

PEC 3

Análisis de puertos, vulnerabilidades y protocolos

Pablo Riutort Grande

16 de mayo de 2020

Linux Server

- a) Para instalar Snort se han seguido las instrucciones de la página oficial de Snort [1]. Primero se instalaron algunas dependencias necesarias [2]:

```
1 apt-get install -y gcc make libpcap-dev zlib1g-dev liblua5.1-dev libpcap-dev openssl  
libssl-dev libnhttp2-dev libdumbnet-dev bison flex libdnet
```

La instalación consiste en primero instalar DAQ (Data Acquisition library):

```
1 wget https://www.snort.org/downloads/snort/daq-2.0.7.tar.gz  
2 tar xvfz daq-2.0.7.tar.gz  
3 cd daq-2.0.7  
4 ./configure && make && sudo make install
```

Durante la instalación hubo algunos problemas de compilación que se solventaron mediante autoreconf

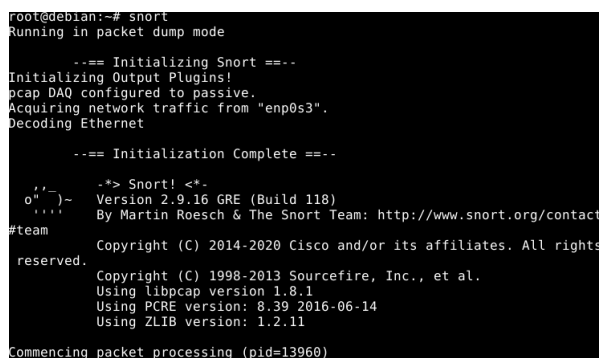
```
1 autoreconf -f -i; ./configure && make && sudo make install
```

Posteriormente podemos instalar Snort:

```
1 tar xvfz snort-2.9.16.tar.gz  
2  
3 cd snort-2.9.16  
4 ./configure --enable-sourcefire && make && sudo make install
```

Finalmente, pasamos a ejecutar el comando ldconfig que crea los links necesarios y cachea las diferentes librerías que utilizará Snort [4].

```
1 ldconfig
```



```
root@debian:~# snort  
Running in packet dump mode  
  
--== Initializing Snort ==--  
Initializing Output Plugins!  
pcap DAQ configured to passive.  
Acquiring network traffic from "enp0s3".  
Decoding Ethernet  
  
--== Initialization Complete ==--  
  
.*> Snort! <*.  
o" )~ Version 2.9.16 GRE (Build 118)  
" " By Martin Roesch & The Snort Team: http://www.snort.org/contact  
#team  
Copyright (C) 2014-2020 Cisco and/or its affiliates. All rights reserved.  
Copyright (C) 1998-2013 Sourcefire, Inc., et al.  
Using libpcap version 1.8.1  
Using PCRE version: 8.39 2016-06-14  
Using ZLIB version: 1.2.11  
  
Commencing packet processing (pid=13960)
```

Figura 1: Snort instalado en el sistema Debian

- b) Para este apartado primero tendremos que configurar Snort para funcionar como un NIST (Network Intrusion Detection System). Este modo requiere de tener una estructura de ficheros donde guardar las reglas de Snort y los logs:

```
1 mkdir -p /etc/snort/rules  
2 chmod -R 5775 /etc/snort  
3 mkdir /var/log/snort  
4 chmod -R 5775 /var/log/snort  
5 mkdir /usr/local/lib/snort_dynamicrules  
6 chmod -R 5775 /usr/local/lib/snort_dynamicrules
```

Movemos la configuración de Snort a los nuevos ficheros:

```
1 mkdir -p /etc/snort/rules
2 chmod -R 5775 /etc/snort
3 mkdir /var/log/snort
4 chmod -R 5775 /var/log/snort
5 mkdir /usr/local/lib/snort_dynamicrules
6 chmod -R 5775 /usr/local/lib/snort_dynamicrules
```

Creamos los ficheros que contengan las reglas que Snort utilizará para detectar los paquetes:

```
1 touch /etc/snort/rules/white_list.rules
2 touch /etc/snort/rules/black_list.rules
3 touch /etc/snort/rules/local.rules
```

Editamos local.rules:

```
1 alert icmp any any -> $HOME_NET any (msg:"uoc - ping"; itype: 8; sid:1; rev:1;)
```

Esta regla indica que cualquier paquete ICMP de cualquier origen y cualquier puerto dirigido a la red local y a cualquier puerto será registrado como uoc - ping. Además, se le añade la opción de que itype sea 8 para que detecte los paquetes echo request del protocolo ICMP (ping) [5]

```
1 #define ICMP_ECHO 8 /* Echo Request */
```

Listing 1: Extracto de src/decode.h de Snort donde se incluyen los distintos tipos de ICMP

Para utilizar estas reglas debemos editar el fichero de configuración en /etc/snort/snort.conf indicando el path correcto de las reglas de Snort y comentar aquellas que no tengamos pero que Snort espera encontrar:

```
1 var RULE_PATH rules
2 var SO_RULE_PATH so_rules
3 var PREPROC_RULE_PATH preproc_rules
```

Listing 2: Los path de los rules quedan ahora bajo /etc/snort/

```
1 # site specific rules
2 include $RULE_PATH/local.rules
3
4 #include $RULE_PATH/app-detect.rules
5 #include $RULE_PATH/attack-responses.rules
6 ...
```

Listing 3: Quedan deshabilitadas las reglas a excepción de local.rules

Podemos validar la configuración mediante:

```
1 snort -T -c /etc/snort/snort.conf
```

Finalmente podemos ejecutar Snort en modo NIST aplicando las reglas y la configuración mediante el comando:

```
1 snort -A console -i enp0s3 -c /etc/snort/snort.conf
```



```
Preprocessor Object: SF_DNS ve
Commencing packet processing (pid=15474)
```

Figura 2: Snort empieza a escuchar conexiones

- c) El servicio SSH ya quedó instalado para la PEC anterior, para configurarlo podemos editar el archivo /etc/ssh/sshd_config mediante el editor de vim. Para este ejercicio se realizarán prácticamente las mismas acciones con vim sobre distintas líneas del archivo sshd_config:

1. Buscar el contenido correspondiente a la acción a ejecutar con el comando “/<palabra(s) a buscar>”
 2. Descomentar la línea si está comentada borrando el carácter “#” del inicio de línea con el comando “x”.
 3. Cambiar el parámetro situándonos sobre él mediante el comando “w”, editándolo mediante “cw” y escribiendo el contenido deseado.
 4. Guardamos el contenido del archivo pasando a modo normal (Esc.) y escribiendo el comando “:w”.
 5. Después de cada edición será necesario reiniciar el servicio mediante el comando “systemctl ssh restart”.
- Para cambiar el puerto para que el servicio se ejecute en el puerto 3333 esta acción buscamos el puerto 22 con el comando de búsqueda “/Port 22”. Lo descomentamos borrando el carácter “#” del inicio y cambiamos el número 22 por el 3333:
 - Para evitar que el root se conecte de forma remota podemos editar la línea del archivo donde pone PermitRootLogin a PermitRootLogin No.

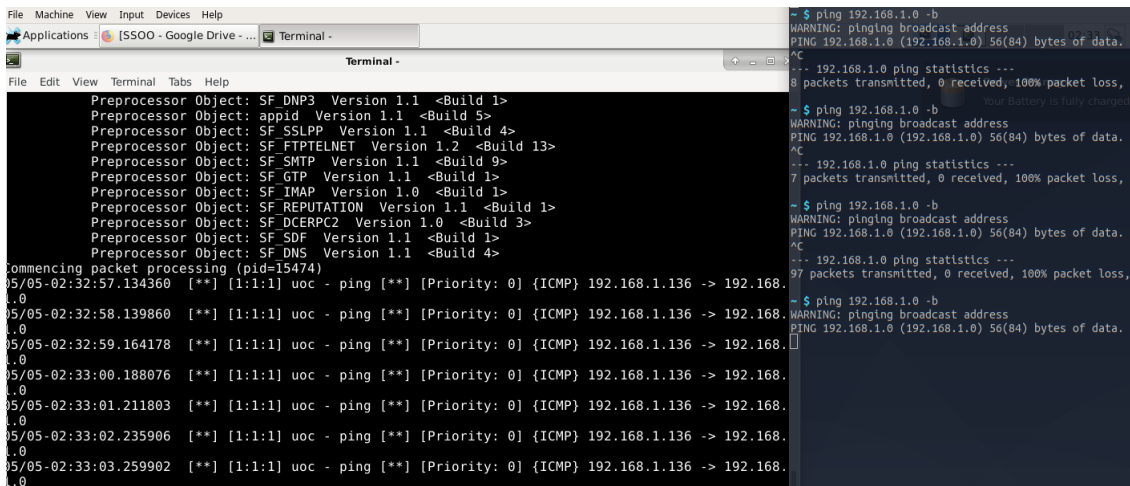


Figura 3: Lanzamos ping desde la máquina local y es detectado por Snort

```
12
13 Port 3333
14 #AddressFamily any
```

Figura 4: Edición del archivo sshd_config para configurar el puerto 3333

```
30
31 #LoginGraceTime 2m
32 PermitRootLogin no
33 #StrictModes yes
```

Figura 5: Edición del archivo sshd_config para restringir el acceso root

- Para limitar el número máximo de intentos a 3 podemos cambiar la línea donde pone MaxAuthTries a MaxAuthTries 3.

```
31 #LoginGraceTime 2m
32 PermitRootLogin no
33 #StrictModes yes
34 MaxAuthTries 3
35 #MaxSessions 10
36
```

Figura 6: Edición del archivo sshd_config para configurar el máximo número de intentos de autenticación a 3

- Para limitar el tiempo máximo de login a 60 segundos podemos editar la línea donde pone LoginGraceTime a LoginGraceTime 1m. Si pasado el tiempo límite se introduce una contraseña, el sistema cierra la conexión y muestra el mensaje: "Connection closed by 192.168.1.199 port 3333"

```
# Authentication:
LoginGraceTime 60
PermitRootLogin no

~ $ ssh uoc@192.168.1.199 -p 3333
uoc@192.168.1.199's password:
Connection closed by 192.168.1.199 port 3333
~ $
```

Figura 7: Edición del archivo sshd_config para limitar el tiempo que se permite para hacer login y una muestra del mensaje recibido por parte de la máquina virtual en caso de exceder dicho tiempo.

- Para impedir el login mediante de password se puede editar la línea que contiene PasswordAuthentication por PasswordAuthentication no
- Para configurar el uso de clave pública-privada para poder acceder al servidor primero generamos una clave SSH en el host [6]:

```
1 ssh-keygen -t rsa -b 4096 -C "pablo.riutort@gmail.com"
```

```

55 # To disable tunneled clear t
56 PasswordAuthentication no
57 #PermitEmptyPasswords no

```

Figura 8: Edición del archivo sshd_config para restringir el acceso por password

Después de seguir el proceso de generación, este comando generará el directorio .ssh en el directorio del usuario en /home que a su vez contendrá los archivos id_rsa e id_rsa.pub que son la clave privada y pública respectivamente. Para poder copiar la clave SSH pública tenemos que desactivar momentáneamente la restricción de acceso por contraseña y podemos ejecutar el comando [9]:

```
1 ssh-copy-id -i .ssh/id_rsa.pub uoc@192.168.1.199 -p 3333
```

Que nos copiará la clave SSH del host para acceder únicamente con la clave pública.

Ahora, modificamos el archivo de configuración editando la línea que contiene PubkeyAuthentication a PubkeyAuthentication yes y volvemos a aplicar la restricción de PasswordAuthentication del punto anterior y ya podemos acceder sin password únicamente con nuestra clave SSH[10].

```

35 #MaxSessions 10
36
37 PubkeyAuthentication yes
38

```

Figura 9: Edición del archivo sshd_config para configurar el acceso mediante clave pública

```

~ $ ssh-copy-id -i .ssh/id_rsa.pub uoc@192.168.1.199 -p 3333
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: ".ssh/id_rsa.pub"
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys
uoc@192.168.1.199's password:

Number of key(s) added: 1

Now try logging into the machine, with:  "ssh -p '3333' 'uoc@192.168.1.199'"
and check to make sure that only the key(s) you wanted were added.

~ $ ssh uoc@192.168.1.199 -p 3333
Linux debian 4.19.0-8-amd64 #1 SMP Debian 4.19.98-1 (2020-01-26) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
uoc@debian:~$

```

Figura 10: Ejemplo del uso del ssh-copy-id y un acceso con éxito a la máquina virtual mediante ssh sin password

- d) Para este ejercicio se ha realizado un escaneo de tipo avanzado mediante la aplicación de Nessus sobre la IP de la máquina virtual de Windows. El programa ha encontrado un total de 49 vulnerabilidades, 12 de las cuales son de riesgo medio, 1 de riesgo alto y 2 de riesgo crítico y las restantes son de carácter informativo. En la tabla adjunta [Cuadro 1] se comentan algunas de las vulnerabilidades encontradas, sus posibles exploits y soluciones.

| Riesgo de seguridad | Descripción | Exploits | Solución |
|--|---|---|------------------------------------|
| Nivel crítico | | | |
| KB4025339: Windows 10 Version 1607 Cumulative Update | Falta la actualización de seguridad KB4025339 | Algunas vulnerabilidades son: <ul style="list-style-type: none"> ■ Ejecución remota de código ■ Escaladas de privilegios ■ Vulneración de la privacidad de información | Aplicar la actualización KB4025339 |

| | | | |
|---|---|---|--|
| <i>Mozilla Firefox < 76.0</i> | La versión de Firefox es anterior a 76.0 | <p>Algunas vulnerabilidades son:</p> <ul style="list-style-type: none"> ■ Bloqueo de la app potencialmente explotable ■ Desbordamiento de buffer ■ Inyección de comandos | Actualizar versión de Firefox |
| Nivel alto | | | |
| <i>Security Updates for Windows Defender (April 2020)</i> | La versión del motor de Microsoft Windows Defender instalada en el host remoto de Windows es anterior a 4.18.2001.112 | Elevación de privilegios de enlace duro | Habilitar las actualizaciones automáticas para actualizar el motor de escaneo para las aplicaciones anti-malware relevantes. |
| Nivel medio | | | |
| <i>TLS Version 1.1 Protocol Detection</i> | El servicio acepta conexión encriptadas con TLS 1.1 y este protocolo no tiene soporte para las soluciones de cifrado actuales y recomendadas | <p>El uso de versiones antiguas de TLS conlleva ciertos riesgos [19], entre ellos:</p> <ul style="list-style-type: none"> ■ POODLE[10] ■ BEAST[11] ■ Man-in-the-middle[12] | Dar soporte para TLS 1.2 o 1.3 y deshabilitar el 1.1 |
| <i>TLS Version 1.0 Protocol Detection</i> | El servicio acepta conexión encriptadas con TLS 1.0 y este protocolo no tiene soporte para las soluciones de cifrado actuales y recomendadas | <ul style="list-style-type: none"> ■ POODLE[10] ■ BEAST[11] ■ Man-in-the-middle[12] | Dar soporte para TLS 1.2 o 1.3 y deshabilitar el 1.0 |
| <i>SSL Self-Signed Certificate</i> | La cadena de certificados X.509 para este servicio no está firmada por una autoridad certificadora reconocida. Si el host remoto es un host público en producción, queda anulado el uso de SSL | <ul style="list-style-type: none"> ■ Man-in-the-middle[12] | Comprar o generar un certificado SSL apropiado |
| <i>SSL RC4 Cipher Suites Supported</i> | El host remoto admite el uso de cifrado RC4. El cifrado RC4 es defectuoso a la hora de generar un flujo pseudo aleatorio de bytes introduciendo varios pequeños bias reduciendo así la aleatoriedad. Si un texto es cifrado repetidas veces un atacante podría deducir el texto original. | <ul style="list-style-type: none"> ■ Bar Mitzvah[13] | Reconfigurar los servicios para que eviten el uso de RC4. Se recomienda utilizar TLS 1.2 con AES-GCM. |

| | | | |
|--|---|---|--|
| <i>SSL Medium Strength Cipher Suites Supported</i> | El host remoto admite el uso de cifrados SSL de fuerza media (cifrados que usan longitudes de entre 64 y 112 bits). | <ul style="list-style-type: none"> ■ SWEET32[14][17] | Reconfigurar los servicio para que eviten el uso de RC4. Se recomienda utilizar TLS 1.2 con AES-GCM. |
| <i>SSL Certificate Wrong Hostname</i> | El 'commonName' (CN) del certificado SSL presentado es para una máquina distinta. | <p>Tiene varias vulnerabilidades [18], entre ellas:</p> <ul style="list-style-type: none"> ■ Spoof Certificates[15] ■ Homograph attack[16] ■ Man-in-the-middle[12] | Comprar o generar un certificado SSL apropiado |
| <i>SSL Certificate Cannot Be Trusted</i> | El certificado X.509 del servidor no es de confianza. | <ul style="list-style-type: none"> ■ Man-in-the-middle[12] | Comprar o generar un certificado SSL apropiado |
| <i>Windows Speculative Execution Configuration Check</i> | El host no ha mitigado adecuadamente una serie de vulnerabilidades de ejecución especulativas conocidas | <p>Algunos exploits son:</p> <ul style="list-style-type: none"> ■ <i>Branch Target Injection</i> ■ <i>Bounds Check Bypass</i> ■ <i>Rogue Data Cache Load</i> | Aplicar la configuración recomendada por el proveedor. |
| <i>Security Updates for Windows 10 / Windows Server 2016 (August 2018)</i> | Al host remoto de Windows le falta una actualización de seguridad. | Faltan actualizaciones de microcódigo para mitigar vulnerabilidades de hardware conocidos como <i>Meltdown</i> y <i>Spectre</i> [23]. | Aplicar las actualizaciones de seguridad de Microsoft para Windows 10. |

Cuadro 1: Vulnerabilidades encontradas por el programa Nessus

- e) La ejecución de Lynis muestra una serie de componentes analizados divididos en secciones. En cada sección hay una serie de elementos que muestra el objeto a analizar y el resultado obtenido. Por ejemplo, en la sección de SSH el análisis considera que el `ClientAliveInterval` es aceptable, sin embargo tiene sugerencias para las opciones de `AllowTcpForwarding`, `ClientAliveCountMax`, `Compression`, `LogLevel`, `MaxSessions`, `TCPKeepAlive`, `X11Forwarding` y `AllowAgentForwarding`.

Los resultados finales de Lynis son 1 advertencia (Warning) sobre el módulo de iptables, que está cargado en el sistema y no tiene reglas activas [FIRE-4512] y 45 sugerencias que paso a resumir a continuación:

- Se debería considerar el endurecimiento de servicios de sistema.
- Deshabilitar explícitamente el core dump del archivo `/etc/security/limits.conf`.
- Instalar un módulo de PAM para revisar la fuerza de los passwords. Revisar la configuración de PAM.
- Configurar un algoritmo de encriptación mínimo y máximo en el archivo `/etc/login.defs`. También propone un tiempo máximo y mínimo para las contraseñas.
- Añadir fecha de expiración para las cuentas protegidas con contraseña.
- Deshabilitar módulos del kernel que no se utilizan
- Deshabilitar los drivers de almacenamiento de USB cuando no se usen
- Revisar la configuración del DNS
- Utilizar una herramienta que revise periódicamente las actualizaciones
- Revisar si una serie de protocolos se utilizan en el sistema
- Cambiar la configuración de HTTPS y SSL
- Endurecer la configuración de SSH.
- Revisar archivos eliminados en uso y su razón
- Instalar algún software de detección de malware

Finalmente, Lynis muestra los detalles del escaneo: *hardening index* de 66, 261 tests realizados y la presencia del componente de Firewall pero también la ausencia de un detector de malware. El escaneo ha sido realizado en modo normal y los módulos eran los de *Security Audit* y *Vulnerability Scan*.

Windows Server

- f) Los sistemas que utilizan NTLM (Windows NT LAN Manager) guardan las credenciales del usuario en memoria y concretamente, guardan un hash del password del usuario que desea autenticarse llamado *NTLM Hash Password*. Esta memoria está gestionada por el proceso *Local Security Auth* o LSASS.EXE. De esta forma, se consigue efectuar el *Single Sign-On* evitando que el usuario deba autenticarse múltiples veces para acceder a recursos de red: Cuando se desea acceder a un recurso se produce un proceso de autenticación entre el recurso, el LSASS y el *Domain Controller*, que guarda el hash NTLM de cada usuario para hacer pruebas de autenticación.

El ataque *Pass-the-Hash* o PtH consiste en obtener los credenciales (nombre de usuario y hash NTLM) guardados en memoria por el LSASS y utilizarlos para acceder lateralmente a otros sistemas de la red y hacer escalada de privilegios. No es necesario descifrar el hash para obtener el texto plano, el ataque vulnera el protocolo de autenticación ya que el hash del password permanece estático pero sí que es necesario tener permisos de administrador local para llevarlo a cabo ya que es necesario leer la memoria de LSASS. [20]

Las buenas prácticas de seguridad son la manera de mitigar el PtH, entre ellas:

- **Modelo de seguridad con privilegios mínimos:** Reducir la escalada de privilegios del atacante. El limitar los derechos de administración innecesarios reduce la posibilidad de tener un NTLM hash accesible para un atacante.
- **Rotación frecuente de contraseñas**
- **Separación de privilegios:** Reducir el alcance de uso de cuentas de administrador separando las cuentas privilegiadas de las no privilegiadas y reducir así el movimiento lateral.

Otras maneras de prevenir este tipo de ataques es utilizar herramientas de seguridad como antivirus, firewalls o IDS o configurar el sistema para que no utilice NTLM.

Microsoft LAPS (Local Administrator Password Solution) es una herramienta que permite administrar y rotar contraseñas de administrador local [21] en ordenadores de un mismo dominio de tal forma que estas son

únicas en cada ordenador, generadas aleatoriamente y almacenadas de manera segura en la infraestructura del ActiveDirectory y protegidas en el transporte con cifrado del protocolo Kerberos v5, mitigando así la vulnerabilidad de PtH impidiendo el movimiento lateral y la escalada de privilegios [22].

Una vez instalado el programa podremos editar los parámetros de las contraseñas como una GPO desde el editor de políticas.

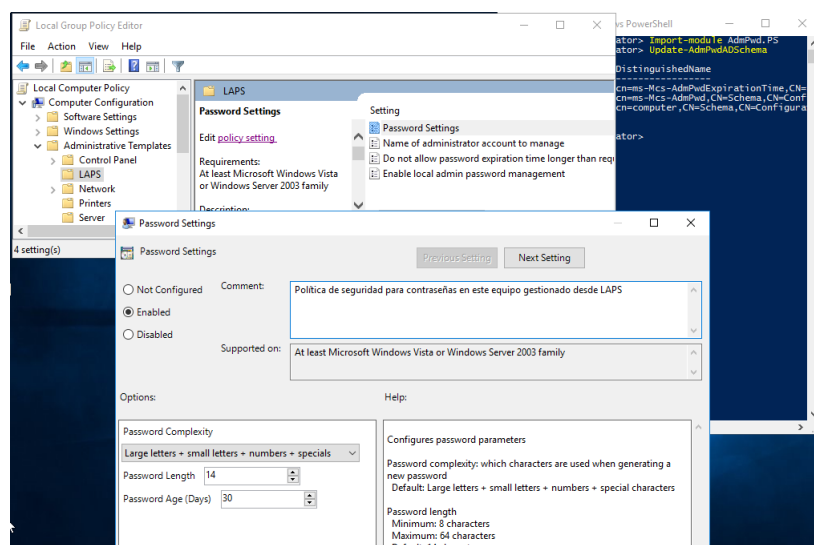


Figura 11: Uso de LAPS desde el editor de políticas

En la imagen adjunta podemos ver cómo después de habilitar el módulo desde PowerShell (derecha), el módulo de LAPS está disponible como una Local Computer Policy. En el menú de LAPS (izquierda) tendremos varias opciones de las comentadas anteriormente, entre ellas encontramos la primera, Password Settings, que nos permite definir los parámetros de las contraseñas con opciones como la la complejidad, que este contexto son los grupos de caracteres de los que se compone, longitud o la duración de su validez (abajo).

Las siguientes configuraciones hacen referencia a la cuenta de administrador sobre la que aplicar estas restricciones, limitar la expiración de la contraseña a lo que dicte esta política y habilitar la delegación de la gestión de la contraseña del administrador local a esta política.

Referencias

- [1] Snort,
Get started,
<https://www.snort.org/#get-started>
- [2] Upcloud,
Installing snort on Debian,
<https://upcloud.com/community/tutorials/installing-snort-on-debian/>
- [3] Stack Overflow,
How to overcome “aclocal-1.15’ is missing on your system” warning?,
<https://stackoverflow.com/questions/33278928/how-to-overcome-aclocal-1-15-is-missing-on-your-system-warning>
- [4] ldconfig,
ldconfig(8) - Linux man page,
<https://linux.die.net/man/8/ldconfig>
- [5] ICMP echo request,
Internet Control Message Protocol (ICMP) Parameters - Type 8,
<http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xhtml#icmp-parameters-codes-8>
- [6] GitHub.com,
Generar una nueva clave SSH y agregarla al ssh-agent,
<https://help.github.com/es/github/authenticating-to-github/generating-a-new-ssh-key-and-adding-it-to-the-ssh-agent>
- [7] Nixhat solutions,
HARDENING SSH CONFIGURATION,
<http://www.nixhat.com/2016/04/hardening-ssh-configuration/>
- [8] The geek stuff,
7 Default OpenSSH Security Options You Should Change in /etc/ssh/sshd_config,
<https://www.thegeekstuff.com/2011/05/openssh-options/>
- [9] ssh.com,
ssh-copy-id,
<https://www.ssh.com/ssh/copy-id>
- [10] National Vulnerability Database (NIST),
CVE-2014-3566 - PODDLE,
<https://nvd.nist.gov/vuln/detail/CVE-2014-3566>
- [11] National Vulnerability Database (NIST),
CVE-2011-3389 - BEAST,
<https://nvd.nist.gov/vuln/detail/CVE-2011-3389>
- [12] Common Vulnerabilities and Exposures (CVE),
CVE-2009-3555 - Man-in-the-middle,
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2009-3555>
- [13] National Vulnerability Database (NIST),
CVE-2015-2808 - Bar Mitzvah,
<https://nvd.nist.gov/vuln/detail/CVE-2015-2808>
- [14] National Vulnerability Database (NIST),
CVE-2016-2183 - SWEET32,
<https://nvd.nist.gov/vuln/detail/CVE-2016-2183>
- [15] Common Vulnerabilities and Exposures (CVE),
CVE-2003-0355 - Multiple Web Browsers do not do not validate CN on certificates,
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-0355>
- [16] threat post,
Certificates Spoofing Google, Facebook, GoDaddy Could Trick Mobile Users,
<https://threatpost.com/certificates-spoofing-google-facebook-godaddy-could-trick-mobile-users/104259/>

- [17] iweb,
SSL/TLS issues - POODLE/BEAST/SWEET32 attacks and the End of SSLv3 + OpenSSL Security Advisory,
<https://bit.ly/3cwPV70>
- [18] Common Weakness Enumeration (CWE),
CWE-297: Improper Validation of Certificate with Host Mismatch,
<https://cwe.mitre.org/data/definitions/297.html>
- [19] PCI Security Standards Council,
Are You Ready for 30 June 2018? Saying Goodbye to SSL/early TLS,
<https://blog.pcisecuritystandards.org/are-you-ready-for-30-june-2018-sayin-goodbye-to-ssl-early-tls>
- [20] Beyond Trust,
How do you Prevent Pass-the-Hash Attacks,
<https://www.beyondtrust.com/resources/glossary/pass-the-hash-ptb-attack>
- [21] Insider Threat Security Blog,
Running laps in the race to security,
<https://blog.stealthbits.com/running-laps-in-the-race-to-security/>
- [22] Microsoft Download Center,
Protección de dispositivos Windows contra ataques de canal lateral de ejecución especulativa,
<https://www.microsoft.com/en-us/download/details.aspx?id=46899>
- [23] Windows Support,
Protección de dispositivos Windows contra ataques de canal lateral de ejecución especulativa,
<https://support.microsoft.com/es-es/help/4073757/protect-windows-devices-from-speculative-execution-side-channel-attack>