**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.

**3. REACTIVOS**

¿Cuál es la función principal de Nmap?

1. Escanear y mapear redes, identificando puertos y servicios abiertos.
2. Monitorear trafico en tiempo real en una red.
3. Analizar vulnerabilidades en aplicaciones web
4. Crear políticas de firewall

¿Qué comando se utiliza en Nmap para realizar un escaneo de todos los puertos?

1. Nmap -sS <IP>
2. Nmap -p- <IP>
3. Nmap -sV- <IP>
4. Nmap -Pn- <IP>

¿Qué afirmación es verdadera con respecto a Nessus?

1. Nessus es una herramienta de código abierto.
2. Nessus permite detectar vulnerabilidades conocidas y sugerir correcciones.
3. Nessus realiza solo escaneos de puertos.
4. Nessus permite programar escaneos de seguridad automáticos.

¿Qué escaneos realiza Nessus por defecto?

1. Escaneo de puertos TCP únicamente.
2. Escaneo de vulnerabilidades basados en políticas predefinidas.
3. Escaneo de puertos UDP únicamente.
4. Escaneo de tráfico en tiempo real.

¿Cuáles son los comandos validos de Nmap para realizar un escaneo?

1. Nmap -sT <IP>
2. Nmap -A <IP>
3. Nmap -sU <IP>
4. Nmap -N <IP>