**PRÁCTICA N°1**

**TEMA: “Evaluación y Protección de Vulnerabilidades en Windows”**

**1. OBJETIVOS**

1.1 Familiarizar al estudiante con las vulnerabilidades en Windows

1.2 Implementar Políticas de seguridad en Windows para disminuir riesgos.

1.3 Introducir al estudiante en el uso de herramientas de exploración de red y auditoria de seguridad.

**5. INFORME**

5.1 Analizar los temas abordados en la sesión práctica y presentar un resumen.

Conocer las herramientas de escaneo para tener la claridad de como utilizar e interpretar los resultados del escaneo permite tener correcciones sobre las brechas de seguridad encontrada en as redes y puertos de una organización.

Nessus permite hacer escaneo de la red completa de una organización generando un reporte con las vulnerabilidades encontradas como falta de actualización del software.

Nmap permite realizar escaneo de puertos e identificar cuales se encuentra abiertos y poder corregís de igual manera los servicios.

5.2 Identificar las Vulnerabilidades encontradas en la red.

#### **Resultados del escaneo Nessus**

Luego de ejecutar el escaneo de puertos, Nessus genera un informe sobre las vulnerabilidades descubiertas. En la Figura 1 se muestra el resultado de ejecutar el escaneo, indicando que existen 6 vulnerabilidades de tipo Media y 89 de información según el cvss.

La política aplicada al escaneo es Avanzada, basándose en la base de gravedad del sistema de puntuación de vulnerabilidades cvss versión 3.0.

Captura de pantalla de computadora

Descripción generada automáticamente

Figura 1: Resultado de escaneo

En la Figura 2 se ingresa a los resultados del escaneo y se visualiza las vulnerabilidades en un listado.

Captura de pantalla de computadora

Descripción generada automáticamente

Figura 2: Listado de Vulnerabilidades

La primera vulnerabilidad que se observa, médium con un score de 5.3, de la familia Misceláneo. cómo se indica en la Figura 3 la vulnerabilidad con la descripción de “No se requiere firma SMB”, es decir que al no solicitar la firma al servidor SMB remoto, un atacante no autorizado puede aprovechar esta puerta para poder enviar un ataque al servidor SBM.

Nessus recomienda imponer la firma SMB, realizando configuraciones en Windows > configuraciones > configuración de políticas > Servidor de red de Microsoft.

El puerto asociado a este escaneo es el 445/tcp/cifs.

Captura de pantalla de computadora

Descripción generada automáticamente

Figura3: Vulnerabilidad Media: No se requiere firma SBM

La siguiente Vulnerabilidad es la segunda fila, la cual dice MIXED (Figura 4), de la familia general como se muestra en la Figura 5, ingresando a la carpeta, se visualiza dos vulnerabilidades de tipo Medio con un escore de 6,5.

Captura de pantalla de computadora

Descripción generada automáticamente

Figura 4: Carpeta Mixed 1

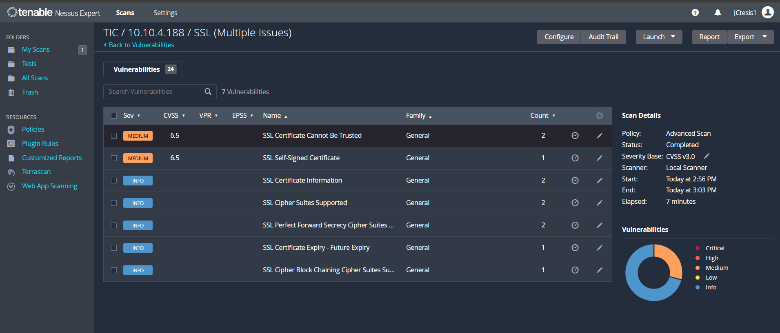


Figura 5: Primera Carpeta Mixed

En la Figura 6 se observa la vulnerabilidad “No se puede confiar en el certificado SSL”, esta indica que se puede romper la cadena de confianza de tres maneras diferentes:

Texto

Descripción generada automáticamente con confianza baja

Figura 6: Vulnerabilidad: No se puede confiar en el certificado SSL

La certificación enviada por el servidor no podría descender de una autoridad de certificación publica conocida, es decir, la certificación no puede ser reconocida o faltan certificados intermedios.

La cadena de certificaciones cuenta con un certificado no valido al momento de realizar el escaneo.

El certificado puede contener una firma que no coincida con la información del certificado o no se pudo verificar la autenticidad de esta, como se muestra en la Figura 7.

Captura de pantalla de computadora

Descripción generada automáticamente

Figura 7: Certificado Firmado por un desconocido

La solución para prevenir ser vulnerados es generar un certificado SSL adecuado para el servicio.

La siguiente Vulnerabilidad de tipo Media con un score de 6,5 dentro de la primera carpeta Mixed, indica que el Certificado auto firmado SSL (Figura 8), es decir, que no está firmado por una autoridad de certificación reconocida, como se muestra en la Figura 9.

Captura de pantalla de computadora

Descripción generada automáticamente con confianza media

Figura 8: Certificado Auto firmado SSL

Captura de pantalla de computadora

Descripción generada automáticamente

Figura 9: Resultado de certificado auto firmado

La recomendación ante esta vulnerabilidad, al igual que la anterior, se recomienda comprar o generar un certificado SSL adecuado para el servicio.

En la última carpeta de Mixed como se muestra en la Figura 10, se observa 2 vulnerabilidades de tipo Medio, con un score de 6.5 dentro del esquema de puntuación de vulnerabilidades cvss.

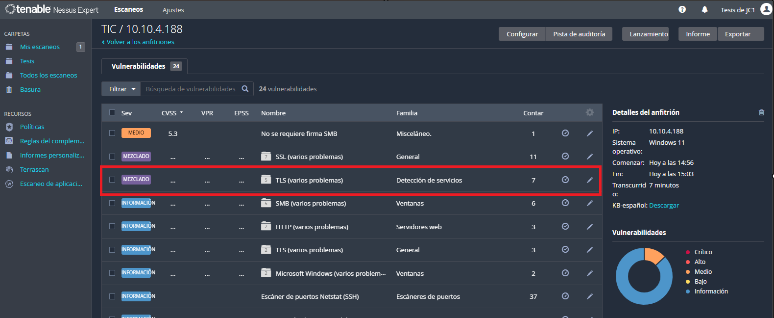


Figura 10: Carpeta Mixed 2

La primera vulnerabilidad se trata de la Detección del protocolo TLS versión 1.0 (Figura 11), presenta una serie de fallas en el diseño criptográfico, es decir, impide a los navegadores tener una conexión segura son algún sitio web (Figura 12).

Captura de pantalla de computadora

Descripción generada automáticamente

Figura 11: Vulnerabilidad: Detección del protocolo TLS versión 1.0

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Figura 12: TLSv1 Activado

Lo recomendable para mitigar esta vulnerabilidad es actualizar las conexiones cifradas mediante TSL1.2 Y TSL 1.3.

La segunda Vulnerabilidad es el Protocolo TLS versión 1.1 en desuso como lo muestra la Figura 13.

Captura de pantalla de computadora

Descripción generada automáticamente

Figura 13: Vulnerabilidad TLS versión 1.1 en desuso

Este protocolo no es compatible con los cifrados actuales y recomendados (Figura 14), lo recomendable es actualizar al protocolo TLS 1.2 y/o 1.3, de esta manera se tiene correcto funcionamiento de los navegadores web y proveedores principales.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Figura 14: TLS versión 1.1 Habilitado

5.3 Identificar el estado de los puertos y vulnerabilidades encontradas con la herramienta Nmap.

#### **Resultados del escaneo INTERFAZ NMAP**

Luego de realizar el escaneo mostrado en la Figura 3.15 del puerto 80 comúnmente utilizado para servicios HTTP, el estado señala que se encuentra cerrado, por tal razón indica que no existe servidor web en funcionamiento sobre el dispositivo o como es este caso se configuro para que el servicio o responda a ese puerto.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Figura 3. 15: Resultados escaneo puerto 80

En la Figura 3.16 indica los resultados de un escaneo completo de puertos

Interfaz de usuario gráfica, Texto

Descripción generada automáticamente

Figura 3. 16

#### **Resultados del escaneo INTERFAZ CMD**

A continuación de realizar el escaneo por la interfaz de nmap, se realiza el mismo escaneo por el cmd mostrando en la Figura 17 que el dispositivo asociado a la dirección IP 102.168.100.74 está activo pero el puerto 80 que está configurado para TCP se encuentra cerrado lo que indica que no está disponible para conexiones.

Texto

Descripción generada automáticamente

Figura 17

Al realizar un escaneo completo de todos los puertos el resultado de la Figura 18 informa que el puerto 135, 139 y 455 tienen servicios de red de Windows activos el dispositivo puede ser vulnerable a ataques.

Texto

Descripción generada automáticamente

Figura 18