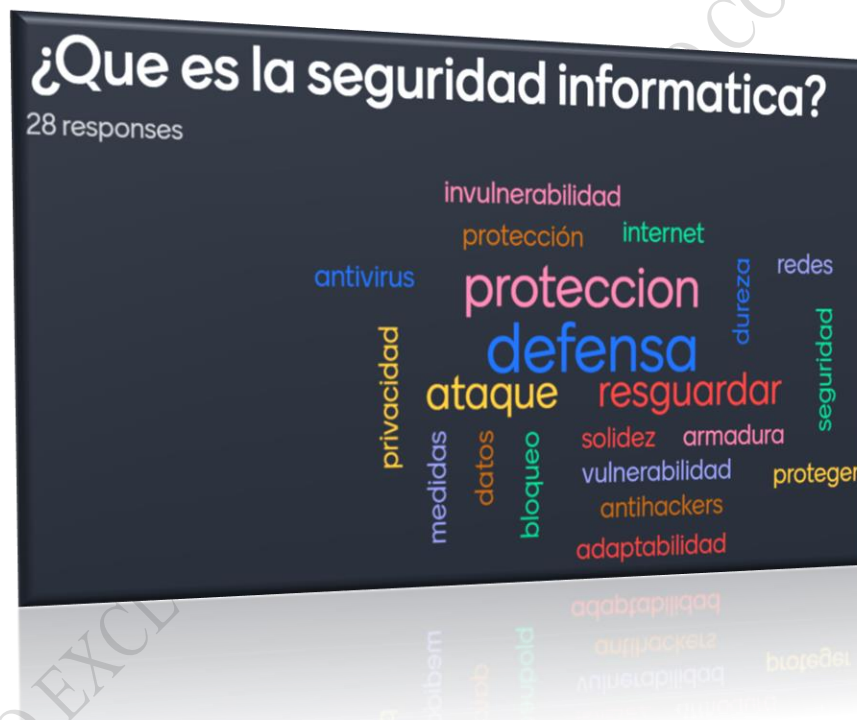


Universidad Paraguay Aleman



UNIVERSIDAD PARAGUAYO ALEMANA  
HEIDELBERG - ASUNCIÓN



Seguridad TICs

Prof.: Chrystian Ruiz Diaz

## Contenido

Nota de Uso Académico.....	3
Tarea: Uso de Nmap en Kali Linux .....	4
Objetivo:.....	4
Materiales Necesarios: .....	4
Arquitectura.....	4
Parte 1: Instalación y Configuración de Nmap .....	5
Parte 2: Escaneos Básicos .....	5
Parte 3: Escaneos Avanzados.....	5
Parte 4: Técnicas de Evasión y Bypass de Firewalls .....	6
Parte 5: Scripts NSE de Nmap .....	6
Parte 6: Documentación y Reportes .....	6
Evaluación y Entrega: .....	7
Conclusión: .....	7

### **Nota de Uso Académico**

Este documento ha sido preparado exclusivamente para el uso académico del docente. Este documento no puede ser distribuido a ninguna otra parte ni utilizado para ningún otro propósito, diferente al establecido como alcance en el proyecto académico de la **UNIVERSIDAD PARAGUAYO ALEMANA**. El uso indebido del material fuera del ámbito académico no representa ninguna responsabilidad del docente.

USO EXCLUSIVO EN LABORATORIO CONTROLADO

**Tarea: Uso de Nmap en Kali Linux****Objetivo:**

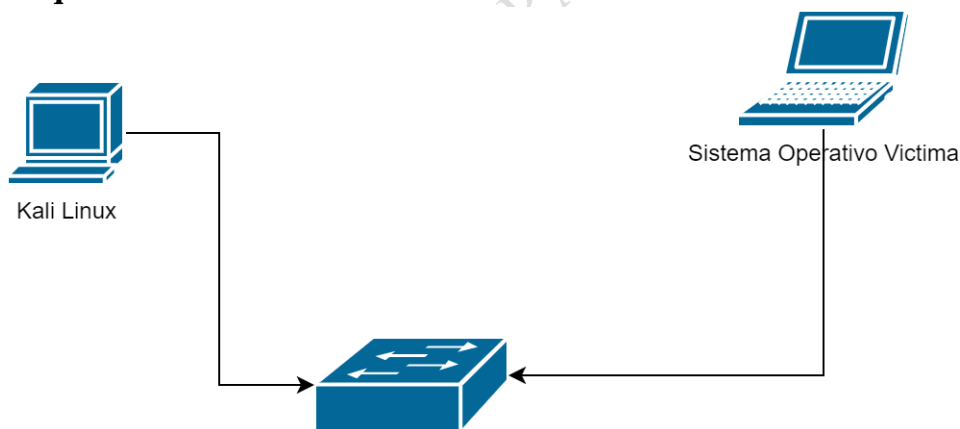
El objetivo de esta tarea es familiarizarse con el uso de Nmap, una herramienta poderosa de escaneo de redes y auditoría de seguridad, en Kali Linux. Al completar esta tarea, los estudiantes deberían ser capaces de realizar diferentes tipos de escaneos, interpretar los resultados y comprender cómo se pueden utilizar estas técnicas en evaluaciones de seguridad.

**Materiales Necesarios:**

- Una computadora con Kali Linux instalado.
- Conexión a internet para instalar paquetes adicionales si es necesario.
- Acceso a una red de pruebas (puede ser una red interna controlada para evitar problemas legales y éticos).



*Instrucciones:*

La funcionalidad de conectividad de red será explicada en clase

**Arquitectura****Requerimientos**

Descargar las VMs

<https://mega.nz/folder/I9UR0aLT#TpD0mySElIZWPbwtOwZ34A>

Name	
	WebServer.zip
	Windows7Ultimatex64.zip

El primero es un servidor web vulnerable y el segundo una VM Windows 7

## Parte 1: Instalación y Configuración de Nmap

### 1. Instalación de Nmap:

- Verifica si Nmap está instalado ejecutando `nmap -v` en la terminal.
- Si no está instalado, instala Nmap con el siguiente comando:

```
sudo apt-get update
sudo apt-get install nmap
```

### 2. Configuración de Permisos:

- Asegúrate de tener permisos de superusuario para ejecutar escaneos que requieran privilegios elevados, utilizando `sudo`.

## Parte 2: Escaneos Básicos

### 1. Escaneo de Hosts Activos en la Red:

- Utiliza Nmap para descubrir hosts activos en tu red. Ejecuta:

```
sudo nmap -sn <IP_VICTIMA>
sudo nmap -sn 192.168.1.0/24
```

- Documenta los hosts activos y sus direcciones IP.

### 2. Escaneo de Puertos Abiertos:

- Escanea un host específico para detectar puertos abiertos:

```
sudo nmap -sT 192.168.1.1
```

- Anota los puertos abiertos y los servicios que se ejecutan en ellos.

## Parte 3: Escaneos Avanzados

### 1. Escaneo de Puertos Específicos:

- Escanea un rango específico de puertos en un host:

```
sudo nmap -p 20-80 192.168.1.1
```

### 2. Detección del Sistema Operativo:

- Realiza un escaneo para identificar el sistema operativo del host:

```
sudo nmap -O 192.168.1.1
```

**3. Detección de Versiones de Servicios:**

- Escanea para determinar las versiones de los servicios que se ejecutan en los puertos abiertos:

```
sudo nmap -sV 192.168.1.1
```

**Parte 4: Técnicas de Evasión y Bypass de Firewalls****1. Fragmentación de Paquetes:**

- Utiliza la fragmentación de paquetes para evadir algunos tipos de firewalls:

```
sudo nmap -f 192.168.1.1
```

**2. Escaneo con Spoofing de Dirección IP:**

- Realiza un escaneo con una dirección IP falsificada:

```
sudo nmap -S 192.168.1.100 192.168.1.1
```

**Parte 5: Scripts NSE de Nmap****1. Uso de Scripts NSE para Análisis Avanzado:**

- Explora scripts NSE (Nmap Scripting Engine) para realizar auditorías de seguridad avanzadas:

```
sudo nmap --script vuln 192.168.1.1
```

- Documenta las vulnerabilidades descubiertas utilizando scripts NSE.

**Parte 6: Documentación y Reportes****1. Generación de Reportes:**

- Guarda los resultados del escaneo en un archivo para su análisis posterior:

```
sudo nmap -oN scan_results.txt 192.168.1.1
```

**2. Generación de Reportes en Formato XML:**

- Genera un reporte en formato XML para su integración con otras herramientas de análisis:

```
sudo nmap -oX scan_results.xml 192.168.1.1
```

**3. Análisis de Resultados:**

- Revisa y analiza los resultados obtenidos de los diferentes escaneos. Identifica posibles vulnerabilidades y áreas de mejora en la seguridad de la red.

**Evaluación y Entrega:****1. Informe Final:**

- Prepara un informe final que incluya:
  - Descripción de los escaneos realizados.
  - Resultados obtenidos en cada tipo de escaneo.
  - Interpretación de los resultados y posibles implicaciones de seguridad.
  - Recomendaciones para mejorar la seguridad basada en los hallazgos.

**2. Presentación:**

- Presenta tus hallazgos y recomendaciones en PDF destacando las técnicas utilizadas y los resultados más importantes.

**Conclusión:**

Esta tarea proporcionará una comprensión profunda del uso de Nmap para la auditoría de seguridad y la exploración de redes. Asegúrate de seguir todas las prácticas éticas y legales durante la realización de estos ejercicios.