



Carrera: Ingeniería de Software

Curso: NETWORK SECURITY (100000S75F)

Práctica Calificada – Seguridad en Redes

Parte I: Preguntas Teóricas (8 puntos)

Instrucciones: Responde con claridad. Cada pregunta vale 2 puntos.

1. (2 pts) Menciona y explica brevemente los tres principios fundamentales de la seguridad en redes.
2. (2 pts) ¿Cuál es la diferencia entre un virus, un gusano (worm) y un troyano? Da un ejemplo de cada uno.
3. (2 pts) ¿Qué es una botnet y cómo representa una amenaza para la seguridad de una red?
4. (2 pts) ¿Qué es el modelo AAA y para qué sirve en la seguridad de redes?

Parte II: Caso Práctico – Configuración de servidor AAA (12 puntos)

Tema: Implementación de un servidor AAA usando RADIUS para autenticar acceso a un router.

[pc1_ElkinRivera.pkt](#)

Objetivo:

- Configurar un entorno de red simple donde el acceso a un router esté controlado mediante autenticación centralizada a través de un servidor AAA.

Requisitos:

- Un router.
- Un switch.
- Tres PCs: PC1 (usuario autorizado), PC2 (usuario no autorizado), PC3 (uso administrativo).
- Un servidor AAA (RADIUS).
- Acceso Telnet habilitado y protegido por autenticación AAA.

Tareas a realizar:

5. Diseña la red en Packet Tracer.
6. Configura el servidor AAA con los siguientes usuarios:
 - admin1 / cisco123 (acceso autorizado).
 - user2 / test456 (acceso denegado).
7. Configura el router como cliente AAA, autenticando por RADIUS.
8. Habilito acceso por consola y Telnet con autenticación AAA.
9. Verifica:
 - El acceso correcto de admin1.
 - El rechazo de user2.
10. Adjunta:
 - Capturas de la configuración.
 - Resultados de pruebas de acceso.
 - Breve resumen explicativo (máx. 150 palabras).

Puntaje del caso práctico (12 puntos):

Criterio	Puntaje
Diseño correcto de red	2 pts
Configuración del servidor AAA	2 pts
Configuración AAA en router	3 pts
Pruebas de acceso correctas	3 pts
Capturas y resumen explicativo	2 pts