



ANÁLISIS DE
CRİPTOGRAFÍA Y
SEGURIDAD



AUDITORÍA DE SEGURIDAD

Presentación ejecutiva

Proyecto presentado por:

Diego Olalde Tristán - AO1612555

Ana Camila Saavedra Casillas - AO1252957

Carlos Alberto Gómez San Pedro - AO1658377

Arath Mendivil Mora - AO1660670

Facundo Bautista Barbera - AO1066843

Índice

- O1 Introducción
- O2 Metodología
- O3 Etapa 1
- O4 Etapa 2
- O5 Etapa 3
- O6 Conclusiones

Introducción

A continuación en la presentación abordaremos los temas de la seguridad informática y gestión de vulnerabilidades en redes privadas, comenzando con los resultados de un escaneo de vulnerabilidades realizado con Nessus, en donde se identificaron 41 vulnerabilidades, algunas críticas, lo que destaca la importancia de fortalecer la seguridad.


Se propone una metodología detallada basada en lecciones aprendidas, enfocada en identificar y evaluar debilidades en la red. Se destaca la selección de herramientas adecuadas para un análisis efectivo. Además, se describe la implementación de Nessus para el inventario de activos y detección de vulnerabilidades, crucial para la gestión de riesgos y seguridad de la información. En conjunto, estos enfoques ofrecen una solución integral para los desafíos de seguridad en redes privadas.





Metodología

La auditoría se dividió en tres etapas clave:

1. Inventario de la Empresa: Se realizó un escaneo inicial para identificar los activos de la red y sus vulnerabilidades.
 2. Diseño e Implementación de un Plan de Evaluación: Uso de Nessus para un análisis detallado y la implementación de un sistema Honeypot para capturar amenazas adicionales.
 3. Plan de Mitigación de Vulnerabilidades: Desarrollo de estrategias específicas para abordar y mitigar las vulnerabilidades encontradas.
- 



ETAPA I

INVENTARIO DE LA EMPRESA



Objetivo: Realizar un escaneo detallado para identificar todos los activos de la red y sus vulnerabilidades existentes.

Herramienta Utilizada: Nessus bajo licencia “Essentials”.

Resultados Clave: Identificación de 16 hosts y un total de 41 vulnerabilidades, categorizadas desde baja hasta crítica.

Resultados del inventario

El escaneo de vulnerabilidades realizado con Nessus reveló un total de 41 vulnerabilidades en nuestra red, clasificadas desde bajas hasta críticas. Estos hallazgos resaltan la importancia de realizar auditorías de seguridad detalladas para proteger la infraestructura tecnológica contra posibles ataques.



ETAPA II

DISEÑO E IMPLEMENTACIÓN DE UN PLAN DE EVALUACIÓN DE LA EMPRESA



Configuración de Nessus

Actualización y Configuración

Asegurar su última versión y configurar un perfil de escaneo.

Ejecución de Nessus

Realizar un escaneo completo.

Revisión de reportes de Nessus

Identificar y priorizar las vulnerabilidades encontradas.

NESSUS



Implementación de sistema Honeypot

Selección y Configuración

Elegir un software de “honey-potting” adecuado para entornos domésticos, como Honeyd o Kippo, y configurarlo para simular sistemas vulnerables atractivos para los atacantes.

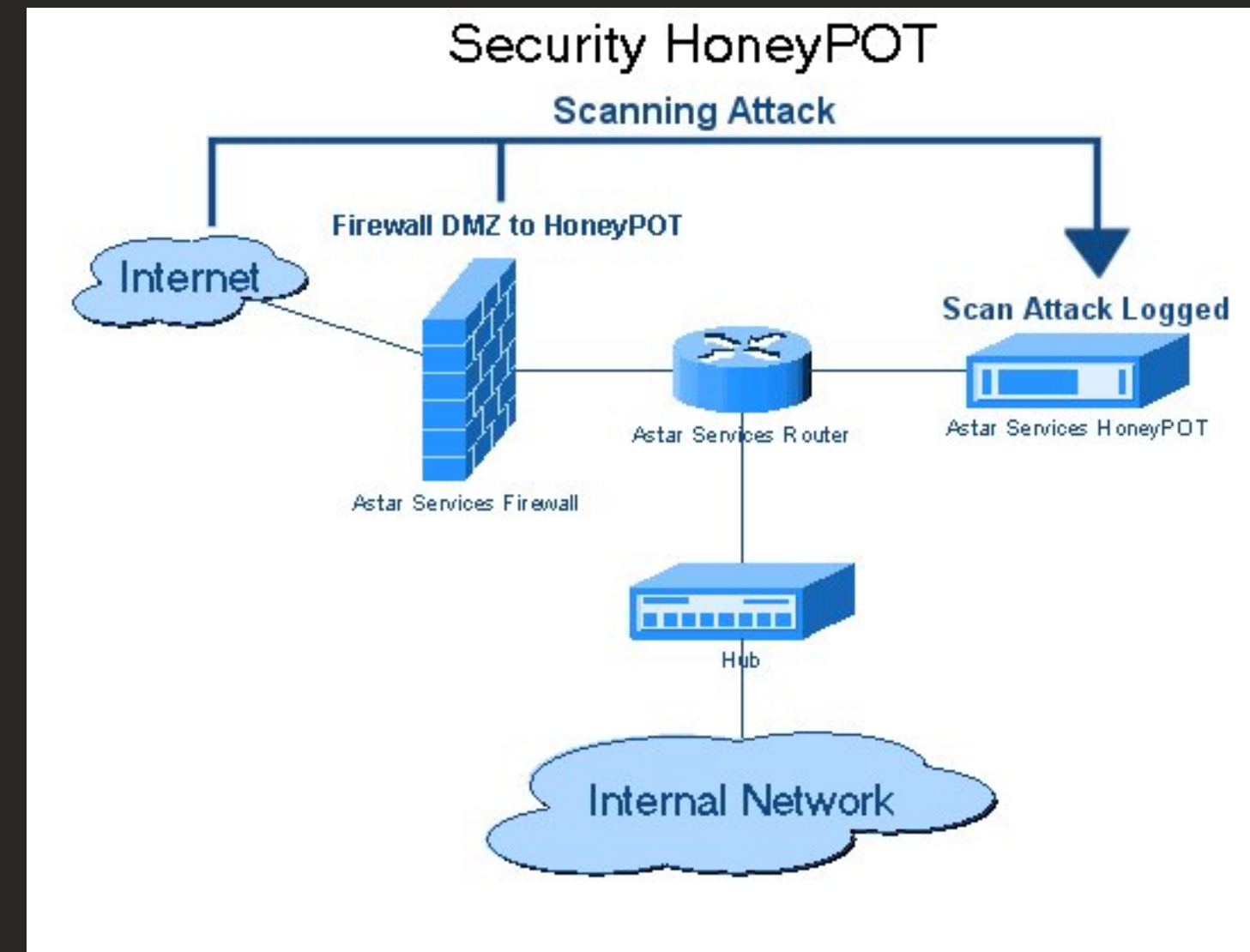
Monitoreo del sistema Honeypot

Para identificar intentos de ataque o patrones sospechosos.

Evaluación de la actividad

Evaluar los datos recopilados por el honeypot para entender mejor las amenazas específicas a las que la red está expuesta.

SISTEMA HONEYPOT



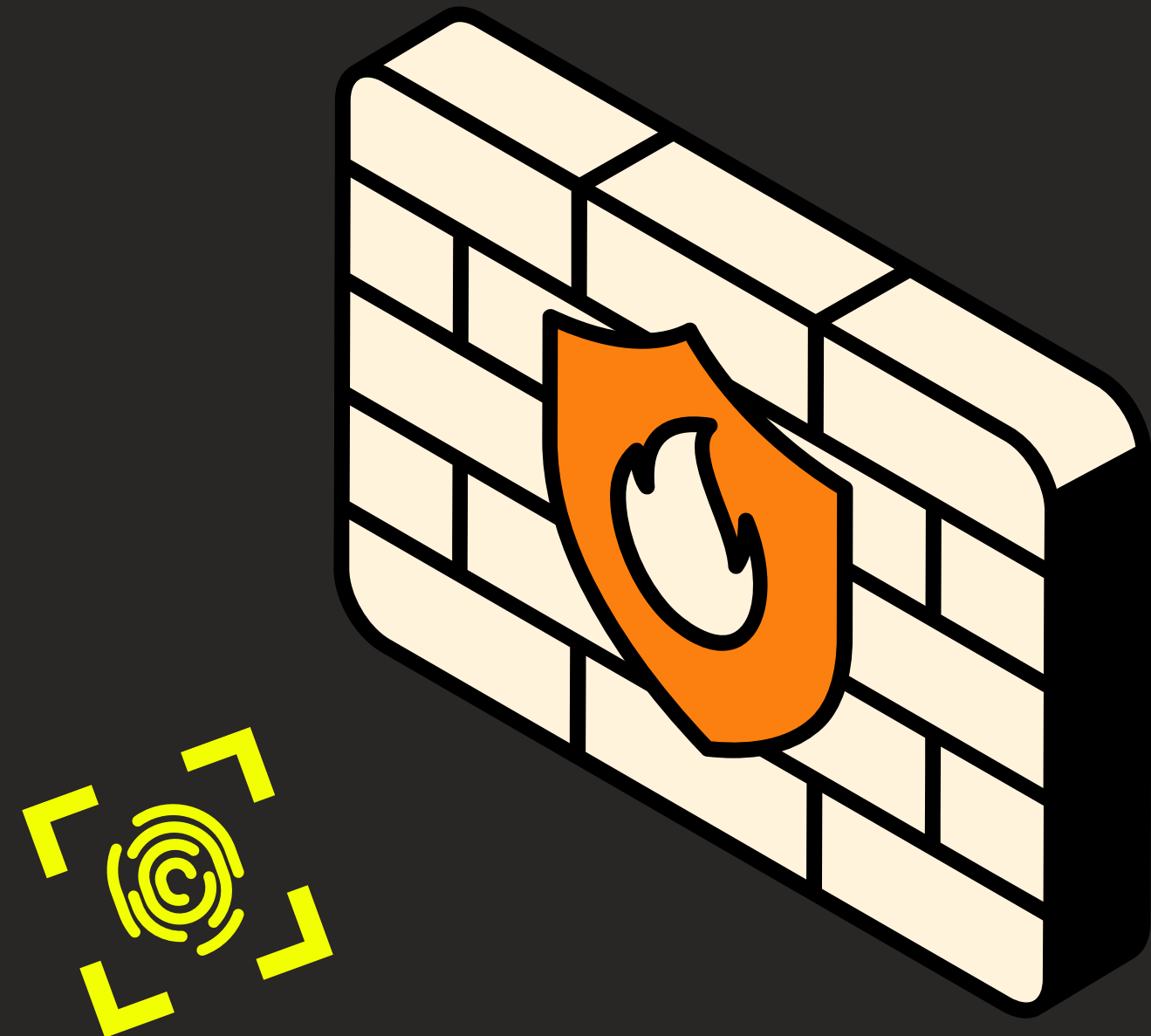
Configuración del Firewall

Un firewall es un dispositivo de seguridad de red que controla el tráfico de red entrante y saliente y decide si permite o bloquea cierto tráfico de acuerdo con un conjunto de reglas de seguridad.

Revisión y fortalecimiento

Evaluar la configuración actual del firewall para identificar posibles debilidades.
Fortalecer las reglas del firewall para bloquear tráfico no deseado.

FIREWALL



Desarrollo de un plan de remediación

Acciones a partir de Nessus

Desarrollar un plan de acción que incluya la aplicación de parches, cambios de configuración y otras medidas de mitigación.

Fortalecimiento a partir del sistema Honeypot

Desarrollar estrategias de defensa contra ataques específicos o patrones de ataque observados.

Mejoras de la configuración del firewall

Con base en los resultados del análisis de vulnerabilidades y la actividad del honeypot, realizar ajustes continuos en la configuración del firewall.



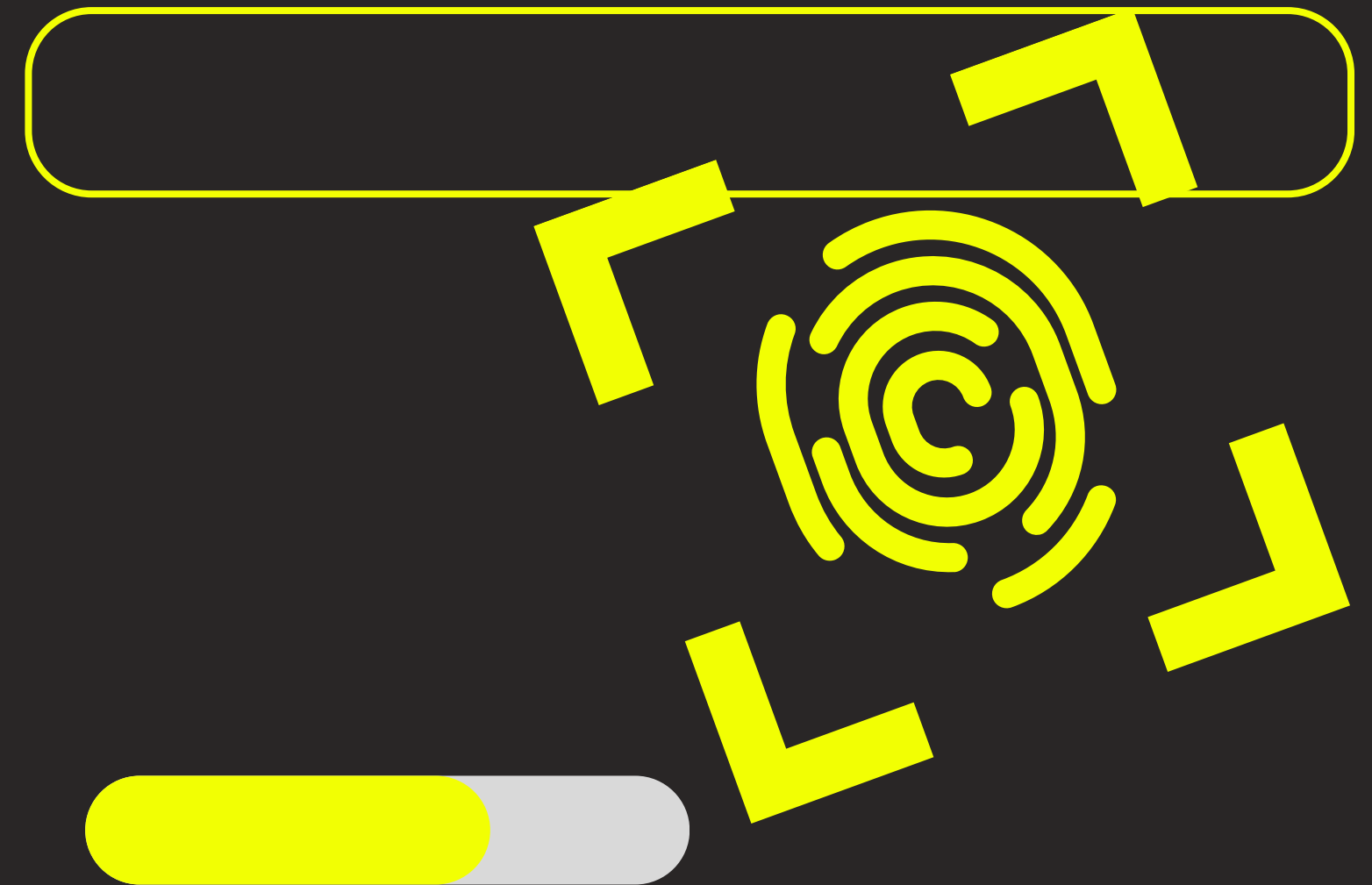
Implementación y seguimiento

Ejecución del Plan de Remediación

Implementar las acciones correctivas planificadas.

Monitoreo continuo

Detectar y responder rápidamente a nuevas vulnerabilidades o intentos de ataque





ETAPA III

PLAN DE MITIGACIÓN DE VULNERABILIDADES DE LA EMPRESA

Desarrollamos un plan de remediación que incluye la aplicación de parches, cambios en la configuración, y mejoras en la infraestructura de seguridad basándonos en las vulnerabilidades identificadas por Nessus y la actividad observada en el Honeypot. Este plan es crítico para mitigar los riesgos detectados y reforzar la seguridad de nuestra red.

Desarrollo de un Plan de Remediación: Basado en vulnerabilidades identificadas y la información del Honeypot.

Acciones Específicas: Aplicación de parches, cambios de configuración y mejoras en la seguridad.

Monitoreo Continuo: Implementación de monitoreo activo para detectar y responder a nuevas vulnerabilidades o ataques.



Conclusiones

Nuestra auditoría de seguridad demuestra la importancia crítica de una evaluación exhaustiva y continua de las vulnerabilidades. A través de las etapas de inventario, análisis y mitigación, hemos desarrollado un enfoque integral para proteger nuestra infraestructura contra ataques cibernéticos, subrayando la necesidad de vigilancia constante y mejora de la seguridad.



Referencias

07

Introducing Tenable.io. (s.f.). Tenable®.

<https://www.tenable.com/products/nessus>

KeepCoding, R. (2023). Escaneo básico con Nessus | KeepCoding Bootcamps. KeepCoding Bootcamps.

<https://keepcoding.io/blog/escaneo-basico-con-nessus/>

¿Qué es un análisis de vulnerabilidades? – SAYNET. (s.f.).

<https://saynet.com.mx/que-es-un-analisis-de-vulnerabilidades/>

¿Qué es un firewall? (2023). Cisco.

https://www.cisco.com/c/es_mx/products/security/firewalls/what-is-a-firewall.html

¿Qué es un honeypot? (2023). latam.kaspersky.com.

<https://latam.kaspersky.com/resource-center/threats/what-is-a-honeypot>

Security, P. (2023). Evaluación de vulnerabilidad: qué es y cómo realizarla. Panda Security Mediacenter.

<https://www.pandasecurity.com/es/mediacenter/evaluacion-vulnerabilidad/>

