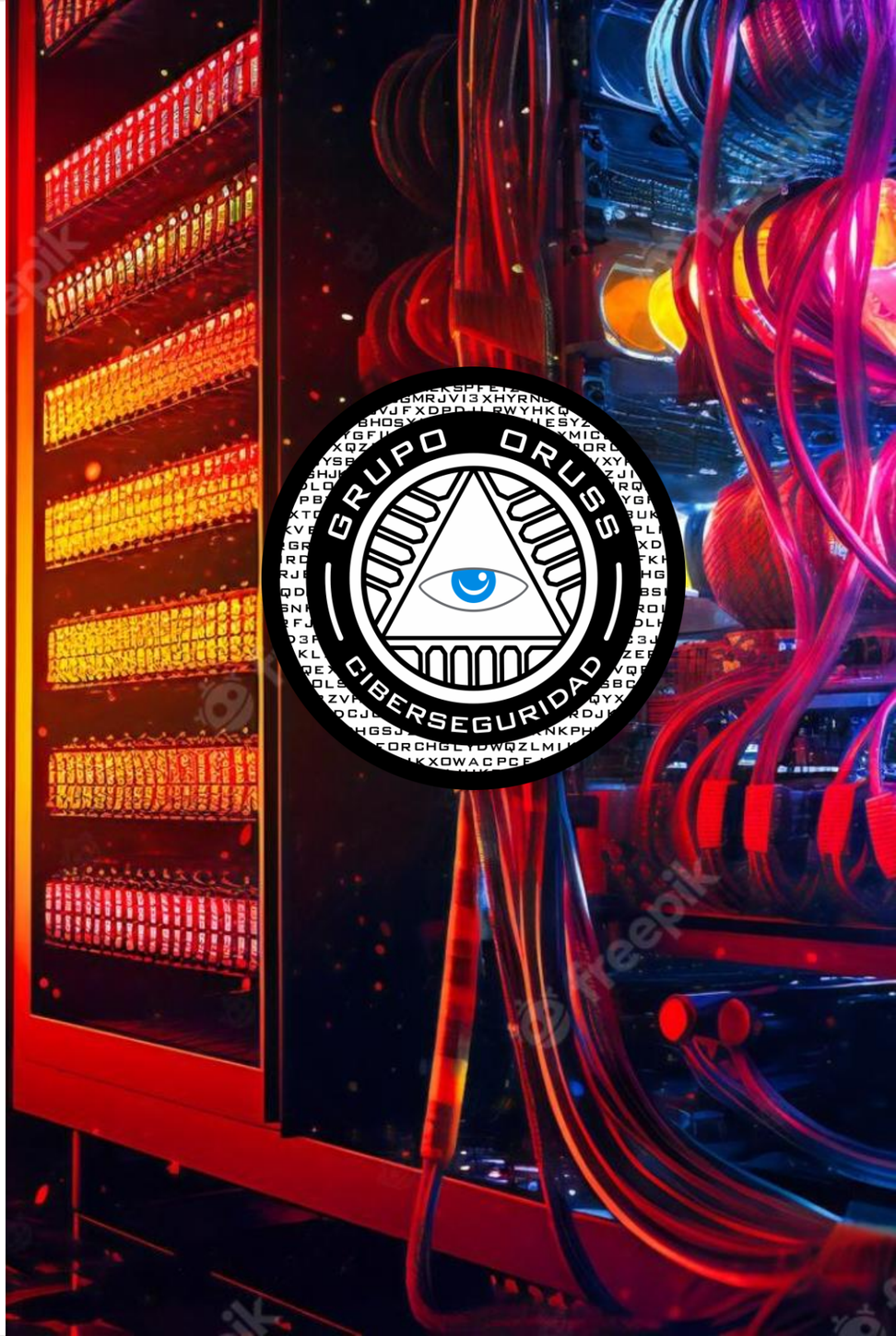
Pentesting de Red Interna

Explora cómo identificar y prevenir vulnerabilidades en una red interna mediante pruebas de penetración.



¿Qué es el pentesting de red interna?

Definición

Es una técnica de ciberseguridad que simula un ataque informático por parte de un atacante interno para identificar posibles debilidades de la red.

Objetivos

Evaluar la efectividad de las políticas de seguridad de la organización, identificar áreas áreas vulnerables y proponer soluciones para fortalecer los controles de seguridad.

Diferencias con el pentesting externo

El pentesting de red interna se centra en evaluar la seguridad de la red desde dentro de la organización, mientras que el pentesting externo se enfoca en evaluar la seguridad desde fuera.

Importancia de identificar vulnerabilidades desde dentro

Equipo interno

Los empleados pueden ser involuntariamente negligentes en la seguridad informática, exponiendo la red a amenazas internas.

Prevención de incidentes

Realizar pruebas de penetración internas ayuda a prevenir y detectar tempranamente posibles incidentes de seguridad internos.

Mejora de controles

Al identificar los puntos débiles de la red, es posible tomar medidas para fortalecer los controles de seguridad y reducir los riesgos de incidentes de seguridad.

Metodología de pentesting de red interna

1

Recolección de información

Se identifican los objetivos y se recopila información útil para el análisis de vulnerabilidades, como direcciones IP y rangos de puertos abiertos.

2

Escaneo de vulnerabilidades

Se utilizan herramientas de escaneo para identificar vulnerabilidades y debilidades en la red interna.

3

Recolección y análisis de datos del sistema

Se profundiza en la recolección y análisis de datos, como el sistema operativo, versiones específicas de software y configuraciones de seguridad.

4

Explotación y post-explotación

Se explotan las vulnerabilidades encontradas para crear una post-explotación en la red interna y documentar el impacto en la infraestructura y datos de la organización.

Herramientas utilizadas en pentesting de red interna

Metasploit

Software de código abierto para pruebas de penetración y desarrollo de exploits.

Nmap

Herramienta de escaneo de puertos y diagnóstico de red.

Wireshark

Analizador de paquetes de red utilizado para solucionar problemas de red y seguridad.

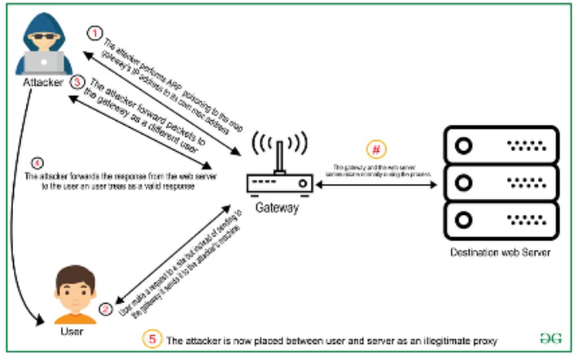
John the Ripper

Programa de recuperación de contraseñas.

Ejemplos de vulnerabilidades comunes

Contraseñas débiles

Las contraseñas débiles son un problema común en todos los sistemas informáticos, pero representan un gran riesgo en una red interna.



Ataques Man-in-the-Middle

Este ataque se produce cuando un atacante se interpone en la comunicación entre usuarios y sistemas para interceptar o manipular la información transmitida.

Obsolescencia de sistemas

El uso de sistemas y software obsoletos puede dejar la red interna vulnerable a ciberataques y a fallos en la infraestructura.

Conclusiones y recomendaciones

1

Proactividad

Adoptar una actitud proactiva que busque fortalecer los mecanismos de seguridad y reducir los riesgos de posibles ataques internos.

2

Actualización constante

Mantener actualizada la infraestructura de la red interna y asegurarse de instalar actualizaciones de seguridad que cubra el software y los sistemas utilizados.

3

Formación

Procurar que el personal de la organización reciba formación en concienciación de ciberseguridad para prevenir y reducir el riesgo de amenazas internas.

Apoya tu proceso de remediaciones con:

ALINA

ALINA es un innovador chatbot impulsado por Inteligencia Artificial que te ayudará a resolver las remediaciones propuestas en este informe.

https://grupooruss.com/alina

¡Gracias!

www.grupooruss.com