Pràctica 4: Auditories de seguretat

Objectius

Aquesta pràctica té com a objectiu utilitzar 2 eines de Linux per realitzar informes que permeten auditar la seguretat del sistema Linux. En concret, permeten comprovar l'estat dels permisos de directoris i fitxers, auditar la configuració i estat dels principals serveis (cron, ssh, NFS, SAMBA, LDAP, FTP, NTP, etc..), auditar comptes d'usuaris i contrasenyes, auditar groups, executar rootkits, auditar l'estat dels arxius de log, si hi ha backups, fer comprovacions de l'estat de directoris importants com el directori /, etc.. Un cop realitzades totes les comprovacions, genera un fitxer que pot ser utilitzar per auditar l'estat del sistema i la seva seguretat.

NOTA: Treballa amb la màquina **asix2m01uf4pr3** que vaig passar-vos per fer les pràctiques de logs i monitorització.

Exercici 1: Creació d'una auditòria de seguretat amb l'eina Tiger

a) Actualitza la llista de programes disponibles des del dipòsits. Executa: **sudo aptitude update**

b) Instal·la **Tiger.** Executa: **sudo aptitude install tiger** i respon:
- A la primera pregunta només pots respondre OK
- Do you wish to create/use your site key passphrase during installation? → Yes
- Rebuild Tripwire configuration file? → Yes
- Enter site-key passphrase: FjeClot2020#
- Enter local key passphrase: ClotFje0202@

c) Executa l'escaneig per defecte de Tiger. Executa: **sudo tiger** . Aquest procés pot durar uns minuts, sobretot la part de **system specific checks**. Al final de l'escaneig Tiger indica a quin directori i amb quin nom s'ha desat l'informe.

d) Com usuari **asix2** obre amb **geany** el fitxer de l'informe generat per **Tiger**. Indica:
- Quantes línies té l'informe?
- D'acord amb l'informe, hi ha cap problema amb les contrasenyes?. Quin és el problema?. Mostra la línia a on ho indica.
- Penseu que s'han de canviar les contrasenyes?. Per què?
- Dóna cap avís sobre el directori **/var/mail**?. Quin és l'avis?. Mostra la línia a on ho indica.
- Dóna cap avis sobre el programa **/usr/bin/passwd**. Quin és. Mostra la línia a on ho indica.
- Penseu que s'han de canviar els permisos de **/usr/bin/passwd**?. Per què?
- Dóna cap avis sobre el gestor d'arrancada **GRUB**?. Quin és. Mostra la línia a on ho indica.
- S'ha configurat cap firewall?. Mostra la línia a on ho indica.

Exercici 2: Creació d'una auditòria de seguretat amb l'eina Lynis

a) Actualitza la llista de programes disponibles des del dipòsits. Executa: **sudo aptitude update**

b) Instal·la **Lynis**. Executa: **sudo aptitude install lynis**

c) Executa l'escaneig per defecte de Lynis. Executa: **sudo lynis audit system**

d) Com usuari **asix2** obre amb **geany** el fitxer de l'informe generat que es troba a **/var/log/**. Indica:
- Comprova si el Kernel instal·lat és la darrera versió de kernel disponible. Has de buscar una línia que indiqui que s'ha executat el test KRNL-5788 i llegir les línies que hi ha a continuació. Mostra les línies que indiquen la versió instal·lada, la versió candidata disponible i el resultat.
- Comprova si hi ha més d'un usuari amb UID=0 a part de root. Busca el test AUTH-9204. Mostra la lína que indica el resultat. Per què s'ha de buscar aquest tipus de compte?
- Comprova si tots els comptes d'usuaris són únics. Busca el test AUTH-9208. Mostra la lína que indica el resultat. Per què s'han de buscar si els comptes d'usuaris són únics?.

- Comprova el test STRG-1928. Indica un servei que possiblement no cal que es trobi en execució. Indica el motiu. Mostra les línies que ho indiquen.
- Comprova el test HTTP-6643. Quin mòdul d'apache2 instal·laries per millorar la seguretat contra atacs?. Mostra la lína que ho indica.
- Comprova el test SSH-7408. Busca dins del test el Port que utilitza SSH. Indica si és una bona configuració d'acord amb Lynis. Mostra la lína que ho indica.

Exercici 3: Comprova paquets vulnerables amb debsecan

a) Actualitza la llista de programes disponibles des del dipòsits. Executa: **sudo aptitude update**

b) Instal·la **Debian Security Analyzer**. Executa: **sudo aptitude install debsecan**

c) Executa l'escaneig de paquets per defecte de **Debian Security Analyzer** per Debian 10.1 (Buster). Passa a ser **root** i executa: **debsecan --suite buster > /var/log/debsecan.log**

d) Com usuari **asix2** obre amb **geany** el fitxer de l'informe generat. Indica:
- El servei CUPS del sistema té alguna vulnerabilitat coneguda. Ha estat solucionada. Mostra la línia que dóna aquesta informació.
- Quantes vulnerabilitats conegudes té la versió del paquet samba-common instal·lada en el sistema?.
- Quina vulneralibilitat té el paquet telnet instal·lat en el sistema. Indica el codi, la seva severitat i una breu descripció de la vunerabilitat. Per trobar aquesta informació accedeix a la següent web: **https://nvd.nist.gov/vuln/search**. Què faries amb aquest paquet?
- Hi ha cap vulnerabilitat del bash?. Quin és el seu codi?. Quin és el seu estat?. Mostra la línia que dóna aquesta informació.

Indicacions

Forma de lliurament de l'informe
1- Treball individual
2- El nom del fitxer ha de tenir el següent format **asix2_*cognom_nom_m01uf4pr4.pdf***
3- Envieu la solució proposada per correu electrònic:
Adreça: ***cf@collados.org***
Assumpte: ***asix2_cognom_nom_m01uf4pr4***
4- La **data límit** de lliurament de la pràctica és el **dilluns** dia **5/05/20** a les **12 de la nit**
5- Format Lletra: **Arial 10**
6- Marges (superior, inferior, esquerra, dreta): **2cm**

Respostes
El **dilluns** dia **6-4-20** penjaré les solucions.