

Proyecto 1 - Seguridad Informática Básica – Gpo. 2 Fecha de entrega: 31 /10/ 23

Equipo 4 || Integrantes:

Castelan Ramos Carlos	317042711
Martínez González Héctor Eduardo	316322122
Martínez Sánchez Berenice Vianney	317581223
Pineda González Rodrigo	317224397
Vega Alvarez Marcos	420054432

10

Indicaciones:

Trabaje con su equipo siguiendo las siguientes indicaciones. Fecha de entrega: 31-octubre-2023 Nombre del archivo: EquipoXProyecto1.pdf Donde X se sustituye con el número de su equipo Suponga que va a dar un curso de capacitación en una organización y necesita que los asistentes refuercen lo visto en el curso mediante la puesta en práctica de los conocimientos adquiridos. Con su equipo diseñe 3 prácticas para cumplir con esto, para ello:

1. Considere los 3 temas del temario de la asignatura, ya vistos en la clase:
 - I. Fundamentos teóricos
 - II. Amenazas y vulnerabilidades
 - III. Identificación de ataques y técnicas de intrusión
2. Realice una propuesta de 3 prácticas de laboratorio (una por cada tema), para reforzar el tema visto en la clase.
3. Cada práctica debe contener:
 - a) Nombre de la práctica
 - b) Tema a reforzar
 - c) Objetivo u objetivos que se deben cubrir
 - d) Material a utilizar (puede ser físico o digital, o la combinación de ambos)
 - e) Paso por paso el planteamiento detallado y claro de las actividades que se deben ir desarrollando y la manera en la que se deben ir presentando los resultados.
4. Cada equipo propondrá su formato, puede emplear imágenes, tablas, diversas fuentes y colores para hacer su escrito.
5. En el proyecto se considerará:
 - 25% Diseño, desarrollo completos y viables de la práctica correspondiente al Tema I
 - 25% Diseño, desarrollo completos y viables de la práctica correspondiente al Tema II
 - 25% Diseño desarrollo completos y viables de la práctica correspondiente al Tema II
 - 25% Presentación del proyecto (Orden, redacción, ortografía, claridad en la exposición de ideas, el archivo debe contener las 3 prácticas donde visiblemente se note dónde empieza una y acaba la otra)



Temas a reforzar

"En este documento, se llevará a cabo una práctica con el propósito de fortalecer los conceptos del primer tema de la asignatura de Seguridad Informática Básica, titulado 'Fundamentos Teóricos'."

Objetivo(s) de aprendizaje

El alumno aplicará los conceptos teóricos relacionados con la seguridad informática, incluyendo los conceptos, objetivos y antecedentes históricos, como base para llevar a cabo una práctica que le permitirá reforzar y mejorar su comprensión, dentro del marco histórico y utilizando los modelos de seguridad existentes.

Material a utilizar

1. Hojas blancas
2. Lápiz
3. Plumas
4. Colores
5. Dispositivo con acceso a internet (Laptop, smartphone o tablet)

Planteamiento teórico

La seguridad informática es un campo crucial en la era digital, donde la información y la tecnología son activos valiosos. La seguridad informática se refiere a la protección de bienes o activos, ya sean tangibles o intangibles, y está amenazada por diversos factores que pueden poner en riesgo la confidencialidad, integridad y disponibilidad de la información. Estos factores se conocen como amenazas y vulnerabilidades. Existen dos tipos de seguridad con respecto a la naturaleza de la amenaza: lógica y física.

En el ámbito de la seguridad informática, los bienes son los activos que se desean proteger. Estos pueden ser información, sistemas, aplicaciones, infraestructura, entre otros. Es importante identificar estos bienes para poder aplicar medidas preventivas y correctoras para eliminar los riesgos asociados o para reducirlos a niveles que puedan transmitir o tomar el riesgo. Los objetivos de la seguridad informática pueden verse satisfechos si se garantizan los seis servicios de seguridad:

- **Integridad:** Garantizar que los datos sean los que se supone que son, sin modificaciones no contempladas.
- **Confidencialidad:** Asegurar que sólo los individuos autorizados tengan acceso al bien o recurso.
- **Disponibilidad:** Garantizar el correcto funcionamiento de los sistemas de información cuando se desee acceder, en los horarios establecidos para esto.
- **No repudio:** Certificar que una operación realizada no pueda ser negada.
- **Control de acceso:** Avalar que sólo los individuos autorizados tengan acceso al bien o a los recursos.
- **Autenticación:** Verificar que la persona sea quien dice ser.

Por otro lado, el ciclo PDCA (Planificar, Hacer, Verificar y Actuar) es un modelo de mejora continua que se puede aplicar a la seguridad informática para mejorar continuamente los procesos de seguridad. Finalmente, una de las responsabilidades principales de las organizaciones es garantizar la seguridad de su información, protegiéndola de riesgos que puedan afectar los objetivos que resguardan los servicios de seguridad. Para lograr esto, se deben establecer normas y políticas que se apliquen tanto a los sistemas que manejan los datos como a cada uno de los miembros de la empresa. Estas normativas establecen los requisitos mínimos para garantizar la seguridad de los sistemas y datos. Usualmente estas normativas no proporcionan detalles sobre cómo implementar específicamente un Sistema de Gestión de Seguridad de la Información (SGSI), sino que establecen pautas que se adaptan a cada empresa u organización que, al estar estandarizadas, facilita su evaluación.

Desarrollo

Modo de trabajo:

La práctica se desarrollará en equipos de tres integrantes. Tiempo estimado: 2 horas.

Actividad 1. Introducción a la seguridad informática.

Cada integrante del equipo, deberá resolver individualmente el siguiente juego online, deberán escribir sus nombres con el orden en el que ganaron y el puntaje obtenido.

Link del juego;
<https://www.cerebriti.com/juegos-de-tecnologia/introduccion-a-la-seguridad-informatica>

Primer lugar y puntaje:

Segundo lugar y puntaje:

Tercer lugar y puntaje:

Actividad 2. Identificación de bienes.

Imaginemos una clínica médica llamada "Salud Total" que maneja información crítica de sus pacientes, incluyendo registros médicos, historiales de tratamiento, información personal y financiera. La clínica se preocupa por la seguridad de estos datos debido a la creciente amenaza de ciberataques y la necesidad de cumplir con las regulaciones de privacidad de la salud.

Con esta información, identifica y redacta detalladamente lo siguiente:

a) ¿Qué se quiere proteger?

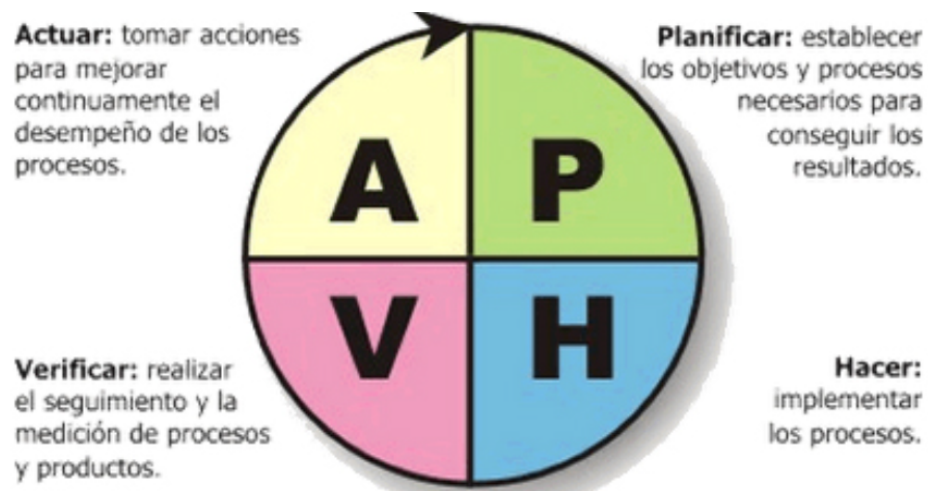
b) ¿De qué se quiere proteger?

c) ¿Cómo se va a proteger?

Actividad 3. Ciclo PDCA.

Basado en el escenario anterior, con su equipo de trabajo dibujen en una hoja blanca el ciclo PDCA (Plan (planificar), Do (hacer), Check (verificar) y Act (actuar)), donde van a escribir en cada etapa del ciclo, las acciones que van a desarrollar para salvaguardar a la “Salud total”.

Ejemplo:



Ciclo PDCA / PHVA

Actividad 4. Normas de seguridad informática.

A continuación, relaciona las normativas de seguridad con sus características y años, posteriormente escribe cuál crees que es la que podríamos adaptar a nuestro escenario de nuestra clínica. Justifica tu respuesta.

Normas de seguridad informática	Corresponde a (inciso)
ISO/IEC 27000	(___)
ISO/IEC 17799	(___)
BS 7799	(___)
ISO 15408	(___)
ITSEC	(___)
CTCPEC	(___)
CCITSE TCSEC	(___)

Descripciones
A. Estándar internacional para la gestión de la seguridad de la información.
B. Se centra en la evaluación de la seguridad de los productos y sistemas de tecnología de la información.
C. También conocida como ISO/IEC 27002, se enfoca en los controles de seguridad de la información.
D. Norma británica que fue precursora de la serie ISO/IEC 27000.
E. Estándar de seguridad utilizado en la evaluación de productos y sistemas de tecnología de la información en el Reino Unido.
F. Establece requisitos y evaluación de la seguridad de los productos de tecnología de la información.

Norma para nuestro escenario (justifique):

Actividad 5. Servicios de seguridad.

Supongamos que trabajan como consultores de seguridad para una empresa de servicios financieros llamada "FinTech Secure." FinTech Secure es una empresa que ofrece servicios financieros en línea, incluyendo gestión de inversiones, transferencias de fondos y banca en línea. La empresa almacena información financiera confidencial de sus clientes y debe garantizar la seguridad de sus sistemas y datos. Su trabajo es identificar cómo y dónde implementar los servicios de seguridad, no olviden ningún detalle para establecerlos, de ello depende tu trabajo y el correcto funcionamiento de la empresa.

Confidencialidad

Autenticación

Integridad

No repudio

Control de acceso

Disponibilidad

Conclusiones (Individuales):

Presentación de resultados

Para esta práctica, los resultados se entregan en el propio cuerpo de este documento. En caso de requerirse, se pueden agregar respuestas en hojas blancas, donde para cada una se especifique el número de la actividad o pregunta, seguida de su respuesta y anexar dichas hojas al final de este documento.

Referencias

- Tcm. (2022, 28 julio). *Qué es el ciclo PDCA. fases y ejemplos*. TCM Consultoría y Formación.
<https://www.tcmetrologia.com/blog/que-es-el-ciclo-pdca-fases-y-ejemplos/>
- Flores Román, L.H & Hernández Hernández, G.G. (2011). Pruebas de Hacking Ético en un Laboratorio de la Facultad de Ingeniería de la UNAM. Tema 1. Fundamentos teóricos [Tesis de Titulación, Universidad Nacional Autónoma de México]. Repositorio Institucional – Ptolomeo.
<http://www.ptolomeo.unam.mx:8080/jspui/bitstream/132.248.52.100/203/4/A4.pdf>



*NOTA: El texto escrito en **rojo** representan posibles respuestas que el profesor puede considerar para evaluar, este texto no debe aparecer en la versión final, solo es una muestra para la propuesta de práctica.*

Temas a reforzar

Esta práctica reforzará los conceptos sobre amenazas y vulnerabilidades, así como su detección e identificación de forma preceptiva, además se desarrollarán habilidades para la aplicación de software para la detección de vulnerabilidades en equipos computacionales.

Objetivo(s) de aprendizaje:

- El alumno reforzará su comprensión de las amenazas y vulnerabilidades en seguridad informática.
- El alumno se familiarizará con la identificación y mitigación de amenazas y vulnerabilidades.
- El alumno aplicará la aplicación de medidas de seguridad para proteger un sistema.

Material a utilizar

1. Computadora con acceso a internet.
2. Herramienta de escaneo de vulnerabilidades "Nessus".
3. Documentación sobre amenazas y vulnerabilidades comunes.
4. Papel y pluma para anotaciones.

Planteamiento teórico

La seguridad es un elemento crucial para la protección de bienes o activos, ya sean tangibles o intangibles, así entonces la seguridad es un campo crucial en la era digital, donde la información y la tecnología son activos valiosos. Sin embargo, esta seguridad está amenazada por diversos factores que pueden poner en riesgo la confidencialidad, integridad y disponibilidad de la información. Estos factores se conocen como amenazas y vulnerabilidades.

Amenazas en Seguridad Informática:

Las amenazas son eventos o circunstancias que tienen el potencial de causar daño a un sistema o a la información. Pueden ser internas o externas y pueden ser maliciosas o no maliciosas.

Vulnerabilidades en Seguridad Informática:

Las vulnerabilidades son debilidades o fallas en un sistema que pueden ser explotadas por amenazas para comprometer la seguridad. Estas debilidades pueden residir en software, hardware, configuraciones o incluso en prácticas de seguridad deficientes.

Herramientas de escaneo de vulnerabilidades:

Una herramienta de escaneo de vulnerabilidades es un software o programa diseñado para identificar y evaluar vulnerabilidades en sistemas informáticos, redes, aplicaciones o dispositivos. Estas herramientas son utilizadas por profesionales de seguridad informática y administradores de sistemas para identificar posibles debilidades que podrían ser explotadas por amenazas, como hackers o malware.

Nessus:

Nessus es una herramienta de escaneo de vulnerabilidades ampliamente reconocida y utilizada en el campo de la seguridad informática. Ofrece un escaneo automatizado de sistemas y redes para identificar una amplia variedad de vulnerabilidades, desde problemas de configuración hasta debilidades de software y sistemas operativos. Nessus cuenta con una base de datos de vulnerabilidades actualizada constantemente y proporciona evaluaciones de riesgos detalladas para priorizar las correcciones. La herramienta permite la generación de informes personalizables y la programación de escaneos regulares para un monitoreo continuo de la seguridad. Disponible en varias ediciones, Nessus es una opción versátil que contribuye a mejorar la seguridad informática y el cumplimiento regulatorio en organizaciones de diferentes tamaños.

Desarrollo

Modo de trabajo:

La práctica se desarrollará en equipos de 2 integrantes. Tiempo estimado: 2-4 horas.

Actividad 1. Definición de amenazas y vulnerabilidades.

Junto a su compañero, escriba 5 por integrante en los cuales existan amenazas o vulnerabilidades dentro de una de las bibliotecas de la Facultad de Ingeniería (Enrique Rivero Borrell (Edificio L), Antonio Dovalí Jaime (Conjunto Norte) o Enzo Levi (Edificio W)); a continuación su compañero deberá decir si el evento es una amenaza o vulnerabilidad y cómo podría solucionarse.

Alumno 1.

Evento	Amenaza / Vulnerabilidad ¿Por qué?
1.	
2.	
3.	
4.	
5.	

Tabla Alumno 1

Alumno 2.

Evento	Amenaza / Vulnerabilidad ¿Por qué?
1.	
2.	
3.	
4.	
5.	

Tabla Alumno 2

Actividad 2. Identificación de amenazas y vulnerabilidades.

En esta actividad, los alumnos tendrán la oportunidad de identificar amenazas y vulnerabilidades en el entorno de seguridad de una pequeña empresa de comercio electrónico llamada "RodriShop". La empresa vende productos en línea y almacena datos de clientes y transacciones en su sistema. El objetivo es que el alumno analice la situación y proponga medidas de mitigación.

Escenario:

RodriShop es una pequeña empresa de comercio electrónico que vende productos electrónicos y dispositivos móviles. La empresa ha experimentado un rápido crecimiento en los últimos meses y está interesada en mejorar su seguridad informática. Un estudiante de seguridad informática es contratado como consultor para evaluar la seguridad de la empresa.

Tareas del Alumno:

Actividad 2.1.1 Identificación de Activos Críticos:

El alumno debe identificar los activos y bienes que podrían ser atacados.

(Como datos de clientes, información de tarjetas de crédito, registros de ventas, y el sistema de comercio electrónico.)

Actividad 2.1.2 Identificación de Amenazas Potenciales:

El estudiante debe identificar posibles amenazas que afecten los bienes

(Como ataques de hacking, malware, robo de datos, ataques de denegación de servicio (DoS), y errores humanos.)

Actividad 2.1.3 Identificación de Vulnerabilidades:

El alumno debe analizar el sistema de seguridad actual de RodriShop y detectar vulnerabilidades potenciales.

(Como:

- **Contraseñas débiles o mal gestionadas**
- **Falta de cifrado de datos confidenciales.**
- **Falta de actualizaciones de software.**
- **Acceso no autorizado a sistemas y datos.**
- **Insuficiente protección contra malware y phishing.)**

Actividad 2.1.4 Evaluación de Riesgos:

El estudiante debe evaluar el riesgo asociado a cada amenaza identificada y a las vulnerabilidades encontradas. Debe considerar el impacto potencial y la probabilidad de explotación.

Actividad 2.1.5 Propuesta de Medidas de Mitigación:

Basándose en la identificación de amenazas, vulnerabilidades y riesgos, el alumno debe proponer medidas de mitigación específicas para fortalecer la seguridad de RodriShop. **(Esto puede incluir la implementación de políticas de contraseñas más seguras, actualizaciones regulares de software, la adopción de soluciones de seguridad y la capacitación del personal.)**

Preguntas Teóricas:

Pregunta 2.2: ¿Cuáles son las amenazas más críticas para la empresa y por qué?

Pregunta 2.3: ¿Cómo pueden las vulnerabilidades específicas afectar la seguridad de la empresa?

Pregunta 2.4: ¿Cuáles son los principios clave de una buena gestión de contraseñas?

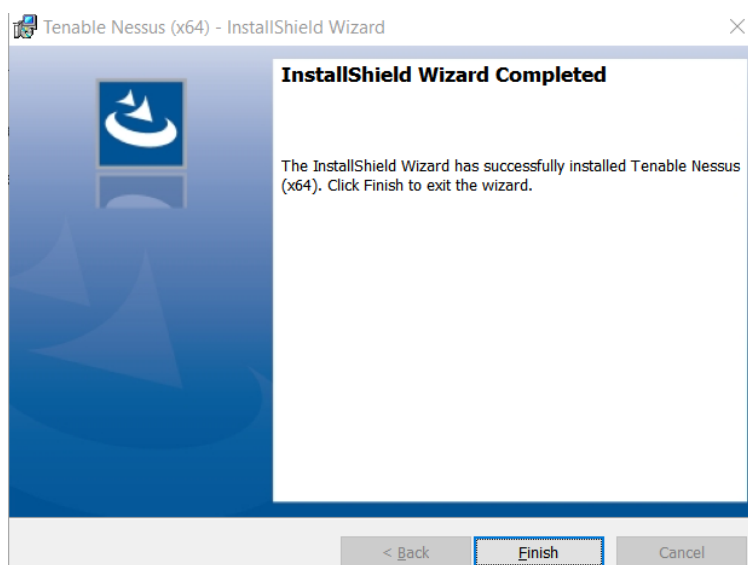
Pregunta 2.5: ¿Qué medidas de seguridad podrían proteger contra ataques de malware y phishing?

Pregunta 2.6: ¿Cómo se puede garantizar la seguridad de los datos de tarjetas de crédito?

Actividad 3. Herramienta de escaneo de vulnerabilidades Nessus.

Como ya se mencionó, Nessus es una herramienta de escaneo de vulnerabilidades demasiado utilizada en el campo de la seguridad informática, otorgando diferentes herramientas para la detección de vulnerabilidades en diferentes sistemas y redes. Nessus es capaz de otorgar soluciones a los problemas ya que cuenta con información detallada de las vulnerabilidades comunes en equipos.

Para poder iniciar el servicio es necesario instalar previamente la herramienta, que puede obtenerse a través del siguiente enlace: <https://www.tenable.com/downloads/nessus?loginAttempted=true>. Existe el soporte para diversas plataformas; para el desarrollo de esta práctica, se propone utilizar la versión 10.6.1 de la herramienta. A continuación, se muestra un instalador genérico, donde después de aceptar los términos y condiciones del uso de la herramienta, lo único que se define es la ruta de instalación. Una vez instalado se muestra una notificación como la siguiente:



Instalación exitosa.

Una vez instalado, se pueden realizar los siguientes pasos:

Paso 1. Iniciar el servicio:

Abrir un explorador y colocar: <https://localhost:8834/#/>

Paso 2. Iniciar sesión:

Colocar las credenciales otorgadas por el profesor. En caso de no contar con estas, necesitará un correo perteneciente a la organización (comunidad.unam, .edu, entre otros) para poder generar las credenciales de la versión gratuita (Nessus Essentials).

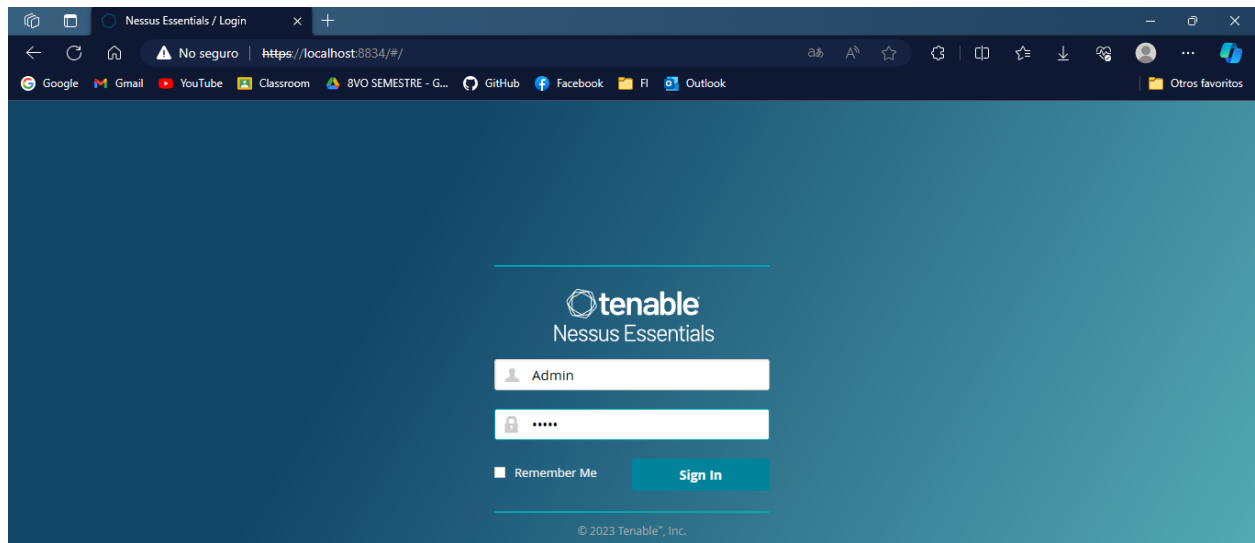


Imagen 1

Paso 3. Revisar las funcionalidades del servicio:

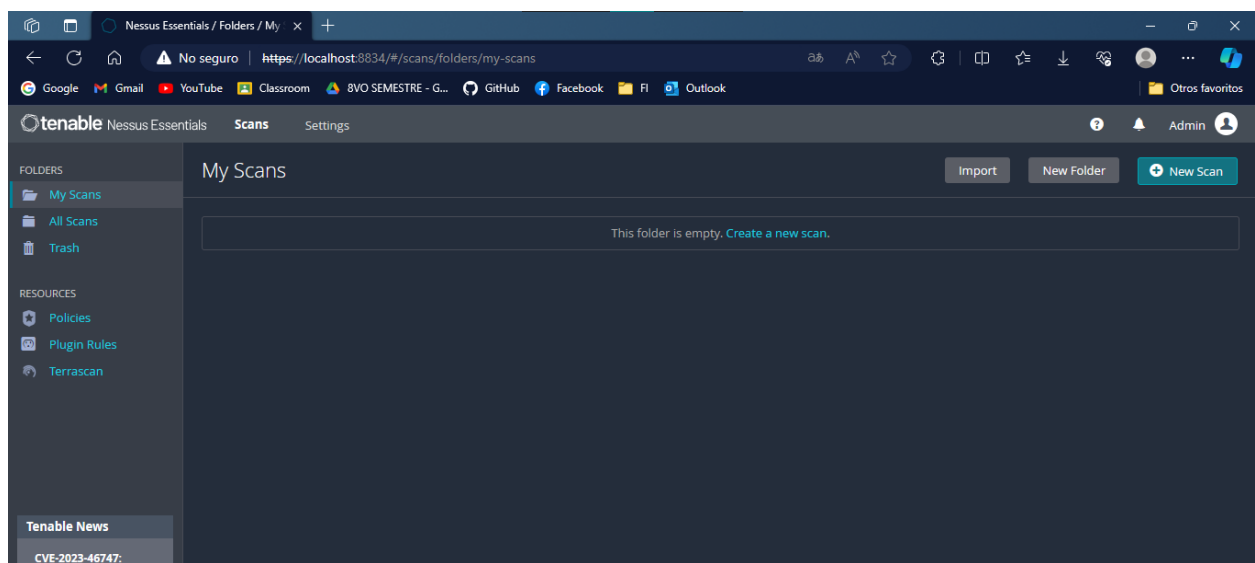


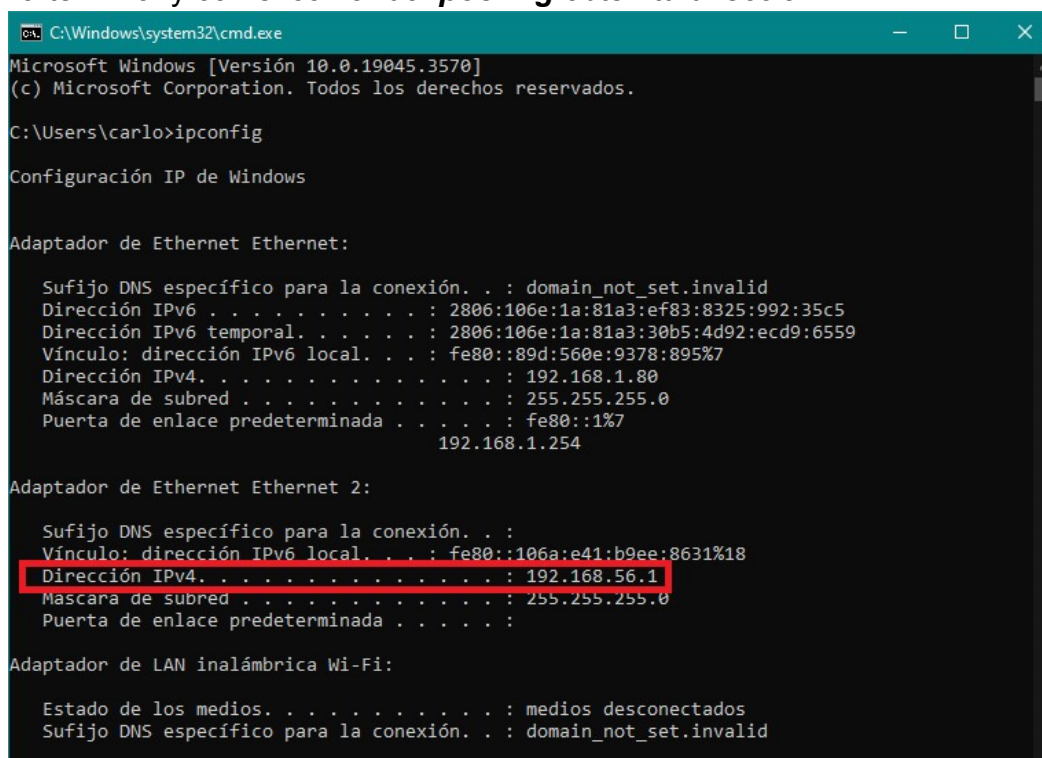
Imagen 2

Actividad 3.1 Búsqueda de vulnerabilidades en un equipo local conectado a internet.

En esta actividad el alumno realizará un escaneo de vulnerabilidades en la conexión del equipo que está utilizando.

Paso 1. Obtención de dirección IP.

Abre una terminal y con el comando **ipconfig** obtén tu dirección IPv4.



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Versión 10.0.19045.3570]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\carlo>ipconfig

Configuración IP de Windows

Adaptador de Ethernet Ethernet:

    Sufixo DNS específico para la conexión. . . : domain_not_set.invalid
    Dirección IPv6 . . . . . : 2806:106e:1a:81a3:ef83:8325:992:35c5
    Dirección IPv6 temporal. . . . . : 2806:106e:1a:81a3:30b5:4d92:ecd9:6559
    Vínculo: dirección IPv6 local. . . : fe80::89d:560e:9378:895%7
    Dirección IPv4. . . . . : 192.168.1.80
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . : fe80::1%7
                                                192.168.1.254

Adaptador de Ethernet Ethernet 2:

    Sufixo DNS específico para la conexión. . . :
    Vínculo: dirección IPv6 local. . . : fe80::106a:e41:b9ee:8631%18
    Dirección IPv4. . . . . : 192.168.56.1
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . :

Adaptador de LAN inalámbrica Wi-Fi:

    Estado de los medios. . . . . : medios desconectados
    Sufixo DNS específico para la conexión. . . : domain_not_set.invalid
```

Imagen 3

Coloca aquí tu dirección IPv4: _____

Paso 2. Realizar un nuevo escaneo:

Presiona el botón **New Scan**.

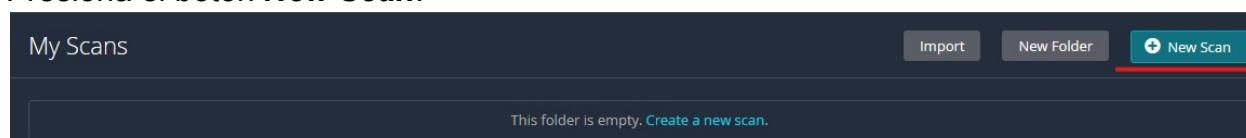


Imagen 4

Paso 3. Seleccionar y configurar servicio.

Selecciona la opción de **Basic Network Scan**.

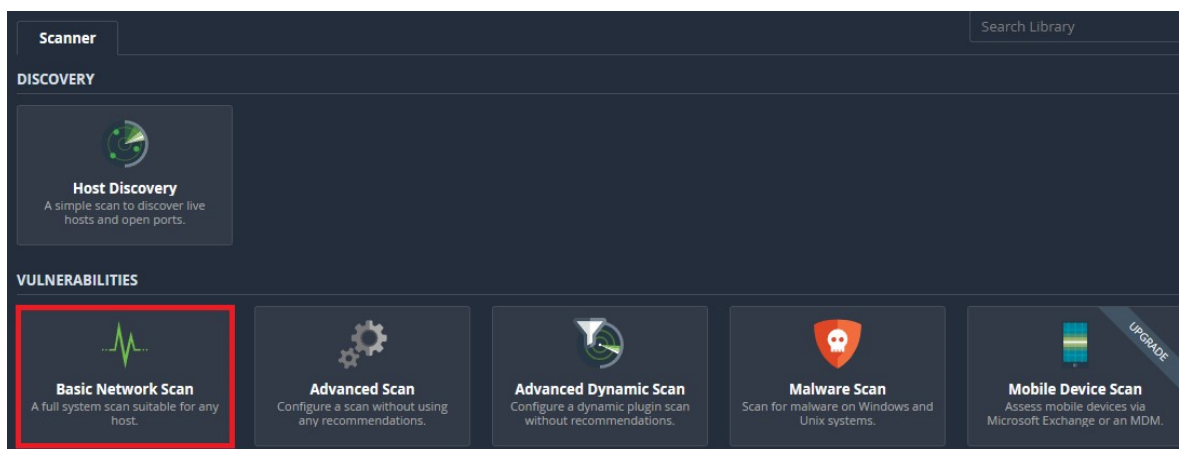


Imagen 5

Configura el servicio:

- Título: Actividad3.1 || Targets: Tu dirección IPv4(ejemplo 192.168.56.1)

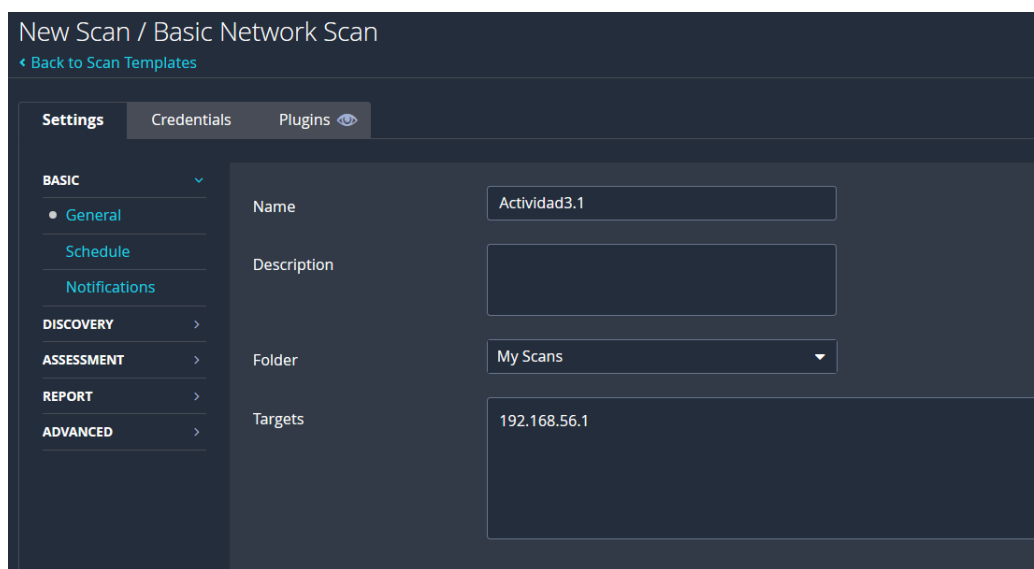


Imagen 6

Dar **Save**, para guardar la configuración.

Paso 4. Iniciar Escaneo.

La configuración estará guardada en la página principal, inicia el escaneo y espera los resultados. **NOTA: El escaneo puede tardar de 5 a 10 minutos.*

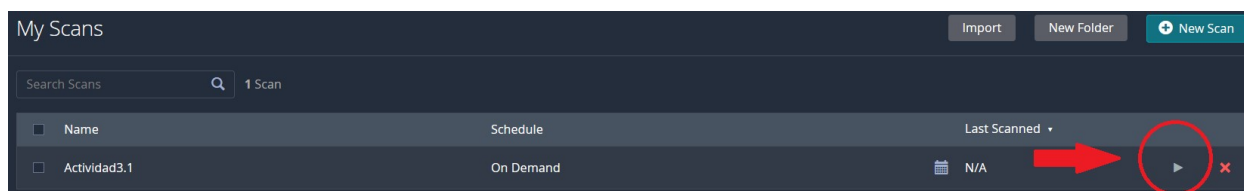


Imagen 7

Paso 5. Visualización de resultados.

Para observar los resultados presiona el escaneo cuando haya terminado y analiza las estadísticas.

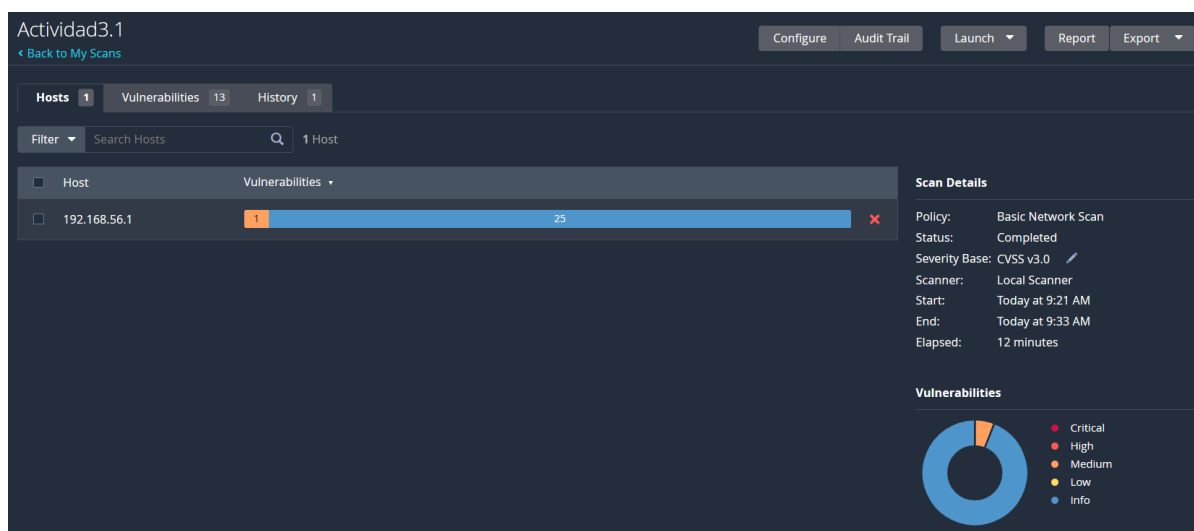


Imagen 8

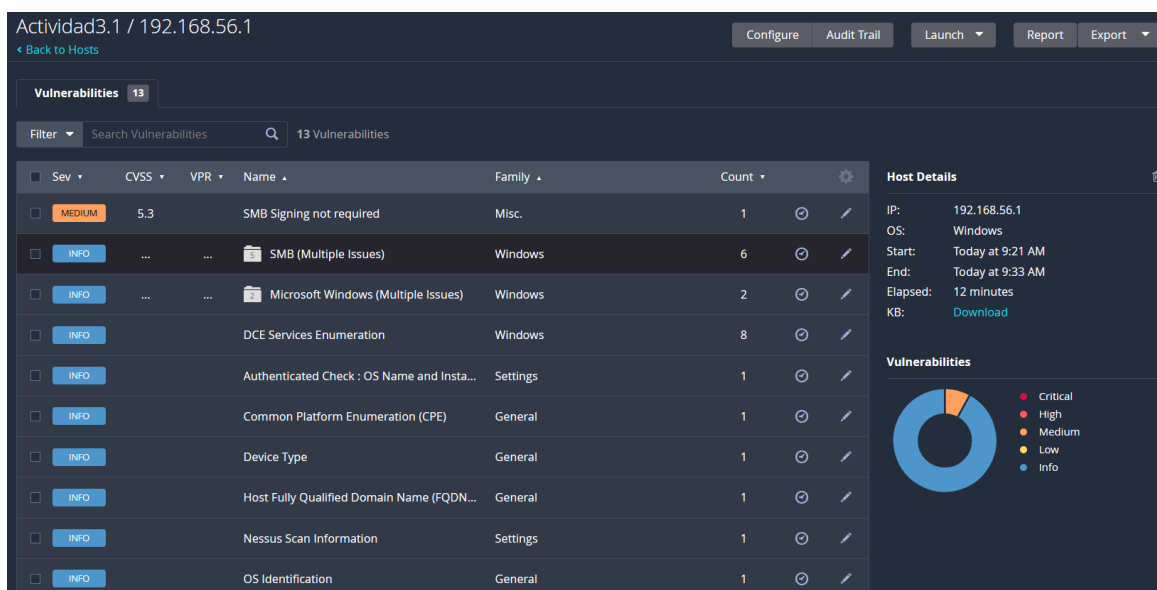


Imagen 9

Finalmente enlista los resultados de vulnerabilidades en tu equipo e investiga el de mayor nivel de amenaza que muestran los resultados. Si todos son del mismo nivel de amenaza, elige uno de tu interés.

Actividad 3.2 Búsqueda de vulnerabilidades en una página web.

En esta actividad el alumno realizará un escaneo de vulnerabilidades de una página web de su interés.

Paso 1. Realizar un nuevo escaneo:

Presiona el botón **New Scan**.

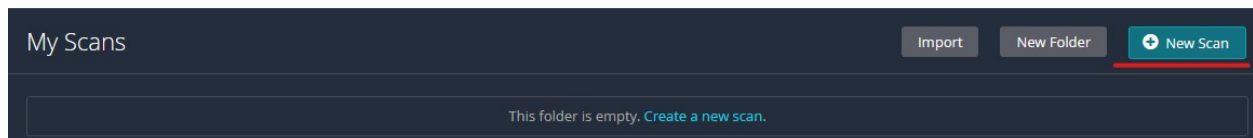


Imagen 10

Paso 2. Seleccionar y configurar servicio.

Selecciona la opción de **Advanced Scan**.

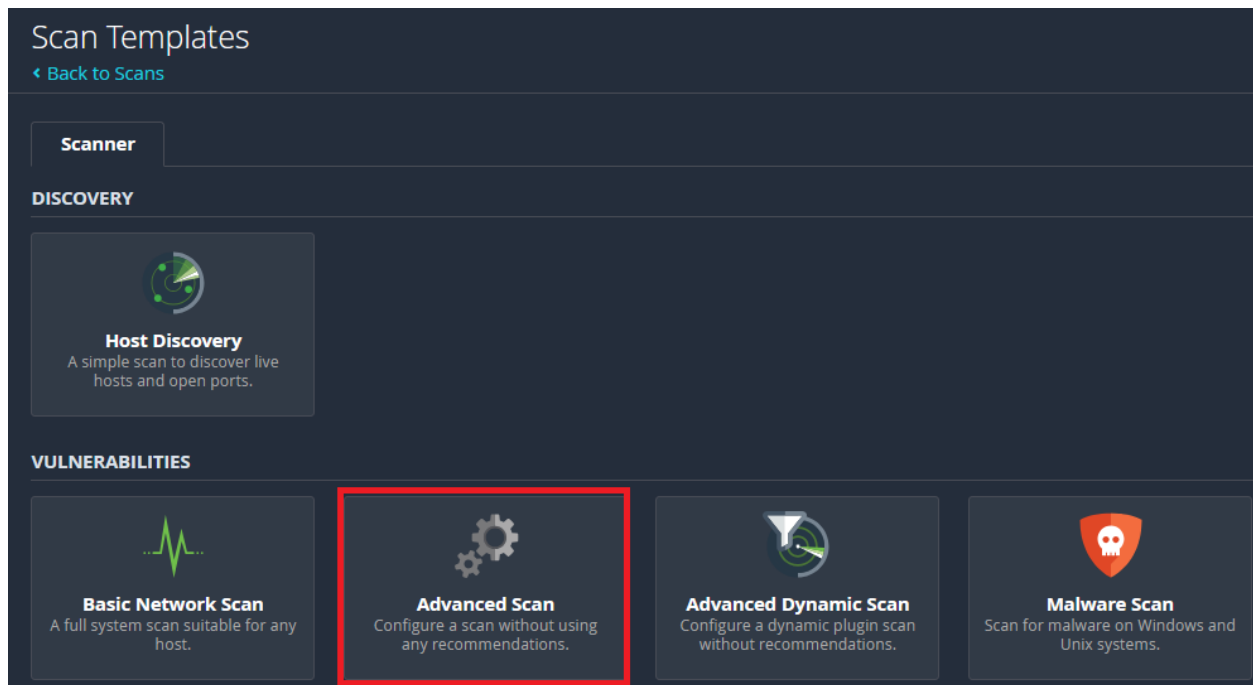


Imagen 11

Configura el servicio:

- Título: Actividad3.2
- Targets: Tu dirección de interés(www.ssa.ingenieria.unam.mx)
 - Es necesario quitar todo "/" y certificados ("http" o "https"), pues únicamente requiere el dominio.

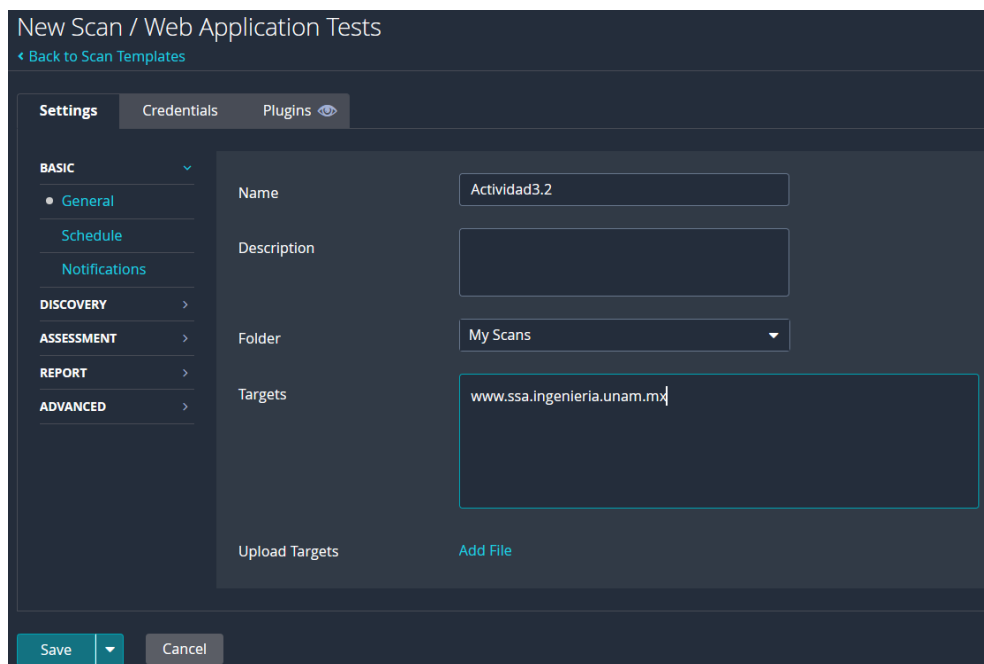


Imagen 12

Dar **Save**, para guardar la configuración.

Paso 4. Iniciar Escaneo.

La configuración estará guardada en la página principal, inicia el escaneo y espera los resultados.



Imagen 13

**NOTA: El escaneo puede tardar de 5 a 10 minutos.*

Paso 5. Visualización de resultados.

Para observar los resultados presiona el escaneo cuando haya terminado analiza las estadísticas. En caso de que hayas elegido el mismo dominio propuesto en esta práctica, puedes observar una salida similar a la siguiente. Recuerda que el dominio a analizar debe ser otro de tu elección.

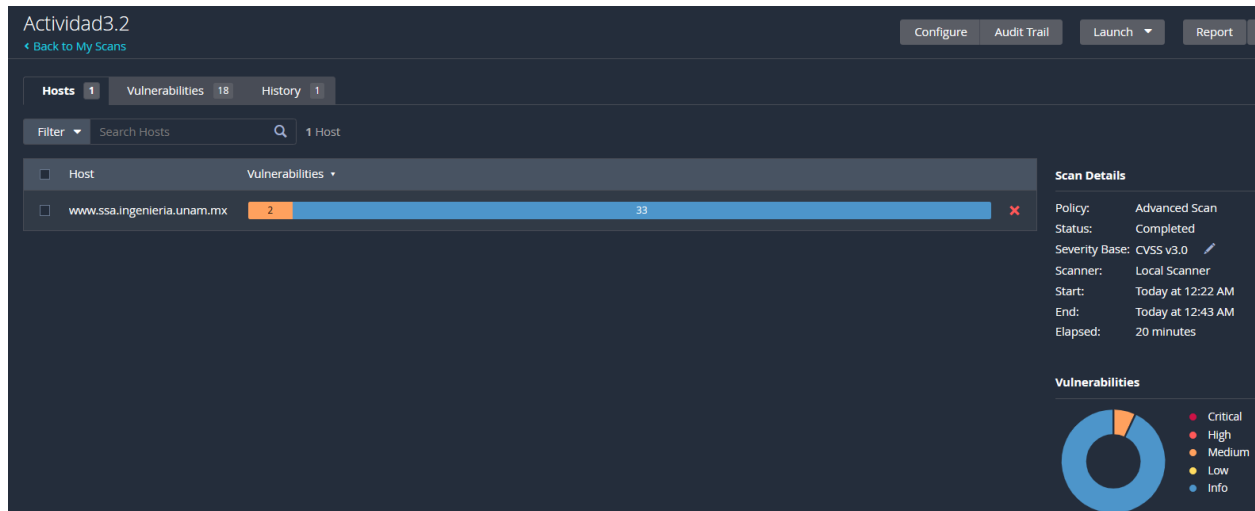


Imagen de ejemplo 14

Si la página web seleccionada no contiene muchas amenazas de nivel crítico, se recomienda intentar con otro dominio para poder tener un panorama más amplio. Por ejemplo, analizando el dominio de la ENP 1, se observa lo siguiente.

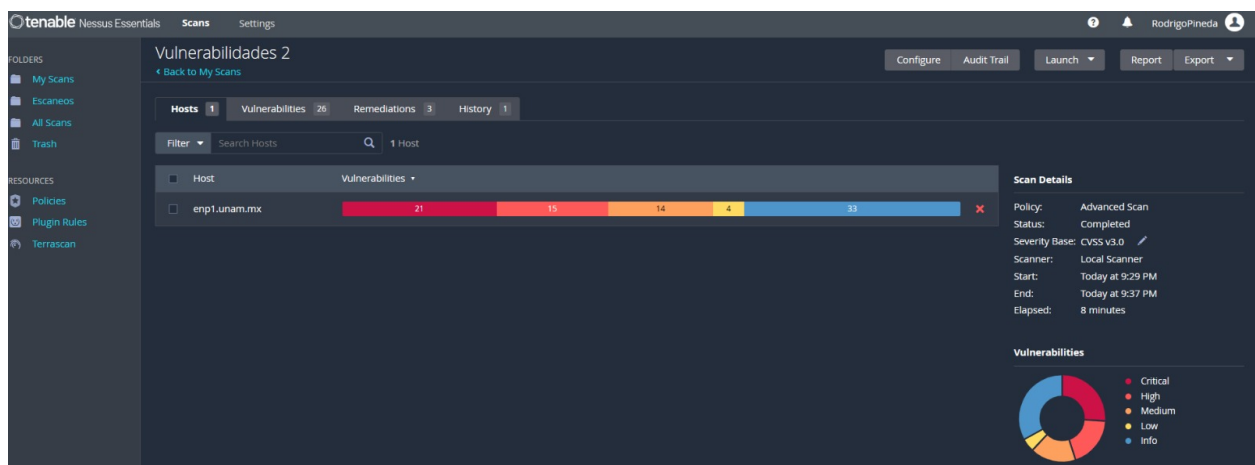



Imagen de ejemplo 15

Finalmente, enlista de manera general los resultados de vulnerabilidades de la página web e investiga las sugerencias mostradas en la pestaña “Remediations” en caso de existir. Puedes anexar hojas blancas con la lista en caso de requerir.

[illegible]



Práctica 3: Identificación de ataques y técnicas de intrusión



Temas a reforzar

Esta práctica se enfocará en la identificación de diversos ataques y técnicas de intrusión en entornos de seguridad informática, aplicando conceptos en casos prácticos.

Objetivo(s) de aprendizaje:

- Los estudiantes adquirirán habilidades en la identificación de ataques y técnicas de intrusión.
- Los estudiantes identificarán las fases de un ataque al aplicar la psicología del intruso y reafirmarán los conceptos relacionados con mecanismos de seguridad.
- La práctica fomentará la comprensión de los tipos de ataques comunes y preparará a los estudiantes para abordar situaciones de seguridad informática en entornos del mundo real.

Material a utilizar

1. Computadoras con acceso a Internet.
2. Lápiz o pluma.
3. Hojas blancas.

Planteamiento teórico

La seguridad informática es un tema de vital importancia en la actualidad. Debido al desarrollo de las telecomunicaciones, y con ello de la sociedad, la información se ha vuelto un recurso muy valioso para muchas personas siendo que su protección ya no solo se limita al ámbito físico, sino que también ha dado el salto al mundo digital. Los métodos, tanto de los defensores como de los atacantes, son cada vez más avanzados y complicados, por lo que debemos tener en cuenta que las amenazas siempre están presentes en nuestra vida, y constantemente nos encontramos con la necesidad de mitigar estos potenciales ataques.

La identificación de ataques y técnicas de intrusión es una habilidad indispensable para resguardar nuestros sistemas frente a posibles ataques, los cuales pueden provenir de fuentes tan diversas como la naturaleza misma de los bienes: cibernéticos, físicos, intangibles, sociales, y a ninguno de estos debe restarse importancia, pues lo que podemos considerar bienes, ya sean propios, de la empresa u organización, están en juego.

Por lo tanto, la identificación de riesgos y amenazas es esencial para asegurar la identificación de los ataques, pues se busca ayudar a evitar la culminación de las amenazas. Asimismo, saber las técnicas más habituales empleadas por los atacantes puede ayudarnos a estar más preparados para combatirlos, sin perder de vista que a pesar de que un ataque se haya consumado exitosamente o no, se debe contemplar en nuestras medidas de protección después del ataque.

A lo largo del desarrollo de la práctica, mediante diversas actividades, se complementan y amplían estos conceptos al mismo tiempo que se busca mejorar la comprensión.

Desarrollo

Modo de trabajo:

La práctica se desarrollará en equipos de 2 integrantes. Tiempo estimado: 2 horas.

Actividad 1. Descifrando el concepto de ataque.

Cuando hablamos de seguridad, un ataque no es lo mismo que una amenaza, entonces nos surge el cuestionamiento: ¿qué es un ataque?

Podemos definir un ataque como una eventualidad que se está presentando o que ya se presentó, y que causó o está causando algún tipo de daño. Si nos enfocamos al área de cómputo, podemos hacernos diversas preguntas para empezar a entender un poco mejor el tema.

De forma individual y con base en su experiencia responda las siguientes preguntas:

Pregunta 1.1: ¿Alguna vez ha sido víctima de un ataque informático? Cuente brevemente su experiencia:

Pregunta 1.2: ¿Qué prácticas o herramientas de seguridad está utilizando actualmente en su computadora para protegerse contra ataques informáticos?

Pregunta 1.3: ¿Cómo protege su información actualmente en otros dispositivos (tableta, teléfono)?

Discuta de forma grupal su experiencia con el grupo.

Actividad 2. Identificación de tipos de ataques.

Si bien, en la actividad 1 identificamos que es un ataque y lo aterrizamos a nuestro entorno de computación, los ataques van más allá de eso: los ataques atentan contra cualquier bien del que disponga una organización, afectando cuestiones como información, dinero, el personal y muchos bienes más. Para identificar los tipos de ataques podemos clasificarlos de diferentes formas:

1. Por el servicio de seguridad contra el que atentan
 - **Intercepción:** Atenta contra la confidencialidad.
 - **Interrupción:** Atenta contra la disponibilidad.
 - **Modificación:** Atenta contra la integridad.
 - **Suplantación:** Atenta contra la autenticación.
2. Por el lugar donde se presentan
 - **Externo:** Le afecta a alguien externo a mí o ajeno a mi organización.
 - **Interno:** Me afecta a mí o a mi organización.
3. Por el objetivo
 - **No intencionado:** Surge por un accidente.
 - **Intencionado:** La realización del mismo implica una planeación.

4. Por que tan evidente es el ataque

****Activo:** Notas el ataque.

****Pasivo:** No te has dado cuenta del ataque.

En parejas, basándose en el siguiente caso de estudio, identifiquen los ataques que enfrenta la empresa para ayudar a fortalecer su seguridad. Posteriormente clasifíquenlos en la tabla 1.

En la empresa “Desafortunados Inc.”, la cual se dedica a la producción de juguetes, han surgido una serie de problemas en cuanto a su seguridad:

Un día, uno de los empleados recibió un correo electrónico que parecía provenir de su banco. El correo solicitaba información personal y financiera. Sin pensarlo dos veces, el empleado respondió al correo proporcionando detalles confidenciales. Este incidente dejó en evidencia la vulnerabilidad del personal de la empresa.

Poco tiempo después, el servidor de la empresa sufrió un intento masivo de inicio de sesión con contraseñas incorrectas durante varias horas. Aunque los atacantes no lograron acceder al sistema, esta situación generó un gran número de registros en el mismo. La empresa comenzó a preocuparse por su capacidad para proteger su red.

Simultáneamente, otro empleado accedió a un enlace que lo llevó a un sitio web malicioso. Sin darse cuenta, su computadora fue infectada con un software espía. La empresa se dio cuenta de que su falta de capacitación en temas de seguridad podría ser un problema.

Los problemas se agravaron cuando los archivos críticos de la empresa desaparecieron misteriosamente del servidor y se reemplazaron por una nota de rescate que exigía un pago en criptomonedas a cambio de la recuperación de los archivos. La empresa se enfrentó a la difícil decisión de pagar o no.

Para empeorar las cosas, durante un robo en las instalaciones se perdió una memoria USB que contenía el único respaldo de los archivos críticos de la empresa. La memoria USB no estaba cifrada y carecía de medidas de seguridad, además de que durante el suceso, el sistema de videovigilancia se desconectó misteriosamente, lo que impidió que se obtuvieran pruebas cruciales de quiénes eran los responsables.

Tabla 1. Tipos de ataques

<i>Ataque</i>	<i>Servicio</i>	<i>Lugar</i>	<i>Objetivo</i>	<i>Notoriedad</i>

Comparta con el grupo sus resultados.

Actividad 3. Técnicas de intrusión.

Una técnica de intrusión, en el contexto de seguridad informática, es un método o enfoque utilizado por un atacante para obtener acceso no autorizado a un sistema informático o red. Algunas de las técnicas de intrusión más conocidas son:

****Ingeniería social:** Hacerse de la información de la víctima por medio de la socialización. Consiste en técnicas de manipulación donde el delincuente se hace pasar por otra persona.

****Software pirata:** El uso de software no oficial puede contener código malicioso que se instala junto con el software.

****Permisos inadecuados:** Una mala gestión en los permisos del personal y los usuarios provoca que personal no autorizado pueda acceder a recursos que no debería.

****Dispositivos de almacenamiento extraíble:** Ya sea para almacenar información valiosa o por el riesgo de ser víctima de un software malicioso, el uso de estos dispositivos siempre debe controlarse.

****Software sin actualizaciones:** Tener aplicaciones y sistemas operativos que no estén actualizados, puede provocar brechas en la seguridad ante ataques nuevos.

La psicología del intruso, consiste en pensar como lo haría el atacante, es decir, ponernos en su lugar. Esto nos ayuda a tomar ventaja reconociendo vulnerabilidades y amenazas en caso de realizarlo antes de un ataque reconocido, o replantear nuestros modelos de seguridad tras un ataque. Un ataque intencionado consta de 3 etapas: Preparación, Activación y Ejecución:

En pareja, seleccionen una o varias técnicas de intrusión, y desarrollen un ataque siguiendo la psicología del intruso, ante el siguiente caso de estudio.

En la empresa en la que ustedes trabajan, saben que la información más valiosa de la empresa está guardada en algún lugar de la oficina de su jefe en forma física y protegida por acceso limitado solo para el jefe y administradores, en forma digital. Su jefe constantemente habla de tener una caja fuerte en su oficina y presumiendo que solo él tiene acceso, gracias a las credenciales que emplean para entrar por el control de la puerta, aunque no es del todo cierto ya que las credenciales del personal de seguridad sirven también para ingresar a todas las oficinas. Más información de la que disponen es que el edificio se encuentra cerrado para todos desde las 20:00 horas del viernes hasta las 07:00 del lunes, donde la única vigilancia son 3 guardias en turnos de 8 horas, donde el guardia nocturno siempre se mofa de dormir ya que “nunca pasa nada” además de que confía plenamente en las cámaras de vigilancia. Con respecto al sistema informático, se sabe que no existe la gestión de contraseñas y como la empresa no invierte en la capacitación continua sobre seguridad al creer que es un gasto que se puede omitir, muchos trabajadores ponen sus contraseñas en papeles en sus oficinas y/o usan contraseñas débiles.

Actividad 4. Conceptos de interés (Opcional).

Investigue y conteste con su pareja, las siguientes preguntas:

Pregunta 4.1: ¿Qué es un ataque de inyección de base de datos y cuáles son las contramedidas efectivas para prevenirlo?

Pregunta 4.2: ¿Cuáles son las consecuencias más comunes de un ataque de ransomware en una organización y cuáles estrategias de recuperación y mitigación recomendarían después del incidente?

Pregunta 4.3: ¿Qué es el secuestro de sesiones y cuáles son las prácticas recomendadas para prevenirlo?

Pregunta 4.4: Además de la configuración incorrecta de seguridad, ¿qué otros factores pueden contribuir a la probabilidad de sufrir un ataque informático?

Pregunta 4.5: ¿En qué consiste el ataque de salto de directorio?

Conclusiones (Individuales):

Presentación de resultados

Para esta práctica, los resultados se entregan en el propio cuerpo de este documento. En caso de requerirse, se pueden agregar respuestas en hojas blancas, donde para cada una se especifique el número de la actividad o pregunta, seguida de su respuesta y anexar dichas hojas al final de este documento.

Referencias

- Departamento de Automática y Computación. (s.f.). Práctica 1: Técnicas de intrusión.
https://www.tlm.unavarra.es/pluginfile.php/12065/mod_resource/content/0/practic as/practica1/Practica_1_Tecnicas_de_intrusion.pdf
- Pérez Ponce, M. (s.f.). Identificación de ataques y técnicas de intrusión.
<https://slideplayer.es/slide/13389615/>
- Flores Román, L.H & Hernández Hernández, G.G. (2011). Pruebas de Hacking Ético en un Laboratorio de la Facultad de Ingeniería de la UNAM. Tema 2. Identificación de ataques y técnicas de intrusión [Tesis de Titulación, Universidad Nacional Autónoma de México]. Repositorio Institucional – Ptolomeo.
<http://www.ptolomeo.unam.mx:8080/xmlui/bitstream/handle/132.248.52.100/203/A5.pdf?sequence=5>
- Vulnerabilidades y técnicas de intrusión. (s.f.). Calameo.
<https://www.calameo.com/read/003805094dae5de3b2f3e>