RESUMEN EJECUTIVO PRUEBA DE PENETRACION

Propiedades del documento

Título	Informe de pruebas de penetración gray box
Versión	V1.0
Autores	Oscar Novoa
Pentesters	Esteban Rojas, Luis Vera
Revisado por	
Aprobado por	
Clasificación	Confidencial

Control de versiones

Versión	Fecha	Autor	Descripción
V1.0	27 junio 2023	O Novoa	Borrador Final

Contenido

1. Resumen Ejecutivo

Este documento detalla la evaluación de seguridad en el modo gray box que consiste en una prueba de penetración de qascd.avo.cl, todas las actividades se llevaron a cabo de una manera que simulaba un agente de amenaza ejecutando un ataque dirigido contra qascd.avo.cl con los objetivos de:

- Identificar si un atacante remoto podría penetrar las defensas de qascd.avo.cl
- Determinar el impacto de una brecha de seguridad en la confidencialidad, integridad y disponibilidad de los datos privados de la empresa.

Se pusieron esfuerzos en la identificación y explotación de las debilidades de seguridad que podrían permitir a un atacante remoto obtener acceso no autorizado a los datos de la organización. Los ataques se realizaron con el nivel de acceso que tendría un usuario general de Internet. La evaluación se realizó en acuerdo con las recomendaciones descritas en NIST SP 800-1151 con todas las pruebas y acciones siendo realizado en condiciones controladas.

1.1 Alcance del trabajo

Esta evaluación de seguridad cubre la prueba de penetración remota de 1 sistema web accesible alojado en la dirección qascd.avo.cl. La evaluación se llevó a cabo desde una perspectiva de Gray box, con la información suministrada de la dirección del sistema web y tecnologías utilizadas. No se asumió ninguna otra información al inicio de la evaluación

1.2 Objetivos del Proyecto

Esta evaluación de seguridad se lleva a cabo para medir el estado de seguridad del sistema web qascd.avo.cl frente a las amenazas de Internet. El resultado de la evaluación se analiza en busca de vulnerabilidades.

Dado el escaso tiempo que se dispone para realizar la evaluación, solo se han probado los servicios inmediatamente explotables. A las vulnerabilidades se les asigna una calificación de riesgo basada en la amenaza, la vulnerabilidad y el impacto.

1.3 Supuesto

Al redactar el informe, asumimos que la dirección IP se considera IP pública, se ha firmado la Autorización del Pentesting, las reglas de compromiso y basándonos en la fase de recopilación de información, el nombre de la empresa es Void IT Solutions.

1.4 Línea de Tiempo

El calendario de prueba es el siguiente:

Pruebas de penetración	Fecha y hora de inicio	Fecha y hora de termino
Gray box	19 junio 2023 01:23 UTC-4	21 junio 2023 03:48 UTC-4

Tabla 1 Línea de tiempo de la prueba de penetración.

1.5 Resumen de los resultados

Calificación	Vulnerabilidades
Crítica	0
Importante	0
Moderada	2
Baja	6

Tabla 2 Calificación total de vulnerabilidades.

Figura 1 Vulnerabilidades totales

Se llevó a cabo un exhaustivo proceso de pentesting en qascd.avo.cl. A continuación, se presentan los resultados del pentesting, los cuales indican que no se encontraron vulnerabilidades significativas que representen una amenaza para la seguridad de la organización.
Siguiendo las mejores prácticas de pentesting, se utilizaron herramientas automatizadas y manuales para identificar posibles vulnerabilidades en la infraestructura de red y las aplicaciones web. Se llevaron a cabo pruebas de penetración en sistema operativo, servicios y aplicaciones.

Tras realizar las pruebas de penetración, no se encontraron vulnerabilidades críticas o de alto riesgo en los sistemas evaluados. A continuación, se detallan los resultados por área evaluada:

- Infraestructura de red:

No se encontraron puertos abiertos innecesarios o servicios expuestos de forma insegura.

- Aplicación web:

La aplicacion web evaluada no presentó vulnerabilidades significativas como inyecciones SQL, cross-site scripting (XSS) o autenticación deficiente.
Los controles de acceso y la gestión de sesiones se implementaron de manera segura, sin encontrar problemas de autenticación o autorización.
Si fue posible clonar el sitio web, que puede permitir crear un sitio fraudulento.

- Sistema operativo:

El sistema operativo del servidor estaba debidamente actualizado y configurado de forma segura.

- Certificado SSL/TLS:

El sitio no cuenta con un certificado SSL, lo que puede permitir a un agente de amenaza ver y modificar los datos afectando la confidencialidad e integridad de la información.

- Librería JS Vulnerable:

Librería jquery deprecada.

- No fue posible conseguir un acceso no autorizado al sistema, escalar privilegios ni pivot lateral.

1.6 Resumen de Recomendaciones

Dado que no se encontraron vulnerabilidades críticas, se recomienda realizar una valoración del riesgo aceptable para mitigar las vulnerabilidades encontradas y continuar con las prácticas de seguridad actuales y realizar revisiones periódicas para mantener la postura de seguridad actual. También se sugiere llevar a cabo pruebas de pentesting regularmente para detectar posibles vulnerabilidades en caso de cambios en la infraestructura o en las aplicaciones web.

- Se recomienda implementar controles de seguridad en la instancia de QA ya que un escenario de falla de la instancia de PRODUCCION, QA la reemplaza si esta tiene vulnerabilidades conocidas dando información valiosa para una agente de amenaza.

2. Metodología

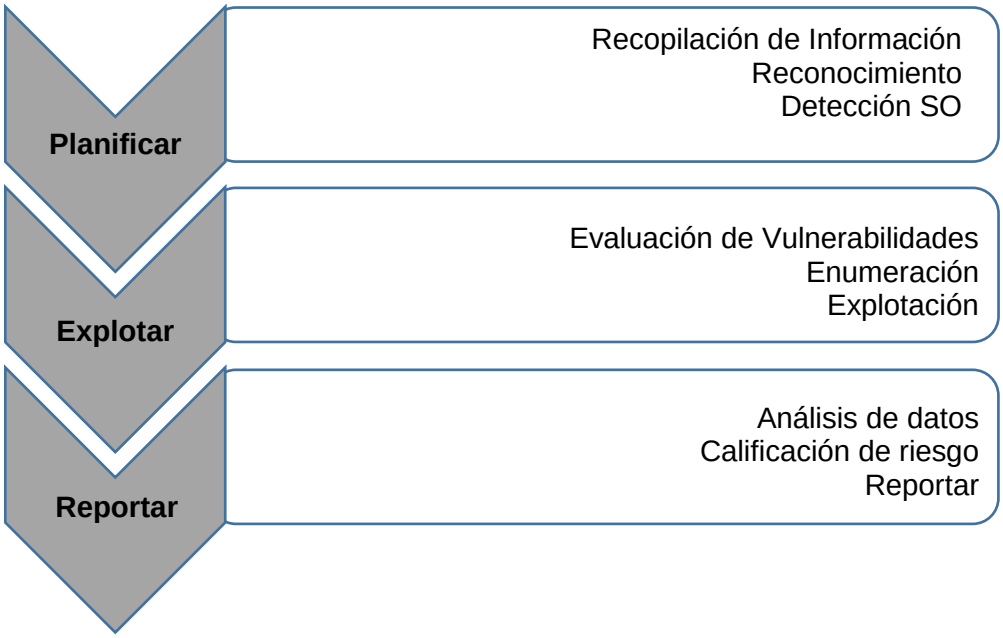

Figura 2 Metodología de las pruebas de penetración

2.1 Planificación

Durante la planificación recopilamos información de fuentes públicas para conocer el objetivo:

- Las personas y cultura.
- La infraestructura técnica.

A continuación, conociendo la dirección qascd.avo.cl consultamos la IP

Detectamos el sistema en vivo su SO y determinamos los servicios en ejecución y sus versiones.

2.2 Explotación

Utilizando la información recopilada en la planificación, empezamos la evaluación de vulnerabilidades en el SO y los servicios que descubrimos.

2.3 Informes

Basándonos en los resultados de los dos primeros pasos, empezamos a analizar los resultados y construir un Resumen Ejecutivo y un Informe Técnico. Nuestra calificación de riesgo se basa en la siguiente matriz:

		Impacto				
		Poco Significativo	Menor	Moderado	Mayor	Catastrofico
Probabilidad	Casi Seguro	Medio	Alto	Alto	Muy Alto	Muy Alto
	Probable	Medio	Medio	Alto	Alto	Muy Alto
	Posible	Bajo	Medio	Medio	Alto	Alto
	Improbable	Bajo	Bajo	Medio	Medio	Medio
	Raro	Bajo	Bajo	Bajo	Medio	Medio

Tabla 3. Matriz de riesgo

Junto con la leyenda de clasificación de vulnerabilidades encontradas

Descripción	Calificación	Color
Vulnerabilidad debil o muy compleja de aprovechar. Causa impacto minimo.	Baja	
Vulnerabilidad moderada que compromete moderadamente uno o mas pilares CIA. Causa un impacto menor.	Moderada	
Vulnerabilidad mas peligrosas. Afecta a un nivel alto los pilares CIA. Causa impacto moderado.	Importante	
Fallo de seguridad critico. Compromete gravemente los pilares CIA. Causa un grave impacto.	Critica	

Tabla 4. Leyenda de clasificación de vulnerabilidades.

3. CONCLUSIONES

La prueba de penetración realizado en qascd.avo.cl revela que la organización presenta una postura de seguridad sólida, ya que no se encontraron vulnerabilidades críticas o de alto riesgo que representen una amenaza significativa. Se siguieron las mejores prácticas de pentesting, utilizando herramientas automatizadas y pruebas manuales para evaluar la infraestructura de red, las aplicaciones web y el sistema operativo.

Se identificaron áreas de mejora, como la posibilidad de clonar el sitio web, la falta de un certificado SSL y el uso de una librería JS deprecada. Estas recomendaciones deben ser abordadas para fortalecer aún más la seguridad en profundidad de la organización.

Se recomienda realizar una valoración del riesgo aceptable para mitigar las vulnerabilidades encontradas y mantener las prácticas de seguridad actuales. Además,

es fundamental realizar revisiones periódicas y llevar a cabo pruebas de pentesting regulares, especialmente ante cambios en la infraestructura o las aplicaciones web.
La implementación de controles de seguridad en la instancia de QA es una recomendación específica para proporcionar una capa adicional de protección contra posibles amenazas.
Controlar la seguridad de la aplicación es un componente importante de la seguridad de la información que debe dar la confianza del desarrollo de un software seguro y debe llevarnos a procesos seguros y usuarios conscientes de los riesgos ya que son el vector principal de ataque.
En general, el informe de pentesting refleja una buena postura de seguridad de la organización, pero es importante mantenerse vigilante y estar preparado para enfrentar nuevas amenazas mediante la aplicación continua de medidas de seguridad y la realización regular de pruebas de penetración.