



# Tecnológico de Monterrey

Escuela de Ingeniería y Ciencias: Departamento de Computación

## **Evidencia 1. Auditoría de Seguridad: Reporte Técnico**

Análisis de criptografía y seguridad (Gpo 201)

Profesor: Oscar Eduardo Labrada Gomez  
Joaquin Moreno de los Santos

### **Equipo 2**

Integrantes:

Antonio Noemi Torres A01026100

Braulio Miguel Martínez Jiménez A00573980

Christoph Freiter Silva A0083080

Fernando Soto Lopez A01252884

Maximiliano García Suástegui A01657689

*29 de abril de 2024*

# Levantamiento de inventario

## Introducción

La empresa ha mantenido su posición líder gracias a un enfoque implacable en la calidad de sus productos y la eficiencia de sus operaciones. Para respaldar esta misión, Güera Shoes ha invertido considerablemente en una infraestructura tecnológica sólida y adaptable, que impulsa todas las facetas de su negocio, desde la administración hasta la logística y las ventas.

En este reporte técnico, analizaremos en detalle la infraestructura informática de Güera Shoes, examinando sus equipos activos, la configuración de su red, así como los sistemas y software especializados que utilizan para gestionar sus operaciones diarias. Desde el corazón de su oficina hasta cada una de sus tiendas.

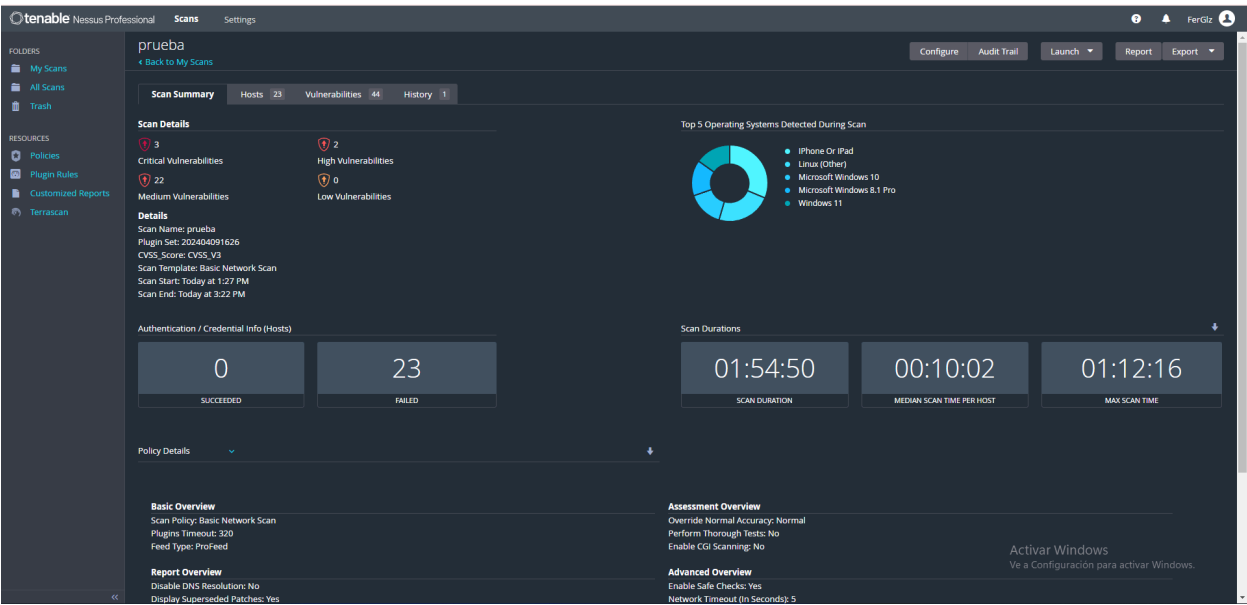
## Reporte técnico

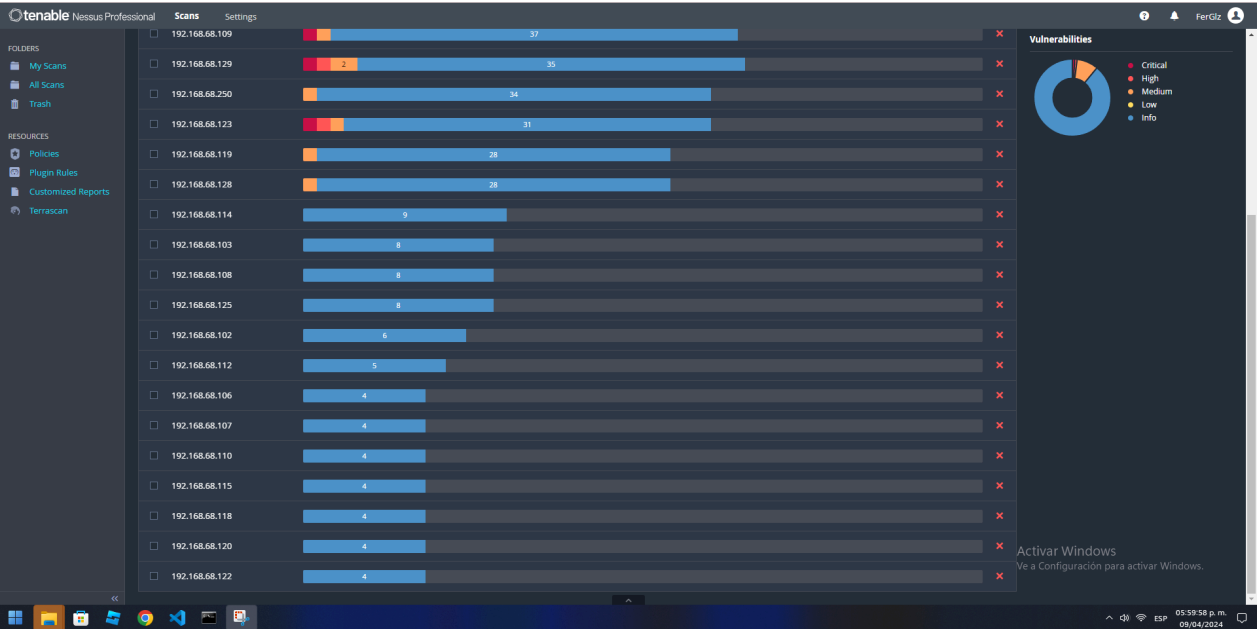
Empresa: Güera Shoes



Empresa dedicada a la venta de zapatos al mayoreo con más de 20 años de experiencia.

## Equipos activos





## Conclusión

Para realizar un inventario de manera automatizada y a bajo costo, existen varias herramientas y enfoques que podrían ser útiles para Güera Shoes. Aquí hay algunas opciones a considerar:

1. **Software de inventario gratuito o de código abierto:** Existen numerosas soluciones de software de inventario de código abierto o gratuitas disponibles en línea.
2. **Aplicaciones móviles de escaneo de códigos de barras:** Utilizar aplicaciones móviles que permitan escanear códigos de barras puede ser una forma económica y práctica de realizar inventarios.
3. **Herramientas de hojas de cálculo:** Aunque más manual en comparación con las soluciones automatizadas, las hojas de cálculo como Microsoft Excel o Google Sheets pueden ser herramientas efectivas para realizar inventarios de manera económica.
4. **Sistemas de gestión de inventario en la nube:** Algunas plataformas ofrecen sistemas de gestión de inventario basados en la nube que pueden ser accesibles y rentables para empresas de menor tamaño.
5. **Automatización con tecnología IoT (Internet de las cosas):** En un enfoque más avanzado, se puede considerar la utilización de tecnología IoT para automatizar ciertos aspectos del inventario, como la monitorización remota de existencias y la gestión de inventario en tiempo real.

Dependiendo de las necesidades específicas y el presupuesto de Güera Shoes, cualquiera de estas opciones podría ser una solución viable para realizar inventarios de manera automatizada y a bajo costo. Es importante evaluar cuidadosamente cada opción en función de los requisitos del negocio y la capacidad de integración con los sistemas existentes.

En resumen, realizar un levantamiento de inventario en una empresa es esencial para una gestión eficiente de los recursos de TI, garantizando la seguridad, el cumplimiento normativo, la disponibilidad de recursos y la capacidad de respuesta ante situaciones adversas.

## **Diseño e implementación de un plan de evaluación**

Para abordar las brechas de seguridad encontradas implementamos un plan estratégico de solución, un plan de mitigación y un plan de mantenimiento.

### **Glosario**

- SMB (Server Message Block): Es un protocolo de comunicación que se utiliza para el acceso compartido a archivos, directorios, impresoras, puertos serie y otros recursos de una red. también proporciona un mecanismo de comunicación entre procesos (IPC) autenticado.
- SSL Certificate (Secure Sockets Layer): Es un certificado digital que autentica la identidad de un sitio web y permite una conexión cifrada. Crea un cifrado entre un servidor web y un navegador web y evita que los delincuentes lean o modifiquen la información transferida entre dos sistemas. Las empresas u organizaciones necesitan agregar este certificado a sus sitios web para proteger transacciones en línea y mantener la información del cliente privada y segura. Cuando sale un ícono de candado al lado de la URL en la barra de direcciones, significa que SSL protege el sitio web.
- ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE, ETERNALSYNERGY: Fueron desarrollados por la Agencia de Seguridad Nacional de los Estados Unidos (NSA) en su programa de armamento de vulnerabilidades. Divulgados el 14/04/2017 por un grupo conocido como Shadow Brokers después de hacer un ciberataque a la NSA.
- Wanna Cry: Es el nombre de un ataque mundial de ransomware gracias al exploit de ETERNALBLUE. Se propagó a un ritmo de 10 000 dispositivos por hora y llegó a infectar más de 230 000 equipos Windows en 150 países en un solo día.
- EternalRocks: Es un gusano informático que utiliza siete vulnerabilidades de Equation Group.
- Petya: Es un ransomware que primero utiliza CVE-2017-0199, una vulnerabilidad en Microsoft Office, y luego se propaga a través de ETERNALBLUE.

### **Parte I**

**Objetivo del análisis:** Evaluar y fortalecer la seguridad de la infraestructura tecnológica de Güera Shoes para protegerla contra amenazas , garantizando la continuidad de las

operaciones comerciales y la integridad y confidencialidad de la información crítica y sensible. Este análisis busca identificar y priorizar vulnerabilidades en los activos tecnológicos identificados.

**Herramientas:** En nuestro plan de análisis de vulnerabilidades, utilizaremos **Tenable Nessus Professional** debido a su eficacia en identificar vulnerabilidades activos tecnológicos. Esta herramienta es ideal para realizar escaneos detallados, permitiéndonos evaluar la seguridad de la infraestructura de Güera Shoes y garantizar su integridad operativa. Debido a su eficacia automática y periodo de utilización gratuito es una excelente herramienta para el análisis de vulnerabilidades.

### **Metodología de Análisis:**

**Identificación de vulnerabilidades:** Utilizando la herramienta seleccionada de Nessus se realizan escaneos de los sistemas y redes.

**Evaluación de vulnerabilidades:** Se determina el nivel de riesgo asociado a cada vulnerabilidad encontrada y se priorizan.

**Análisis y reporte de vulnerabilidades:** Se documenta las vulnerabilidades y los riesgos asociados. Se analizan las vulnerabilidades para entenderlas en su totalidad y plantear una solución y plan de mitigación.

**Mitigación:** Con el conocimiento sobre las vulnerabilidades, se realizan planes concretos que se apliquen a los dispositivos y red, el objetivo es que estos mitiguen o den solución a la vulnerabilidad.

## **Parte II**

### **Análisis de vulnerabilidades**

Vulnerabilidades críticas			
Host	Vulnerabilidad	Descripción	Mitigación/Solución
192.168.68.109 (Microsoft Windows 7 Ultimate)	Unsupported Windows OS (remote)	A la versión de Microsoft Windows le falta un paquete de servicio o ya no es compatible. Es	Actualizar a una versión compatible y compatible con parches de seguridad.

192.168.68.129 (Microsoft Windows 8.1 Pro)		probable que contenga vulnerabilidades de seguridad.	
192.168.68.123 (Microsoft Windows 8.1 Pro)			

Vulnerabilidades altas			
Host	Vulnerabilidad	Descripción	Mitigación/Solución
192.168.68.129 (Microsoft Windows 8.1 Pro)	MS17-010: Security update for Microsoft Windows SMB server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (Wanna Cry) (EternalRocks) (Petya) (Uncredentialed check)	Existen múltiples vulnerabilidades de ejecución remota de código en Microsoft Server Message Block 1.0 (SMBv1) debido al manejo inadecuado de ciertas solicitudes. Un atacante remoto autenticado a través de un paquete especialmente diseñado puede ejecutar un código arbitrario.	Aplicar el parche de seguridad MS17-010 y deshabilitar SMBv1 si no es necesario.
192.168.68.123 (Microsoft Windows 8.1 Pro)			

Vulnerabilidades medias			
Host	Vulnerabilidad	Descripción	Mitigación/Solución
192.168.68.130 (Windows 11)	SMB Signing not required	No es necesario iniciar sesión en el servidor SMB remoto. Un atacante remoto no identificado puede aprovechar esto para realizar ataques de intermediario contra el servidor SMB.	Aplicar la firma de mensajes en la configuración del host. Windows-Configuración de política-"Servidor de red Microsoft: firmar digitalmente las comunicaciones"-Siempre
192.168.68.116 (Microsoft Windows)			
192.168.68.121 (Windows 11)			
192.168.68.109			

(Microsoft Windows 7 Ultimate) 192.168.68.129 (Microsoft Windows 8.1 Pro) 192.168.68.123 (Microsoft Windows 8.1 Pro) 192.168.68.119 (Microsoft Windows 10) 192.168.68.128 (Microsoft Windows 10)			e.
192.168.68.130 Windows 11 192.168.68.121 (Windows 11) 192.168.68.117 (Linux Kernel 2.6) 192.168.68.250 (Linux Kernel 2.6)	SSL Certificate cannot be trusted	1- Es posible que la parte superior de la cadena de certificados enviada por el servidor no descienda de una autoridad pública certificada conocida. 2- La cadena de certificados puede contener un certificado no válido en el momento del análisis. 3- La cadena de certificados puede contener una firma que no coincide con la información del certificado o no se puede verificar.	Verificar la validez del certificado SSL y corregir la cadena de certificados según sea necesario
192.168.68.130 Windows 11 192.168.68.121 (Windows 11) 192.168.68.117 (Linux Kernel 2.6)	SSL Self-signed certificate	La cadena de certificados X.509 para este servicio no está firmada por una autoridad de certificación reconocida. Si el host remoto es público, esto anula el uso de SSL ya que cualquiera podría hacer un ataque de intermediario contra el host remoto.	Instalar un certificado SSL firmado por una autoridad de certificación reconocida para garantizar la autenticidad del servidor.
192.168.68.121	SSL certificate	El "Common Name" (CN)	Corregir la configuración



(Windows 11)	with wrong hostname	del certificado SSL de este servicio es para una máquina diferente	del certificado SSL para que coincida con el nombre de host correcto.
192.168.68.117 (Linux Kernel 2.6)	SSL certificate expiry	Este “plugin” verifica las fechas de vencimiento de los certificados asociados con servicios habilitados de SSL e informa si alguno ya ha expirado.	Renovar o actualizar el certificado SSL para evitar su expiración.
192.168.68.129 (Microsoft Windows 8.1 Pro)	MS16-047: Security update for SAM and LSAD remote protocols (3148527) (Badlock) (Uncredentialed check)	El host remoto de Windows se ve afectado por una vulnerabilidad de elevación de privilegios en el “Security Account Manager” (SAM) y el “Local Security Authority (Domain Policy)” (LSAD) debido a una mala negociación del nivel de autenticación a través de los canales de “Remote Procedure Call” (RPC). Un atacante capaz de interceptar las comunicaciones entre un cliente y un servidor con una base de datos SAM puede forzar la reducción de nivel de autenticación, lo que le permite hacerse pasar por un usuario autenticado y acceder a la base de datos SAM.	Aplicar el parche de seguridad MS16-047 para corregir la vulnerabilidad.

## Plan de solución

- Vulnerabilidad: Unsupported Windows OS (remote)

Solución: Actualizar a una versión compatible y compatible con parches de seguridad. Estas actualizaciones incluyen actualizaciones de seguridad que pueden ayudar a proteger su PC de virus dañinos, spyware y otro software malintencionado que puede robar su información personal. Windows Update también instala las actualizaciones de software más recientes para mejorar la confiabilidad de Windows, como nuevos controladores para el hardware.

- Vulnerabilidad: MS17-010: Security update for Microsoft Windows SMB server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (Wanna Cry) (EternalRocks) (Petya) (Unauthenticated check)

Solución: Microsoft ha lanzado un conjunto de parches para Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10 y 2016. En nuestro caso los host que tienen esta vulnerabilidad son sistemas operativos Microsoft Windows 8.1 Pro. No tenemos que deshabilitar el SMBv1 ya que eso solo aplica para sistemas de Windows XP.

Los parches se pueden descargar en el [Boletín de seguridad de Microsoft MS17-010 - Crítico](#)

Sistema operativo	CVE-2017-0143 <a href="#">↗</a>	CVE-2017-0144 <a href="#">↗</a>	CVE-2017-0145 <a href="#">↗</a>	CVE-2017-0146 <a href="#">↗</a>	CVE-2017-0147 <a href="#">↗</a>	CVE-2017-0148 <a href="#">↗</a>	Actualizaciones reemplazadas
-------------------	---------------------------------	---------------------------------	---------------------------------	---------------------------------	---------------------------------	---------------------------------	------------------------------

#### Windows 8.1

Windows 8.1 solo para sistemas de 32 bits <a href="#">↗</a> (4012213) <sup>1</sup>	<b>Crítico</b> Ejecución remota de código	<b>Crítico</b> Ejecución remota de código	<b>Crítico</b> Ejecución remota de código	<b>Crítico</b> Ejecución remota de código	<b>Importante</b> Divulgación de información	<b>Crítico</b> Ejecución remota de código	Ninguno
Paquete acumulativo mensual de Windows 8.1 para sistemas de 32 bits <a href="#">↗</a> (4012216) <sup>1</sup>	<b>Crítico</b> Ejecución remota de código	<b>Crítico</b> Ejecución remota de código	<b>Crítico</b> Ejecución remota de código	<b>Crítico</b> Ejecución remota de código	<b>Importante</b> Divulgación de información	<b>Crítico</b> Ejecución remota de código	<a href="#">3205401</a> <a href="#">↗</a>
Windows 8.1 para sistemas basados en x64 <a href="#">↗</a> (4012213) Solo seguridad <sup>1</sup>	<b>Crítico</b> Ejecución remota de código	<b>Crítico</b> Ejecución remota de código	<b>Crítico</b> Ejecución remota de código	<b>Crítico</b> Ejecución remota de código	<b>Importante</b> Divulgación de información	<b>Crítico</b> Ejecución remota de código	Ninguno
Paquete acumulativo mensual de Windows 8.1 para sistemas basados en x64 <a href="#">↗</a> (4012216) <sup>1</sup>	<b>Crítico</b> Ejecución remota de código	<b>Crítico</b> Ejecución remota de código	<b>Crítico</b> Ejecución remota de código	<b>Crítico</b> Ejecución remota de código	<b>Importante</b> Divulgación de información	<b>Crítico</b> Ejecución remota de código	<a href="#">3205401</a> <a href="#">↗</a>

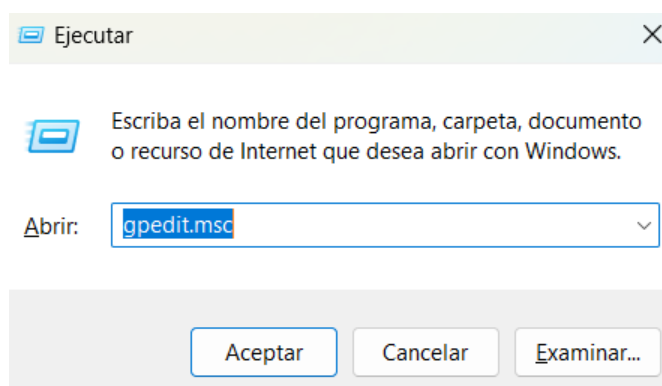
En nuestro caso instalamos el paquete de [Windows 8.1 para sistemas basados en x64](#)

Título	Productos	Clasificación	Última actualización	Versión	Tamaño	Descargar
<a href="#">Actualización de calidad solo referente a la seguridad (marzo de 2017) para Windows 8.1 sistemas basados en x64 (KB4012213)</a>	Windows 8.1	Actualizaciones de seguridad	28/03/2017	n/d	37,0 MB	Descargar

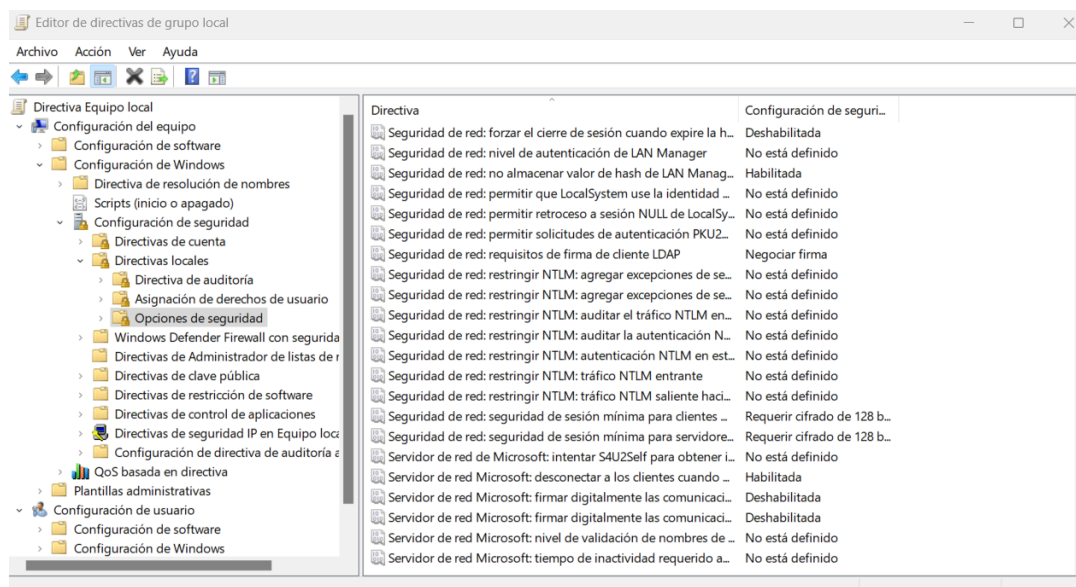
- Vulnerabilidad: SMB Signing not required

Solución: Para versiones anteriores a Windows 10 Home seguir los siguientes pasos:



1. Pulsar a la vez las teclas **Windows** y **R** para abrir la pestaña de ejecutar.
2. Escribir **gpedit.msc** y pulsar aceptar para abrir el Editor de directivas de grupo local



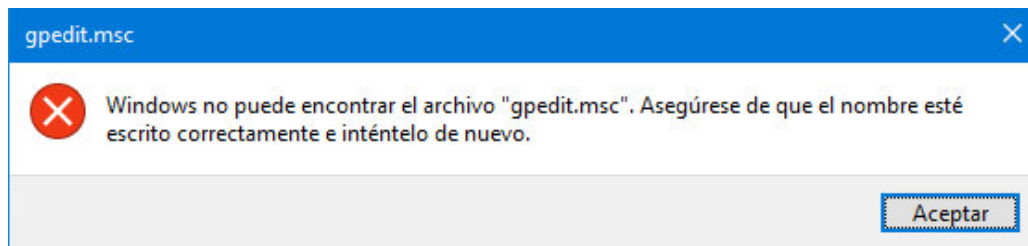
3. Dentro del editor seguir el camino de Configuración del equipo-Configuración de Windows-Configuración de Seguridad--Directivas Locales-Opciones de Seguridad



4. Localiza la opción de Servidores de red Microsoft: firmar digitalmente las comunicaciones (siempre)

	Servidor de red Microsoft: firmar digitalmente las comunicaciones (si el cliente lo permite)	Deshabilitada
	Servidor de red Microsoft: firmar digitalmente las comunicaciones (siempre)	Deshabilitada

Para versiones de Windows 10 Home en adelante u otras versiones el comando *gpedit.msc* no está incluido



Para añadirlo al sistema operativo seguimos este [tutorial](#) para añadirlo a nuestro equipo Windows 11 y después hicimos los pasos de arriba.

- Vulnerabilidad: SSL Certificate cannot be trusted

Solución:

1. Verificar la Autoridad Certificadora (CA): Asegurarse de que el certificado SSL/TLS esté emitido por una CA confiable.
2. Renovar Certificados Expirados: Renovar cualquier certificado que haya caducado.
3. Configurar Correctamente el Servidor: Usar solo protocolos seguros como TLS 1.2 o TLS 1.3 y asegurar una configuración correcta del servidor.
4. Comprobar el Nombre del Dominio: Asegurarse de que el nombre en el certificado coincida con el nombre del dominio al que se accede.
5. Utilizar Herramientas de Verificación: Examinar la configuración SSL/TLS con herramientas como OpenSSL o SSL Labs' SSL Test.
6. Aplicar Mejores Prácticas: Seguir las recomendaciones actuales de seguridad para la implementación de SSL/TLS.
7. Implementar HSTS: Considerar el uso de HSTS para reforzar el uso de conexiones seguras.

## 8. Vulnerabilidad: SSL Self-signed certificate

Solución:

1. Adquirir un Certificado de una Autoridad Certificadora (CA) Confiable: Obtener un certificado SSL/TLS de una CA reconocida.
2. Instalar y Configurar el Nuevo Certificado: Instalar el nuevo certificado en el servidor y configurar el servidor para utilizarlo.
3. Redirigir el tráfico a HTTPS: Configurar el servidor para redirigir automáticamente todo el tráfico de HTTP a HTTPS.
4. Implementar HSTS: Activar la Política de Seguridad de Transporte Estricto de HTTP (HSTS) en el servidor.
5. Monitorizar y Renovar los Certificados: Establecer procedimientos para renovar el certificado antes de que expire y verificar regularmente la configuración del SSL/TLS.

Vulnerabilidad: SSL certificate with wrong hostname

Solución:

1. Verificar el nombre del dominio en el certificado.
2. Obtener un nuevo certificado con el nombre correcto.
3. Instalar y configurar el nuevo certificado en el servidor.
4. Redirigir todo el tráfico a HTTPS.
5. Utilizar certificados wildcard o SAN si es necesario.
6. Testear la configuración del certificado.
7. Monitorear y renovar los certificados regularmente.

Vulnerabilidad: SSL certificate expiry

Solución:

La vulnerabilidad "SSL certificate expiry" ocurre cuando un certificado SSL/TLS utilizado en un servidor ha expirado, lo que puede resultar en advertencias de seguridad en los

navegadores, disminución de la confianza de los usuarios y potencial interrupción de los servicios. Aquí está una solución resumida para esta vulnerabilidad:

1. Monitorear la Fecha de Expiración: Implementar un sistema de monitoreo para alertar antes de la fecha de expiración del certificado.
  2. Renovar el Certificado a Tiempo: Solicitar y renovar el certificado antes de que expire, preferiblemente varios días o semanas antes.
  3. Instalar el Nuevo Certificado: Configurar el servidor con el nuevo certificado y asegurarse de que está activo.
  4. Verificar la Configuración: Testear el sitio web utilizando herramientas como SSL Labs para asegurarse de que el nuevo certificado esté funcionando correctamente.
  5. Automatizar el Proceso de Renovación: Considerar la implementación de soluciones como Let's Encrypt para la renovación automática de certificados.
- 
6. Vulnerabilidad: MS16-047: Security update for SAM and LSAD remote protocols (3148527) (Badlock) (Unauthenticated check)

Solución: Esta actualización de seguridad está clasificada como importante para todas las ediciones compatibles de Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows 8.1, Windows Server 2012, Windows Server 2012 R2, Windows RT 8.1 y Windows 10. En nuestro caso el host que tiene esta vulnerabilidad es sistema operativo Microsoft Windows 8.1 Pro.

El parche se puede descargar en el [Boletín de seguridad de Microsoft MS16-047 - Importante](#)

Sistema operativo	Vulnerabilidad de degradación de Windows SAM y LSAD: CVE-2016-0128 <a href="#">↗</a>	Actualizaciones reemplazadas*
Windows 8.1		
<a href="#">Windows 8.1 para sistemas de 32 bits</a> <a href="#">↗</a> (3149090)	<b>Importante</b> Elevación de privilegios	3050514 en <a href="#">MS15-052</a> <a href="#">↗</a>
<a href="#">Windows 8.1 para sistemas basados en x64</a> <a href="#">↗</a> (3149090)	<b>Importante</b> Elevación de privilegios	3050514 en <a href="#">MS15-052</a> <a href="#">↗</a>

En nuestro caso descargamos la [Actualización de seguridad para Windows 8.1 \(KB3149090\)](#)

## **Plan de mitigación**

- Firewalls:

Configurar firewalls para restringir el acceso no autorizado a los servicios y recursos de red.

- Políticas de acceso:

Crear políticas de acceso para limitar los privilegios de usuario y restringir el acceso a recursos e información sensibles.

## **Plan de mantenimiento**

- Gestión de parches:

Desarrollar un proceso para la gestión de parches para garantizar que los sistemas estén siempre actualizados con los últimos parches de seguridad requeridos.

- Formación y concientización:

Realizar campañas de formación y concientización en materia de ciberseguridad a los empleados para reducir el riesgo de caer en estafas y trampas digitales y prevenir posibles ataques o infecciones del equipo de la empresa.

- Plan de respuesta a incidentes:

Desarrollar un plan detallado de respuesta a posibles ataques para abordar rápidamente cualquier brecha de seguridad dentro de los equipos y minimizar su impacto.

- Actualización de políticas de seguridad:

Revisar y actualizar regularmente las políticas de seguridad para prepararse de las nuevas amenazas y adaptarse a las tecnologías emergentes.

## **Evaluación final**

Al evaluar finalmente las vulnerabilidades nos dimos cuenta que los host 192.168.68.109 (Microsoft Windows 7 Ultimate), 192.168.68.129 (Microsoft Windows 8.1 Pro) y 192.168.68.123 (Microsoft Windows 8.1 Pro) que compartían la misma vulnerabilidad de Unsupported Windows OS (remote) no tenían instalado ese sistema operativo que nos

arrojaba el análisis de Nessus, todos estos host tienen instalado actualmente el OS Windows 10, investigando nos dimos cuenta que Nessus muchas veces daba falsos errores en este tipo de vulnerabilidad.

Este error también hizo que la vulnerabilidad MS17-010: Security update for Microsoft Windows SMB server encontrada en esos mismos host ya había sido solucionada puesto que Windows 10 ya incluye el parche para esa vulnerabilidad.

La vulnerabilidad de SMB Signing not required fue resuelta en todos los dispositivos posibles y la vulnerabilidad MS16-047 encontrada en el host 192.168.68.129 también fue solucionada con Windows 10.

Por último, las vulnerabilidades de SSL no se necesitan solucionar de manera inmediata ya que por el momento la página web de la empresa se encuentra en reestructuración y se dejó de pagar el certificado SSL hasta que la página web entre en funcionamiento nuevamente.

## **Conclusiones finales**

La evaluación detallada de vulnerabilidades de ciberseguridad en la infraestructura tecnológica de La Güera Shoes nos dio una visión clara de los riesgos y deficiencias existentes. A través del uso de la herramienta Tenable Nessus Profesional, pudimos realizar un escaneo de vulnerabilidades y eso nos permitió identificarlas y priorizar sus soluciones en nuestro plan de medidas correctivas, preventivas y de mitigación efectiva.

En el proceso de solución, se identificaron varias vulnerabilidades que ya habían sido abordadas de manera indirecta, esto con actualizaciones automáticas de los propios equipos. Además de que las vulnerabilidades relacionadas con los certificados SSL no requerían de atención inmediata por una reestructuración en la página web de la empresa.

Gracias al análisis realizado pudimos tener una base sólida para la solución y mitigación de las vulnerabilidades, sin embargo, es de suma importancia realizar seguimiento constante y si es necesario actualizar las políticas de ciberseguridad de la empresa, así como realizar planes de mitigación y mantenimiento con la ayuda de expertos en el área, y garantizar una participación proactiva con todos los colaboradores de la empresa a través de capacitaciones en la seguridad cibernética.



## **Referencias**

Qué es un certificado SSL: definición y explicación. (2024, 19 marzo). latam.kaspersky.com.

<https://latam.kaspersky.com/resource-center/definitions/what-is-a-ssl-certificate>

Protocolo SMB. (2023, 3 noviembre). IBM documentation.

<https://www.ibm.com/docs/es/aix/7.3?topic=management-smb-protocol>