FUNDAMENTOS DE SEGURIDAD EN LINUX

OpenWebinars

ÍNDICE

INTRODUCCIÓN

- Protección de sistemas
- Requiere configuración
- Múltiples herramientas

¿QUÉ ES UN FIREWALL?

- Control del tráfico de red
- Reglas definidas o terminal
- Ejemplos:
  - iptables
  - ufw

IPTABLES

- Control avanzado de red
- Por terminal:

```
iptables -A INPUT -p tcp --dport 80 -j ACCEPT

iptables -A INPUT -p tcp --dport 80 -s 10.0.1.1 -j REJECT
```

UFW

- Uncomplicated firewall
- Interfaz simple de iptables
- Ejemplos:

    ufw enable

    ufw allow 80/tcp

    ufw status

¿QUÉ ES APPARMOR?

- Control de acceso a procesos
- Permite usar recursos a una aplicación
- Ruta: /etc/apparmor.d/

APPARMOR

- Estado AppArmor

  apparmor_status

APPARMOR

- Habilitar y activar AppArmor

  systemctl enable apparmor

  systemctl start apparmor

APPARMOR

- Habilitar un perfil

  apparmor_parser -r
  /etc/apparmor.d/perfil

¿QUÉ ES SELINUX?

- Security-Enhanced Linux
- Políticas de control de acceso por usuario, grupo o proceso
- Ruta: /etc/selinux/config

SELINUX

- Ver el estado de SELinux:

  sestatus

- Cambiar el modo de SELinux:

  sudo setenforce 1 # Permissive mode

  sudo setenforce 0 # Enforcing mode

BUENAS PRÁCTICAS SEGURIDAD

- Mantener el sistema actualizado
- Configurar y revisar las políticas de firewall

BUENAS PRÁCTICAS SEGURIDAD

- Usar herramientas como AppArmor, SELinux
- Monitorizar logs y eventos de seguridad