**PRÁCTICA N°1**

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

**1. OBJETIVOS**

1.1 Familiarizar al estudiante con las vulnerabilidades en Windows

1.2 Implementar Políticas de seguridad en Windows para disminuir riesgos.

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

**2. DESARROLLO DEL TRABAJO PREPARATORIO**

***2.1. ¿Describir detalladamente que es una vulnerabilidad y como se clasifican?***

Las vulnerabilidades son conocidas como debilidades o fallos en los sistemas de información, al ser encontradas estas vulnerabilidades pueden llegar a ser explotadas por amenazas que comprometan los sistemas o redes [1].

Las vulnerabilidades se clasifican de diferentes formas:

1. Vulnerabilidades según su Origen

* Vulnerabilidades de software: Son errores que comprometen los códigos o configuraciones.
* Vulnerabilidades de hardware: Son fallas presentes en los componentes físicos.
* Vulnerabilidades humanas: Son errores cometidos por el eslabón más débil, es decir, por usuarios o personal.

1. Vulnerabilidades según la naturaleza del Acceso.

* Vulnerabilidades Locales: Requieren de acceso físico o lógico en el sistema para ser explotadas.
* Vulnerabilidades Remotas: Son explotadas a través de la red sin necesidad de acceso previo.

***2.2 Consultar y describir brevemente como se realizar un escaneo de puertos.***

El escaneo de puertos es un método utilizado para identificar puertos abiertos en un sistema o en una red, con el propósito de determinar lo servicios que se están ejecutando y determinado las posibles vulnerabilidades [2].

Para ejecutar un escaneo de puertos se debe seguir los siguientes pasos:

1. Preparar la herramienta de escaneo.
2. Identificar las IP
3. Filtrar los hosts
4. Seleccionar los puertos a escanear o hacer un escaneo completo de todos los puertos
5. Con la herramienta seleccionada previamente se inicia el escaneo.
6. Finaliza el escaneo e identifica los puertos abiertos.

***2.3 Investigue herramientas para hacer escaneo de puertos.***

* Nmap: Herramienta utilizada para el escaneo de puertos y auditorias de seguridad [3].
* Netcat: Es una herramienta fácil de utilizar para el escaneo de puertos [4].
* Angry IP Scanner: Herramienta de puertos multiplataforma [5].
* Nessus: Herramienta de evaluación de vulnerabilidades incluyendo escaneo de puertos [6].

**BIBLIOGRAFÍA.**

[1] M. Bishop, *Introduction to computer security*, 6. repr. Boston Munich: Addison-Wesley, 2011.

[2] «Port Scanning Basics | Nmap Network Scanning». Accedido: 20 de enero de 2025. [En línea]. Disponible en: https://nmap.org/book/man-port-scanning-basics.html

[3] «Chapter 15. Nmap Reference Guide | Nmap Network Scanning». Accedido: 20 de enero de 2025. [En línea]. Disponible en: https://nmap.org/book/man.html#man-description

[4] «Ncat - Netcat for the 21st Century». Accedido: 20 de enero de 2025. [En línea]. Disponible en: https://nmap.org/ncat/

[5] «Angry IP Scanner - About». Accedido: 20 de enero de 2025. [En línea]. Disponible en: https://angryip.org/about/

[6] «Escáner de vulnerabilidades Nessus:Solución de seguridad en la red», Tenable®. Accedido: 20 de enero de 2025. [En línea]. Disponible en: https://es-la.tenable.com/products/nessus