**PRÁCTICA N°1**

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

**1. OBJETIVOS**

1.1 Familiarizar al estudiante con las vulnerabilidades en Windows

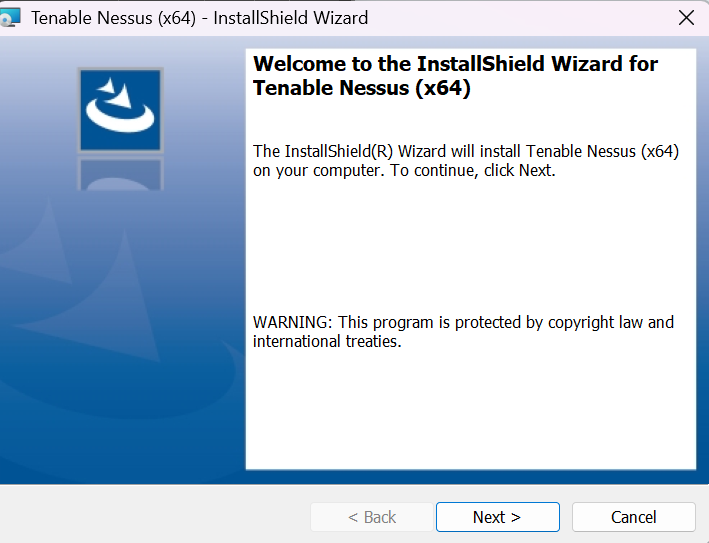
1.2 Implementar Políticas de seguridad en Windows para disminuir riesgos.

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

**4. PRÁCTICA**

#### **Escaneo de vulnerabilidades**

1. Acceder al enlace de descarga del Anexo I, registrarse para acceder a los pasos de instalación.
2. Descargar el instalador y continuar con las instrucciones de instalación del software como muestra la Figura 1.



*Figura 1: Instalador de Nessus*

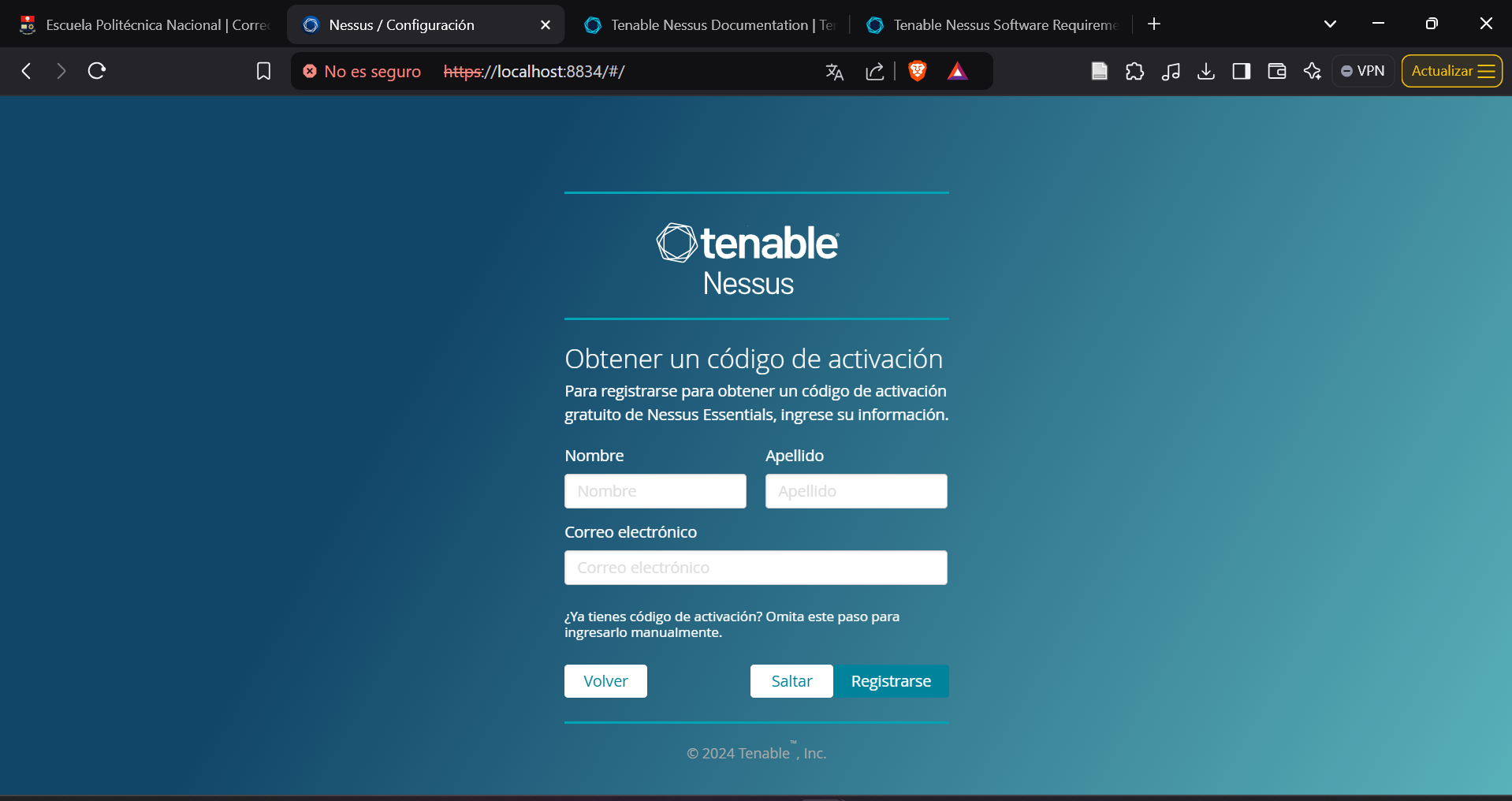
1. Una vez instalado espera que se inicialice el software de Nessus Figura 2.

Interfaz de usuario gráfica

Descripción generada automáticamente

*Figura 2: Pantalla de inicialización de Nessus*

1. Registrar y obtener el código de activación del producto. En la Figura 3, solicita ingresar nombre, apellido y el correo institucional.



*Figura 3: Pantalla de datos de activación del software*

1. Ingresar al sistema y esperar que se descarguen todos los componentes necesarios para ejecutar el escaneo (Figura 4).



*Figura 4: Pantalla de descarga de componentes*

1. Después de completar la descarga, se muestra la pantalla de inicio de Nessus, el cual debemos ingresar la IP que se desea hacer el escaneo (figura 5).

*Captura de pantalla de un celular

Descripción generada automáticamente*

*Figura 5: Pantalla de Inicio de Nessus, Solicitud de IP a escanear*

1. Nessus realiza un escaneo del host (Figura 6), en el caso de encontrar varios hosts se debe seleccionar uno para continuar con el escaneo.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

*Figura 6: Escaneo de Hosts*

1. Al ejecutar el escaneo (Figura 7) este puede tardar de 5 a 10 min, dependiendo la cantidad de puertos, archivos, páginas que se estén ejecutando en la máquina.

Captura de pantalla de un celular

Descripción generada automáticamente

*Figura 7:Ejecución de escaneo*

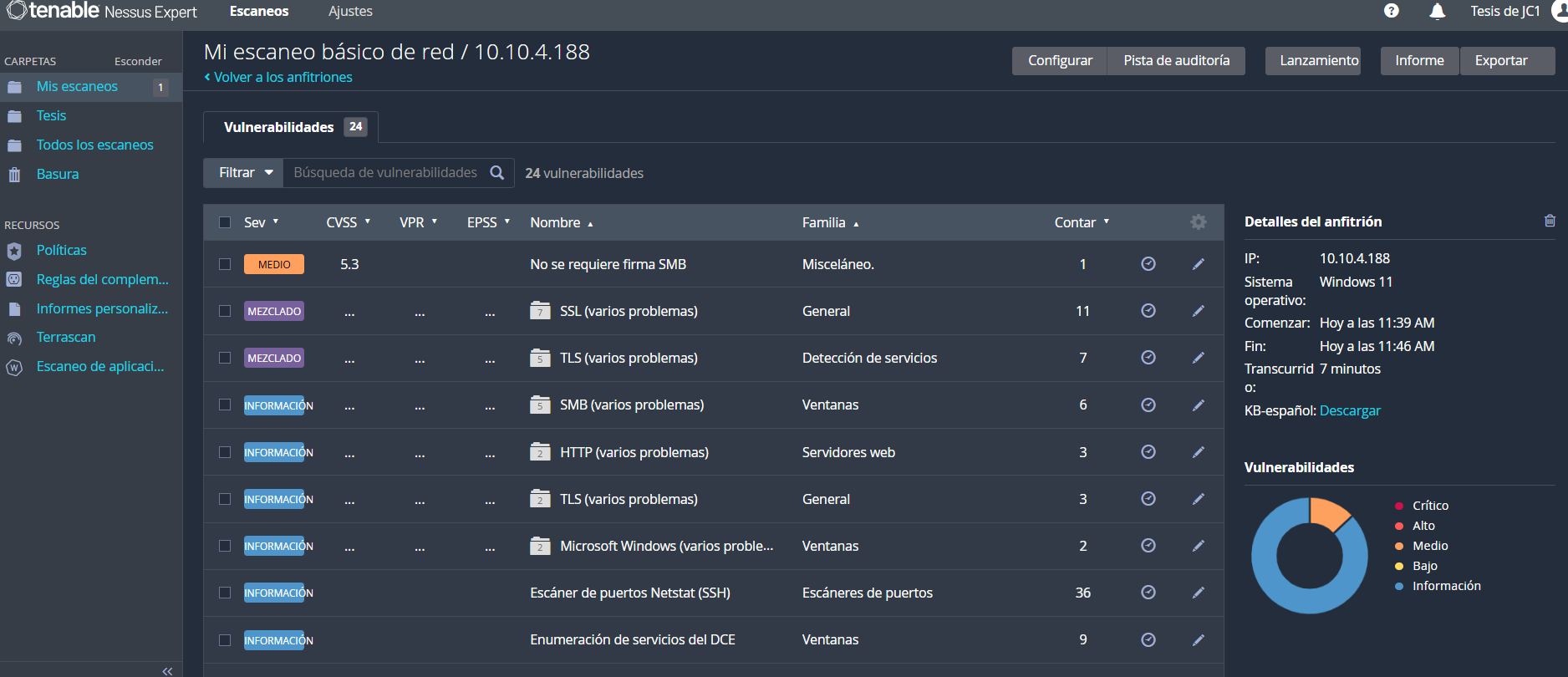
1. Al completar el escaneo, se observa una pequeña pantalla con información básica del escaneo, en la esquina inferior derecha se muestra un gráfico de con el porcentaje de vulnerabilidades (Figura 8).

Captura de pantalla de computadora

Descripción generada automáticamente

*Figura 8: Resultados del escaneo.*

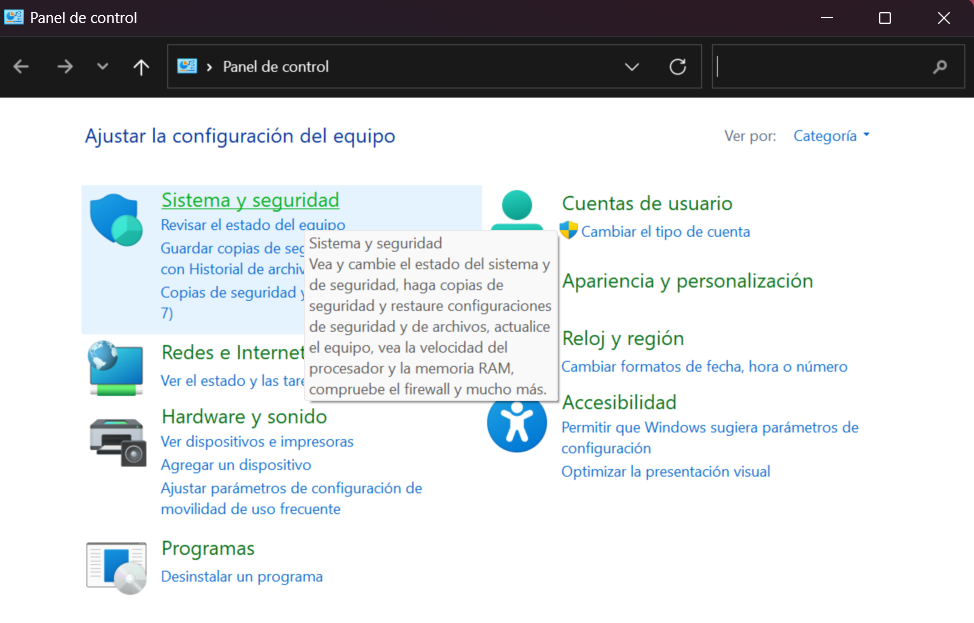
1. Al ingresar al escaneo se observa los resultados (Figura 9).



*Figura 9: Resultados Escaneo*

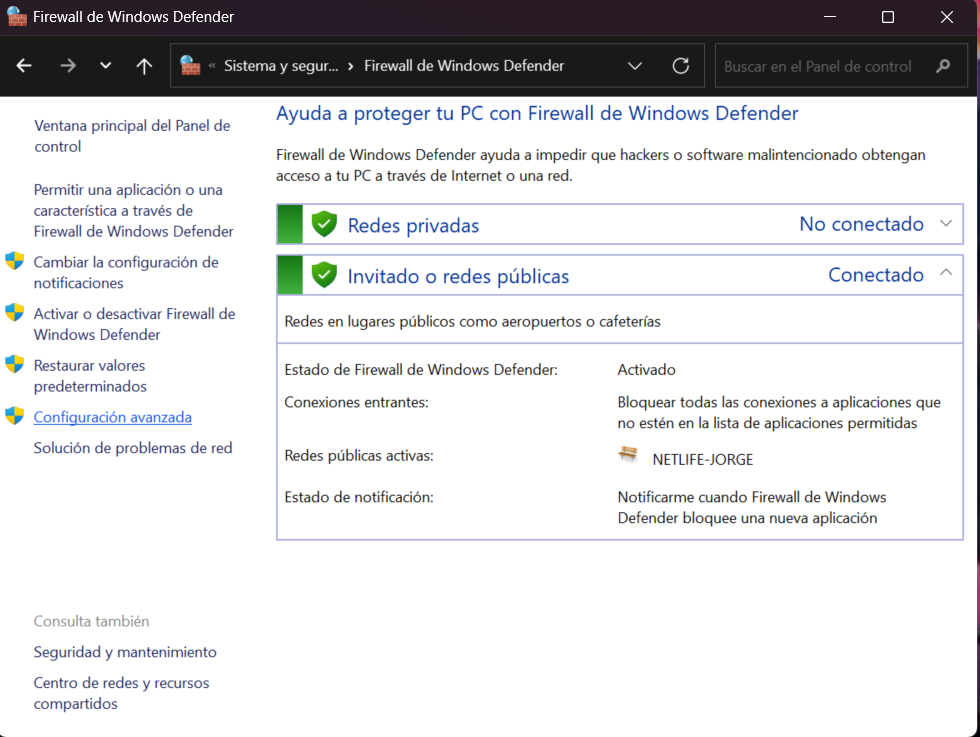
#### **CONFIGURACIÓN REGLAS DE FIREWALL**

1. Abrir el panel de control > Sistema y Seguridad, como se muestra en la Figura 10.



*Figura 10: Opciones de Panel de Control*

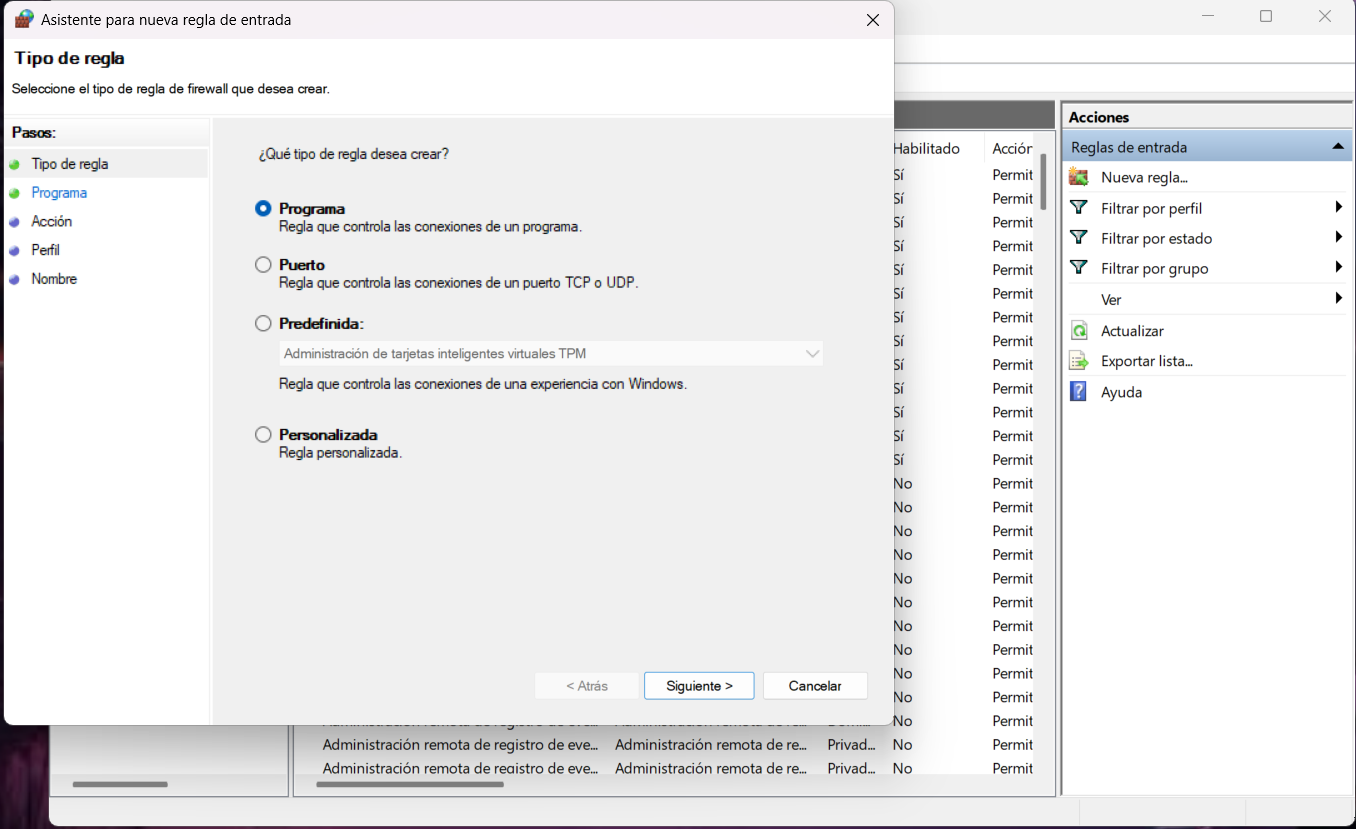
1. Dentro de la Opción Sistema y Seguridad, hacer clic en Firewall de Windows como muestra la Figura 11 e ingresar a la configuración Avanzada.



*Figura 11: Configuración Avanzada de Firewall*

1. En la consola de configuración de Firewall, crear reglas de entrada:

* Clic “Nueva Regla”, en el Panel del lado izquierdo como se muestra en la Figura 12.



*Figura 12: Nueva Regla de Entrada de Firewall*

* Seleccionar el tipo de regla:
  + Programa: Permite usar o bloquear programas en específico.
  + Puerto: Permite habilitar o bloquear un puerto en específico.
  + Personalizado: Permite configurar opciones avanzadas como direcciones IP y protocolos.
* Configuración de Firewall, Regla de Entrada:
  + Seleccionar “Puerto”, Figura 13.

Interfaz de usuario gráfica, Aplicación, Teams

Descripción generada automáticamente

*Figura 13: Personalizar Regla*

* + Escoger el protocolo (TCP o UDP)
  + Introducir el número de puerto (80), como se muestra en la Figura 14.

Interfaz de usuario gráfica, Aplicación, Teams

Descripción generada automáticamente

*Figura 14: Protocolo al que se le aplica la regla y el puerto*

* + Seleccionar “Bloquear la conexión” como se muestra en la Figura 15.

*Interfaz de usuario gráfica, Aplicación, Teams

Descripción generada automáticamente*

*Figura 15: Bloquear la conexión*

* + Asignar un nombre a la regla, Ejemplo: Ejercicio de Practica (Figura 16).

Interfaz de usuario gráfica, Aplicación, Teams

Descripción generada automáticamente

*Figura 16: Aplicar Regla creada*

* + Realizar el mismo procedimiento en la regla de salida

#### **Instalar NMAP**

* Ingresar al enlace de descarga Anexo I y descargar la opción de Windows (Figura 17) que sea el adecuado para el equipo del usuario.



*Figura 17: Pagina de descarga NMAP*

* Ejecutar el instalador y seguir todos los pasos hasta terminar la instalación del Nmap (Figura 18).

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

*Figura 18: Instalador de Nmap*

#### **Escaneo con Nmap**

1. Abrir la interfaz Gráfica de Nmap como se muestra en la Figura 19.

Interfaz de usuario gráfica, Aplicación, Word

Descripción generada automáticamente

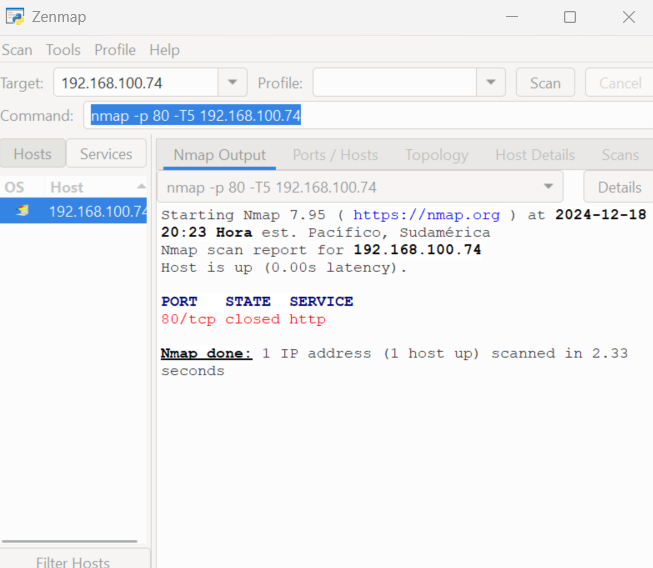
Figura 19: Interfaz Nmap

1. En la interfaz configurar los siguientes campos (Figura 20):
   * Target (Objetivo): Dirección IP objetivo

**172.168.100.74**

* + Command: Ejecutar el siguiente comando –

**nmap -p 80 -T5 192.168.100.74**



*Figura 20: Resultado del escaneo del puerto*

1. Escaneo completo de Puertos, como se muestra en la Figura 21.

**nmap -sS -v 192.168.100.74**

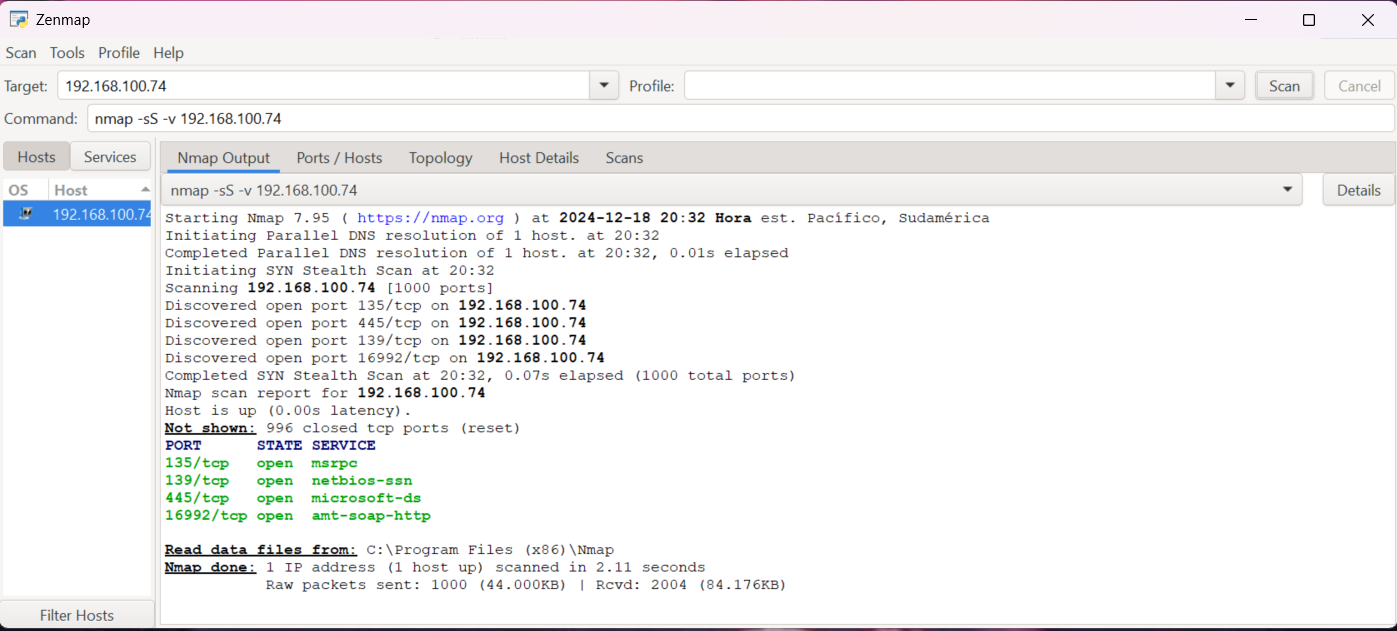
**

Figura 21: Escaneo Completo de Puertos

#### 2.2.1.8 **Escaneo con CMD**

1. Abrir el terminar de Windows (CMD: Command Prompt), como se muestra en la Figura 22.

Texto

Descripción generada automáticamente

*Figura 22: Pantalla CMD*

1. Ejecutar un Escaneo de puertos tal como se detalla en la Figura 23:

**nmap -p 80 192.168.100.74**

Texto

Descripción generada automáticamente

*Figura 23: Ejecutar Escaneo de Puertos*

1. En la Figura 24, se observa el escaneo completo de puertos:

**nmap -sS 192.168.100.74**

Texto

Descripción generada automáticamente

*Figura 24: Escaneo completo de puertos*