Nombres: Rivera Calderón, Elkin Jenner

Código: U19311223

Carrera: Ingeniería de Software

Curso: NETWORK SECURITY (100000S75F)

Práctica Calificada 02 – Seguridad en Redes

SECCIÓN I – CASO PRÁCTICO (12 puntos)

Caso: Seguridad en SecureNet S.A.

SecureNet S.A. es una empresa que tiene una red interna, acceso a internet, y servicios como servidor web, base de datos y correo. Últimamente han notado problemas como:

- Muchos intentos fallidos para entrar a los equipos.
- Escaneos de puertos desde fuera.
- Tráfico raro dentro de la red.

La empresa quiere mejorar su seguridad con estas acciones:

1. Usar un servidor AAA con TACACS+ para controlar el acceso a routers y switches.
2. Crear reglas de firewall para permitir y bloquear tráfico.
3. Instalar sistemas para detectar ataques.
4. Usar honeypots para analizar a los atacantes.

Responde estas 4 preguntas breves:

1. ¿Qué pasos seguirías para configurar un servidor AAA en un router Cisco con TACACS+? Menciona los comandos más importantes y para qué sirven.

```
enable
configure terminal
aaa new-model
aaa authentication login default group tacacs+ local
tacacs-server host 192.168.1.100 key ClaveSegura
line vty 0 4
 login authentication default
exit
```

2. Escribe 3 reglas básicas de firewall que hagan lo siguiente:

- Permitan navegar por internet desde la red interna (HTTP/HTTPS).
- Permitan conexión SSH solo desde una IP autorizada.
- Bloqueen todo lo demás.
  Explica por qué estas reglas ayudan a proteger la red.

```
access-list 100 permit tcp 192.168.0.0 0.0.0.255 any eq 80
access-list 100 permit tcp 192.168.0.0 0.0.0.255 any eq 443
access-list 100 permit tcp host 192.168.0.10 any eq 22
access-list 100 deny ip any any
```

Explicación:

- Las dos primeras reglas permiten que los usuarios naveguen por internet (HTTP y HTTPS).
- La tercera permite que solo una IP específica acceda vía SSH.
- La última regla bloquea todo tráfico no autorizado, aumentando la seguridad al aplicar el principio de **"deny all"** por defecto.

3. Explica dónde y para qué usarías un HIDPS y un NIDPS en esta empresa. ¿Qué tipo de ataques detecta cada uno?

HIDPS (Host-Based Intrusion Detection System):

- **Ubicación:** Directamente en servidores críticos (web, correo, base de datos).
- **Función:** Detectar alteraciones en archivos del sistema, accesos no autorizados y malware.
- **Ejemplo de ataque detectado:** Escalamiento de privilegios o instalación de rootkits.
- **NIDPS (Network-Based Intrusion Detection System):**

- **Ubicación:** Segmento de red central o zona DMZ, monitoreando tráfico de red.
- **Función:** Detectar escaneos de puertos, patrones sospechosos, ataques DoS o exploits.
- **Ejemplo de ataque detectado:** Escaneo desde el exterior, tráfico anómalo o intrusiones.

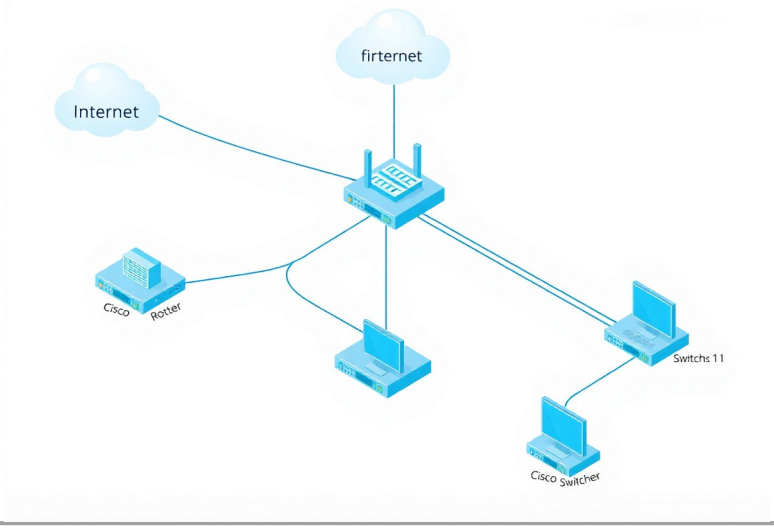
4. ¿Qué es un honeypot y cómo puede ayudar a la empresa? ¿Qué tipo usarías y cómo te asegurarías de que no ponga en peligro la red real?

Un honeypot es un sistema o recurso deliberadamente expuesto para simular vulnerabilidades y atraer a posibles atacantes. Puede ayudar a una empresa a estudiar tácticas y herramientas usadas por los atacantes sin poner en riesgo activos reales. También sirve para alertar sobre intentos de intrusión tempranamente.

Beneficios en Medidas de seguridad:

- Ubicar el honeypot en una red aislada (DMZ).
- Restringir todo acceso desde el honeypot hacia la red real mediante firewalls.
- Monitorear constantemente su actividad.

El diseño simulado en PacketTrace **(Opcional)**



SECCIÓN II – PREGUNTAS TEÓRICAS (12 puntos)

Pregunta 1: Tipos de firewall

Explica con tus propias palabras las diferencias entre estos 3 tipos de firewall:

- Firewall de filtrado de paquetes (packet-filtering)
- Firewall con inspección de estado (stateful inspection)
- Firewall tipo proxy (application-level gateway)

Para cada uno, escribe:

- Qué hace
- Una ventaja
- Una desventaja
- Un ejemplo donde se podría usar

---

1. Firewall de filtrado de paquetes (Packet-Filtering Firewall)

¿Qué hace?
Analiza encabezados de paquetes (IP, puerto, protocolo) y permite o bloquea según reglas predefinidas. No mantiene información de conexiones previas.

Ventaja	Desventaja
Rápido y consume pocos recursos.	No analiza el contenido del tráfico ni el contexto de la conexión (puede ser menos seguro).

Ejemplo de uso:
En routers básicos para bloquear o permitir puertos y direcciones IP (por ejemplo, bloquear el puerto 23 para evitar Telnet).

2. Firewall con inspección de estado (Stateful Inspection Firewall)

¿Qué hace?
Monitorea el estado de las conexiones (TCP/UDP) y permite solo paquetes relacionados con conexiones válidas. Guarda una tabla de estado.

Ventaja	Desventaja
Más seguro que el filtrado de paquetes; detecta paquetes no válidos o anómalos.	Mayor uso de recursos, especialmente en redes con mucho tráfico.

Ejemplo de uso:
En empresas medianas donde se quiere permitir solo respuestas a solicitudes salientes (ej. navegación web) y bloquear conexiones no iniciadas internamente.

3. Firewall tipo proxy (Application-Level Gateway)

¿Qué hace?
Actúa como intermediario entre el usuario y la aplicación final. Examina el contenido del tráfico a nivel de aplicación (HTTP, FTP, etc.).

Ventaja	Desventaja
Ofrece el mayor nivel de análisis y control por aplicación.	Más lento y complejo de configurar; puede afectar el rendimiento.

Ejemplo de uso:
En organizaciones que necesitan filtrar tráfico web, registrar actividad o aplicar políticas específicas por usuario (como escuelas o empresas con alto control).

Pregunta 2: Políticas de acceso

¿Qué es una política de control de acceso en un firewall?
Luego escribe una política que cumpla lo siguiente:

- Permitir acceso HTTP desde la red interna al servidor web (que está en la zona DMZ).
- Bloquear todo el tráfico ICMP (ping).
- Registrar (hacer log) cualquier intento de acceso no permitido.

Explica cómo esto ayuda a proteger la red.

Una política de control de acceso en un firewall es un conjunto de reglas que definen qué tipo de tráfico está permitido o bloqueado dentro de una red. Estas reglas se

basan en criterios como dirección IP, puerto, protocolo, zona de red, etc. Su objetivo es proteger los recursos internos, permitiendo solo el tráfico autorizado y bloqueando lo que no sea necesario o potencialmente peligroso.

🔐 Política solicitada (en lenguaje ACL genérico de firewall):

```
allow tcp from 192.168.1.0/24 to 10.0.0.10 port 80
deny icmp any any
deny any any log
```

Permitir acceso HTTP
Permite que cualquier equipo de la red interna (192.168.1.0/24) acceda al servidor web en la zona DMZ (10.0.0.10) por el puerto 80 (HTTP).

Bloquear ICMP (ping)
Elimina la posibilidad de que cualquier host haga ping a cualquier otro, lo que dificulta la detección de dispositivos activos para los atacantes.

Registrar accesos no permitidos
Cualquier intento de tráfico no autorizado se bloquea y registra, permitiendo a los administradores detectar y analizar comportamientos sospechosos.

¿Cómo protege esto a la red?

- Restringe el acceso solo a servicios necesarios, reduciendo la superficie de ataque.
- Bloquea protocolos innecesarios (como ICMP) que podrían ser usados para reconocimiento.
- Registra intentos fallidos o sospechosos, lo que permite generar alertas y tomar decisiones proactivas ante posibles amenazas.

Pregunta 3: HIDPS, NIDPS y honeypots

Explica con tus propias palabras qué son estos tres sistemas:

- HIDPS
- NIDPS
- Honeypots

Para cada uno indica:

- Dónde se coloca (en qué parte de la red)
- Qué tipo de ataques detecta mejor
- Si actúa de forma pasiva (solo mira) o activa (responde)
- En qué situación lo usarías

Al final, explica por qué es buena idea usar los tres juntos para proteger una red.

1. HIDPS (Host-Based Intrusion Detection System)

¿Qué es?
Es un sistema que se instala en un dispositivo específico (como un servidor o PC) para monitorear su comportamiento interno.

Dónde se coloca:
En servidores o estaciones críticas (ej. servidor web, base de datos).

Detecta mejor:

- Accesos no autorizados
- Cambios en archivos del sistema
- Escalamiento de privilegios
- Instalación de malware local

Tipo de acción:
Mayormente pasiva, pero puede actuar (por ejemplo, desconectar procesos).

Usos recomendados:
En servidores de producción que manejan datos sensibles o donde es clave controlar qué ocurre dentro del sistema.

---

2. NIDPS (Network-Based Intrusion Detection System)

¿Qué es?
Monitorea el tráfico que circula por la red, analizando patrones para detectar ataques o comportamientos sospechosos.

Dónde se coloca:
En puntos clave de la red, como:

- Entre el router/firewall y la red interna
- En la DMZ (zona de servidores públicos)

Detecta mejor:

- Escaneos de puertos
- Ataques de red como DoS
- Tráfico malicioso entre equipos
- Intentos de intrusión desde fuera

Tipo de acción:
Pasiva (solo detecta), aunque algunos sistemas pueden alertar o bloquear (IDS vs IPS).

Usos recomendados:
Para monitoreo general del tráfico de red en tiempo real, sin afectar el rendimiento de dispositivos.

---

3. Honeypot

¿Qué es?
Es un sistema falso o vulnerable a propósito que simula un objetivo real para atraer a atacantes y estudiar su comportamiento.

Dónde se coloca:
En una zona aislada (como la DMZ), lejos de los sistemas reales.

Detecta mejor:

- Técnicas de ataque reales usadas por intrusos
- Reconocimiento de red
- Herramientas y exploits comunes

Tipo de acción:
Pasiva, pero diseñada para interactuar con los atacantes sin poner en riesgo el resto de la red.

Usos recomendados:
En laboratorios de seguridad o redes empresariales para detectar y analizar amenazas desconocidas.

Por otro lado, utilizar **HIDPS, NIDPS y honeypots** combinados mejora significativamente la seguridad porque:

- Se cubren diferentes niveles (host, red y engaño).
- Se detectan más tipos de ataques, desde internos hasta externos.
- Se puede reaccionar con mayor precisión según el tipo de amenaza.
- El honeypot puede desviar al atacante, mientras los IDS detectan y alertan.