UNIVERSIDAD TECNOLÓGICA DE CHILE
INSTITUTO PROFESIONAL
CENTRO DE FORMACIÓN TÉCNICA

Evaluación Sumativa #4: (25%)
Ejecución del proceso de despliegue, integración de servicios, hardenización de dispositivos dentro entornos de sistemas operativos Linux.

ÁREA ACADÉMICA	Tecnologías de Información y Ciberseguridad	**CARRERA**	Ingeniería en informática / Analista Programador / Ingeniería en Ciberseguridad
ASIGNATURA	***Sistemas Operativos***		
SEDE	La Serena	**DOCENTE**	***Alex Díaz Araos***
DURACIÓN	1 semana	**FECHA**	15-07-2025
A. Esperado:	3.1.5. Utiliza gestores de paquetes en la actualización e instalación de productos en base a los requerimientos comunes del mercado.		

NOMBRE ESTUDIANTE:	Apellido Paterno Apellido Materno Nombres
RUT:	☐☐☐☐☐☐☐☐ ☐
NOMBRE ESTUDIANTE:	Apellido Paterno Apellido Materno Nombres
RUT:	☐☐☐☐☐☐☐☐ ☐
NOMBRE ESTUDIANTE:	Apellido Paterno Apellido Materno Nombres
RUT:	☐☐☐☐☐☐☐☐ ☐

PUNTAJE MÁXIMO	7.0		**NOTA:**	Firma conforme
PUNTAJE OBTENIDO				
Solicita re-corrección	**Sí**	**No**	**Motivo:**	

I. Contexto:

Una empresa de cualquier rubro (restaurant, hotel, casino, colegio, aeropuerto, clínica u otro) ha solicitado la instalación de un sistema de acceso a Internet controlado mediante portal cautivo y firewall para gestionar la seguridad y el acceso de sus clientes o usuarios internos.

El objetivo es ofrecer conexión controlada, con restricción de acceso a ciertos sitios web y servicios no permitidos, garantizando una experiencia segura y alineada a las políticas de uso de la red.

II. Requerimientos:

El trabajo se realizará en equipos de no más de 3 integrantes, por tanto, cada equipo deberá:

1. Implementar dos máquinas virtuales:
   - Cliente Windows (Windows 10 o Windows 11).
   - Firewall/Router con FreeBSD pfSense o Untangle.

2. Configurar la red virtual:
   - Conectar ambas máquinas en red virtual simulando un entorno real.

3. Configurar el portal cautivo:
   - Personalizar una página de login acorde al contexto del cliente simulado.
   - Debe incluir: logo, nombre del negocio, mensaje de bienvenida y campos de login.

4. Validar el acceso:
   - Configurar usuarios válidos para autenticarse.
   - Comprobar redireccionamiento a una página de inicio o sitio por defecto tras login.

5. Configurar reglas de firewall:
   - Bloquear mínimo 3 sitios web (dominios) mediante reglas de filtrado.
   - Bloquear al menos un servicio o aplicación mediante filtrado por puerto (por ejemplo, bloquear FTP, SSH o cualquier otro según contexto).

6. Evidenciar funcionamiento:
   - Presentar evidencias (capturas de pantalla) del portal cautivo en uso, autenticación exitosa y bloqueo efectivo de los sitios y puerto.

7. Entregar documentación técnica:
   - Describir configuración de red, reglas de firewall, parámetros del portal cautivo y pasos para replicar la instalación.

III. Producto esperado:

1. 2 máquinas virtuales funcionales.
2. Página de login personalizada.
3. Documento técnico en PDF (máximo 5 páginas).
4. Evidencias de pruebas en video o imágenes.

IV. Lista de Cotejo:

Criterio	Puntaje Máximo	Puntaje Logrado	Observaciones
1. Se entregaron dos máquinas virtuales funcionales.	1,0		
2. La red virtual permite la comunicación cliente-firewall.	0,5		
3. El portal cautivo presenta página de login personalizada con identidad del cliente simulado.	1,0		
4. El portal cautivo valida credenciales y redirige correctamente al sitio por defecto.	1,0		
5. Se evidencia bloqueo de al menos 3 sitios web no permitidos.	1,0		
6. Se evidencia bloqueo de al menos un servicio o puerto específico.	1,0		
7. Se entrega documentación clara con pasos de configuración de red, portal cautivo y firewall.	0,5		
8. Se adjuntan capturas comprobando funcionamiento y pruebas.	0,5		
9. El trabajo muestra coherencia entre cliente simulado, políticas de acceso y restricciones aplicadas.	0,3		
10. Presentación organizada y entregada dentro del plazo.	0,2		