Hardening de Sistemas – Fortalecimiento de Servidores y Redes

Fase 1: Análisis inicial del estado del sistema

• Evaluación del sistema con Lynis:

Para auditar el servidor, se utiliza la herramienta Lynis:

```
sudo apt install lynis
sudo lynis audit system
```

• Revisión manual de configuraciones críticas:

Se analizan los archivos /etc/ssh/sshd_config, /etc/passwd, /etc/shadow y /etc/sudoers.

• Servicios activos en el sistema:

```
systemctl list-units --type=service
netstat -tulpn
```

• Búsqueda de configuraciones por defecto y módulos innecesarios:

Se revisan los módulos del kernel con:

```
lsmod
```

Fase 2: Refuerzo de configuración de acceso y autenticación

• Deshabilitar acceso SSH como root:

Editar /etc/ssh/sshd_config y cambiar:

```
PermitRootLogin no
```

• Forzar autenticación por clave pública:

Se debe tener configurado el archivo ~/.ssh/authorized_keys en el servidor.

• Caducidad y bloqueo de contraseñas:

sudo chage -M 90 usuario
sudo pam_tally2 --user usuario
sudo faillock --user usuario

• Mensaje legal de advertencia:

Configurar en /etc/issue.net:

Advertencia: Acceso no autorizado será perseguido.

Fase 3: Desactivación de servicios no esenciales y endurecimiento del kernel

• Desactivar servicios innecesarios:

sudo systemctl disable cups
sudo systemctl disable avahi-daemon
sudo systemctl disable nfs-server

• Configurar parámetros de seguridad en /etc/sysctl.conf:

net.ipv4.conf.all.rp_filter = 1
net.ipv4.tcp_syncookies = 1
net.ipv4.conf.all.accept_redirects = 0

• Aplicar cambios:

sudo sysctl -p

Fase 4: Protección de archivos y estructuras del sistema

• Revisar permisos de archivos sensibles:

sudo chmod 600 /etc/shadow
sudo chmod 644 /etc/passwd
sudo chown root:root /var/log
sudo chmod 750 /var/log

• Activar auditd para auditoría del sistema:

```
sudo apt install auditd
sudo systemctl enable auditd
```

• Configurar AIDE para detección de integridad:

```
sudo apt install aide
sudo aideinit
sudo cp /var/lib/aide/aide.db.new /var/lib/aide/aide.db
sudo aide --check
```

Fase 5: Seguridad de red y detección de intrusiones

• Activar firewall con UFW:

```
sudo apt install ufw
sudo ufw default deny incoming
sudo ufw default allow outgoing
sudo ufw allow OpenSSH
sudo ufw enable
```

• Configurar fail2ban:

```
sudo apt install fail2ban
sudo systemctl enable fail2ban
```

Editar jail.local para configurar filtros personalizados.

• Detección de conexiones anómalas:

Instalar y configurar psad o portsentry:

```
sudo apt install psad
sudo apt install portsentry
```

• Revisar logs y configurar alertas automáticas:

```
journalctl -xe
tail -f /var/log/auth.log
```