Informe ejecutivo para

MasterD

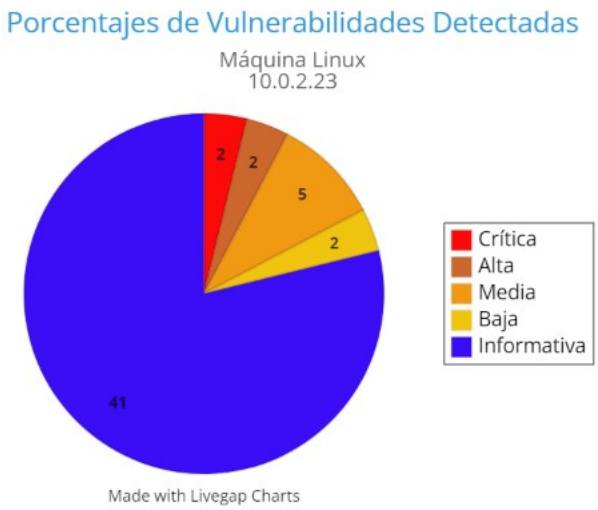
Fecha: 09-05-2024
Nombre del documento: Trabajo Final de Curso Ethical Hacking

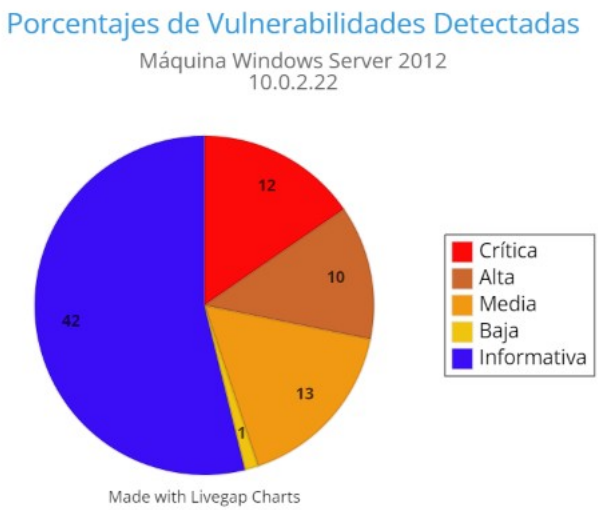
Autor: Julián Gordon

INFORME EJECUTIVO

El presente Informe Ejecutivo detalla los hallazgos obtenidos a partir del proceso de pentesting realizado en dos máquinas de la red corporativa de MasterD. El objetivo principal de esta evaluación fue identificar y analizar las vulnerabilidades presentes en la infraestructura de ambas máquinas, con el fin de evaluar el nivel de riesgo para la seguridad de la red y proporcionar recomendaciones para su mitigación.

Durante el proceso, se identificaron múltiples vulnerabilidades clasificadas en distintos niveles de criticidad, desde aquellas consideradas como muy altas o críticas hasta aquellas de menor riesgo pero que aún representan una amenaza para la seguridad. Se realizó un análisis detallado de cada vulnerabilidad, evaluando su impacto potencial en la seguridad de la infraestructura y proponiendo medidas correctivas para su mitigación.





Vulnerabilidad	Cantidad	Porcentaje
Muy Alta / Crítica	14	10,85%
Alta	12	9,30%
Media	18	13,95 %
Baja	3	2,32 %
Informativa	82	63,56%
Total Máquina Linux	52	40,31%
Total Máquina Windows	77	59,68%
Total	129	100%

Descripción de la Situación Actual

En el análisis de la máquina Linux (Máquina 1 - 10.0.2.23) se identificaron múltiples vulnerabilidades que representan riesgos significativos para la seguridad de la infraestructura. Entre las vulnerabilidades encontradas, se destacan:

1. **Inyección SQL (Muy Alta / Crítica)**: Esta vulnerabilidad permite a los atacantes ejecutar comandos SQL no autorizados, lo que puede conducir a la manipulación de la base de datos y la exfiltración de datos confidenciales.
2. **Browsable Web Directories (Alta)**: Esta vulnerabilidad expone directorios del servidor web que no deberían ser públicamente visibles, lo que facilita la recopilación de información por parte de atacantes.
3. **FTP Service allows anonymous login (Muy Alta / Crítica)**: El servicio FTP permite conexiones anónimas, lo que puede llevar a accesos no autorizados y potencialmente a la exfiltración de datos sensibles.
4. **Web Application Potentially Vulnerable to Clickjacking (Media)**: La aplicación web puede ser vulnerable a ataques de clickjacking, donde un atacante engaña a un usuario para que haga clic en elementos de la página web de manera inadvertida.
5. **SSH server vulnerable (Media)**: El servidor SSH es vulnerable a una debilidad de truncamiento de prefijo, lo que puede permitir a un atacante eludir los controles de integridad y reducir la seguridad de la conexión.
6. **ICMP Timestamp Request Remote Date Disclosure (Media)**: El host remoto responde a solicitudes de marca de tiempo ICMP, lo que permite a un atacante conocer la fecha y hora del sistema.

Recomendaciones Generales

Para abordar estas vulnerabilidades y mejorar la seguridad de la infraestructura, se recomiendan las siguientes acciones:

1. **Parcheo y Actualización de Software**: Actualizar y parchear todos los sistemas y aplicaciones afectados por las vulnerabilidades identificadas. Esto incluye actualizar el software de servidor web, FTP y SSH a las versiones más recientes que aborden las vulnerabilidades conocidas.
2. **Configuración Segura del Servidor**: Configurar adecuadamente los servidores web, FTP y SSH para desactivar características inseguras, como el acceso anónimo y la exposición de directorios de forma inadvertida.
3. **Implementación de Medidas de Seguridad Adicionales**: Utilizar herramientas de seguridad, como firewalls de aplicaciones web (WAF), sistemas de detección de intrusiones (IDS) y sistemas de prevención de intrusiones (IPS) para monitorear y proteger la infraestructura contra posibles ataques.
4. **Educación y Concientización del Personal**: Capacitar al personal en buenas prácticas de seguridad, incluida la creación y gestión de contraseñas seguras, la detección de ataques de ingeniería social y la identificación de actividades sospechosas en la red.

5. **Auditorías de Seguridad Regulares**: Realizar auditorías de seguridad periódicas para identificar y remediar posibles vulnerabilidades antes de que puedan ser explotadas por atacantes.

En el análisis de la máquina Windows Server 2012 (Máquina 2 - 10.0.2.22), se identificaron múltiples vulnerabilidades que representan riesgos significativos para la seguridad de la infraestructura. Entre las vulnerabilidades encontradas, se destacan:

1. **Denegación de Servicio (DoS)** (Muy Alta / Crítica): Esta vulnerabilidad permite a los atacantes llevar a cabo ataques de denegación de servicio que pueden resultar en la interrupción o inutilización de los servicios ofrecidos por el servidor.
2. **PHP Unsupported Version Detection** (Muy Alta / Crítica): La detección de versiones no compatibles de PHP puede exponer al servidor a vulnerabilidades conocidas y a la explotación por parte de atacantes.
3. **Browsable Web Directories** (Alta): Esta vulnerabilidad expone directorios del servidor web que no deberían ser públicamente visibles, lo que facilita la recopilación de información por parte de atacantes.
4. **Web Application Information Disclosure** (Media): La aplicación web puede estar exponiendo información sensible que podría ser utilizada por atacantes para llevar a cabo ataques dirigidos.
5. **WordPress User Enumeration** (Media): La enumeración de usuarios en WordPress puede facilitar a los atacantes la identificación de cuentas válidas y potencialmente eludir los mecanismos de autenticación.
6. **SMB Signing not required** (Media): La falta de requerimiento de firmado SMB puede exponer al servidor a ataques de tipo "man-in-the-middle" y a la interceptación de datos sensibles transmitidos a través de SMB.
7. **HTTP TRACE / TRACK Methods Allowed** (Media): Permitir los métodos TRACE / TRACK HTTP puede exponer al servidor a ataques de tipo Cross-Site Tracing (XST) que podrían facilitar el robo de credenciales de sesión.

Recomendaciones Generales

Para abordar estas vulnerabilidades y mejorar la seguridad de la infraestructura de Windows Server 2012, se recomiendan las siguientes acciones:

1. **Parcheo y Actualización de Software:** Actualizar y parchear todos los sistemas y aplicaciones afectados por las vulnerabilidades identificadas. Esto incluye actualizar PHP a una versión compatible y corregir las configuraciones de seguridad del servidor web para desactivar características inseguras.
2. **Configuración Segura del Servidor:** Configurar adecuadamente el servidor web y los servicios relacionados para desactivar características inseguras y limitar la exposición de información sensible.

3. **Implementación de Medidas de Seguridad Adicionales:** Utilizar herramientas de seguridad, como firewalls de aplicaciones web (WAF), sistemas de detección de intrusiones (IDS) y sistemas de prevención de intrusiones (IPS) para monitorear y proteger la infraestructura contra posibles ataques.
4. **Educación y Concientización del Personal:** Capacitar al personal en buenas prácticas de seguridad, incluida la detección de ataques de denegación de servicio, la identificación de vulnerabilidades en aplicaciones web y la protección contra técnicas de enumeración de usuarios.
5. **Auditorías de Seguridad Regulares:** Realizar auditorías de seguridad periódicas para identificar y remediar posibles vulnerabilidades antes de que puedan ser explotadas por atacantes.

En cuanto a la valoración del auditor, se considera que las vulnerabilidades identificadas representan un riesgo significativo para la seguridad de la infraestructura y requieren una acción inmediata para mitigar los riesgos y proteger los activos de la organización contra posibles ataques. Se recomienda que se implementen las recomendaciones sugeridas lo antes posible para mejorar la postura de seguridad de la infraestructura.