Trabajo Práctico Final: Reingeniería de Infraestructura y Seguridad Perimetral

1. Escenario y Contexto

La organización (puede ser una Pyme o un Departamento de Facultad) ha crecido desordenadamente. Pasó de 15 a 200 empleados. Cuenta con diferentes servicios (dos web al público y una web interna administrativa). Actualmente su arquitectura no está segmentada, los servicios están expuestos sin controles claros, y el acceso externo no está adecuadamente protegido. Recientemente sufrieron un incidente de seguridad donde un servidor web comprometido afectó los sistemas de administración.

Usted ha sido designado como el Arquitecto de Infraestructura para rediseñar la red desde cero. Su tarea será **diseñar, documentar y justificar una nueva infraestructura de red**, basada en los conceptos y prácticas abordados en la materia.

El objetivo es que puedan proponer un diseño moderno, seguro y funcional, que permita a la organización operar correctamente y publicar servicios hacia Internet sin comprometer su seguridad.

La reingeniería debe contemplar no solo el funcionamiento, sino también la mitigación del riesgo. Se espera que el estudiante argumente cómo su diseño reduce la superficie de ataque y mejora la disponibilidad de los servicios críticos.

2. Objetivos Técnicos

El estudiante deberá implementar una solución que demuestre dominio sobre:

- **Virtualización:** Uso de Proxmox para gestión de recursos (VMs y CTs).
- **Segmentación de Red:** Implementación de zonas de seguridad (mínimo WAN, LAN, DMZ).
- **Routing y Firewall:** Configuración de pfSense como gateway perimetral.
- **Publicación de Servicios:** NAT y Port Forwarding.

3. Requerimientos de Infraestructura (La Implementación)

1. Definir el escenario y necesidades de la organización.
2. Diseñar una **topología de red**.
3. Implementar una arquitectura virtualizada en **Proxmox**, con las VMs y/o contenedores necesarios.
4. Configurar un firewall **pfSense** con reglas justificadas.
5. Publicar servicios hacia Internet mediante **Port Forwarding** seguro y DMZ ruteada.
6. Documentar buenas prácticas de seguridad aplicadas.

7. Presentar evidencias de funcionamiento, pruebas y capturas.

4. Políticas de Seguridad y Conectividad (Las Reglas)

1. Acceso a Internet para Empleados:

- Debe tener acceso irrestricto a Internet (Navegación, ping, descargas).
- La IP de la Estación de Trabajo debe ser asignada automáticamente por un servidor **DHCP**.

2. Publicación de Servicios (Port Forwarding y ruteo):

- Desde internet, cualquier usuario debe poder ver la página web del servidor (Puerto 80).

3. Aislamiento de la DMZ (Regla de Oro):

- Si el Servidor Web es hackeado, el atacante **NO debe poder iniciar conexiones hacia las Estaciones de Trabajo**.
- Se debe bloquear explícitamente el tráfico con destino en las Estaciones de Trabajo.
- Los servicios sí pueden tener salida a Internet (para actualizaciones del sistema).

5. Entregables

El alumno deberá presentar: Documento en PDF, sugerido 8 a 12 páginas, diagrama obligatorio, captura de pantallas.

1. **Documento con:**
    - Nombre de la organización, integrante, fecha, nombre de la materia
    - Definición del escenario y necesidades de la organización, problemas y riesgos existentes
    - Tipo de servicios y puertos
    - Descripción de la virtualización en Proxmox: VMs, contenedores, Bridge y mapeo
      Sugerencia: Cada uno podrá utilizar los bridges preexistentes en Proxmox (vmbr0, vmbr1, etc.) o crear otros si lo considera necesario, explicando su elección.
    - **Diagrama de Topología:** Un esquema gráfico indicando las zonas, subredes, direcciones IP, máscaras, gateways, IP de los servidores/clientes, y las interfaces del pfSense, rangos dhcp, flujo de tráfico entre zonas.
      Nota: Se recomienda utilizar rango de direcciones similares a la que utilizamos en la práctica

    - **Tabla de Reglas de Firewall:** Un reporte breve explicando las reglas de firewall creadas y su orden de prioridad por cada zona, descripción de amenazas posibles (al menos 3).
    - Análisis breve de amenazas y cómo las reglas y segmentación propuestas las mitigan.
    - Descripción de buenas prácticas de seguridad aplicadas.Porque se segmenta así, Porque se eligió VM o contenedor en cada caso.
    - Conclusión: qué aprendieron, qué hubieran agregado, reflexión final
2. **Demostración en Vivo:**
    - Mostrar la arquitectura y configuración de interfaces en Proxmox, VMs y contenedores.
    - Configurar un firewall **pfSense** con reglas justificadas.
    - Publicar un servicio hacia Internet mediante **Port Forwarding** seguro.
    - Publicar un servicio hacia Internet mediante **ruteo** seguro.
    - Desde la PC: Navegar por internet y hacer ping a Google.
    - Desde la PC: Acceder al sitio web, Proxmox y PfSense
    - Desde una PC externa: Acceder al sitio web.
    - Pruebas mediante ping, traceroute y ssh

6. Criterio de evaluación

El trabajo se evaluará por calidad del diseño, claridad de la documentación, funcionamiento de la demo y correcta aplicación de conceptos de seguridad.