**UNIVERSIDAD AUTÓNOMA DE BAJA CALIFORNIA**

FACULTAD DE CIENCIAS QUÍMICAS E INGENIERÍA PROGRAMA DE
INGENIERO EN SOFTWARE Y TECNOLOGÍAS EMERGENTES

**Gestión y Seguridad en Redes**

# ¿Como fortalecer un servidor Linux y Windows?

**25 de Septiembre 2023**

---

**Docente:**
Felicitas Perez Ornelas

**Participante(es):**
Luis Eduardo Galindo Amaya (1274895)

# Índice

**Universidad Autónoma de Baja California**
**Facultad de ciencias químicas e ingeniería**

Ingeniero en software y tecnologías emergentes

**Información de la materia**

**Nombre de la materia y clave**: Gestión y Seguridad en Redes
**Grupo y periodo**: 571 (2023-2)
**Profesor**: Felicitas Perez Ornelas.

**Información de la actividad**

**Nombre de la actividad**: ¿Como fortalecer un servidor Linux y Windows?
**Lugar y fecha**: 25 de Septiembre 2023
**Carácter de la actividad**: Individual.

**Reporte de actividades**

# 1. Lista de verificación de refuerzo Linux

unknown unknown, s.f.

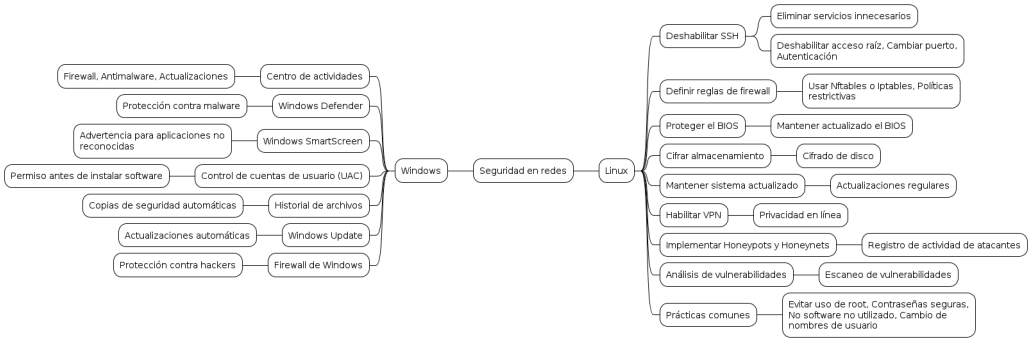
1. Deshabilitar SSH
2. Deshabilitar acceso raíz SSH
3. Cambiar puerto predeterminado de SSH
4. Deshabilitar la autenticación de contraseña SSH
5. Definir las reglas adecuadas de Nftables o Iptables
6. Implementar IDS (Sistema de detección de intrusos)
7. Asegurar el BIOS
8. Cifrar dispositivos de almacenamiento y particiones
9. Proteja el sistema contra rootkits
10. Mantenga el sistema actualizado
11. VPN (red privada virtual)
12. Habilitar SELinux (Linux con seguridad mejorada)
13. Implementar Honeypots y Honeynets
14. Análisis externo de su dispositivo en busca de vulnerabilidades

## 2. Lista de verificación de refuerzo Windows

Alex, 2021

1. Nunca conecte un servidor IIS a Internet hasta que esté completamente protegido.
2. Coloque el servidor en un lugar físicamente seguro.
3. Utilice dos interfaces de red en el servidor: una para el administrador y otra para la red.
4. Instale service packs, parches y hotfix.
5. Ejecute el kit de herramientas de cumplimiento de seguridad de Microsoft.
6. Ejecute IIS Lockdown en el servidor
7. Deshabilite los servicios de Windows innecesarios.
8. Asegúrese de que los servicios se ejecuten con los privilegios mínimos cuentas.
9. Desactive el servicio Telnet.
10. Desactive el servicio de estado ASP.NET si no lo utilizan sus aplicaciones.
11. Desactive la creación y el control de versiones distribuidos en la web si la aplicación no lo utiliza, o asegúrelo si es necesario.
12. No instale Microsoft Data Access Components (MDAC) a menos que sea específicamente necesario.
13. No instale la versión HTML de Internet Services Manager.
14. No instale Microsoft Index Server a menos que sea necesario.
15. No instale Microsoft FrontPage Server Extensions (FPSE) a menos que sea necesario.
16. Fortalezca la pila de TCP / IP.
17. Desactive NetBIOS y el bloque de mensajes del servidor: cierre los puertos 137, 138, 139 y 445.
18. Reconfigure las políticas de datos del sistema de archivos de páginas y papelera de reciclaje.
19. Configuración segura de CMOS (semiconductor complementario de óxido de metal).
20. Medios físicos seguros: unidad de CD-ROM, etc.

## 3. Diagrma




## 4. Conclusión

A lo largo de esta practica aprendi que cosas se deben tomar en cuenta para mantener un sistema operativo de manera segura, con la simplicidad de intara un sistema operativo hoy en dia se puede dar espacio no configurar adecuadamente los acesso al sistema.

## 5. Referencias

Alex. (2021). Lista de Verificación de Refuerzo del Servidor Windows IIS. https://kryptonsolid.com/lista-de-verificacion-de-refuerzo-del-servidor-windows-iis/

unknown unknown, u. (s.f.). Lista de Verificación de refuerzo de seguridad de linux. https://es.linux-console.net/?p=14823