Son entre 120 y 150 palabras por minuto

Solo las secciones escritas en *cursiva* no son el texto a decir tal cual, es decir que todo lo demás puede ser simplemente leído en el video.

1. **ZAIRA 1min 12s**

Buenas, nosotros somos el grupo 9 y exploraremos Pfsense, una potente herramienta de firewall y enrutamiento. Analizaremos su aplicación en un entorno educativo para abordar desafíos de seguridad comunes.

Para ilustrarla veamos el escenario de la escuela secundaria Lionel Andrés Messi, la cual cuenta con más de 200 alumnos, 30 profesores y personal administrativo, todos con la capacidad de conectarse a la red institucional.

Entre sus problemas podemos encontrar que

* Los estudiantes intentan acceder a redes sociales y juegos en horas de clase.
* La red carece de un control de tráfico que prevenga acciones malintencionadas.
* Las oficinas administrativas y profesores necesitan privacidad y protección de datos sensibles.
* No hay control sobre el uso del ancho de banda, saturando la red.
* Los profesores quieren poder conectarse a la red de forma segura desde donde quieran para ciertas actividades como subida de calificaciones.

El objetivo de esta experiencia es evaluar la capacidad de pfSense para resolver necesidades reales de seguridad y control en redes, analizando qué tan efectiva resulta su implementación.

Previo a la demostración definimos algunos conceptos que nos serán de utilidad:

Ubicándonos en el manejo de riesgo, se tienen cuatro estrategias genéricas para ello:

* Prevenir el riesgo: Consiste en evitar las amenazas a las que se exponen los activos.
* Asumir el riesgo: Para cuando la organización puede tolerar la pérdida esperada sin excesiva incomodidad.
* Reducir el riesgo: Implementar medidas que bajan la probabilidad de ocurrencia y y/o la pérdida relacionada a las fallas.
* Transferir el riesgo: Es que los costos resultantes de una falla los soporte un tercero, generalmente a través de seguros.

Las estrategias de manejo de riesgo se implementan a través de controles y contramedidas, mostrándose tres etapas de ellas, referidas como líneas de defensa.

* La primera línea es de prevención, dedicada a prevenir amenazas.
* La segunda es de detección, orientada a cuando falla la prevención y hay que detectar la concreción de la amenaza.
* La tercera es de recuperación, para recuperarse con pérdidas mínimas de la falla.

Definimos una amenaza como una condición del entorno del sistema de información que, dada una oportunidad, podría dar lugar a una violación de seguridad, como ser de confidencialidad, integridad, disponibilidad, etc.

1. Bruno

Algunos conceptos de redes oportunos sintetizados son:

**Dirección IP**: Número para identificar a un dispositivo dentro de una red.

**Máscara de subred**: La manera que se tiene para saber qué parte de la IP corresponde a identificar la red.

**VPN**: Red privada virtual que hace uso de la estructura del Internet.

**Firewall**: Dispositivo hardware o software para filtrar el tráfico entrante y saliente de una red.

Un router es un dispositivo que conecta dos o más redes diferentes y enruta paquetes entre ellas basándose en las direcciones IP.

// esta es la seccion que digo q hagamos todos

***-recursos utilizados-***

*configuraciones de las MV y mencionar que se usaron dos máquinas, una para hostear y para simular un atacante, y otra para demostrar el uso de la VPN y se aprovecha para decir que Pfsense es un firewall y router.*

***-esquema- bruno***

*En la muestra del esquema, aparte de describirlo rápido diciendo algo así como “acá podemos ver el esquema de lo hecho en la experiencia, con lo mencionado anteriormente de las máquinas virtuales”… bla bla bla continuando la descripción, acá se dice que Pfsense se jacta de ser uno de los pocos firewalls de código abierto que te ofrece tener un respaldo sincronizado que PREVIENE (palabra clave) que te quedes sin la protección del firewall*

***–demostración– todos***

*En la demostración se va describiendo qué hace Pfsense y se menciona que si bien en este escenario el captive portal sería fácilmente reemplazado por una clave WiFi, hay contextos donde sí tendría más utilidad su uso, por ejemplo hoteles que quieran individualizar el servicio de acceso a internet para visitantes.*

…

1. Amilcar

Es entonces que la implementación de Pfsense protege al activo información, evitando que se exploten vulnerabilidades como la la exposición a Internet o la falta de segmentación de red, de amenazas como el hacking, recordando que se define al hacking simplemente como un acceso no autorizado a un sistema, caso del cual Lardent menciona que lo más normal es que ocurra por personas internas sin finalidad delictiva. De igual manera de esta prevención de entrada de intrusos se desprende la protección también contra cosas como el phishing, malware, etcétera.

Otro activo que protege es la red, refiriendo a la vulnerabilidad de capacidad de procesamiento, protegiendo respecto a la amenaza de que se interrumpa la disponibilidad de la red.

1. Amilcar

Por lo que mencionamos antes y resaltando la naturaleza conceptual de un firewall como dispositivo que regula el tráfico evitando filtraciones de intrusos del exterior hacia la red y escapes de información confidencial o acceso a páginas no deseadas, consideramos que la implementación del Pfsense sería útil para la primera línea de defensa, la de prevención de amenazas.

Cabe decir que tiene la opción de ser ampliado a segunda línea al integrarle una extensión de Snort (un sistema de detección de intrusos), pero no es una funcionalidad por defecto de Pfsense y el trabajo lo está realizando Snort que es toda una herramienta distinta al nivel de que incluso la exponen otros compañeros, razón por la cual consideramos pertinente dejarlo solo como mención.

1. Juli

Para concluir, en definitiva, como administradores de sistemas comenzaríamos por establecer una política de seguridad prohibitiva donde los alumnos podrán acceder a sitios educativos propuestos por los profesores, los docentes y personal administrativo podrán acceder a su contenido respectivo estando previamente autenticados en el sistema, y, además, las conexiones a la red deben respetar protocolos seguros.

Por otro lado, en una estrategia genérica de prevención del riesgo implementaríamos el uso de Pfsense por ser una muy buena herramienta confiable, multifunción y además de código abierto, como primera línea de defensa para situaciones en las que querramos ayudar a la red y escudar a la información de nuestra organización, que es el recurso más importante que tenemos.

Esta fue la presentación del grupo 9 sobre la herramienta pfSense en el marco del Laboratorio de Seguridad de SI para la materia Administración de SI. Gracias por su atencion

Amenaza: La condicion del entorno que podria dar lugar a un ataqueo violacion de la seguridad.

Clasificacion de ataques a cada activo:

Para la red es del tipo interrupcion, ya que son ataques a la disponibilidad.

Para la informacion es del tipo intercepcion, ya que son ataques contra los activos.

la innuestro activo

Politica permisiva: no se puede entrar a redes sociales. (a lo demás si)

Politica prohibitiva:

* solo se puede usar los sitios educativos. (el resto no)
* Solo los alumnos autenticados pueden tener acceso a la red