



# Manual de prácticas del Laboratorio de Seguridad Informática Básica

CÓDIGO:

P1

VERSIÓN:

1.0

PÁGINA:

1/59

FECHA DE  
EMISIÓN:

15/04/2024

Facultad de Ingeniería

Área/Departamento: Laboratorio de Redes y Seguridad

La impresión de este documento es una copia no controlada

Seguridad informática básica

Grupo :1

30/Abril/2024

# Manual de prácticas del Laboratorio de Seguridad Informática Básica

10

Elaborado por:

- Angeles Estrada Ricardo 317014187
- Crisantos Martinez Diego Jair 317029264
- Macias Flores Alejandro 317028494
- Medina Segura Fernando 317174948

	<b>Manual de prácticas del Laboratorio de Seguridad Informática Básica</b>	CÓDIGO:	P1
		VERSIÓN:	1.0
		PÁGINA:	2/59
		FECHA DE EMISIÓN:	15/04/2024
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

## Índice de Prácticas

Práctica 1. Identificación y Clasificación de Bienes de Información.....	3
Práctica 2. Amenazas.....	13
Práctica 3. Identificación y Mitigación de Vulnerabilidades.....	25
Bibliografía.....	59



# Manual de prácticas del Laboratorio de Seguridad Informática Básica

CÓDIGO:

P1

VERSIÓN:

1.0

PÁGINA:

3/59

FECHA DE  
EMISIÓN:

15/04/2024

Facultad de Ingeniería

Área/Departamento: Laboratorio de Redes y Seguridad

La impresión de este documento es una copia no controlada

## Práctica 1:

# Identificación y Clasificación de Bienes de Información



# Manual de prácticas del Laboratorio de Seguridad Informática Básica

CÓDIGO:

P1

VERSIÓN:

1.0

PÁGINA:

4/59

FECHA DE  
EMISIÓN:

15/04/2024

Facultad de Ingeniería

Área/Departamento: Laboratorio de Redes y Seguridad

La impresión de este documento es una copia no controlada

## 1. Tema a reforzar:

Bienes

## 2. Objetivo de aprendizaje:

El objetivo de la práctica es que los participantes puedan identificar y clasificar los diferentes tipos de bienes de información en sus hogares, lo cual les permitirá comprender mejor la importancia de proteger estos activos y cómo contribuir a la seguridad de sus bienes.

## 3. Conceptos Teóricos

En el ámbito de la seguridad informática, los bienes de información son activos de una organización que poseen un valor significativo y cuya protección es crucial para garantizar el funcionamiento adecuado de la misma. Estos activos pueden abarcar una amplia gama de elementos, que van desde los datos almacenados en sistemas informáticos hasta los dispositivos físicos utilizados para procesar, almacenar o transmitir información.

La protección de los bienes de información es esencial para salvaguardar la integridad, la confidencialidad y la disponibilidad de los mismos. La integridad se refiere a garantizar que la información no ha sido alterada de manera no autorizada y que se mantiene íntegra y precisa. La confidencialidad se relaciona con la restricción del acceso a la información solo a aquellos usuarios autorizados, protegiéndola de divulgaciones no autorizadas. Por último, la disponibilidad implica asegurar que la información esté disponible y accesible cuando sea necesario para los usuarios autorizados.

La protección de estos activos es fundamental, ya que su compromiso puede resultar en consecuencias graves para una organización, como pérdida de reputación, pérdidas financieras, violaciones de la privacidad o interrupciones en las operaciones comerciales. Por lo tanto, es crucial que las organizaciones identifiquen y clasifiquen adecuadamente sus bienes de información, para implementar las medidas de seguridad adecuadas y mitigar los riesgos asociados con su protección insuficiente o inadecuada.



# Manual de prácticas del Laboratorio de Seguridad Informática Básica

CÓDIGO:

P1

VERSIÓN:

1.0

PÁGINA:

5/59

FECHA DE EMISIÓN:

15/04/2024

Facultad de Ingeniería

Área/Departamento: Laboratorio de Redes y Seguridad

La impresión de este documento es una copia no controlada

## 4. Equipo y material necesario

Para llevar a cabo esta práctica, los participantes necesitarán disponer de los siguientes materiales:

- Bolígrafo (de cualquier color, preferentemente negro).
- Equipo de cómputo con conexión a internet.



## 5. Desarrollo

En estas actividades, los participantes pondrán en práctica sus conocimientos sobre los bienes de información en el contexto de la seguridad informática. A lo largo de las actividades, los participantes investigarán conceptos clave relacionados con los bienes de información, identificarán diferentes tipos de



# Manual de prácticas del Laboratorio de Seguridad Informática Básica

CÓDIGO:

P1

VERSIÓN:

1.0

PÁGINA:

6/59

FECHA DE  
EMISIÓN:

15/04/2024

Facultad de Ingeniería

Área/Departamento: Laboratorio de Redes y Seguridad

La impresión de este documento es una copia no controlada

bienes en una organización y los clasificará según su importancia y sensibilidad.

Para llevar a cabo las actividades, los participantes seguirán una serie de pasos que les permitirán comprender la importancia de proteger los activos de información y cómo pueden contribuir a la seguridad de la organización. Al finalizar las actividades, los participantes habrán adquirido habilidades prácticas para identificar, clasificar y proteger los bienes de información en un entorno organizacional.

A lo largo de las actividades, se fomentará la participación activa y el trabajo en equipo, ya que los participantes colaborarán en la investigación y clasificación de los bienes de información. Además, se alentará la creatividad y el pensamiento crítico, ya que los participantes deberán aplicar los conceptos aprendidos de manera práctica y reflexionar sobre la importancia de proteger los activos de información en una organización.

## 5.1. Exploración y Comprensión de Conceptos Clave sobre Bienes de Información

En el ámbito de la seguridad informática, es fundamental comprender los diferentes tipos de bienes de información y su importancia en el contexto organizacional. En esta actividad, se investigarán conceptos clave relacionados con los bienes de información, como la información confidencial, la información privada y la información pública. Estos conceptos son fundamentales para comprender cómo identificar y clasificar los activos de información en una organización, lo cual es esencial para implementar medidas de seguridad adecuadas. A través de esta investigación, los participantes ampliarán su conocimiento sobre la importancia de proteger los activos de información y cómo pueden contribuir a la seguridad de la organización.

**Información confidencial:** Datos que requieren protección especial debido a su sensibilidad y naturaleza privada.

- Bienes:



# Manual de prácticas del Laboratorio de Seguridad Informática Básica

CÓDIGO:	P1
VERSIÓN:	1.0
PÁGINA:	7/59
FECHA DE EMISIÓN:	15/04/2024

Facultad de Ingeniería

Área/Departamento: Laboratorio de Redes y Seguridad

La impresión de este documento es una copia no controlada

- Información privada:

- Información pública:

- Activo de información:

- Integridad de la información:





# Manual de prácticas del Laboratorio de Seguridad Informática Básica

CÓDIGO:

P1

VERSIÓN:

1.0

PÁGINA:

8/59

FECHA DE EMISIÓN:

15/04/2024

Facultad de Ingeniería

Área/Departamento: Laboratorio de Redes y Seguridad

La impresión de este documento es una copia no controlada

- Disponibilidad de la información:

- Autenticidad de la información:

## 5.2. Identificación de activos de información

En esta actividad, los alumnos trabajarán en grupos para identificar los diferentes tipos de activos de información que pueden encontrarse en su vida diaria. Esta actividad les permitirá aplicar los conceptos teóricos aprendidos sobre bienes de información y comprender cómo estos activos son fundamentales para el funcionamiento de una organización y deben ser protegidos adecuadamente.

A continuación, enumera 6 posibles activos de información que pueden encontrarse en tu vida diaria. Puedes incluir elementos como teléfonos móviles,





# Manual de prácticas del Laboratorio de Seguridad Informática Básica

CÓDIGO:

P1

VERSIÓN:

1.0

PÁGINA:

9/59

FECHA DE  
EMISIÓN:

15/04/2024

Facultad de Ingeniería

Área/Departamento: Laboratorio de Redes y Seguridad

La impresión de este documento es una copia no controlada

cuentas de redes sociales, documentos personales, entre otros. Justifica brevemente la importancia de proteger cada activo en tu vida diaria.

Activos de Información	Importancia de la Protección

### 5.3. Discusión sobre Activos de Información en la Vida Diaria

Los alumnos discutirán en grupo sobre los activos de información que identificaron en su vida diaria. Esta actividad les permitirá compartir sus puntos de vista y reflexionar sobre la importancia de proteger la información en diferentes aspectos de su entorno personal.

### 5.4. Medidas de Protección para Activos de Información en la Vida Diaria



# Manual de prácticas del Laboratorio de Seguridad Informática Básica

CÓDIGO:	P1
VERSIÓN:	1.0
PÁGINA:	10/59
FECHA DE EMISIÓN:	15/04/2024

Facultad de Ingeniería      Área/Departamento: Laboratorio de Redes y Seguridad

La impresión de este documento es una copia no controlada

En la tabla a continuación, anota 5 medidas de protección que podrías usar para proteger tus bienes de la vida diaria. También incluye una breve justificación para cada medida.

Medidas de Protección	Justificación

## 5.5. Plan de Seguridad Personal



# Manual de prácticas del Laboratorio de Seguridad Informática Básica

CÓDIGO:

P1

VERSIÓN:

1.0

PÁGINA:

11/59

FECHA DE  
EMISIÓN:

15/04/2024

Facultad de Ingeniería

Área/Departamento: Laboratorio de Redes y Seguridad

La impresión de este documento es una copia no controlada

Los alumnos crearán un plan de seguridad personal basado en los activos de información identificados previamente en su vida diaria y las medidas de protección propuestas. Este plan les permitirá aplicar de manera práctica los conceptos aprendidos sobre seguridad de la información y desarrollar estrategias para proteger su información personal en diferentes situaciones.

Empty dashed box for student work.



# Manual de prácticas del Laboratorio de Seguridad Informática Básica

CÓDIGO:

P1

VERSIÓN:

1.0

PÁGINA:

12/59

FECHA DE  
EMISIÓN:

15/04/2024

Facultad de Ingeniería

Área/Departamento: Laboratorio de Redes y Seguridad

La impresión de este documento es una copia no controlada

Empty dashed box for drawing or notes.

## 6. Conclusiones

Anoten sus conclusiones tras revisar los objetivos planteados al inicio de la práctica

Lined area for writing conclusions.



# Manual de prácticas del Laboratorio de Seguridad Informática Básica

CÓDIGO:

P1

VERSIÓN:

1.0

PÁGINA:

13/59

FECHA DE  
EMISIÓN:

15/04/2024

Facultad de Ingeniería

Área/Departamento: Laboratorio de Redes y Seguridad

La impresión de este documento es una copia no controlada

## Práctica 2: Amenazas

	<b>Manual de prácticas del Laboratorio de Seguridad Informática Básica</b>	CÓDIGO:	P1
		VERSIÓN:	1.0
		PÁGINA:	14/59
		FECHA DE EMISIÓN:	15/04/2024
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

### 1. Tema a reforzar:

Amenazas y fuentes de amenazas.

### 2. Objetivo de aprendizaje:

El objetivo de esta práctica es que los participantes puedan identificar, clasificar los diferentes tipos de amenazas que se pueden presentar y las fuentes que los ocasionan comprendiendo así la importancia de salvaguardar los bienes y contribuir a la seguridad de su entorno personal.

### 3. Conceptos Teóricos

Para entender la importancia de proteger los bienes de información, es crucial comprender los siguientes conceptos:

- **Información confidencial:** Datos que requieren protección especial debido a su sensibilidad y naturaleza privada.
- **Información privada:** Datos personales o privados que requieren protección para preservar la privacidad del individuo.
- **Información pública:** Datos que están disponibles para el público en general y no requieren protección especial.
- **Activo de información:** Cualquier recurso que tenga valor para una organización o individuo y que requiera protección.
- **Integridad de la información:** Garantía de que la información no ha sido alterada de manera no autorizada y se mantiene precisa.
- **Disponibilidad de la información:** Asegurar que la información esté disponible y accesible cuando sea necesario para los usuarios autorizados.
- **Autenticidad de la información:** Verificación de que la información proviene de una fuente confiable y es genuina.

### 4. Equipo y material necesario

	<b>Manual de prácticas del Laboratorio de Seguridad Informática Básica</b>	CÓDIGO:	P1
		VERSIÓN:	1.0
		PÁGINA:	15/59
		FECHA DE EMISIÓN:	15/04/2024
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

Para llevar a cabo esta práctica, los participantes necesitarán disponer de los siguientes materiales:

- Bolígrafo (de cualquier color, preferentemente negro).
- Equipo de cómputo con conexión a internet.
- Correos electrónicos falsos y una página web falsa preparados por el instructor.

## 5. Desarrollo

En estas actividades, los participantes formarán grupos de tres integrantes y llevarán a cabo una investigación sobre conceptos clave relacionados con los bienes de información. Identificarán y clasificarán diferentes tipos de bienes en un entorno organizacional, compartiendo luego sus hallazgos con la clase. El objetivo es comprender la importancia de proteger los activos de información, adquirir habilidades para su identificación y clasificación, fomentar la participación activa y el trabajo en equipo, y estimular la reflexión sobre la seguridad de la información en una organización.

### 5.1. Exploración y Comprensión de Conceptos Clave sobre Bienes de Información

Información Confidencial:

---

---

---

---

---

---

Privada:

---

---

---





# Manual de prácticas del Laboratorio de Seguridad Informática Básica

CÓDIGO:

P1

VERSIÓN:

1.0

PÁGINA:

16/59

FECHA DE  
EMISIÓN:

15/04/2024

Facultad de Ingeniería

Área/Departamento: Laboratorio de Redes y Seguridad

La impresión de este documento es una copia no controlada

Pública:

---

---

---

Integridad:

---

---

---

---

---

Disponibilidad:

---

---

---

---

---

Autenticidad de la Información:

---

---

---

---

---

## 5.2. Identificación de Amenazas

En grupos, los alumnos identificarán posibles amenazas o riesgos que podrían afectar a los activos de información que han enumerado previamente, en la actividad 5.2 de la práctica anterior, en sus vidas diarias. Por ejemplo, robo de identidad, malware, pérdida física del dispositivo, etc. Cada grupo presentará sus hallazgos al resto de la clase.



# Manual de prácticas del Laboratorio de Seguridad Informática Básica

CÓDIGO:

P1

VERSIÓN:

1.0

PÁGINA:

17/59

FECHA DE  
EMISIÓN:

15/04/2024

Facultad de Ingeniería

Área/Departamento: Laboratorio de Redes y Seguridad

La impresión de este documento es una copia no controlada

Activos de Información	Amenazas

## 5.3. Evaluación de Impacto y Probabilidad

Los participantes evaluarán el impacto y la probabilidad de cada amenaza identificada. Utilizarán una matriz de riesgos para clasificar las amenazas según su gravedad y probabilidad de ocurrencia. Esto les ayudará a priorizar las medidas de protección a implementar.

Para evaluar el impacto y la probabilidad de cada amenaza identificada, recomendaría utilizar una matriz de riesgos. Esto les permitirá a los participantes visualizar de manera clara y estructurada la relación entre la gravedad de las amenazas y su probabilidad de ocurrencia. Aquí tienes una sugerencia de cómo podrían estructurar la matriz de riesgos:

	<b>Manual de prácticas del Laboratorio de Seguridad Informática Básica</b>	CÓDIGO:	P1
		VERSIÓN:	1.0
		PÁGINA:	18/59
		FECHA DE EMISIÓN:	15/04/2024
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

#### Matriz de Riesgos:

Amenazas	Impacto (Alto/Medio/Bajo)	Probabilidad (Alta/Media/Baja)

En la columna "Impacto", los participantes pueden clasificar el impacto de cada amenaza como Alto, Medio o Bajo. En la columna "Probabilidad", pueden clasificar la probabilidad de ocurrencia de cada amenaza como Alta, Media o Baja. Posteriormente, pueden llenar la matriz asignando un nivel de impacto y probabilidad a cada amenaza identificada.

Después de completar la matriz de riesgos, los participantes podrán visualizar las amenazas que presentan un mayor riesgo para sus activos de información y priorizar las medidas de protección a implementar en función de estos riesgos.

#### 5.4. Planificación de Medidas de Protección



# Manual de prácticas del Laboratorio de Seguridad Informática Básica

CÓDIGO:	P1
VERSIÓN:	1.0
PÁGINA:	19/59
FECHA DE EMISIÓN:	15/04/2024

Facultad de Ingeniería

Área/Departamento: Laboratorio de Redes y Seguridad

La impresión de este documento es una copia no controlada

Basándose en las amenazas identificadas y su evaluación de impacto y probabilidad, los alumnos elaborarán un plan detallado de medidas de protección para cada activo de información.

Para lo anterior realiza los siguientes pasos:

1. **Identificación de Amenazas Prioritarias:** Enumerar las amenazas identificadas en orden de prioridad, basándose en la evaluación de impacto y probabilidad realizada anteriormente.
2. **Medidas de Protección Propuestas:**
  - Para cada amenaza identificada, proponer medidas específicas de protección. Esto puede incluir:
    - Instalación de software de seguridad (antivirus, firewall, etc.).
    - Implementación de controles de acceso (contraseñas robustas, autenticación de dos factores, etc.).
    - Realización de copias de seguridad periódicas de los datos.
    - Encriptación de datos sensibles.
    - Actualización regular de sistemas y software para corregir vulnerabilidades conocidas.
    - Capacitación y concienciación de los usuarios sobre buenas prácticas de seguridad.
    - Establecimiento de políticas y procedimientos de seguridad.
3. **Justificación y Descripción de Medidas:** Para cada medida propuesta, justificar su necesidad y describir cómo contribuirá a mitigar la amenaza identificada. Se pueden incluir ejemplos específicos y casos de uso relevantes.



# Manual de prácticas del Laboratorio de Seguridad Informática Básica

CÓDIGO:

P1

VERSIÓN:

1.0

PÁGINA:

20/59

FECHA DE  
EMISIÓN:

15/04/2024

Facultad de Ingeniería

Área/Departamento: Laboratorio de Redes y Seguridad

La impresión de este documento es una copia no controlada

	<b>Manual de prácticas del Laboratorio de Seguridad Informática Básica</b>	CÓDIGO:	P1
		VERSIÓN:	1.0
		PÁGINA:	21/59
		FECHA DE EMISIÓN:	15/04/2024
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

## 5.5. Práctica de Escenario de Phishing

Los participantes llevarán a cabo un escenario práctico donde simularán un intento de phishing. Para ello el grupo se dividirá en grupos de 3 personas, donde uno de los miembros del grupo actuará como la "víctima" que recibe un correo electrónico de phishing, otro será el "administrador de sistemas" encargado de tomar decisiones y liderar la respuesta del grupo, y el tercer miembro será el "atacante" que enviará el correo falso.

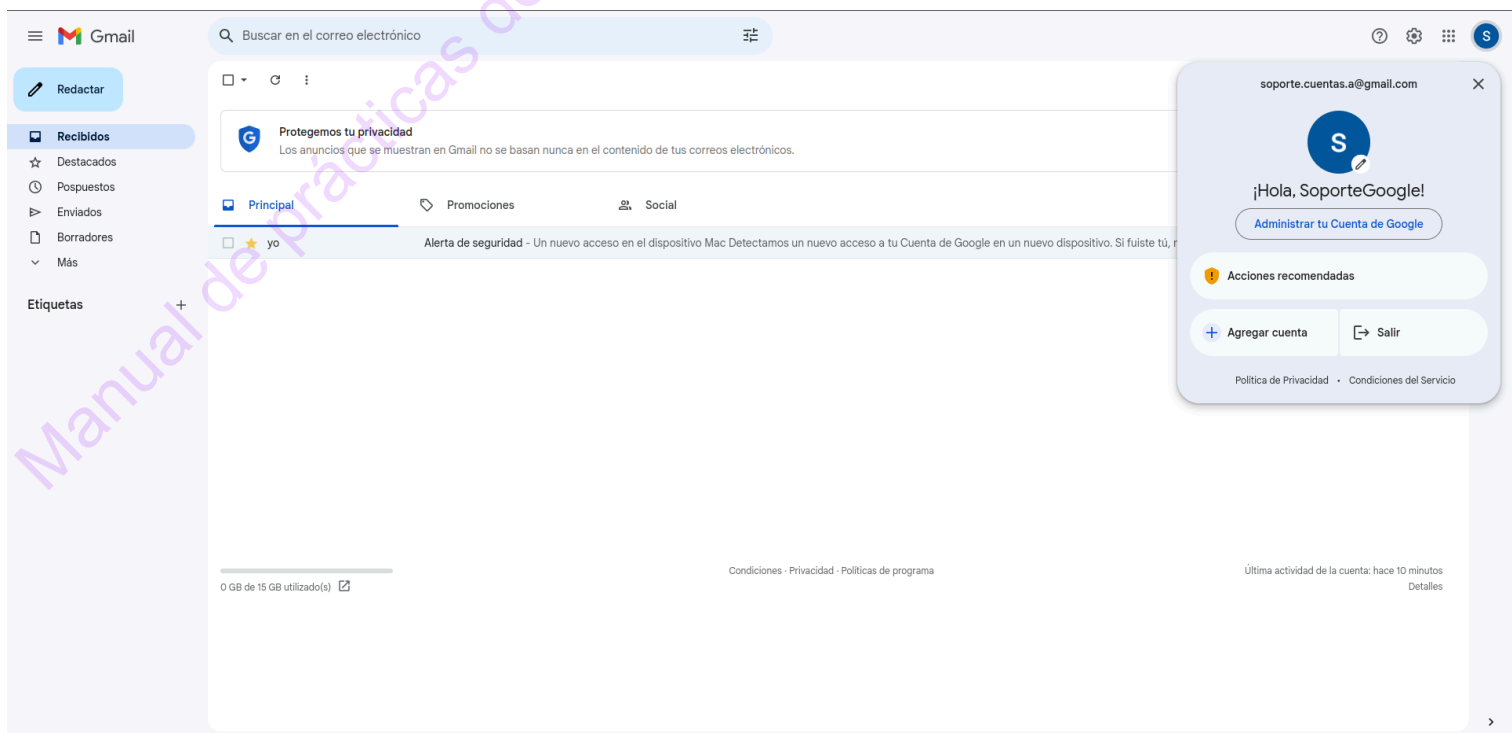
Para ello se realizarán los siguientes pasos:

- **Ingreso a la cuenta de correo electrónico del atacante:**

Para la realización de este ejercicio se creó un correo electrónico que podría ser confundido por la víctima como un correo electrónico legítimo.

En un equipo de cómputo ingrese al correo: [sosporte.cuentas.a@gmail.com](mailto:sosporte.cuentas.a@gmail.com)

Con la contraseña: contrasena1



	<b>Manual de prácticas del Laboratorio de Seguridad Informática Básica</b>	CÓDIGO:	P1
		VERSIÓN:	1.0
		PÁGINA:	22/59
		FECHA DE EMISIÓN:	15/04/2024
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

- **Creación del correo a enviar:**

En la sección de recibidos se encuentra un correo destacado que puede servir como ejemplo para la elaboración de un correo falso.

Alerta de seguridad Recibidos x



**SoporteGoogle** <soporte.cuentas.a@gmail.com>  
para mí ▾

## Un nuevo acceso en el dispositivo Mac

Detectamos un nuevo acceso a tu Cuenta de Google en un nuevo dispositivo. Si fuiste tú, no tienes que hacer nada. De lo contrario, te ayudaremos a proteger tu cuenta.

Puedes ver la actividad de seguridad en  
<https://www.gmail.com/mail/help/intl/es/about.html?iframe>

← Responder
→ Reenviar
😊

La intención del correo es obtener información de la víctima, tomando en consideración dicho objetivo se debe realizar un correo.

- **Envío del correo electrónico.**

El atacante envía el correo a la víctima.

- **Análisis del Correo Electrónico:**

- El grupo se reúne para analizar el correo electrónico recibido.
- La víctima comparte el contenido del correo electrónico con el grupo.
- Los integrantes discuten las posibles señales de phishing presentes en el correo electrónico (errores de ortografía, enlaces sospechosos, solicitudes de información confidencial, etc.).



	<b>Manual de prácticas del Laboratorio de Seguridad Informática Básica</b>	CÓDIGO:	P1
		VERSIÓN:	1.0
		PÁGINA:	23/59
		FECHA DE EMISIÓN:	15/04/2024
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

- **Toma de Decisiones:**

- Basándose en el análisis del correo electrónico, el grupo decide cómo responder al correo electrónico falso.
- El administrador de sistemas puede liderar la discusión sobre las posibles respuestas y acciones a seguir, utilizando el conocimiento adquirido en clase o en investigaciones previas sobre seguridad informática.

- **Acciones a Seguir:**

El grupo decide las acciones a seguir, como ignorar el correo electrónico, marcarlo como spam, informar al equipo de seguridad, etc.

- **Reflexión y Conclusiones:**

A continuación escriban sus reflexiones sobre la experiencia y compartan sus conclusiones con el resto de los participantes.



# Manual de prácticas del Laboratorio de Seguridad Informática Básica

CÓDIGO:

P1

VERSIÓN:

1.0

PÁGINA:

24/59

FECHA DE EMISIÓN:

15/04/2024

Facultad de Ingeniería

Área/Departamento: Laboratorio de Redes y Seguridad

La impresión de este documento es una copia no controlada

## Conclusiones

Anoten sus conclusiones tras revisar los objetivos planteados al inicio de la práctica

laboratorio de Seguridad



# Manual de prácticas del Laboratorio de Seguridad Informática Básica

CÓDIGO:

P1

VERSIÓN:

1.0

PÁGINA:

25/59

FECHA DE  
EMISIÓN:

15/04/2024

Facultad de Ingeniería

Área/Departamento: Laboratorio de Redes y Seguridad

La impresión de este documento es una copia no controlada

## Práctica 3:

# Identificación y Mitigación de Vulnerabilidades



# Manual de prácticas del Laboratorio de Seguridad Informática Básica

CÓDIGO:	P1
VERSIÓN:	1.0
PÁGINA:	26/59
FECHA DE EMISIÓN:	15/04/2024

Facultad de Ingeniería

Área/Departamento: Laboratorio de Redes y Seguridad

La impresión de este documento es una copia no controlada

## 1. Tema a reforzar:

Vulnerabilidades

## 2. Objetivo de aprendizaje:

El objetivo de la práctica es que los participantes puedan identificar las vulnerabilidades que se presentan en distintas situaciones, así como implementar estrategias de mitigación adecuadas lo cual les permitirá comprender mejor la importancia de identificar estas vulnerabilidades y minimizar el número de las mismas en cualquier entorno para evitar que sean explotadas y brindar una mayor protección a los bienes.

Analizar una página web con un software de escaneo de vulnerabilidades para la identificación de vulnerabilidades, su nivel de severidad y solución para eliminar las vulnerabilidades con el objetivo de que los participantes conozcan herramientas prácticas para detectar vulnerabilidades en un entorno real.

## 3. Conceptos Teóricos

En el ámbito de la seguridad informática, una vulnerabilidad es una debilidad, es decir, son los puntos débiles que se presentan en los procedimientos de seguridad, diseño, implementación o control interno que podrían ser explotadas, ya sea de manera accidental o intencionada, y que resultan en una brecha de seguridad o una violación de la política de seguridad de los sistemas.

Las vulnerabilidades en los sistemas informáticos pueden ser explotadas en su mayoría por atacantes informáticos para llevar a cabo una amenaza que previamente se estudió y se planteó. En general, las vulnerabilidades comprometen la integridad, la confidencialidad y la disponibilidad del sistema en cuestión, resultando así en robos de datos, interrupciones del servicio y otros daños significativos. Los tipos de vulnerabilidades que existen son la humana, la red, la natural, el hardware, el software y la física, donde la humana es la más común en todos los sistemas.

Para poder llevar a cabo un plan de mitigación de vulnerabilidades es importante resolver las siguientes preguntas: ¿qué fue lo que hizo o hace falta



# Manual de prácticas del Laboratorio de Seguridad Informática Básica

CÓDIGO:

P1

VERSIÓN:

1.0

PÁGINA:

27/59

FECHA DE EMISIÓN:

15/04/2024

Facultad de Ingeniería

Área/Departamento: Laboratorio de Redes y Seguridad

La impresión de este documento es una copia no controlada

en el sistema?, ¿qué no se ha hecho, implementado o considerado en el sistema?, ¿qué es lo que el sistema actualmente no tiene? y ¿qué es lo que se ha omitido o se omitió al desarrollar el sistema?, estas preguntas tienen la finalidad de que se puedan identificar las vulnerabilidades que presenta el sistema informático y así elaborar un plan de mitigación donde se reduzca el número de vulnerabilidades para contrarrestar amenazas, correr menos riesgos y disminuir los ataques a los bienes que se buscan proteger.

Es importante recalcar que una amenaza **NO** es una vulnerabilidad, más bien, las amenazas explotan o aprovechan las vulnerabilidades, y podemos tener una relación de una amenaza explotando una o varias vulnerabilidades, y otra relación de varias amenazas explotando una o varias vulnerabilidades, dicho de otro modo, las amenazas son las acciones que pretenden provocar un daño, y las vulnerabilidades son omisiones, son puntos débiles que el sistema presenta y pueden conllevar a que una amenaza se lleve con éxito.

## 4. Equipo y material necesario

Para llevar a cabo esta práctica, los participantes necesitarán disponer de los siguientes materiales:

- Bolígrafo (de cualquier color, preferentemente negro).
- Equipo de cómputo con conexión a internet.
- Software Tenable Nessus versión 10.7.2 para el escaneo de vulnerabilidades, se puede descargar en la siguiente liga:  
<https://www.tenable.com/downloads/nessus?loginAttempted=true>





# Manual de prácticas del Laboratorio de Seguridad Informática Básica

CÓDIGO:	P1
VERSIÓN:	1.0
PÁGINA:	28/59
FECHA DE EMISIÓN:	15/04/2024

Facultad de Ingeniería

Área/Departamento: Laboratorio de Redes y Seguridad

La impresión de este documento es una copia no controlada

## 5. Desarrollo

En estas actividades, los participantes pondrán en práctica sus conocimientos sobre las vulnerabilidades en el contexto de la seguridad informática. A lo largo de las actividades, los participantes pondrán en práctica los conceptos aprendidos que tengan sobre las vulnerabilidades de un sistema, identificarán diferentes puntos débiles en una organización y desarrollarán un plan de mitigación para mejorar la seguridad de un sistema.

Para llevar a cabo las actividades, los participantes seguirán una serie de pasos que les permitirán comprender la importancia de identificar vulnerabilidades y cómo pueden contribuir a los ataques que se puedan presentar en la organización. Al finalizar las actividades, los participantes habrán adquirido habilidades prácticas para identificar y mitigar vulnerabilidades en un entorno organizacional, así como adquirir conciencia sobre la importancia de la identificación de vulnerabilidades en un sistema informático para brindar una mayor protección a los bienes.

A lo largo de las actividades, se fomentará la participación activa y el trabajo en equipo, ya que los participantes colaborarán en la investigación y mitigación de las vulnerabilidades en un sistema. Además, se alentará la creatividad y el pensamiento crítico, ya que los participantes deberán aplicar los conceptos aprendidos de manera práctica y reflexionar sobre la importancia de identificar vulnerabilidades en una organización.

### 5.1 Identificación de vulnerabilidades

En esta actividad, los alumnos se reunirán en equipos de 4 personas para completar una tabla que presenta una lista de amenazas en la cuál los alumnos deben nombrar tres vulnerabilidades que provoquen que se presenten dichas amenazas, guíense en el ejemplo proporcionado en la tabla.

Amenaza presentada	Vulnerabilidades Relacionadas
I. - Infección por malware	<ol style="list-style-type: none"><li>1. No contar con un antivirus.</li><li>2. No descargar software de fuentes confiables.</li></ol>



# Manual de prácticas del Laboratorio de Seguridad Informática Básica

CÓDIGO:

P1

VERSIÓN:

1.0

PÁGINA:

29/59

FECHA DE  
EMISIÓN:

15/04/2024

Facultad de Ingeniería

Área/Departamento: Laboratorio de Redes y Seguridad

La impresión de este documento es una copia no controlada

	3. No saber que es un malware.
1.- Robo de información confidencial de la organización	
2.- Pérdida de datos por fallo en el sistema de backup	
3.- Ataques de ransomware a los sistemas operativos	
4.- Robo de dispositivos y equipo de cómputo en la organización	
5.- Manipulación de datos en una base de datos	
6.- Ser víctimas de phishing	
7.- Corto circuito en el área de IT	





# Manual de prácticas del Laboratorio de Seguridad Informática Básica

CÓDIGO:

P1

VERSIÓN:

1.0

PÁGINA:

30/59

FECHA DE EMISIÓN:

15/04/2024

Facultad de Ingeniería

Área/Departamento: Laboratorio de Redes y Seguridad

La impresión de este documento es una copia no controlada

8.- Sabotaje de la infraestructura por parte de un empleado	
9.- Robo de las credenciales de acceso a la organización	
10.- Instalación de un troyano en el equipo de cómputo	

## 5.2 Detección de amenazas y vulnerabilidades, y plan de mitigación

### 5.2.1 Diferencia entre amenazas y vulnerabilidades

En esta primera parte de la actividad, los alumnos se reunirán en equipos de 4 personas para identificar si el enunciado es una amenaza o una vulnerabilidad, se tiene una lista con un total de 10 enunciados, deben indicar si se trata de una amenaza (A) o una vulnerabilidad (V), guiense en los ejemplos proporcionados:

I.- Los empleados utilizan contraseñas débiles. (V)

II.- Inyección de SQL a la base de datos de la organización. (A)

1.- Correo electrónico que contiene spam. ( )

	<b>Manual de prácticas del Laboratorio de Seguridad Informática Básica</b>	CÓDIGO:	P1
		VERSIÓN:	1.0
		PÁGINA:	31/59
		FECHA DE EMISIÓN:	15/04/2024
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

- 2.- Firewall configurado incorrectamente que permite tráfico no deseado. ( )
- 3.- Falta de cifrado simétrico o asimétrico en el envío de mensajes. ( )
- 4.- Intercepción de información por medio de un Man-in-the-Middle. ( )
- 5.- Contraseñas almacenadas en texto plano en la base de datos de la organización. ( )
- 6.- Ransomware que cifra información del dispositivo y solicita un rescate. ( )
- 7.- Uso de software obsoleto que ya no se le da mantenimiento. ( )
- 8.- Un empleado abre un archivo que instala un keylogger en el dispositivo. ( )
- 9.- Uso de internet público. ( )
- 10.- Cifrado de datos usando algoritmos de cifrado no estandarizados. ( )

### 5.2.1 Mitigación de las vulnerabilidades

En esta segunda parte de la actividad, se les enlista un total de 7 vulnerabilidades, donde por equipo deben plantear al menos una solución que ayude a eliminar esa vulnerabilidad, investiguen información en internet en caso de ser necesario, guíense en el ejemplo proporcionado:

#### I.- Los empleados utilizan contraseñas débiles.

- Plan de mitigación:

Implementar una política de contraseñas fuertes con una combinación que requiera al menos 10 caracteres, incluyendo letras mayúsculas, minúsculas, números y símbolos. Adicionalmente, utilizar una herramienta de gestión de contraseñas para generar y almacenar contraseñas de manera segura.

- 1.- Falta de cifrado en las comunicaciones de datos entre clientes y servidores.

- Plan de Mitigación:



# Manual de prácticas del Laboratorio de Seguridad Informática Básica

CÓDIGO:

P1

VERSIÓN:

1.0

PÁGINA:

32/59

FECHA DE EMISIÓN:

15/04/2024

Facultad de Ingeniería

Área/Departamento: Laboratorio de Redes y Seguridad

La impresión de este documento es una copia no controlada

2.- Servidores web expuestos a ataques de inyección SQL.

- Plan de Mitigación:

3.- Uso excesivo de máquinas virtuales en un equipo de cómputo.

- Plan de Mitigación:

4.- Sistemas de vigilancia desactualizados y fácilmente manipulables.

- Plan de Mitigación:

5.- Uso del servicio Telnet en la red de la organización.

- Plan de Mitigación:



# Manual de prácticas del Laboratorio de Seguridad Informática Básica

CÓDIGO:

P1

VERSIÓN:

1.0

PÁGINA:

33/59

FECHA DE EMISIÓN:

15/04/2024

Facultad de Ingeniería

Área/Departamento: Laboratorio de Redes y Seguridad

La impresión de este documento es una copia no controlada

6.- Configuración de la red de la organización sin el uso de Vlan's.

- Plan de Mitigación:

7.- Correos electrónicos corporativos que no emplean firmas digitales.

- Plan de Mitigación:

## 5.3 Escaneo de vulnerabilidades con el software Tenable Nessus

En esta actividad, de manera individual los alumnos realizarán un escaneo y análisis de una página web por medio del software Tenable Nessus con el objetivo de que los alumnos identifiquen vulnerabilidades en una aplicación real, para desarrollar esta actividad, primero se debe crear una cuenta para el uso de este software.

### 5.3.1 Manual de instalación del software Tenable Nessus

Para crear una cuenta gratuita, hay que ingresar a la siguiente liga: <https://www.tenable.com/products/nessus/nessus-essentials>

	<b>Manual de prácticas del Laboratorio de Seguridad Informática Básica</b>	CÓDIGO:	P1
		VERSIÓN:	1.0
		PÁGINA:	34/59
		FECHA DE EMISIÓN:	15/04/2024
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

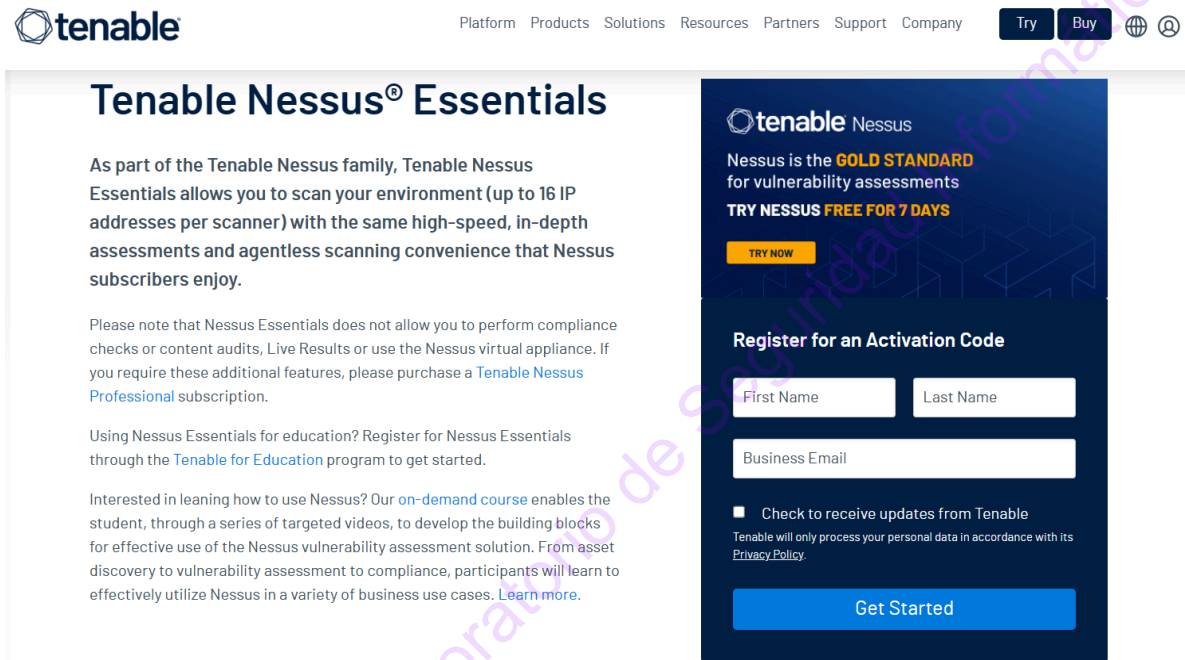


Figura No. 1. Creación de una cuenta en Tenable

Para crear una cuenta, es necesario registrarse con su correo institucional, por ejemplo, usando el dominio [comunidad.unam.mx](mailto:comunidad.unam.mx) o dominio [ingenieria.unam.edu](mailto:ingenieria.unam.edu).

Ya que hayan ingresado sus datos, deben entrar a su cuenta de correo electrónico que hayan registrado, y verificar que les haya llegado un correo confirmando su registro, mismo que tiene una clave de activación.

Una vez que se tiene la clave de activación, ingresamos a la liga de descarga <https://www.tenable.com/downloads/nessus?loginAttempted=true> donde se debe ver la siguiente página:

	<b>Manual de prácticas del Laboratorio de Seguridad Informática Básica</b>	CÓDIGO:	P1
		VERSIÓN:	1.0
		PÁGINA:	35/59
		FECHA DE EMISIÓN:	15/04/2024
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			



Figura No. 2. Página de descarga de Nessus

Deben oprimir el botón “Download” para realizar la descarga.

Una vez instalado el software, se procede a abrir el instalador:

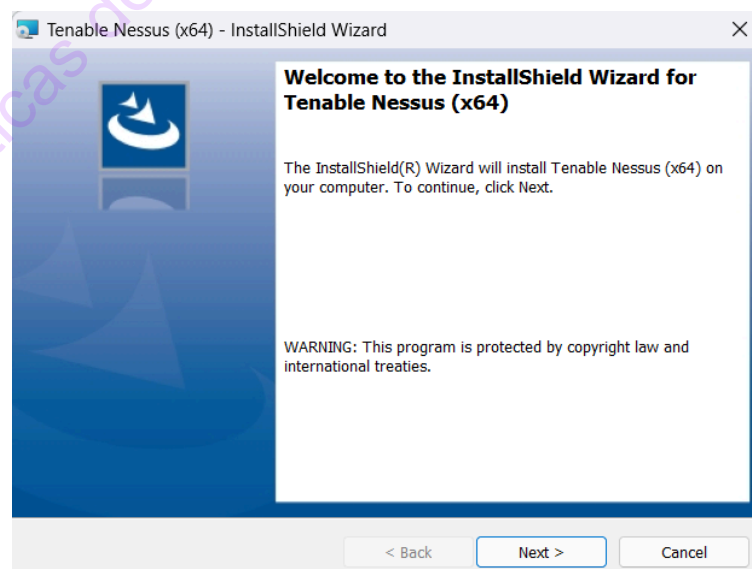


Figura No. 3. Instalación de Nessus I

	<b>Manual de prácticas del Laboratorio de Seguridad Informática Básica</b>	CÓDIGO:	P1
		VERSIÓN:	1.0
		PÁGINA:	36/59
		FECHA DE EMISIÓN:	15/04/2024
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

Se deben aceptar los términos y condiciones para que se permita la descarga.

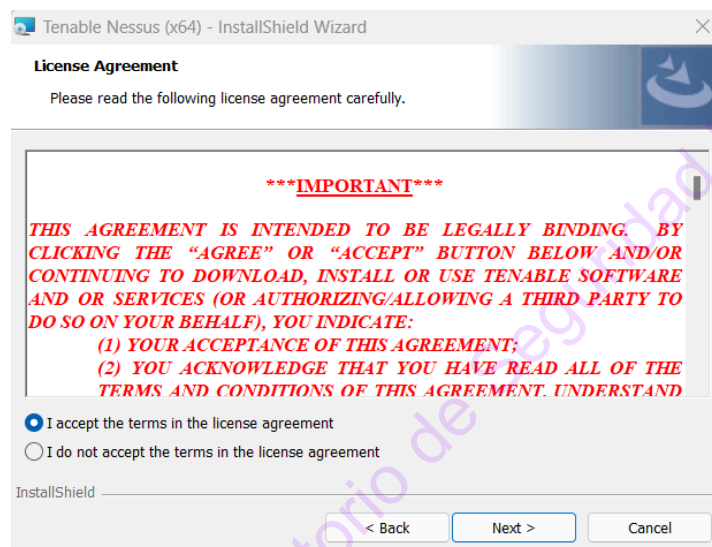


Figura No. 4. Instalación de Nessus II

Posteriormente se muestra la carpeta de instalación, dejando la que nos da por defecto.

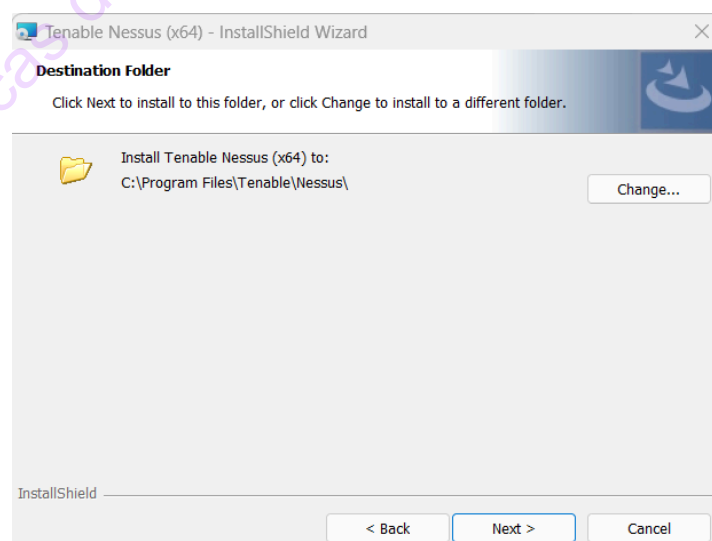


Figura No. 5. Instalación de Nessus III



	<b>Manual de prácticas del Laboratorio de Seguridad Informática Básica</b>	CÓDIGO:	P1
		VERSIÓN:	1.0
		PÁGINA:	37/59
		FECHA DE EMISIÓN:	15/04/2024
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

Una vez terminada la configuración, se oprime el botón “*Install*” para comenzar con la instalación.

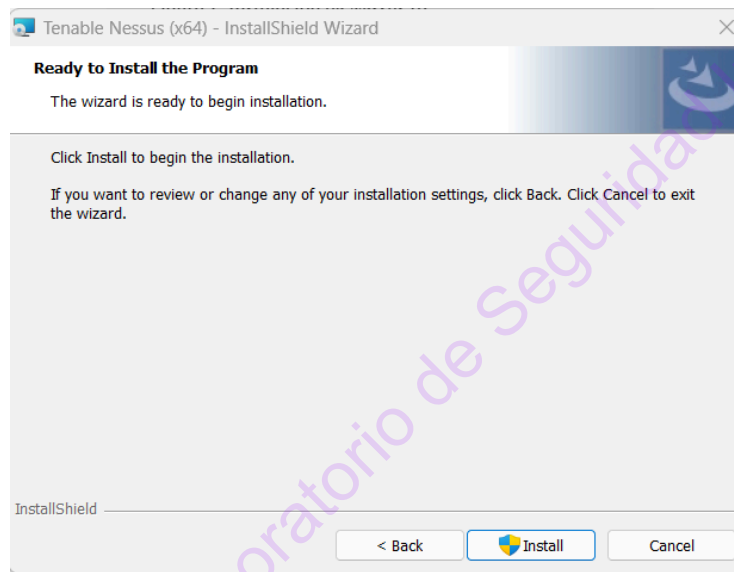


Figura No. 6. Instalación de Nessus IV

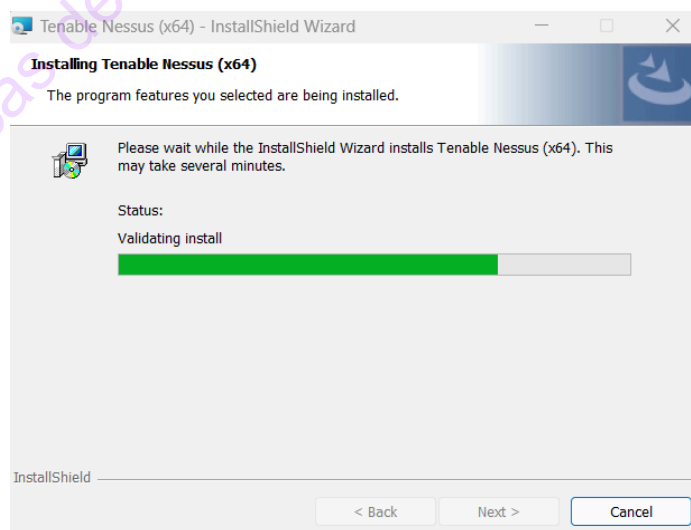


Figura No. 7. Instalación de Nessus V

	<b>Manual de prácticas del Laboratorio de Seguridad Informática Básica</b>	CÓDIGO:	P1
		VERSIÓN:	1.0
		PÁGINA:	38/59
		FECHA DE EMISIÓN:	15/04/2024
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

Después de este paso, se comienza con la instalación del software, después de unos minutos, finaliza la descarga y nos arroja una ventana indicando que el programa se instaló con éxito. Damos click en el botón “*Finish*” para cerrar la ventana.

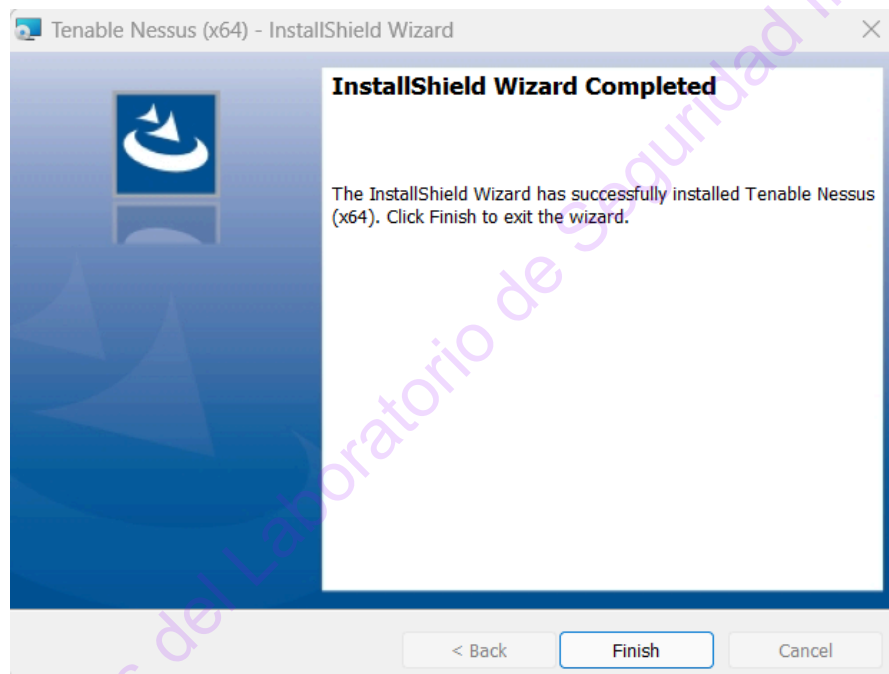


Figura No. 8. Instalación de Nessus VI

Una vez instalado Nessus en el equipo de cómputo dónde se va a trabajar, se abre el siguiente enlace, donde se debe dar click en el botón “*Connect via SSL*”:

	<b>Manual de prácticas del Laboratorio de Seguridad Informática Básica</b>	CÓDIGO:	P1
		VERSIÓN:	1.0
		PÁGINA:	39/59
		FECHA DE EMISIÓN:	15/04/2024
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

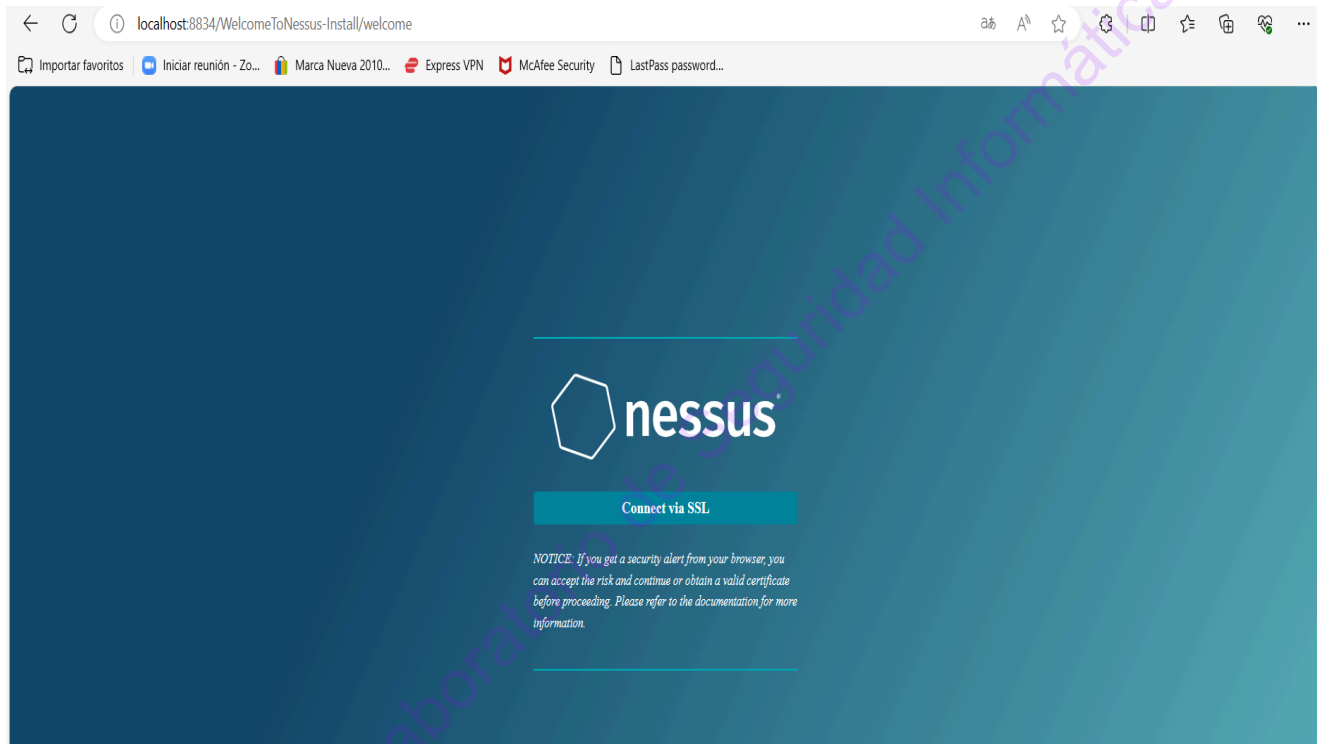


Figura No. 9. Activación de Nessus I

Se muestra una ventana donde se nos indica el modo de registro, para efectos de esta práctica, se elige el modo Online, es decir, damos click directamente en el botón “Continue”

	<b>Manual de prácticas del Laboratorio de Seguridad Informática Básica</b>	CÓDIGO:	P1
		VERSIÓN:	1.0
		PÁGINA:	40/59
		FECHA DE EMISIÓN:	15/04/2024
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

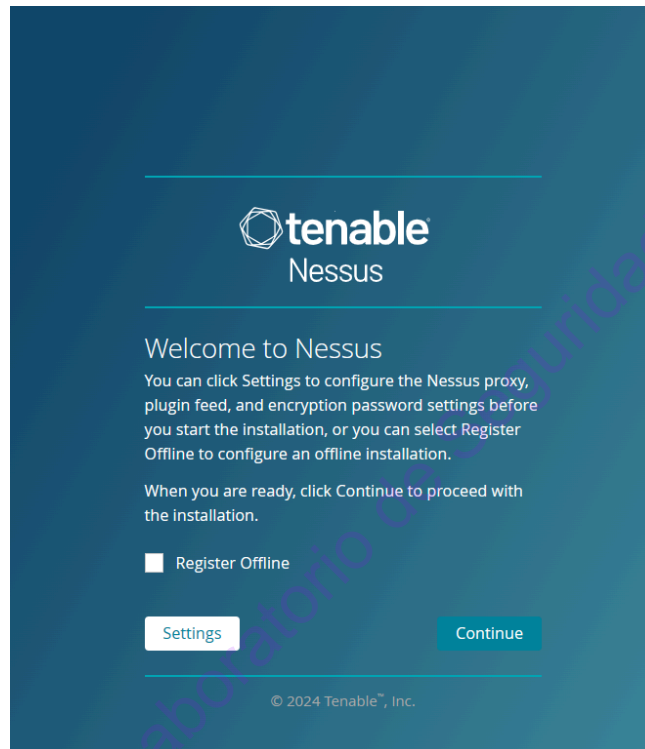


Figura No. 10. Activación de Nessus II

Se muestra otra ventana con varias opciones de activación, dejamos la que esta seleccionada y damos click en “Continue”.

	<b>Manual de prácticas del Laboratorio de Seguridad Informática Básica</b>	CÓDIGO:	P1
		VERSIÓN:	1.0
		PÁGINA:	41/59
		FECHA DE EMISIÓN:	15/04/2024
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

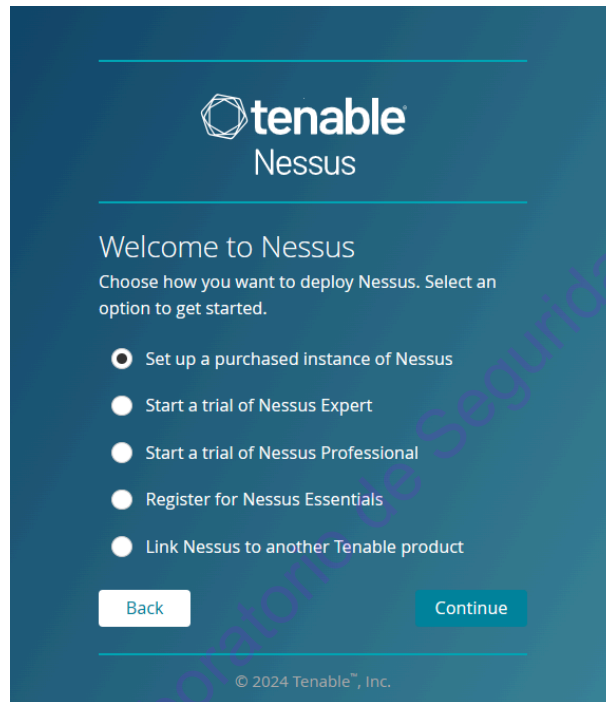


Figura No. 11. Activación de Nessus III

Se muestra una ventana donde se pide el registro, en caso de no haberlo hecho previamente, si ya está registrado, debe dar click en el botón “Skip”.

	<b>Manual de prácticas del Laboratorio de Seguridad Informática Básica</b>	CÓDIGO:	P1
		VERSIÓN:	1.0
		PÁGINA:	42/59
		FECHA DE EMISIÓN:	15/04/2024
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

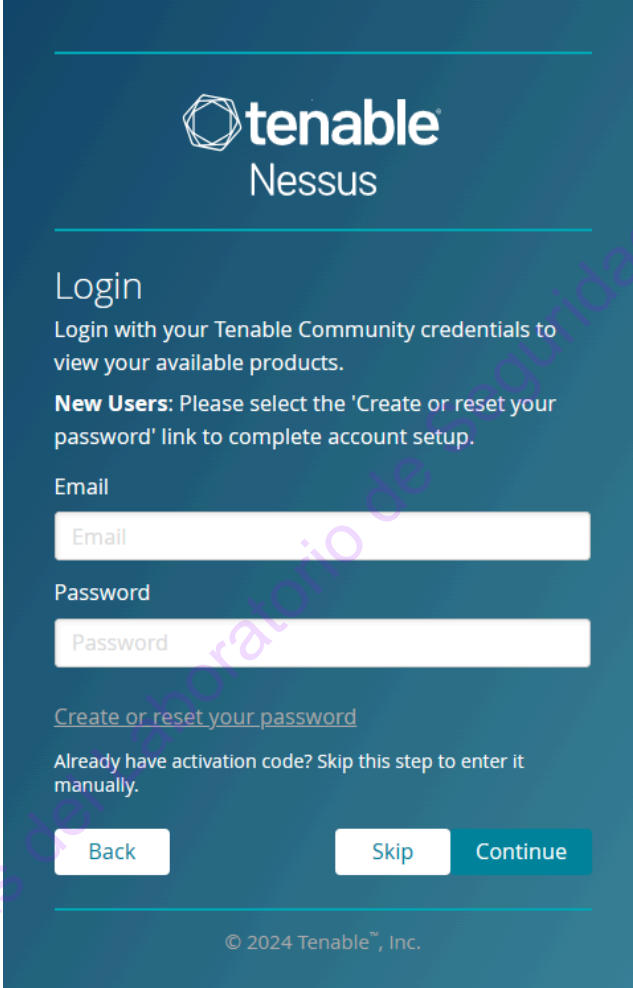


Figura No. 12. Activación de Nessus IV

En la siguiente ventana se debe ingresar el código de activación que se les proporciona en el correo que hayan registrado, lo ingresan y dan click en “Continue”.

	<b>Manual de prácticas del Laboratorio de Seguridad Informática Básica</b>	CÓDIGO:	P1
		VERSIÓN:	1.0
		PÁGINA:	43/59
		FECHA DE EMISIÓN:	15/04/2024
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

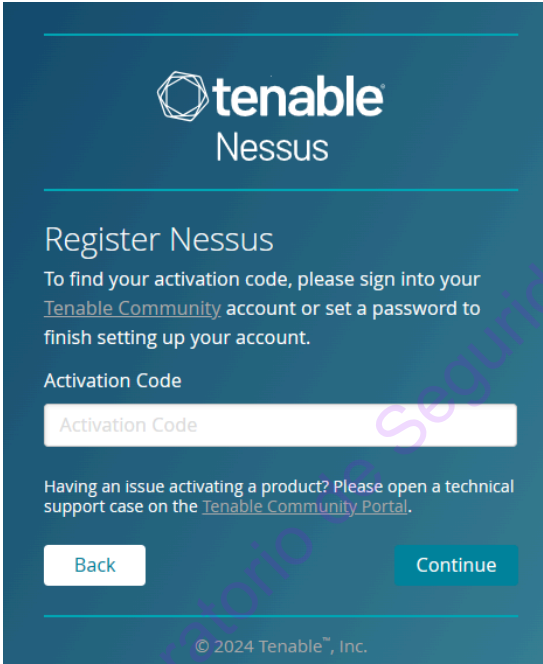


Figura No. 13. Activación de Nessus V

Ya ingresado correctamente el código, se muestra una ventana que confirma la activación, damos click en “Continue”.

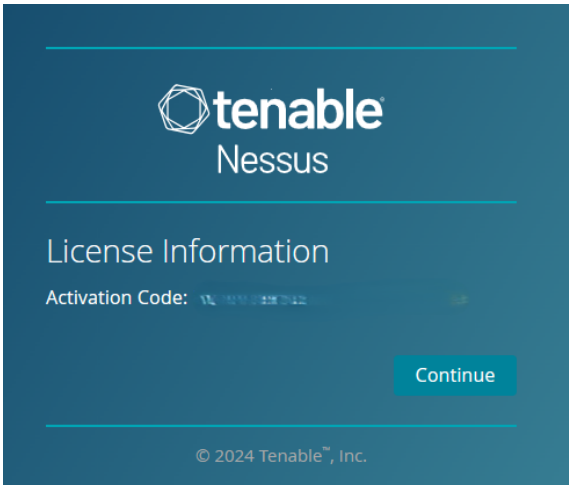


Figura No. 14. Activación de Nessus VI

	<b>Manual de prácticas del Laboratorio de Seguridad Informática Básica</b>	CÓDIGO:	P1
		VERSIÓN:	1.0
		PÁGINA:	44/59
		FECHA DE EMISIÓN:	15/04/2024
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

Ahora se debe crear una cuenta con un nombre de usuario con una contraseña, se recomienda que la contraseña tenga letras mayúsculas, letras minúsculas, números y algún carácter especial para tener un mayor nivel de seguridad, una vez creado su usuario y contraseña, se da click en el botón “Submit”.

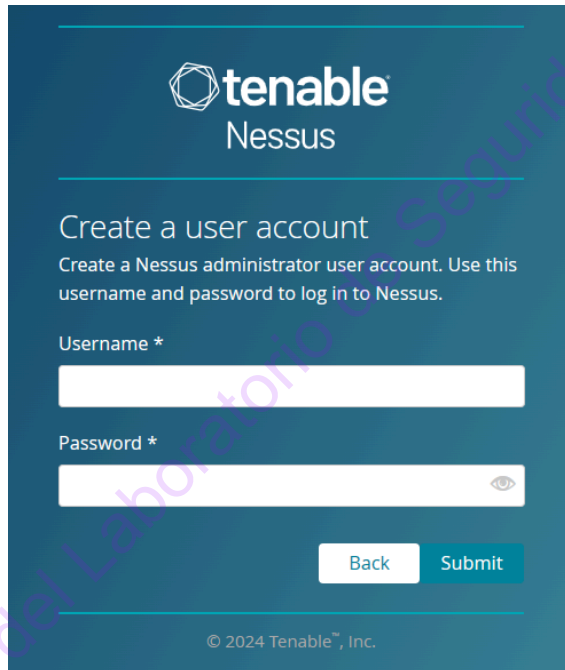


Figura No. 15. Creación de una cuenta en Nessus

Ya ingresados el usuario y la contraseña, Nessus comenzará a subir estos datos para que se pueda usar en cualquier navegador de su equipo de cómputo, esperamos unos minutos hasta que finalice la carga.



	<b>Manual de prácticas del Laboratorio de Seguridad Informática Básica</b>	CÓDIGO:	P1
		VERSIÓN:	1.0
		PÁGINA:	45/59
		FECHA DE EMISIÓN:	15/04/2024
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			



Figura No. 16. Inicio de Nessus en el navegador

### 5.3.2 Escaneo de Vulnerabilidades usando Tenable Nessus

Una vez instalado y activado correctamente el software Nessus, se debe abrir un navegador de internet, como Chrome, Edge o Firefox y se debe ingresar a la siguiente liga: <https://localhost:8834/#/>, donde se muestra una ventana donde se deben ingresar el usuario y contraseña que crearon previamente:

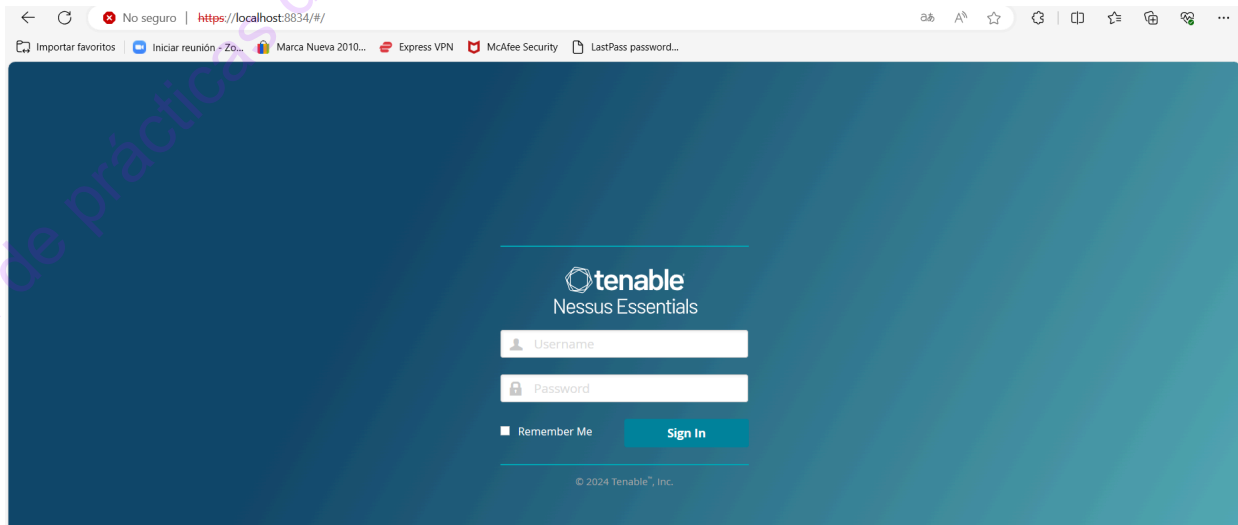


Figura No. 17. Ingreso a Nessus

	<b>Manual de prácticas del Laboratorio de Seguridad Informática Básica</b>	CÓDIGO:	P1
		VERSIÓN:	1.0
		PÁGINA:	46/59
		FECHA DE EMISIÓN:	15/04/2024
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

Ya ingresados sus datos, se muestra la siguiente ventana, para iniciar con un escaneo, se debe dar click en el texto azul “Create a new scan”.

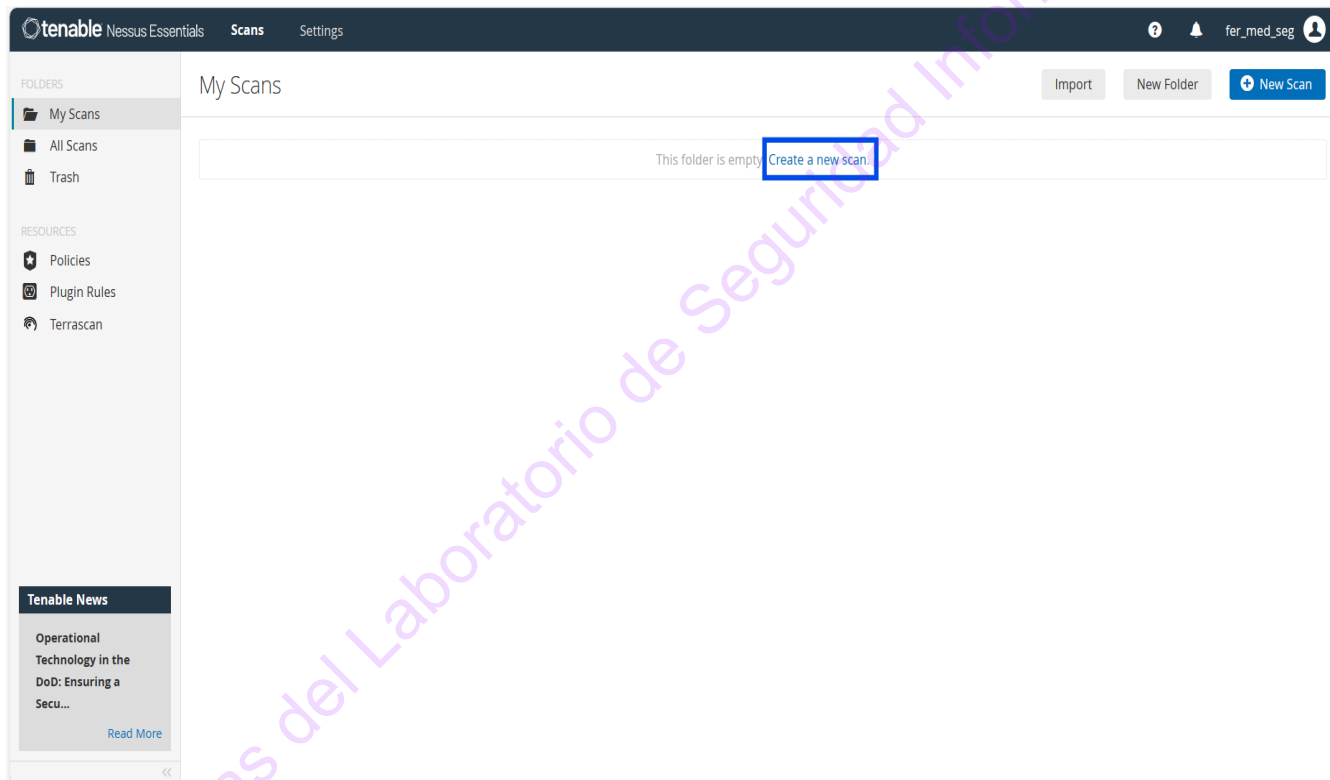


Figura No. 18. Página inicial de Nessus

Se muestra una nueva ventana con varias opciones de escaneo, para esta práctica, se elige la opción “Advanced Scan”.

	<b>Manual de prácticas del Laboratorio de Seguridad Informática Básica</b>	CÓDIGO:	P1
		VERSIÓN:	1.0
		PÁGINA:	47/59
		FECHA DE EMISIÓN:	15/04/2024
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			


## Scan Templates

[Back to Scans](#)

Scanner


Search Lib

DISCOVERY




**Host Discovery**  
A simple scan to discover live hosts and open ports.


VULNERABILITIES




**Basic Network Scan**  
A full system scan suitable for any host.




**Advanced Scan**  
Configure a scan without using any recommendations.




**Advanced Dynamic Scan**  
Configure a dynamic plugin scan without recommendations.




**Malware Scan**  
Scan for malware on Windows and Unix systems.




**Mobile Device Scan**  
Assess mobile devices via Microsoft Exchange or an MDM.




**Web Application Tests**  
Scan for published and unknown web vulnerabilities using Nessus Scanner.




**Credentialed Patch Audit**  
Authenticate to hosts and enumerate missing updates.



**Intel AMT Security Bypass**  
Remote and local checks for CVE-2017-5689.



**Spectre and Meltdown**  
Remote and local checks for CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754



**WannaCry Ransomware**  
Remote and local checks for MS17-010.

Figura No. 19. Selección de un escaneo avanzado

Se muestra una ventana donde hay que indicar el nombre, descripción, ubicación del escaneo y objetivo, el nombre y descripción es a criterio del alumno, y como objetivo se recomienda usar una página web de una escuela, dependencia de la UNAM o de una dependencia gubernamental que no tenga el protocolo https para obtener vulnerabilidades más críticas, una vez ingresados los datos, se da click en el botón “Save”.

	<b>Manual de prácticas del Laboratorio de Seguridad Informática Básica</b>	CÓDIGO:	P1
		VERSIÓN:	1.0
		PÁGINA:	48/59
		FECHA DE EMISIÓN:	15/04/2024
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

New Scan / Advanced Scan

[Back to Scan Templates](#)

**Settings**
Credentials
Plugins

**BASIC**

- General
- Schedule
- Notifications

DISCOVERY >
ASSESSMENT >
REPORT >
ADVANCED >

Name REQUIRED

Description

Folder
My Scans

Targets

Example: 192.168.1.1-192.168.1.5, 192.168.2.0/24, test.com
REQUIRED

Upload Targets
Add File

Save
Cancel

Figura No. 20. Configuración del escaneo de una página web

Por ejemplo, se muestra la configuración de la página web del CCH Naucalpan como objetivo, se debe ingresar únicamente el dominio de la página web, sin el uso de los protocolos http y https.

New Scan / Basic Network Scan

[Back to Scan Templates](#)

Settings

Credentials

Plugins

BASIC

General

Schedule

Notifications

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Name

Práctica Vulnerabilidades

Description

Análisis de la página web del CCH Naucalpan

Folder

My Scans

Targets

www.cch-naucalpan.unam.mx

Upload Targets

Add File

Save

Cancel

Figura No. 21. Ejemplo de configuración de una página web

Ya creada la configuración, se muestra una ventana donde se visualiza el avance del escaneo que se realiza a la página web, el análisis puede tardar algunos minutos en completarse, para comenzar el análisis, debe dar click en el botón de inicio.

<input type="checkbox"/>	Name	Schedule	Last Scanned
<input type="checkbox"/>	Práctica Vulnerabilidades	On Demand	N/A

Figura No. 22. Ejecución del análisis de la página web

	<b>Manual de prácticas del Laboratorio de Seguridad Informática Básica</b>	CÓDIGO:	P1
		VERSIÓN:	1.0
		PÁGINA:	50/59
		FECHA DE EMISIÓN:	15/04/2024
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

Una vez finalizado el análisis, deben dar click en el recuadro de sus escaneos, para desplegar el análisis generado.

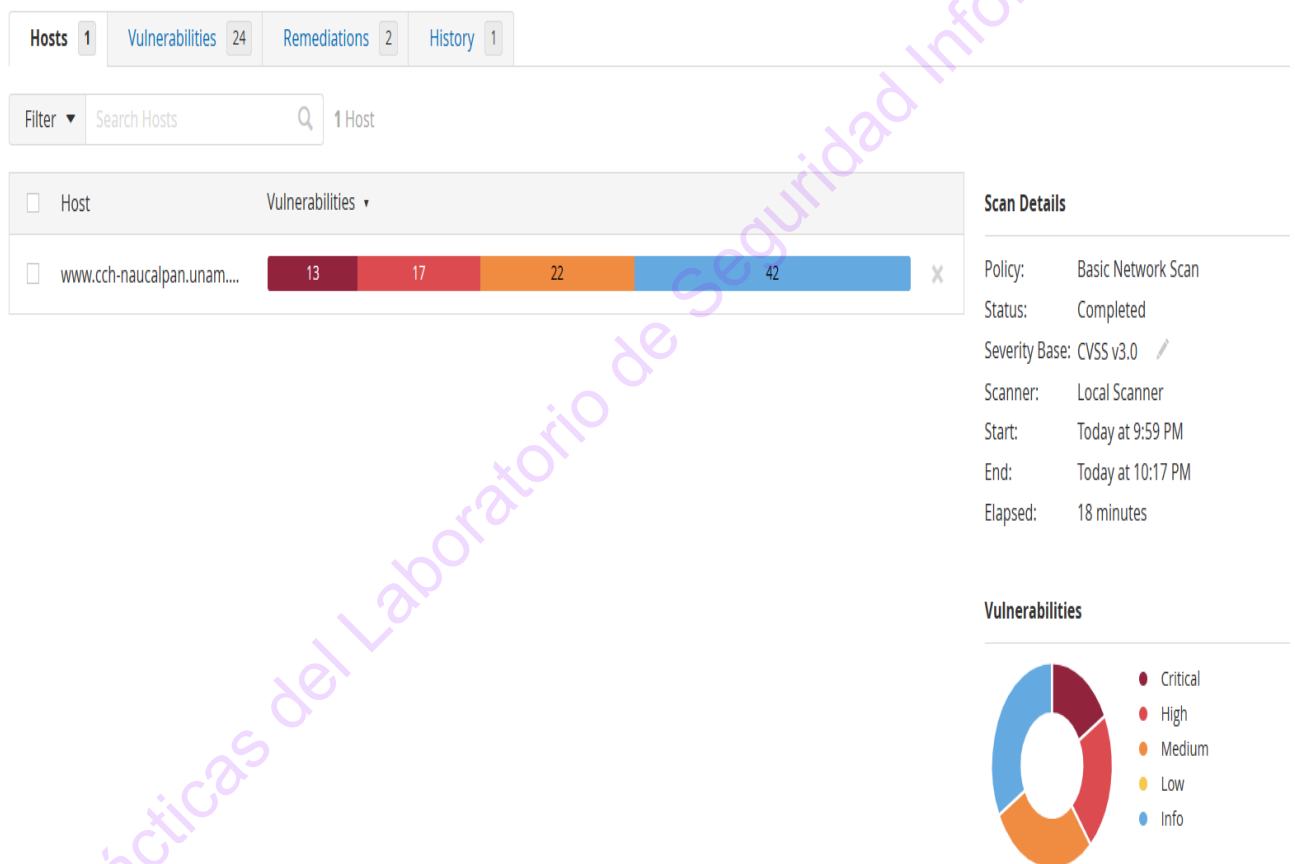


Figura No. 23. Resultados del análisis de la página web

Observe cómo dependiendo de la escala de gravedad de las vulnerabilidades detectadas se distinguen por un color específico, que van desde los amarillos que son los mpas bajos, a los rojos oscuros que son los más críticos y urgentes a resolver, los azules son solo de carácter informativo, no representan una vulnerabilidad.

	<b>Manual de prácticas del Laboratorio de Seguridad Informática Básica</b>	CÓDIGO:	P1
		VERSIÓN:	1.0
		PÁGINA:	51/59
		FECHA DE EMISIÓN:	15/04/2024
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

Ahora de click en la barra de colores y observe con detalle las vulnerabilidades detectadas, observe cómo están listadas de las más críticas a las más leves, así como su respectiva puntuación, donde 10 es el nivel más alto.

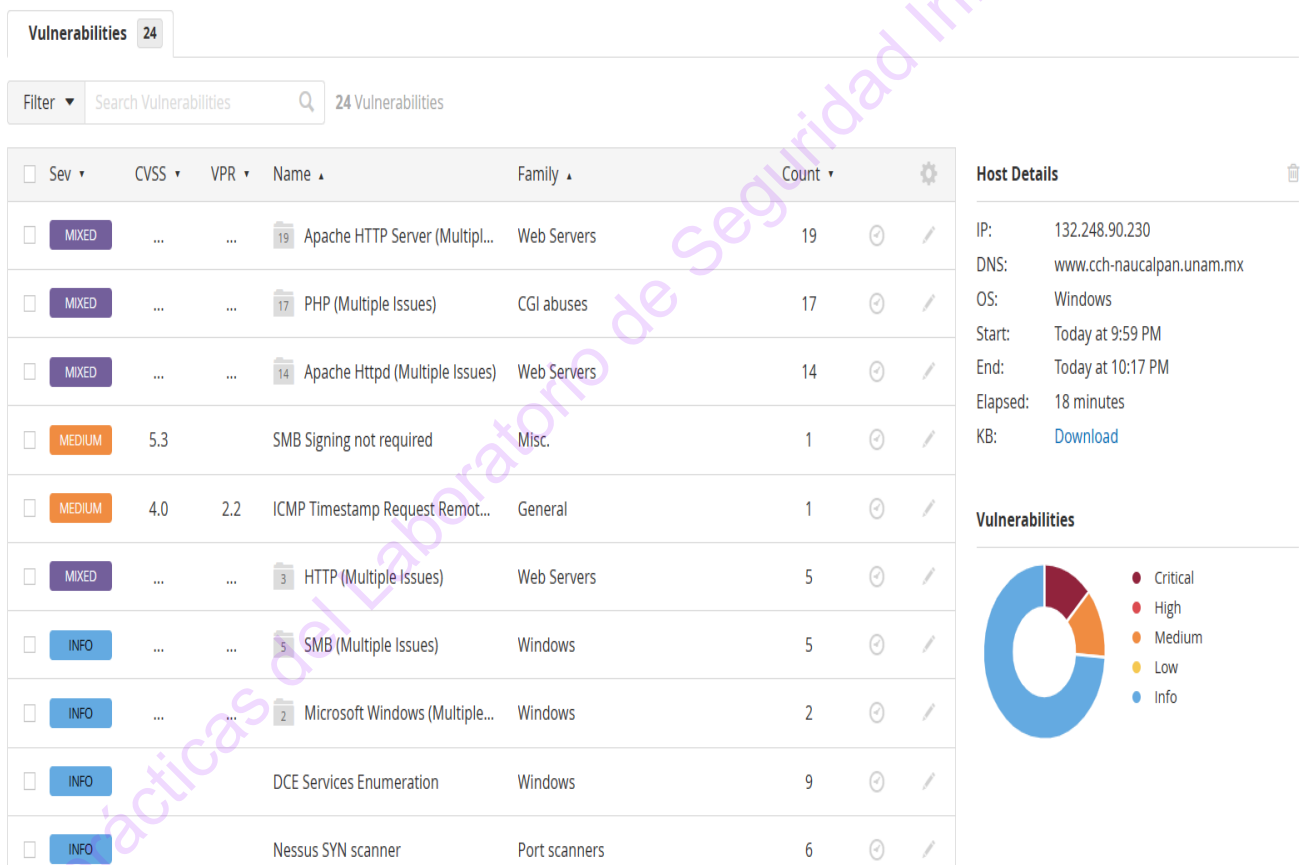


Figura No. 24. Lista de vulnerabilidades detectadas en la página web

Puede explorar con mayor detalle alguna vulnerabilidad que le llame la atención, donde se muestra la descripción de la vulnerabilidad, así como una solución que el software propone.

Por ejemplo, para la vulnerabilidad del servidor Apache, se muestra que el problema está en tener una versión obsoleta, y el software como solución

plantea que se debe actualizar a una versión más reciente, para evitar problemas de mantenimiento en el futuro.

Vulnerabilities24

CRITICAL

Apache HTTP Server SEoL (2.1.x <= x <= 2.2.x)

Description

According to its version, Apache HTTP Server is between 2.1.x and 2.2.x. It is, therefore, no longer maintained by its vendor or provider.  
  
Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities.

Solution

Upgrade to a version of Apache HTTP Server that is currently supported.

See Also

<https://archive.apache.org/dist/httpd/Announcement2.2.txt>

Output

URL: http://www.cch-naucalpan.unam.mx/

Installed version: 2.2.8

Security End of Life: July 10, 2017

Time since Security End of Life (Est.): >= 6 years

To see debug logs, please visit individual host

Port

Hosts

80 / tcp / wwwwww.cch-naucalpan.unam.mx

Plugin Details

Severity: Critical

ID: 171356

Version: 1.5

Type: combined

Family: Web Servers

Published: February 10, 2023

Modified: April 2, 2024

Risk Information

Risk Factor: Critical

CVSS v3.0 Base Score 10.0

CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

CVSS v2.0 Base Score: 10.0

CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:I/C:A/C

Vulnerability Information

CPE: cpe:/a:apache:http\_server

Unsupported by vendor: true

Figura No. 25. Ejemplo de una vulnerabilidad detectada en la página web con su descripción y una solución

Ahora debe analizar alguna otra página web para detectar sus vulnerabilidades, indique cuántas vulnerabilidades detectó el software, de cuántos tipos se detectaron, y observe y analice tres vulnerabilidades detectadas con detenimiento, coloque capturas de pantalla que muestre la gráfica de las vulnerabilidades y la descripción de las vulnerabilidades elegidas como se muestra en las figuras 23 y 25 respectivamente, así mismo, explique con sus propias palabras de las tres vulnerabilidades elegidas por qué el software las

52





# Manual de prácticas del Laboratorio de Seguridad Informática Básica

CÓDIGO:	P1
VERSIÓN:	1.0
PÁGINA:	53/59
FECHA DE EMISIÓN:	15/04/2024

Facultad de Ingeniería

Área/Departamento: Laboratorio de Redes y Seguridad

La impresión de este documento es una copia no controlada

considera como una vulnerabilidad, es decir, que amenazas se pueden presentar si no se elimina esa vulnerabilidad, que daños puede ocasionar, y cómo la solución planteada por el software ayuda a mitigar el nivel de riesgo de la página web, investiga información en internet en caso de ser necesario.

- Captura de Pantalla de la barra y gráfica de vulnerabilidades detectadas:



# Manual de prácticas del Laboratorio de Seguridad Informática Básica

CÓDIGO:

P1

VERSIÓN:

1.0

PÁGINA:

54/59

FECHA DE  
EMISIÓN:

15/04/2024

Facultad de Ingeniería

Área/Departamento: Laboratorio de Redes y Seguridad

La impresión de este documento es una copia no controlada

- Captura de Pantalla de la Vulnerabilidad 1:



# Manual de prácticas del Laboratorio de Seguridad Informática Básica

CÓDIGO:	P1
VERSIÓN:	1.0
PÁGINA:	55/59
FECHA DE EMISIÓN:	15/04/2024

Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada	

- Captura de Pantalla de la Vulnerabilidad 2:





# Manual de prácticas del Laboratorio de Seguridad Informática Básica

CÓDIGO:

P1

VERSIÓN:

1.0

PÁGINA:

56/59

FECHA DE  
EMISIÓN:

15/04/2024

Facultad de Ingeniería

Área/Departamento: Laboratorio de Redes y Seguridad

La impresión de este documento es una copia no controlada

- Captura de Pantalla de la Vulnerabilidad 3:





# Manual de prácticas del Laboratorio de Seguridad Informática Básica

CÓDIGO:	P1
VERSIÓN:	1.0
PÁGINA:	57/59
FECHA DE EMISIÓN:	15/04/2024

Facultad de Ingeniería      Área/Departamento: Laboratorio de Redes y Seguridad

La impresión de este documento es una copia no controlada

- Explicación de la Vulnerabilidad 1:

---

---

---

---

---

---

---

---

---

---

- Explicación de la Vulnerabilidad 2:

---

---

---

---

---

---

---

---

---

---

- Explicación de la Vulnerabilidad 3:

---

---



# Manual de prácticas del Laboratorio de Seguridad Informática Básica

CÓDIGO:	P1
VERSIÓN:	1.0
PÁGINA:	58/59
FECHA DE EMISIÓN:	15/04/2024

Facultad de Ingeniería

Área/Departamento: Laboratorio de Redes y Seguridad

La impresión de este documento es una copia no controlada

## 6. Conclusiones

Anoten sus conclusiones tras revisar los objetivos planteados al inicio de la práctica

	<b>Manual de prácticas del Laboratorio de Seguridad Informática Básica</b>	CÓDIGO:	P1
		VERSIÓN:	1.0
		PÁGINA:	59/59
		FECHA DE EMISIÓN:	15/04/2024
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

## Bibliografía

- Carlos. (2022, diciembre 18). Qué son los activos informáticos y cómo se valoran. Perito Informático - Peritaje informático; Eugenio Picón - Peritos Ingenieros Informáticos.  
<https://peritoinformatico.es/que-es-un-activo-informatico-y-como-se-valoran/>
- SensorsTech, P. (2023, septiembre 26). Qué es una amenaza informática: ejemplos y concepto. SensorsTech.  
<https://sensortechforum.es/que-es-una-amenaza-informatica-y-ejemplos/>
- ¿Qué es una vulneración de seguridad? (2023, abril 19). latam.kaspersky.com.  
<https://latam.kaspersky.com/resource-center/threats/what-is-a-security-breach>
- Pérez, D. C. (s/f). ¿Qué son los escáneres de vulnerabilidad? Ceupe.  
<https://www.ceupe.com/blog/que-son-los-escaneres-de-vulnerabilidad.html>