GOBIERNO DE ESPAÑA
VICEPRESIDENCIA TERCERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

Webinar: Hardening básico de Linux

Material adicional

017 TU AYUDA EN CIBERSEGURIDAD
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

ÍNDICE

INDICE DE CUADROS

1. EJERCICIO PRÁCTICO

El objetivo del ejercicio es configurar el arranque y el firewall de un servidor con la instalación por defecto.

Para el arranque, la configuración que se exige es la siguiente:

- El servidor debe solicitar una contraseña para arrancar.

Y para el firewall:

- Denegar todo el tráfico entrante y saliente.
- Permitir el tráfico entrante a los servicios DNS, HTTP, HTTPS, SNMP y SSH.
- Permitir el tráfico saliente a los servicios DNS y SYSLOG.

Resolución del ejercicio:

Para la configuración del arranque primero se debe crear un *hash* de la contraseña con el comando:

- `grub-mkpasswd-pbkdf2`

Solicita una contraseña, introducimos por ejemplo "*iPSK=BZ]aav*El^N*" y nos devuelve una cadena.

La salida del comando sería una cadena parecida a la siguiente:

```
Enter password:

Reenter password:

PBKDF2 hash of your password is
grub.pbkdf2.sha512.10000.FB11E8E745C23174644A5A14726ABA1883A296AB181DEFA
33055AE739B44D91022D7EB5CDF4A2B5568EF0959220319C1BD2BB82E6D760BA84D55F95
CFDBCA86E.D23381F3EEB6E7B1F19230DFDBA2209EA0551365B13A36711CC1079E36A3D0
1494DC796BD5F6D94057E1A72FD629D5BA567A47343D985246667584BE45427FB3
```

Creamos y editamos el fichero */etc/grub.d/init-pwd* y añadimos las siguientes líneas:

```
cat <<EOF

set superusers="root"

password_pbkdf2 root
grub.pbkdf2.sha512.10000.FB11E8E745C23174644A5A14726ABA1883A296AB181DEFA
33055AE739B44D91022D7EB5CDF4A2B5568EF0959220319C1BD2BB82E6D760BA84D55F95
CFDBCA86E.D23381F3EEB6E7B1F19230DFDBA2209EA0551365B13A36711CC1079E36A3D0
1494DC796BD5F6D94057E1A72FD629D5BA567A47343D985246667584BE45427FB3

EOF
```

Guarda y le damos permisos de ejecución:

```
chmod +x /etc/grub.d/init-pwd
```

Para la configuración del FW, para denegar todo el tráfico debemos ejecutar los siguientes comandos:

```
ufw default deny incoming

ufw default deny outgoing

ufw default deny routed
```

Para habilitar los servicios en el servidor: DNS, HTTP, HTTPS, SNMP y SSH

```
ufw allow in 53/tcp para DNS

ufw allow in 53/udp para DNS

ufw allow in 80/tcp para HTTP

ufw allow in 443/tcp para HTTPS

ufw allow in 161/udp para SNMP

ufw allow in 22/tcp para SSH
```

Y por último para habilitar el acceso a servicios DNS y SYSLOG:

```
ufw allow out to any port 53

ufw allow out to any port 514
```

2. EJERCICIO DE INVESTIGACIÓN

Dado el siguiente fichero de configuración de sudo, el usuario básico incibe tendría permisos de *root* para ejecutar solo el comando /usr/bin/vim ¿Podría el usuario incibe obtener una consola de comandos como *root* y ejecutar cualquier comando como tal? Si es posible, ¿Qué medidas hay que tomar para evitar este tipo de vulnerabilidades?

```
# User privilege specification
root    ALL=(ALL:ALL) ALL
incibe ALL=(ALL:ALL) /usr/bin/vim

# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL
```

Cuadro 1 Configuración de sudo

- **Pista**: Revisar opciones del comando /usr/bin/vim

Resolución del ejercicio: el usuario incibe tiene permisos para ejecutar el binario */usr/bin/vim* con elevación de privilegios. "Vim" es un editor de texto que permite la opción de ejecutar una consola de comandos desde el mismo. Para ello ejecuta el comando

- `sudo /usr/bin/vim prueba.txt`

Una vez en el editor de texto ejecutamos

- `:sh`

Y obtenemos una consola de comandos como *root*.

Otra opción es editar el fichero */etc/shadow*

- `sudo /usr/bin/vim /etc/shadow`

Y cambiar directamente la contraseña de *root*, elevar privilegios con "*su*" y obtener consola interactiva con el usuario *root*.

Para evitar este tipo de vulnerabilidades, siempre se debe asegurar que el comando o comandos que se le permite ejecutar a un usuario como *root*, no permita obtener *shells* dinámicas o un parámetro que permita ejecutar comandos, ni editar ficheros sensibles del sistema.