# Linux Guvenlik Temelleri

**1. Soru: Bir kullanıcı için sudo yetkilerini yalnızca belirli bir komutu çalıştırabilecek şekilde kısıtlayın. Kullanıcının systemctl restart apache2 komutunu koşabilmesi gerekiyor ancak diğer komutlara erişimi olmamalı.**

```
# /etc/sudoers dosyasına şu satır eklenir:
user_name ALL=(ALL) NOPASSWD: /bin/systemctl restart apache2
```

**2. Soru: Bir Linux sisteminde /etc/shadow dosyasına yetkisiz erişimi engellemek için hangi dosya izinleri uygulanmalıdır?**

```
chmod 640 /etc/shadow
chown root:shadow /etc/shadow
```

**3. Soru: Bir dizindeki (örneğin /secure_data) tüm dosyaların sadece belirli bir gruba ait olmasını zorunlu kılacak şekilde otomatik grup sahipliği uygulanmasını sağlayın.**

```
chgrp securegroup /secure_data
chmod g+s /secure_data
```

**4. Soru: Bir kullanıcı hesabını belirli bir süre sonra otomatik olarak kilitlemek için hangi ayar yapılmalıdır? Kullanıcının hesabı 30 gün sonra kilitlenmelidir.**

```
chage -E $(date -d "+30 days" +%Y-%m-%d) user_name
```

**5. Soru: SSH için port değiştirme, root girişini engelleme ve yalnızca belirli bir IP adresine izin verme ayarlarını yapın.**

```
# /etc/ssh/sshd_config dosyasında aşağıdaki değişiklikleri yapın:
Port 2222
PermitRootLogin no
AllowUsers user_name@192.168.1.100

# Değişikliklerden sonra SSH hizmetini yeniden başlatın:
systemctl restart sshd
```

**6. Soru: Bir Linux sunucusunda belirli bir dizine erişim için chroot ortamı oluşturun ve bir kullanıcıyı bu ortamda sınırlandırın.**

1. Chroot ortamı için dizin oluşturun:
   ```
   mkdir -p /chroot_env/{bin,lib}
   ```
2. Gerekli komutları ve kütüphaneleri chroot ortamına kopyalayın.
3. Kullanıcıyı bu dizine kilitleyin ve shell olarak /bin/bash belirtin.

**7. Soru: Fail2ban kurarak SSH üzerinde 5 hatalı denemeden sonra IP adreslerini 1 saatliğine engelleyecek bir kural yazın.**

```
# /etc/fail2ban/jail.local dosyasında aşağıdaki ayarları yapın:
[sshd]
enabled = true
maxretry = 5
bantime = 3600
```

```
systemctl restart fail2ban
```

**8. Soru: Bir dosyanın hash değerini alıp bu değeri kaydeden ve daha sonra dosyada bir değişiklik yapılıp yapılmadığını kontrol eden bir script yazın.**

```
#!/bin/bash
file="/path/to/file"
hash_file="/path/to/hashfile"

if [ "$1" == "--save" ]; then
   sha256sum $file > $hash_file
   echo "Hash kaydedildi."
elif [ "$1" == "--check" ]; then
   sha256sum -c $hash_file
else
   echo "Kullanım: $0 --save|--check"
fi
```

**9. Soru: Bir sistemde root yetkisi gerektiren belirli bir komutun (örneğin, reboot) koşturulması sırasında log kaydı oluşturulmasını sağlayın.**

```
# Komut için bir alias oluşturun ve log kaydı yapın:
alias reboot='logger "Reboot command executed by $(whoami)" && /sbin/reboot'
```

**10. Soru: Bir sistemde USB cihazların takılmasını tamamen engelleyen bir ayar yapın.**

```
echo "blacklist usb-storage" > /etc/modprobe.d/usb-storage.conf
```

**11. Soru: Belli bir dizindeki dosyaların sadece okunabilir olmasını zorunlu kılacak bir ayar yapın.**

```
chmod -R a-w /path/to/directory
```

**12. Soru: Bir sistemde kernel modüllerinin yüklenmesini engelleyecek bir ayar yapın.**

```
echo 1 > /proc/sys/kernel/modules_disabled
```