Fortalecimiento de Servidores y Redes para Codearts Solutions

---

Fase 1: Análisis inicial del estado del sistema

sudo apt update && sudo apt install lynis net-tools -y

sudo lynis audit system

sudo nano /etc/ssh/sshd_config

sudo nano /etc/passwd

sudo nano /etc/shadow

sudo nano /etc/sudoers

systemctl list-units --type=service

netstat -tulpn

lsmod   # Ver módulos del kernel

Fase 2: Refuerzo de acceso y autenticación

Deshabilitar root login

sudo nano /etc/ssh/sshd_config

Cambiar o añadir: PermitRootLogin no

Forzar autenticación por clave pública

Añadir: PasswordAuthentication no

Copiar clave pública al servidor:

ssh-copy-id usuario@servidor

Caducidad de contraseñas

sudo chage -l usuario

sudo chage -M 90 -W 7 -I 30 usuario

Bloqueo tras intentos fallidos

sudo apt install libpam-modules-bin -y

sudo nano /etc/pam.d/common-auth

Añadir: auth required pam_tally2.so deny=5 unlock_time=600

Mensaje legal

echo "Acceso autorizado solo para personal de Codearts Solutions" | sudo tee /etc/issue.net

sudo nano /etc/ssh/sshd_config

Banner /etc/issue.net

Fase 3: Desactivación de servicios y endurecimiento del kernel

Desactivar servicios innecesarios

sudo systemctl stop cups avahi-daemon nfs-server

sudo systemctl disable cups avahi-daemon nfs-server

Configuraciones del kernel

sudo nano /etc/sysctl.conf

Añadir:

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 sistema

Permisos correctos

sudo chmod 600 /etc/shadow

sudo chmod 644 /etc/passwd

sudo chown root:root /var/log

sudo chmod 750 /var/log

Auditoría

sudo apt install auditd -y

sudo systemctl enable --now auditd

AIDE

sudo apt install aide -y

sudo aideinit

sudo mv /var/lib/aide/aide.db.new.gz /var/lib/aide/aide.db.gz

---

Fase 5: Seguridad de red y detección de intrusos

UFW

sudo apt install ufw -y

sudo ufw default deny incoming

sudo ufw default allow outgoing

sudo ufw allow ssh

sudo ufw enable

Fail2ban

sudo apt install fail2ban -y

sudo systemctl enable --now fail2ban

sudo cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local

sudo nano /etc/fail2ban/jail.local

PSAD (o portsentry)

sudo apt install psad -y

sudo systemctl enable --now psad

sudo psad --sig-update

Revisar logs sospechosos

sudo tail -f /var/log/auth.log