# Bloque 1: Seguridad de los usuarios

## Ejercicio L5B1\_LYNIS1: Evaluación del nivel de seguridad actual

sudo lynis audit system > lynis\_$(date +%d\_%m\_%y).txt -> genera un fichero llamado lynis\_fecha actual, con un informe del sistema, donde veremos el indice de hardening de la máquina

## Ejercicio L5B1\_SINGLEUSER: Cuentas y acceso: Evitar el modo de usuario único (single user mode)

CIS benchmark 1.4.3 Ensure authentication required for single user mode.

# significa que estoy con el usuario root

sudo grep -Eq '^root:\$[0-9a-z]' /etc/shadow || echo "root is locked"

devuelve root is locked -> root no tiene contraseña

sudo passwd root

el comando de grep esta mal porque no pilla yesscript asi que hay que modificarlo

su -> cambiar a root

## Ejercicio L5B1\_BANNER: Banners de advertencia

• 1.7.1 Ensure message of the day is configured properly.

• 1.7.2 Ensure local login warning banner is configured properly.

• 1.7.3 Ensure remote login warning banner is configured properly.

grep -Eis "(\\\v|\\\r|\\\m|\\\s|$(grep '^ID=' /etc/os-release | cut -d= -f2 | sed -e 's/"//g'))" /etc/motd busca en el motd (message of the day) que es el banner de

bienvenida si en alguna linea esta la version del SO

\*\*ESTÁ MAL\*\* no tenemos motd, sino motd\_script

cat /etc/issue

grep -E -i "(\\\v|\\\r|\\\m|\\\s|$(grep '^ID=' /etc/os-release | cut -d= -f2 | sed -e 's/"//g'))" /etc/issue

si devuelven resultado -> echo "Authorized uses only. All activity may be monitored and reported." > /etc/issue

cat /etc/issue.net

grep -E -i "(\\\v|\\\r|\\\m|\\\s|$(grep '^ID=' /etc/os-release | cut -d= -f2 | sed -e 's/"//g'))" /etc/issue.net

si devuelven resultado -> echo "Authorized uses only. All activity may be monitored and reported." > /etc/issue.net

## Ejercicio L5B1\_SECSSH: Seguridad adicional para OpenSSH

copia de seguridad:

sudo cp /etc/ssh/sshd\_config /etc/ssh/sshd\_config.factory-defaults

sudo chmod a-w /etc/ssh/sshd\_config.factory-defaults

copiar el script a un archivo script, hacer chmod +x script y ./script

5.2 Configure SSH Server

## Ejercicio L5B1\_PAM: Configuración segura del módulo PAM

apt install libpam-pwquality

editar /etc/security/pwquality.conf y descomentar y editar las lineas minlen=14 y minclass=4

comprobar la salida de grep '^\s\*minlen\s\*' /etc/security/pwquality.conf

grep '^\s\*minclass\s\*' /etc/security/pwquality.conf

• 5.4.1 Ensure password creation requirements are configured.

• 5.4.2 Ensure lockout for failed password attempts is configured.

• 5.4.3 Ensure password reuse is limited.

• 5.4.4 Ensure password hashing algorithm is SHA-512.

• 5.4.5 Ensure all current passwords uses the configured hashing algorithm.

## Ejercicio L5B1\_PWDAGE: Antigüedad de la contraseña y cuentas inactivas

• 5.5.1.1 Ensure password expiration is 365 days or less.

• 5.5.1.2 Ensure minimum days between password changes is configured.

• 5.5.1.3 Ensure password expiration warning days is 7 or more.

• 5.5.1.4 Ensure inactive password lock is 30 days or less.

• 5.5.1.5 Ensure all users last password change date is in the past

## Ejercicio L5B1\_LOGONROOT: Restringir los inicios de sesión de cuentas de root y de servicios del sistema

5.5.2 Ensure system accounts are secured

6.2.10 Ensure root is the only UID 0 account

## Ejercicio L5B1\_COMMONPWD: Evitar el uso de contraseñas comunes

• Instala: sudo apt-get install libpam-cracklib -y

• Descargue la lista de contraseñas comunes:

sudo wget https://raw.githubusercontent.com/danielmiessler/SecLists/master/Passwords/xato-net10-million-passwords-1000000.txt /usr/share/dict/ -O /usr/share/dict/million.txt

• Hacer cumplir el contenido de la lista: sudo create-cracklib-dict /usr/share/dict/million.txt

# Bloque 2: Seguridad de los procesos

## Ejercicio L5B2\_COMPILERS: Compiladores

Hay que deshabilitar todos los compiladores

chmod 000 /usr/bin/byacc

chmod 000 /usr/bin/yacc

chmod 000 /usr/bin/bcc

chmod 000 /usr/bin/kgcc

chmod 000 /usr/bin/cc

chmod 000 /usr/bin/gcc

chmod 000 /usr/bin/\*c++

chmod 000 /usr/bin/\*g++

## Ejercicio L5B2\_COREDUMPS: Deshabilitar volcados de memoria del núcleo (core dumps)

1.5.4 Ensure core dumps are restricted

## Ejercicio L5B2\_APPARMOR: Manejo de AppArmor

1.6.1.1 Ensure AppArmor is installed

1.6.1.3 Ensure all AppArmor Profiles are in enforce or complain mode

*Buscar y aplicar perfiles de AppArmor deshabilitados*

Podemos comprobar si hay perfiles deshabilitados en la carpeta /etc/apparmor.d/disable. Puedes encontrar aquí dos perfiles deshabilitados: Firefox y Rsyslogd. Como Firefox es una aplicación “sensible”, debemos habilitarla siguiendo este procedimiento.

• Instala este paquete: sudo apt install apparmor-utils

• Desde un terminal, escribe: sudo aa-enforce /etc/apparmor.d/usr.bin.firefox

• Si quieres deshabilitarlo de nuevo, haz: sudo ln -s /etc/apparmor.d/usr.bin.firefox /etc/apparmor.d/disable/ sudo apparmor\_parser -R /etc/apparmor.d/usr.bin.firefox

## Ejercicio L5B2\_SECAPT: Instalar software de seguridad apt

## Ejercicio L5B2\_PACCT: Contabilidad de procesos

• Instala el paquete acct: sudo apt install acct

• Crea un archivo de log: sudo touch /var/log/pact

• Activa contabilidad de procesos: sudo accton /var/log/pacct

# Bloque 3. Seguridad de redes en un host

## Ejercicio L5B3\_NETSTACK: Configuración de la pila de red de un servidor individual

• 3.1 Disable unused network protocols and devices

o 3.1.1 Ensure system is checked to determine if IPv6 is enabled

o 3.1.2 Ensure wireless interfaces are disabled

• 3.2 Network Parameters (Host Only)

o 3.2.1 Ensure packet redirect sending is disabled

o 3.2.2 Ensure IP forwarding is disabled

• 3.3 Network Parameters (Host and Router)

o 3.3.1 Ensure source routed packets are not accepted

o 3.3.2 Ensure ICMP redirects are not accepted

o 3.3.3 Ensure secure ICMP redirects are not accepted

o 3.3.4 Ensure suspicious packets are logged

o 3.3.5 Ensure broadcast ICMP requests are ignored

o 3.3.6 Ensure bogus ICMP responses are ignored

o 3.3.7 Ensure Reverse Path Filtering is enabled

o 3.3.8 Ensure TCP SYN Cookies is enabled

o 3.3.9 Ensure IPv6 router advertisements are not accepted

## Ejercicio L5B3\_RAREPROT: Deshabilitar protocolos de red poco comunes

• 3.4 Uncommon Network Protocols

o 3.4.1 Ensure DCCP is disabled

o 3.4.2 Ensure SCTP is disabled

o 3.4.3 Ensure RDS is disabled

O 3.4.4 Ensure TIPC is disabled

# Bloque 4: Log y monitorización

## Ejercicio L5B4\_AUDIT: Configurar reglas de auditoría

• 4 Logging and Auditing

o 4.1 Configure System Accounting (auditd)

§ 4.1.1 Ensure auditing is enabled

• 4.1.1.1 Ensure auditd is installed

• 4.1.1.2 Ensure auditd service is enabled

• 4.1.1.3 Ensure auditing for processes that start prior to auditd is enabled

• 4.1.1.4 Ensure audit\_backlog\_limit is sufficient

§ 4.1.2 Configure Data Retention

• 4.1.2.1 Ensure audit log storage size is configured

• 4.1.2.2 Ensure audit logs are not automatically deleted

• 4.1.2.3 Ensure system is disabled when audit logs are full

§ 4.1.3 Ensure events that modify date and time information are collected

§ 4.1.4 Ensure events that modify user/group information are collected (Scored)

§ 4.1.5 Ensure events that modify the system's network environment are collected

§ 4.1.6 Ensure events that modify the system's Mandatory Access Controls are § collected

§ 4.1.7 Ensure login and logout events are collected

§ 4.1.8 Ensure session initiation information is collected

§ 4.1.9 Ensure discretionary access control permission modification events are § collected

§ 4.1.10 Ensure unsuccessful unauthorized file access attempts are collected

§ 4.1.11 Ensure use of privileged commands is collected

§ 4.1.12 Ensure successful file system mounts are collected

§ 4.1.13 Ensure file deletion events by users are collected

§ 4.1.14 Ensure changes to system administration scope (sudoers) is collected

§ 4.1.15 Ensure system administrator actions (sudolog) are collected

§ 4.1.16 Ensure kernel module loading and unloading is collected

§ 4.1.17 Ensure the audit configuration is immutable

## Ejercicio L5B4\_SYSSTAT: Instalar sysstat para ver el consumo de recursos

sudo apt install sysstat

• iostat informa de estadísticas de CPU y de entrada/salida para dispositivos de bloque y particiones.

• mpstat informa de estadísticas individuales o combinadas relacionadas con el procesador.

• pidstat informa de estadísticas para tareas (procesos) de Linux: E/S, CPU, memoria, etc.

• tapestat informa de estadísticas de unidades de cinta conectadas al sistema.

• cifsiostat informa de estadísticas de CIFS (Common Internet File System).

## Ejercicio L5B4\_GLANCES: Instalar glances

sudo apt install glances y usarlo ejecutando glances en la línea de comandos.

## Ejercicio L5B4\_LYNIS2: Evaluación del nivel de seguridad final con Lynis

Evaluar Lynis como al principio para ver si ha mejorado el hardening

## Ejercicio L5B4\_WAZUH: HIDS gracias a una XDR profesional: Wazuh como monitorización de archivos, procesos y usuarios

Cómo instalar un HIDS:

• 1.3 Filesystem Integrity Checking

o 1.3.1 Ensure AIDE is installed (Automated)

o 1.3.2 Ensure filesystem integrity is regularly checked (Automated)

• Haz el clon enlazado de la MV de la asignatura como te indicamos al principio del laboratorio, con 6Gb de RAM y 4 cores

• Hay varias formas de instalar Wazuh, pero la mejor en nuestro caso es Wazuh-Docker, que lo instala usando el mismo sistema que nosotros usamos en la asignatura para desplegar los laboratorios. Las instrucciones concretas las puedes encontrar aquí: https://documentation.wazuh.com/current/deployment-options/docker/wazuh-container.html, y de ellas tienes que asegurarte de lo siguiente:

o El tipo de instalación que vamos a hacer es Single-node deployment. Es igual de funcional que la otra, pero con todo en una máquina (no tenemos recursos para hacer una instalación distribuida).

o En el paso de generar los certificados, nos da dos opciones: generarlos o aportarlos nosotros. En este caso es mejor generarlos con el software que nos proporcionan (generate-indexer-certs.yml). Asegúrate de ejecutarlo una vez antes de lanzar Wazuh como indica la web. No es necesario cambiar ningún fichero de los que proporcionan.

• Lanzar ahora el XDR como indica el tutorial, yendo al directorio donde has descomprimido los contenidos del git y tecleando docker-compose up -d. Por favor, espera unos 30 segundos hasta que todo el sistema se ponga en marcha. Cuando todo esté listo, deberías poder acceder al XDR abriendo el navegador de la MV y yendo a la dirección https://127.0.0.1. La cuenta de usuario por defecto es “admin” y la password “SecretPassword”.

### Wazuh funcionando como HIDS

Un agente se encarga de

• La recopilación de información del sistema en el que está instalado

• Estar configurado para recopilar diferentes tipos de información (cosas como los diferentes logs de las acciones que se producen, firmas de archivos... todo lo que necesitas)

• Enviárselo al XDR mediante comunicaciones cifradas fuertes. De hecho, si juegas un poco con la GUI puedes ver el algoritmo que usa para enviar la información.

Wazuh nos los genera por nosotros.

Hacemos clic en el mensaje que se queja de que no hay agentes y configuramos uno nuevo para monitorizar nuestra propia MV, seleccionando la creación de un agente .deb de 64 bits para Ubuntu con estas características:

Interfaz de usuario gráfica, Texto, Aplicación, Teams

Descripción generada automáticamente

Desde una terminal de nuestra MV copiamos los comandos que nos da el propio Wazuh para instalarlo y arrancarlo. Con esto, Wazuh debería mostrar que tiene 1 agente activo y empezará a recopilar información de la propia máquina que lo ejecuta. Ni que decir tiene que monitorizar más máquinas es lo mismo, y solo tendríamos que indicar la IP donde está la MV en la que has arrancado Wazuh al generar el agente, obviamente asumiendo que dicha IP es alcanzable desde la máquina a vigilar.

Texto

Descripción generada automáticamente

Con esta configuración le estamos diciendo a OSSEC que monitorice todos los cambios en tiempo real de los directorios /etc, /usr/bin y /usr/sbin, que contienen programas ejecutables críticos del SO.

Después, reiniciamos el agente de la MV

sudo systemctl restart wazuh-agent

Y ya podremos detectar los cambios en los ficheros de esos directorios

Para probar:

• Haz un sudo a un comando, pero mete mal la clave para que falle

• Haz un sudo, pero esta vez correcto

• Instala algo con apt o actualiza el SO

• Edita el fichero /etc/passwd y cambia el shell del usuario root de nologin a /bin/bash.