Resumen Seguridad Activa

Objetivos del Tema

- Asimilar el principio básico de minimización de la superficie de ataque.
- Conocer la autenticación de usuarios, políticas de contraseñas y permisos.
- Identificar malware y aplicar medidas de seguridad activas.
- Aprender conceptos clave para fortalecer sistemas informáticos.

4.1 Introducción

La seguridad activa incluye medidas proactivas para proteger sistemas, redes y datos frente a amenazas internas y externas. Los aspectos clave incluyen:

- Minimizar la superficie de ataque.
- Autenticación robusta.
- Protección contra malware.
- Seguridad de redes y privacidad.
- Hardening (reforzamiento) de sistemas.

4.2 Autentificación

Conceptos Básicos

- Verifica la identidad del usuario mediante factores como algo que sabes (contraseña), algo que tienes (token) o algo que eres (biometría).
- Importancia de no iniciar sesión como administrador excepto para tareas específicas.

Política de Contraseñas

- Longitud mínima: Al menos 12 caracteres.

- Complejidad: Combinar mayúsculas, minúsculas, números y caracteres especiales.
- Caducidad: Cambiar cada 60-90 días.
- Restricciones: Limitar reutilización de contraseñas antiguas.

Verificación en Dos Pasos (2FA)

- Añade una capa adicional de seguridad mediante un segundo factor (SMS, aplicación de autenticación, biometría).
- Ventajas: Mayor protección frente a phishing y ataques de fuerza bruta.

Listas de Control de Acceso (ACL)

- Gestionan permisos de acceso a recursos basados en usuarios o grupos.
- Principios clave: Predominio de la denegación, herencia de permisos y control total para administradores.

Autenticación Centralizada

- Permite acceso unificado mediante sistemas como Active Directory (Windows) o LDAP (Linux).
- Single Sign-On (SSO): Simplifica el acceso a múltiples servicios con una sola autenticación.

Sistemas Biométricos

- Usan características únicas (huellas dactilares, reconocimiento facial) para autenticación.
- Ventajas: Alta precisión y personalización.
- Desafíos: Irreversibilidad de los datos biométricos si son comprometidos.

4.3 Malware

Tipos de Malware

- **Virus y gusanos** : Se propagan automáticamente.
- **Ransomware** : Cifra archivos y exige rescate.
- **Spyware y keyloggers** : Espían actividades del usuario.

- **Troyanos** : Se disfrazan de software legítimo.

Software de Seguridad

- Antivirus: Detecta, previene y elimina malware.
- Características clave: Detección en tiempo real, actualizaciones automáticas y protección contra phishing.

Desinfección

- **Windows** : Arrancar en modo seguro, escanear con antivirus y herramientas especializadas.
- **Linux** : Usar herramientas como ClamAV o Chkrootkit, revisar logs y restaurar desde copias de seguridad.

4.4 Hardening

- Refuerza la seguridad mediante:
  - Eliminación de servicios innecesarios.
  - Configuración de permisos estrictos.
  - Actualización constante de sistemas y aplicaciones.
- Beneficios: Reduce vulnerabilidades y mejora la resiliencia.
- Desafíos: Equilibrio entre seguridad y funcionalidad.

4.5 Actualización de Aplicaciones y Sistemas Operativos

- Razones clave: Corregir vulnerabilidades, mejorar rendimiento y cumplir normativas.
- Proceso:
  - **Windows** : Usar Windows Update y Microsoft Store.
  - **Linux** : Comandos como `sudo apt update` y `sudo apt upgrade`.

4.6 Auditorías de Seguridad

- Evalúan la seguridad de sistemas y redes.

- Elementos clave:
  - Objetivo: Identificar vulnerabilidades y evaluar riesgos.
  - Alcance: Infraestructura, aplicaciones, políticas.
  - Resultados: Documentar hallazgos y proponer mejoras.
- Beneficios: Mejora la postura de seguridad y asegura cumplimiento normativo.