sop_server_hardening

Zerbitzariaren Indartze SOP (Debian 12 Kopiatu eta Itsatsi)

Helburua: Zerbitzari Guztiak (App, Data, SecOps, OT) **Erabiltzailea:** Root

1. Sistema Oinarrizko Segurtasuna

Exekutatu komando hauek zerbitzari bakoitzean instalazioa amaitu bezain laster.

```
# 1. Eguneratu eta Instalatu Tresnak
apt update && apt upgrade -y
apt install -y ufw fail2ban curl git htop

# 2. Sortu Root Ez den Erabiltzailea (Interaktiboa)
adduser admin
usermod -aG sudo admin

# 3. Segurtatu Memoria Partekatua
echo "tmpfs /run/shm tmpfs defaults,noexec,nosuid 0 0" >> /etc/fstab
mount -o remount /run/shm
```

2. SSH Indartzea (Kritikoa)

Errotze saioa eta pasahitz erasoak saihesten ditu.

```
# Sortu Indartze Konfigurazio Fitxategia (Debian 12 metodoa)
cat <<EOF > /etc/ssh/sshd_config.d/99-hardening.conf
PermitRootLogin no
PasswordAuthentication no
X11Forwarding no
EOF

# Berrabiarazi SSH
systemctl restart sshd
```

Abisua: Ziurtatu SSH gakoak konfiguratuta dituzula admin *erabiltzailearentzat pasahitzak desgaitu aurretik! Gakoak oraindik ez badituzu konfiguratu, aldi baterako erabili* PasswordAuthentication yes *eta aldatu geroago.*

3. Ostoko Firewall-a (UFW) Konfigurazioa

ZG-App-rako (Web Zerbitzaria)

```
ufw default deny incoming
ufw default allow outgoing
ufw allow ssh
ufw allow 80/tcp
ufw allow 443/tcp
ufw enable
```

ZG-Data-rako (Datu-basea)

```
ufw default deny incoming
ufw default allow outgoing
ufw allow ssh
# Utzi Postgres App Zerbitzaritik soilik
ufw allow from 192.168.20.10 to any port 5432
# Utzi Redis App Zerbitzaritik soilik
ufw allow from 192.168.20.10 to any port 6379
ufw enable
```

ZG-SecOps-rako (Wazuh)

```
ufw default deny incoming
ufw default allow outgoing
ufw allow ssh
ufw allow 443/tcp    # Wazuh Dashboard
ufw allow 1514/tcp   # Agenteen komunikazioa
ufw allow 1515/tcp   # Matrikulazioa
ufw enable
```

ZG-OT-rako (Industriala)

```
ufw default deny incoming
ufw default allow outgoing
ufw allow ssh
ufw allow 8080/tcp   # OpenPLC Web
ufw allow 502/tcp    # Modbus
ufw enable
```

4. Fail2Ban Konfigurazioa

Babestu SSH indar brutu erasotik.

```
# Sortu konfigurazio lokala
cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local

# Gaitu SSH jail-a
cat <<EOF >> /etc/fail2ban/jail.local
[sshd]
enabled = true
port = ssh
filter = sshd
logpath = /var/log/auth.log
maxretry = 3
bantime = 3600
EOF

systemctl restart fail2ban
systemctl enable fail2ban
```