ANTEPROYECTO PARA SOLICITAR LA REALIZACIÓN DEL MÓDULO PROYECTO

Nombre del proyecto: Ataque y Defensa de un entorno de Directorio Activo

Alumno: Daniel Damota Maldonado

Curso: Administración de Sistemas Informáticos en Red

Tutor: Gonzalo Cañadillas Rueda

OBJETIVOS

El objetivo principal de este proyecto es analizar y evaluar la seguridad de un entorno de Directorio Activo mediante la simulación de ataques y la implementación de mecanismos de defensa. Se busca identificar vulnerabilidades comunes, comprender las tácticas utilizadas por atacantes y proponer estrategias efectivas para proteger la infraestructura. Este proyecto será utilizado en entornos de formación y pruebas de seguridad, con el fin de mejorar las capacidades defensivas de los administradores de sistemas y equipos de seguridad informática.

PREANÁLISIS DE LO EXISTENTE

Actualmente, la gestión de la seguridad en entornos de Directorio Activo se realiza de manera estándar mediante políticas de grupo, control de acceso y monitoreo manual. Sin embargo, no siempre se cuenta con un análisis detallado de las amenazas ni con una estrategia proactiva de detección y respuesta ante ataques. En muchos casos, la evaluación de la seguridad se basa en revisiones manuales sin el uso de herramientas especializadas, lo que deja margen para errores y brechas de seguridad.

PREANÁLISIS DEL SISTEMA

El sistema sobre el que se trabajará es un entorno de Directorio Activo implementado en máquinas virtuales dentro de Proxmox. Se identificarán y abordarán los siguientes aspectos:

- Ataques: Enumeración de usuarios, explotación de vulnerabilidades, escalación de privilegios, movimientos laterales y persistencia.
- Defensas: Configuración de políticas de seguridad, implementación de herramientas de monitoreo, auditoría de eventos y respuesta ante incidentes.
- Requisitos a satisfacer: Garantizar un entorno seguro mediante configuraciones adecuadas y el uso de herramientas que permitan la detección y mitigación de ataques.

Para este proyecto se evaluarán herramientas específicas de auditoría y defensa como BloodHound, Mimikatz, Impacket, Nmap, entre otras.

PREDISEÑO DEL SISTEMA

El sistema estará compuesto por varias máquinas virtuales ejecutándose en Proxmox, distribuidas de la siguiente manera:

- Controlador de dominio: Windows Server con Active Directory configurado.
- Estaciones de trabajo: Múltiples máquinas Windows unidas al dominio.
- Máquinas de ataque: Sistemas Kali Linux y Windows.

Requisitos técnicos:

- Hardware: Servidor físico con capacidad para ejecutar múltiples máquinas virtuales con suficiente RAM, CPU y almacenamiento.
- Software:
    - Sistema de virtualización: Proxmox VE.
    - Sistemas operativos: Windows Server 2022, Windows 10/11, Kali Linux.
    - Herramientas de ataque: BloodHound, Mimikatz, Netexec, etc.
    - Herramientas de defensa: Kaspersky, Directivas de grupos, etc.

ESTIMACIÓN DE COSTES

- Hardware: Dependiendo de la infraestructura existente, se puede requerir la compra de un servidor o utilizar hardware disponible.
- Software:
    - Proxmox: Gratuito en su versión comunitaria.
    - Windows Server: Licencia requerida según las necesidades del proyecto.
    - Herramientas de seguridad: La mayoría son gratuitas o de código abierto.
- Tiempo estimado de implementación: 4 a 6 semanas.
- Recursos humanos: Administrador de sistemas y analista de seguridad.