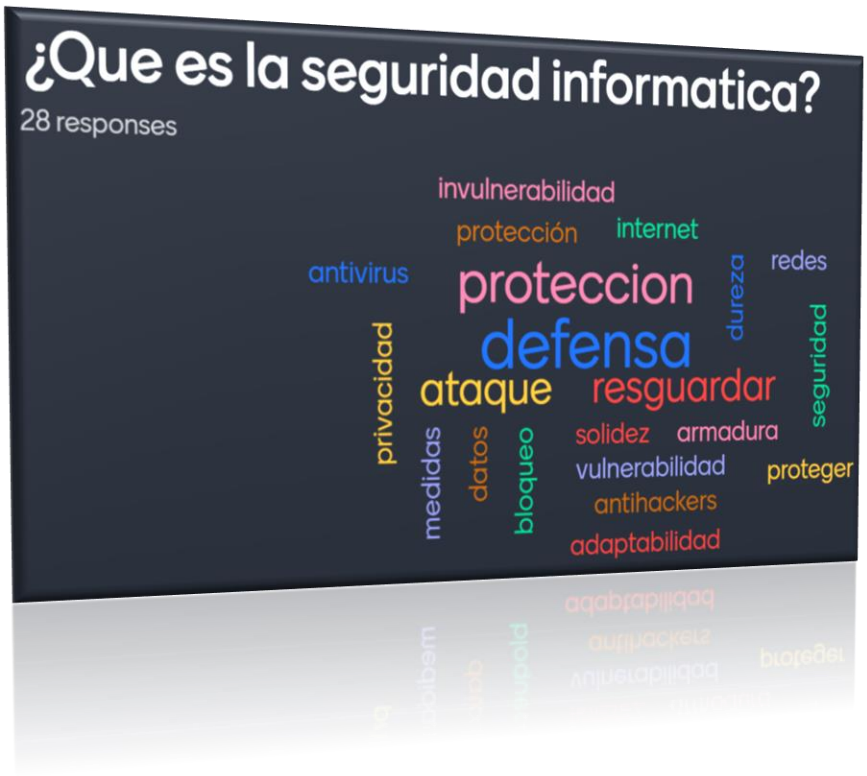
Universidad Paraguayo Alemana

UNIVERSIDAD PARAGUAYO ALEMANA
HEIDELBERG - ASUNCIÓN



Seguridad TICs

Prof.: Chrystian Ruiz Diaz

Contenido

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.

Guía para el Examen de Laboratorio: Análisis y Respuesta a Intentos de Intrusión

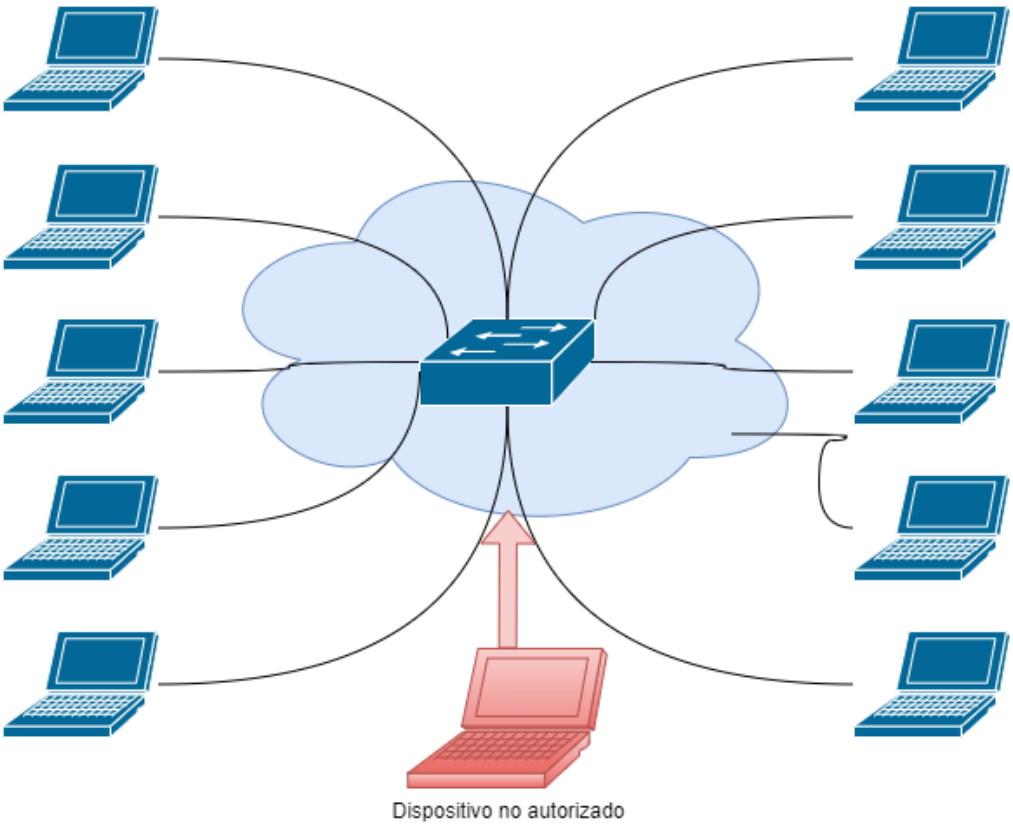
Objetivo

El objetivo de este examen es que cada alumno configure y utilice una máquina virtual (VM) Kali Linux en modo de red bridged, conectada a la red de la universidad, para analizar y responder a intentos de intrusión. Usaremos Apache como servidor web para recibir intentos de login por parte de un atacante.

Restricciones

- Cada alumno debe realizar este examen de manera individual y no puede tener contacto con otros compañeros durante el examen.
- La interpretación y análisis de los resultados forman parte integral de la evaluación.
- Se permite el uso de recursos de internet y materiales complementarios para apoyar en la realización del examen.

Arquitectura de red



Pasos a Seguir

1. **Configurar la Red de la VM**
   - Asegúrate de configurar la red de tu VM en modo bridged para que se conecte a la red de la universidad. Esto se puede hacer desde la configuración de red de tu software de virtualización (por ejemplo, VMware o VirtualBox).
   - Una vez configurada la red, verifica la conexión a la red universitaria.
2. **Obtener la Dirección IP**
   - En tu terminal de Kali Linux, ejecuta el comando `ifconfig` o `ip a` para obtener tu dirección IP.
   - Accede a la planilla de registro en Google Sheets y registra tu dirección IP en la columna correspondiente: Planilla de Registro.
3. **Instalar y Configurar Apache**
   - Apache es un servidor web que vamos a usar para recibir intentos de login por parte del atacante. Al configurarlo, podrás monitorear y analizar estos intentos de intrusión.
   - Instalar Apache:

     ```
     sudo apt install apache2
     ```

   - Iniciar el servicio Apache:

     ```
     sudo systemctl start apache2
     ```

   - Verificar el estado del servicio Apache:

     ```
     sudo systemctl status apache2
     ```

4. **Capturas de Pantalla**
   - Toma capturas de pantalla de cada paso importante, desde la configuración de la red hasta la obtención de la dirección IP y prueba de ICMP a la puerta de enlace.
5. **Documentación**
   - Documenta cada paso realizado, explicando qué hiciste y por qué lo hiciste. Incluye comandos utilizados y su propósito.
6. **Monitoreo del Tráfico de Red**
   - Utiliza herramientas de Kali Linux para monitorear el tráfico de red y detectar intentos de intrusión.
   - Analiza los logs y el tráfico capturado para identificar tipos de ataques, sus orígenes, los protocolos utilizados y los puertos afectados.
   - Asegúrate de documentar toda la información relevante, incluyendo:
     - Tipo de ataque
     - IP de origen
     - Protocolo

- Puerto lógico

7. **Configurar un Sistema de Detección de Intrusiones (IDS)**
   - Captura el tráfico y analiza las alertas generadas por el IDS.
   - Documenta y explica las alertas más relevantes encontradas.

Compilación de la Documentación

- Compila toda la documentación y las capturas de pantalla en un archivo PDF.
- Introducción: Breve descripción del objetivo del laboratorio.
- Metodología: Pasos seguidos durante el ejercicio, herramientas utilizadas, y configuración realizada.
- Resultados: Detalles de los intentos de intrusión detectados, incluyendo análisis detallado.
- Capturas de Pantalla del IDS y Wireshark: Incluye capturas de pantalla de las alertas generadas por el IDS y del análisis de tráfico con Wireshark. Explica cada captura y lo que muestra.

Evaluación

- Evaluación conforme a la rúbrica (examen teórico = 10%, examen práctico = 15%).

Entrega del Archivo PDF

- Sube el archivo PDF con toda la documentación y análisis a la plataforma designada por el instructor (Google Classroom).

Nota Final

El objetivo final de estos pasos es identificar el origen, protocolo, tipo de ataque y el mensaje detectado en el IDS, así como identificar las credenciales de intento de acceso con el sniffer.

