UNIVERSIDAD MARIANO GALVEZ
FACULTAD DE INGENIERIA EN SISTEMAS
CATEDRATICO: MBA, LIC. JOSUÉ IVÁN LÓPEZ CONTRERAS
ALCANCE DEL PROYECTO FINAL

Contenido

UNIVERSIDAD MARIANO GALVEZ
FACULTAD DE INGENIERIA EN SISTEMAS
CATEDRATICO: MBA, LIC. JOSUÉ IVÁN LÓPEZ CONTRERAS
ALCANCE DEL PROYECTO FINAL

Título del Proyecto:

Integración de Firewall PfSense, Directorio Activo, SIEM AlienVault y Políticas de Seguridad de la Información

Objetivo del Proyecto:

El objetivo principal de este proyecto es permitir que los alumnos adquieran conocimientos y experiencia práctica en la configuración, gestión y monitorización de una infraestructura de seguridad de red integral, además de implementar políticas de Seguridad de la información para el minimizar los riesgos con la detección de amenazas y la implementación de controles. A través de este proyecto, los alumnos aprenderán a diseñar, implementar y mantener un entorno de seguridad de red que incluya un Firewall PfSense, un Directorio Activo, un SIEM AlienVault y políticas de Seguridad de la Información.

Requisitos del Proyecto:

Hardware y Software:

- Los estudiantes deberán contar con acceso a una computadora o servidor con capacidad de virtualización.
- Se requerirá una copia de PfSense, un servidor Windows para el Directorio Activo, una instancia de AlienVault y herramientas de monitoreo.
- Se utilizarán máquinas virtuales para simular una red de prueba.

Diseño de Red:

Diseñar una red de laboratorio que conste de al menos tres segmentos de red: LAN y WAN
Definir los rangos de direcciones IP y subredes para cada segmento.

Configuración del Firewall PfSense:

- Implementación de un firewall PfSense funcional con al menos una interfaz LAN y una interfaz WAN.
- Configuración de reglas (mínimo 3) de firewall avanzadas para controlar el tráfico.
- Implementación de NAT para permitir que los dispositivos en la red LAN accedan a Internet a través de la WAN.
- Generar reenvió de log al AlienVault

UNIVERSIDAD MARIANO GALVEZ
FACULTAD DE INGENIERIA EN SISTEMAS
CATEDRATICO: MBA, LIC. JOSUÉ IVÁN LÓPEZ CONTRERAS
ALCANCE DEL PROYECTO FINAL

Implementación del Directorio Activo:

- Configuración de un servidor Windows como Controlador de Dominio de Active Directory.
- Creación de usuarios, grupos (mínimo 3) y políticas de seguridad en el Directorio Activo.
- Generar envió de eventos al AlienVault

Integración de Active Directory con PfSense:

Integración de la autenticación de usuarios entre PfSense y el Directorio Activo.

Implementación del SIEM AlienVault:

- Instalación y configuración de una instancia de AlienVault para la monitorización de eventos de seguridad.
- Configuración de la recopilación de registros de eventos de PfSense, el Directorio Activo y las bitácoras de los eventos en AlienVault.

Políticas de Seguridad de la Información:

- Configuración de políticas de seguridad en Windows para registrar eventos de seguridad relevantes.
- Implementación de herramientas de bitácoras, para la detección de amenazas y la eficacia de los controles.

Requisitos a alto nivel

Es necesario que incluya lo siguiente:

- Cumplimiento completo de los requisitos del proyecto.
- Realización de trabajo escrito con todos los ítems Caratula, Introducción, índice, Contenido de trabajo (no copy paste, no relleno innecesario), minuta de reuniones conclusiones, recomendaciones, e-grafía, bibliografía, anexos de fotografías de reuniones.
- Informe de Implementación y procedimientos.
- Ortografía y Redacción profesional.
- Copy-Paste no es válido y puede anular el trabajo, debe citar fuentes, autores, utilizar formato APA
- Fotografías en trabajo escrito como evidencia.

UNIVERSIDAD MARIANO GALVEZ
FACULTAD DE INGENIERIA EN SISTEMAS
CATEDRATICO: MBA, LIC. JOSUÉ IVÁN LÓPEZ CONTRERAS
ALCANCE DEL PROYECTO FINAL

Enlaces de Apoyo

Firewall PFSense

https://serverspace.io/es/support/help/firewall-configuring-a-server-firewall/
https://docs.ovh.com/us/es/dedicated/firewall-iptables/
https://www.youtube.com/watch?v=dkrC1OFPP54&ab_channel=MauriceFrayssinet
https://www.pfsense.org/download/
https://www.youtube.com/watch?v=YHoECE6bBeY&ab_channel=RobertoMurillo

SIEM AlienVault

https://cybersecurity.att.com/products/ossim

https://www.youtube.com/watch?v=Q55MbgMLGA0&t=1278s&ab_channel=Brier%26ThornMexico

https://www.youtube.com/@attcybersecurity

Directorio Activo

https://zentyal.com/es/inicio/

https://www.microsoft.com/es-es/windows-server

https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/appendix-l--events-to-monitor

https://www.youtube.com/watch?v=nhd7E6RfLJQ&ab_channel=WildITAcademy

https://www.youtube.com/playlist?list=PL_xQRVeBwNGMR5mcnQsE02Ku1ivufG2Nm

Agregaciones entre Firewall SIEM Y AD

https://www.youtube.com/watch?v=2qfXx8-dcSU&ab_channel=MRKSecurity

https://www.youtube.com/watch?v=mFYDYswsOrA&t=24s&ab_channel=RobertoMurillo

https://www.youtube.com/watch?v=NqJBbuqd7f0&ab_channel=EsyTV