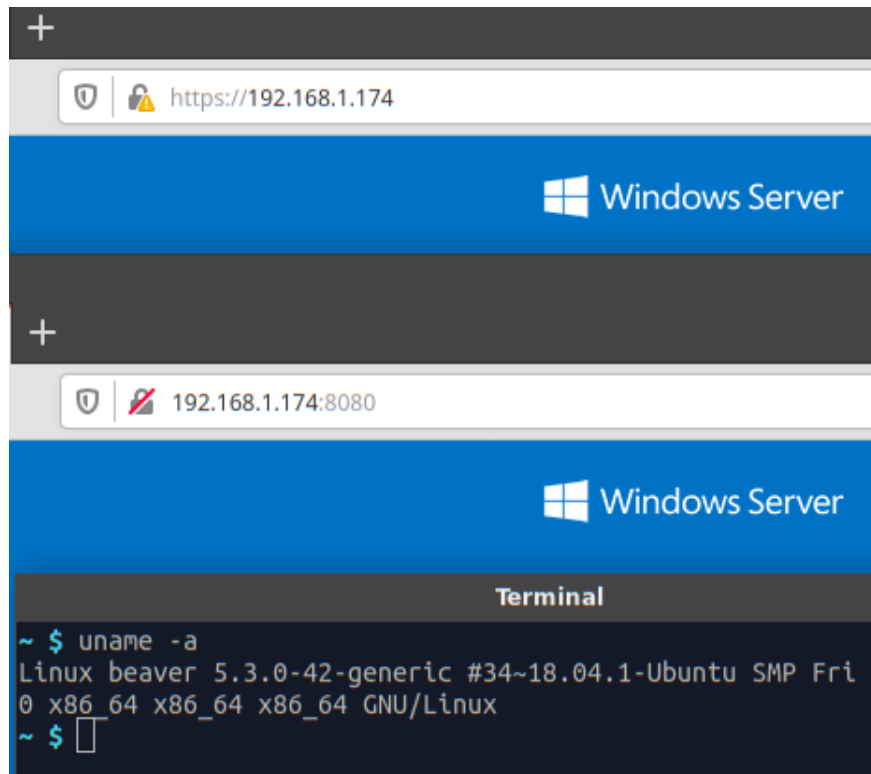


Figura 9: Acceso al mismo site tanto desde el puerto 8080 (HTTP) como desde el 443 (HTTPS) a través de Linux

- j) Para aplicar el modo “Constrained Language” a Powershell a nivel de sistema podemos establecer la variable `__PSLockDownPolicy` a 4. En PowerShell escribimos [9]:

```
1 [Environment]::SetEnvironmentVariable('__PSLockdownPolicy', '4', 'Machine')
```

Si queremos hacer un bypass de este modo, podemos bypassear primero la variable de entorno [10]:

```
1 Set-ItemProperty 'hklm:\SYSTEM\CurrentControlSet\Control\Session Manager\Environment' -name "__PSLockdownPolicy" -Value 8
```

y ejecutar una nueva instancia de PowerShell:

```
1 Start-Process -File PowerShell.exe
```

```
1 PS C:\Users\Administrator> $ExecutionContext.SessionState.LanguageMode
2 FullLanguage
```

AMSI es el acrónimo de *Antimalware Scan Interface* y se trata de un interface que permite a las aplicaciones y servicios integrarse con cualquier producto antimalware existente en la máquina. Ofrece protección antimalware a los usuarios finales y a sus datos [11].

```
PS C:\Users\Administrator> Invoke-Expression (Invoke-WebRequest https://pastebin.com/raw.php?i=JHhn
FV8M)
iex : At line:1 char:1
+ 'AMSI Test Sample: 7e72c3ce-861b-4339-8740-0ac1484c1386'
+ ~~~~~
This script contains malicious content and has been blocked by your antivirus software.
At line:4 char:1
+ iex $string
+ ~~~~~
+ CategoryInfo          : ParserError: (:) [Invoke-Expression], ParseException
+ FullyQualifiedErrorId : ScriptContainedMaliciousContent,Microsoft.PowerShell.Commands.InvokeExpressionCommand
```

Figura 10: AMSI habilitado en Powershell [12]

- k) ■ nmap con la opción `-sn` es el modo *host discovery*, escaneo con ping. [15]

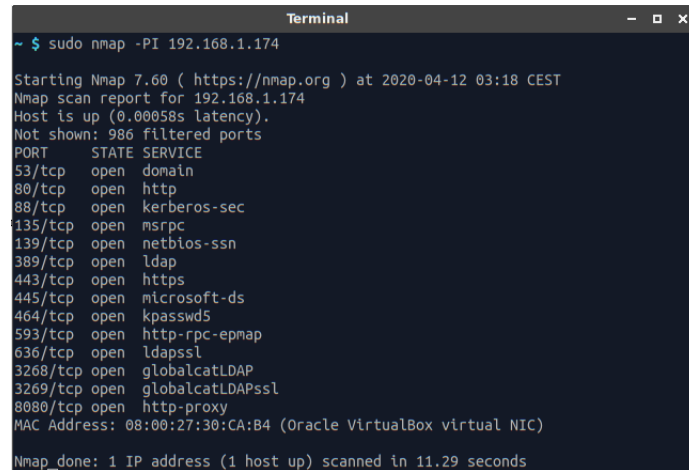


```
Terminal
~ $ nmap -sn 192.168.1.0/24

Starting Nmap 7.60 ( https://nmap.org ) at 2020-04-12 03:02 CEST
Nmap scan report for gateway (192.168.1.1)
Host is up (0.0013s latency).
Nmap scan report for beaver (192.168.1.136)
Host is up (0.00059s latency).
Nmap scan report for (192.168.1.158)
Host is up (0.025s latency).
Nmap scan report for 192.168.1.174 (192.168.1.174)
Host is up (0.0015s latency).
Nmap done: 256 IP addresses (4 hosts up) scanned in 6.98 seconds
```

Figura 11: Listado de hosts en la red

- nmap con la opción `-PI` manda peticiones echo del protocolo ICMP.

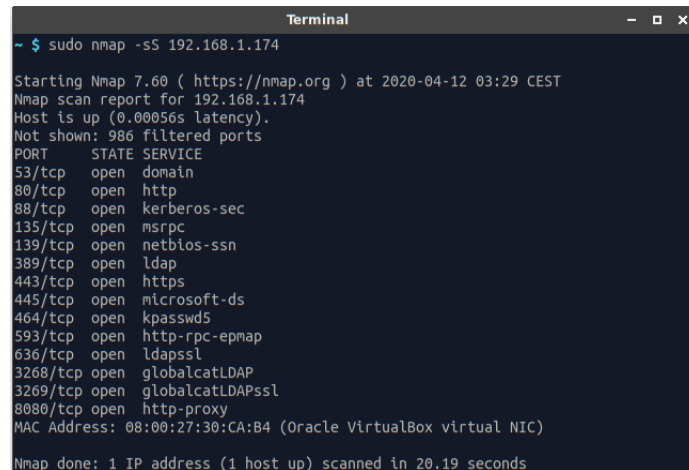


```
Terminal
~ $ sudo nmap -PI 192.168.1.174

Starting Nmap 7.60 ( https://nmap.org ) at 2020-04-12 03:18 CEST
Nmap scan report for 192.168.1.174
Host is up (0.00058s latency).
Not shown: 986 filtered ports
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
443/tcp   open  https
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
8080/tcp  open  http-proxy
MAC Address: 08:00:27:30:CA:B4 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 11.29 seconds
```

Figura 12: Escaneo de la red de Windows

- nmap con la opción `-sS` efectúa un escaneo TCP SYN o *Stealth Scan*.



```
Terminal
~ $ sudo nmap -sS 192.168.1.174

Starting Nmap 7.60 ( https://nmap.org ) at 2020-04-12 03:29 CEST
Nmap scan report for 192.168.1.174
Host is up (0.00056s latency).
Not shown: 986 filtered ports
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
443/tcp   open  https
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
8080/tcp  open  http-proxy
MAC Address: 08:00:27:30:CA:B4 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 20.19 seconds
```

Figura 13: Escaneo SYN TCP de la red de Windows

- nmap con la opción -sT efectúa un escaneo TCP Connect.

```

Terminal
~ $ sudo nmap -sT 192.168.1.174

Starting Nmap 7.60 ( https://nmap.org ) at 2020-04-12 03:32 CEST
Nmap scan report for 192.168.1.174
Host is up (0.00051s latency).
Not shown: 986 filtered ports
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
443/tcp   open  https
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
8080/tcp  open  http-proxy
MAC Address: 08:00:27:30:CA:B4 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 4.87 seconds

```

Figura 14: Escaneo TCP connect de la red de Windows

- nmap con la opción -sU efectúa un escaneo UDP.

```

Terminal
~ $ sudo nmap -sU 192.168.1.174

Starting Nmap 7.60 ( https://nmap.org ) at 2020-04-12 03:40 CEST
Nmap scan report for 192.168.1.174
Host is up (0.0010s latency).
Not shown: 996 open|filtered ports
PORT      STATE SERVICE
53/udp    open  domain
123/udp   open  ntp
137/udp   open  netbios-ns
389/udp   open  ldap
MAC Address: 08:00:27:30:CA:B4 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 17.85 seconds

```

Figura 15: Escaneo UDP de la red de Windows

- nmap con la opción -O activa la detección del sistema operativo.

```

Terminal
~ $ sudo nmap -O 192.168.1.174

Starting Nmap 7.60 ( https://nmap.org ) at 2020-04-12 03:42 CEST
Nmap scan report for 192.168.1.174
Host is up (0.00059s latency).
Not shown: 986 filtered ports
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
443/tcp   open  https
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
8080/tcp  open  http-proxy
MAC Address: 08:00:27:30:CA:B4 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Microsoft Windows Server 2012 or Windows Server 2012 R2 (93%), Microsoft Windows Server 2012 R2 (88%), Microsoft Windows 10 build 10586 - 14393 (87%), Microsoft Windows 7 Professional (87%), Microsoft Windows Phone 7.5 or 8.0 (86%), Microsoft Windows 10 build 14393 (86%), Microsoft Windows 10 build 10586 (86%), Microsoft Windows Server 2008 R2 or Windows 8.1 (86%), Microsoft Windows 7 Professional or Windows 8 (86%), Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (86%)
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 33.98 seconds

```

Figura 16: Escaneo para determinar el sistema operativo

- nmap con la opción -sV nos da la versión de los servicios que se están ejecutando en los puertos.

```
~ $ sudo nmap -sV 192.168.1.174
Starting Nmap 7.60 ( https://nmap.org ) at 2020-04-12 03:44 CEST
Nmap scan report for 192.168.1.174
Host is up (0.00059s latency).
Not shown: 986 filtered ports
PORT      STATE SERVICE        VERSION
53/tcp    open  domain         Microsoft DNS
80/tcp    open  http           Microsoft IIS httpd 10.0
88/tcp    open  kerberos-sec   Microsoft Windows Kerberos (server time:
135/tcp   open  msrpc          Microsoft Windows RPC
139/tcp   open  netbios-ssn    Microsoft Windows netbios-ssn
389/tcp   open  ldap           Microsoft Windows Active Directory LDAP
443/tcp   open  ssl/http       Microsoft IIS httpd 10.0
445/tcp   open  microsoft-ds   Microsoft Windows Server 2008 R2 - 2012
464/tcp   open  kpasswds?
593/tcp   open  ncacn_http     Microsoft Windows RPC over HTTP 1.0
636/tcp   open  ssl/ldap       Microsoft Windows Active Directory LDAP
3268/tcp  open  ldap           Microsoft Windows Active Directory LDAP
3269/tcp  open  ssl           Microsoft SChannel TLS
8080/tcp  open  http           Microsoft IIS httpd 10.0
```

Figura 17: Escaneo para determinar las versiones de los servicios que están en marcha

Referencias

- [1] Techrepublic,
[How to enable SSL on NGINX](#)
- [2] solusan.com,
[Cómo va update-rc.d ? \(editor de niveles de ejecución en Debian\)](#)
- [3] Server Healers,
[How to Disable Ping Response \(ICMP echo \) in Linux](#)
- [4] Ask Ubuntu,
[How do I boot into a root shell?](#)
- [5] geekland,
[Proteger el grub con contraseña](#)
- [6] Microsoft Security Compliance Toolkit 1.0,
[What is the Security Compliance Toolkit \(SCT\)?](#)
- [7] Active Directory 360,
[Group Policy Backup](#)
- [8] PowerShell Constrained Language Mode,
[What is PowerShell Constrained Language?](#)
- [9] IT for Dummies,
[PowerShell Constrained mode](#)
- [10] GitHub - Metoraf007,
[PowerShell - Bypass Constrained Language Mode](#)
- [11] Windows Dev Center,
[Antimalware Scan Interface \(AMSI\)](#)
- [12] Windows Dev Center,
[How the Antimalware Scan Interface \(AMSI\) helps you defend against malware](#)
- [13] Stack Exchange - Superuser,
[What is the difference between nmap and netstat?](#)
- [14] Sophos Community,
[How to Create a Self Signed SSL Certificate with Windows Server](#)
- [15] nmap.org,
[Chapter 15. Nmap Reference Guide](#)