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.**

   Los tres principios de seguridad en redes son:
   Confidencialidad, Integridad y Disponibilidad (CID)

Confidencialidad	Integridad	Disponibilidad
Se refiere en proteger la información contra accesos no autorizados.	Es garantizar que los datos no sean alterados de manera indebida.	Asegura que los recursos estén accesibles para los usuarios autorizados.

2. **(2 pts) ¿Cuál es la diferencia entre un virus, un gusano (worm) y un troyano? Da un ejemplo de cada uno.**

Características	Virus	Gusano(worm)	Troyano
	Es un software malicioso que se propaga en computadoras y dispositivos.	Tipo de software malicioso que se propaga de forma autónoma a través de redes de computadoras	Tipo de malware que se esconde dentro de software aparentemente legítimo para engañar al usuario y que lo ejecute.
Diferencias			
Mecanismo de Propagación	Se activa y réplica al ejecutarse el archivo infectado.	Se autopropaga a través de redes, explotando vulnerabilidades.	Depende de la ejecución o instalación por parte del usuario.
Autonomía	Dependiente de la acción del usuario para su ejecución inicial.	Autónomo en su replicación y propagación.	No autónomo en su propagación.

Objetivo Principal	Variado: daño, robo de información, control del sistema.	Propagación masiva, consumo de recursos, posible puerta trasera.	Acceso no autorizado, robo de información, ejecución de acciones maliciosas.

3. **(2 pts) ¿Qué es una botnet y cómo representa una amenaza para la seguridad de una red?**

   Es una red de dispositivos infectados con malware que están bajo el control de un atacante, conocido como **botmaster**. Estos dispositivos, llamados **bots** o **zombies**, pueden ser computadoras, teléfonos inteligentes, cámaras de seguridad y otros dispositivos conectados a Internet. pueden ser utilizados para realizar ataques coordinados sin el conocimiento de sus dueños, esta red de bots representa una amenaza significativa para la seguridad de una red, ya que puede utilizarse para lanzar ataques DDoS que interrumpen servicios, distribuir malware, enviar spam, robar datos sensibles y realizar otras actividades maliciosas de forma coordinada y a gran escala.

4. (2 pts) ¿Qué es el modelo AAA y para qué sirve en la seguridad de redes?

   El modelo **AAA** por sus siglas (Autenticación, Autorización y Auditoría) es un marco esencial en la seguridad de redes. La **autenticación** verifica la identidad de usuarios o dispositivos, la **autorización** define sus permisos de acceso a los recursos, y la **auditoría** registra sus acciones. En conjunto, el modelo AAA sirve para controlar el acceso a la red, aplicar políticas de seguridad y mantener un registro de actividad, previniendo el acceso no autorizado y fortaleciendo la seguridad general al determinar quién accede, qué puede hacer y qué se hizo.

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

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

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:

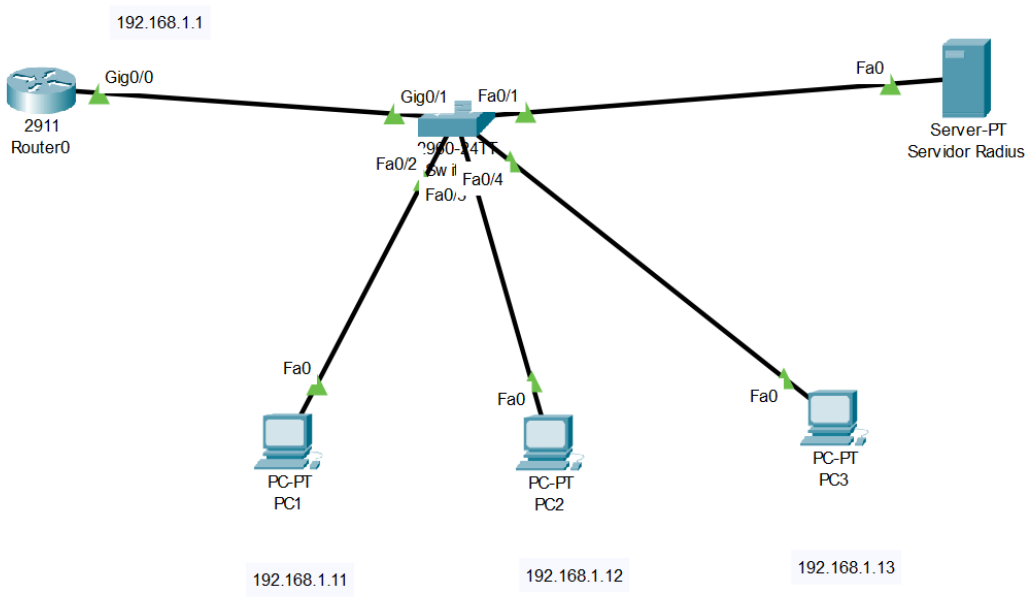
5. Diseña la red en Packet Tracer.
6. Configura el servidor AAA con los siguientes usuarios:
   - admin1 / cisco123 (acceso autorizado).
   - user2 / test456 (acceso denegado).
7. Configura el router como cliente AAA, autenticando por RADIUS.
8. Habilito acceso por consola y Telnet con autenticación 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):

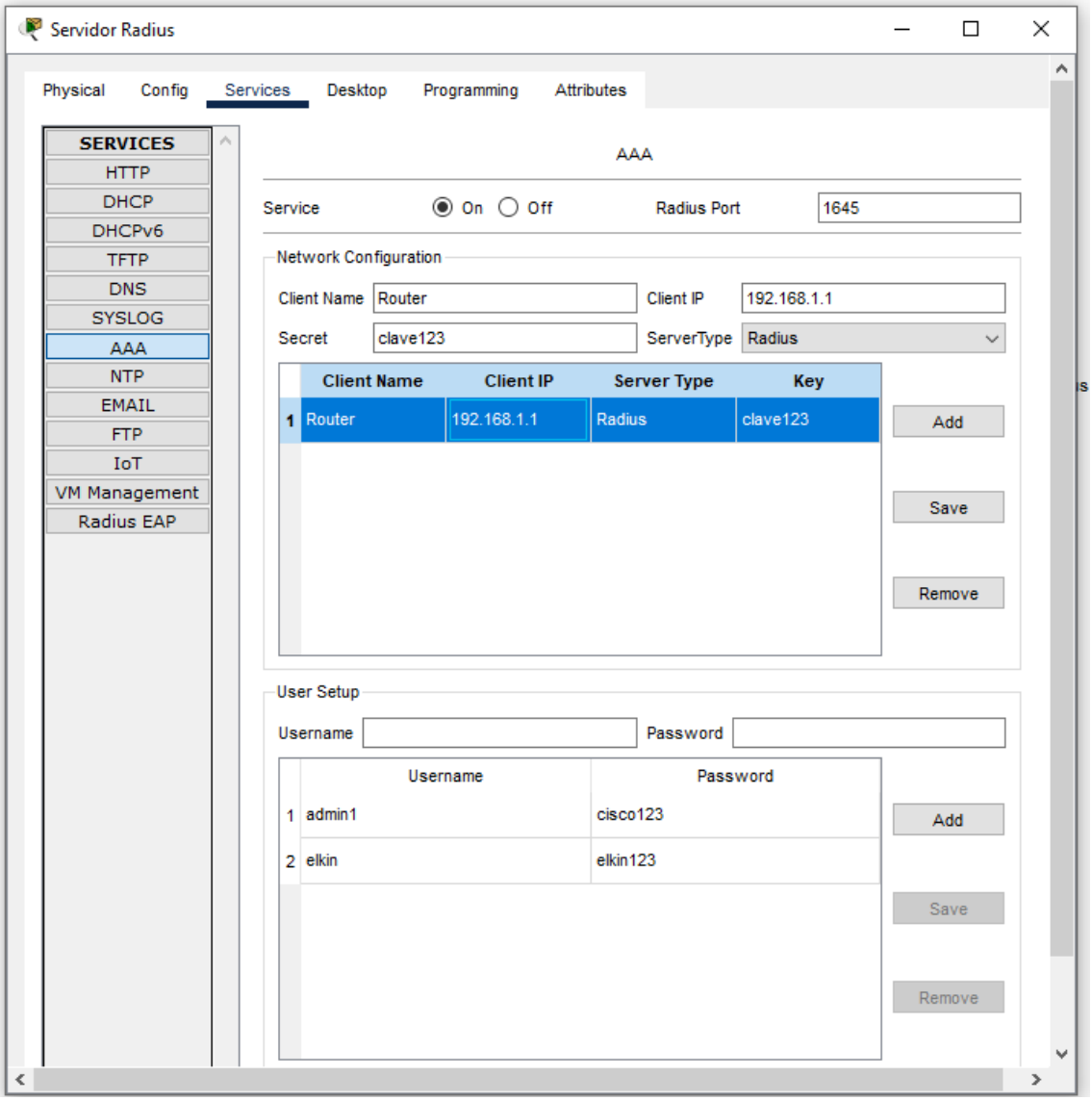
Criterio	Puntaje
Diseño correcto de red	2 pts
Configuración del servidor AAA	2 pts
Configuración AAA en router	3 pts
Pruebas de acceso correctas	3 pts
Capturas y resumen explicativo	2 pts

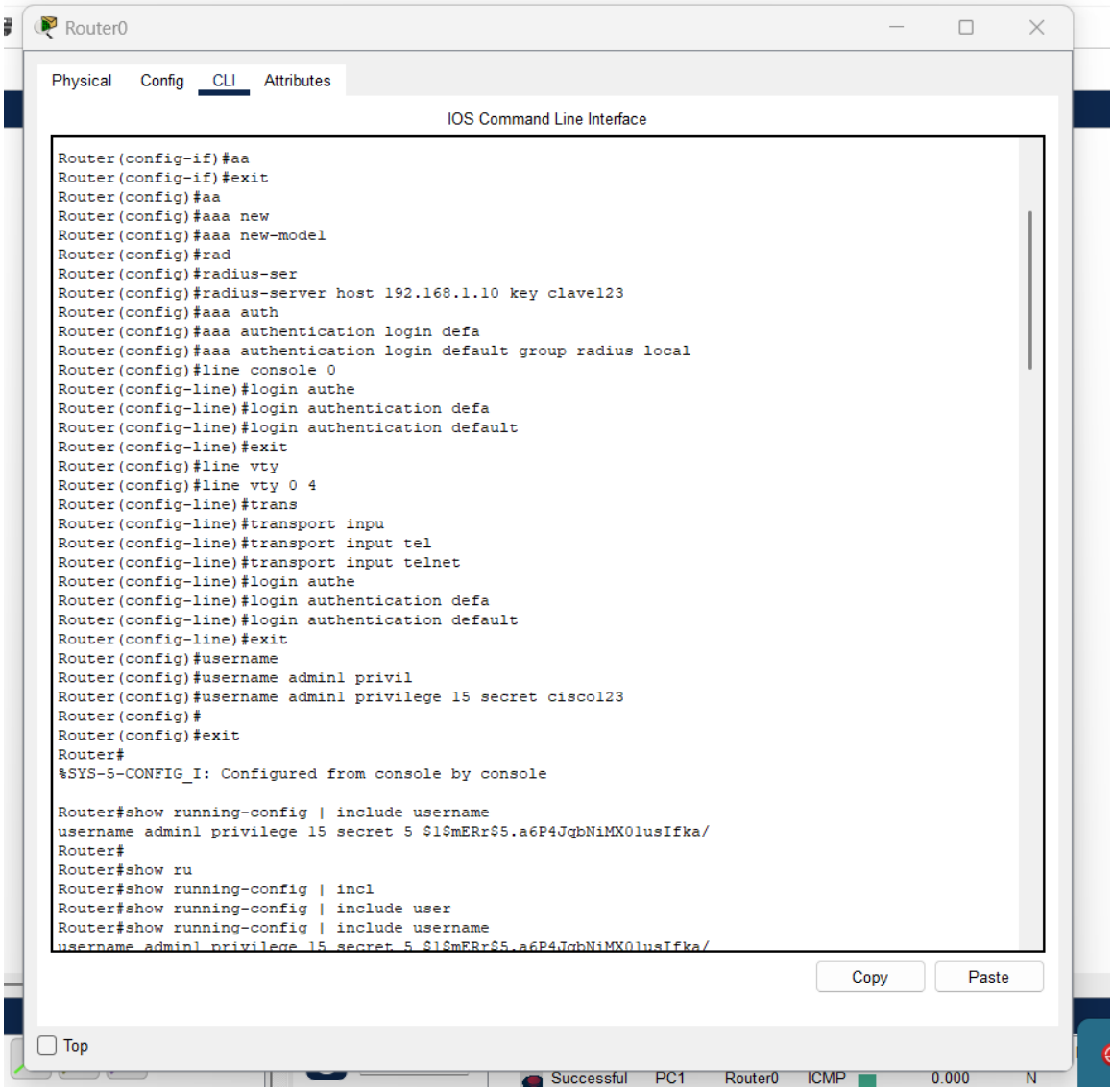
CAPTURAS:

1.Topologia

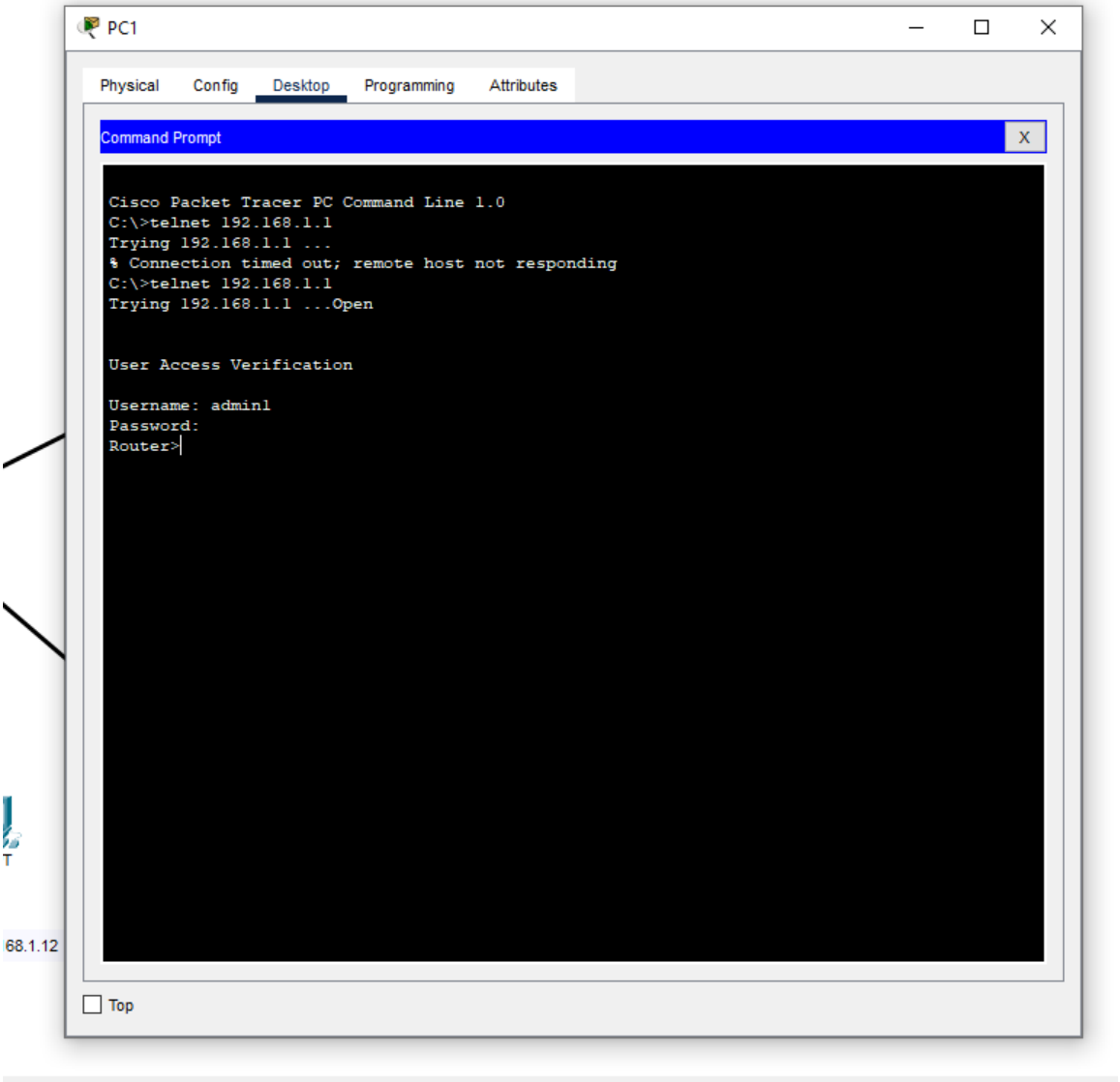


2.Configuración


Servidor Radius
Physical
Config
Services
Desktop
Programming
Attributes
SERVICES
HTTP
DHCP
DHCPv6
TFTP
DNS
SYSLOG
AAA
NTP
EMAIL
FTP
IoT
VM Management
Radius EAP
AAA
Service
On
Off
Radius Port
1645
Network Configuration
Client Name
Router
Client IP
192.168.1.1
Secret
clave123
ServerType
Radius
Client Name
Client IP
Server Type
Key
1
Router
192.168.1.1
Radius
clave123
Add
Save
Remove
User Setup
Username
Password
Username
Password
1
admin1
cisco123
2
elkin
elkin123
Add
Save
Remove



3. Resultados de pruebas de acceso



4. Breve resumen explicativo (máx. 150 palabras).

Respecto a la Implementación de un servidor AAA con RADIUS para la autenticación de acceso a un router, se buscó emular en Packet Tracer la autenticación a través del modelo AAA RADIUS. Este esquema permite el acceso a los equipos configurados en el servidor por medio de los usuarios incorporados en su conjunto. Esto representa una estrategia de seguridad para limitar y otorgar la entrada a los elementos de la red. Asimismo, la ejecución del ejercicio reveló una restricción de Packet Tracer como simulador: si bien la configuración RADIUS en el router posibilita la autorización de usuarios inscritos, la negación de acceso a usuarios particulares solo es viable removiéndolos del grupo de usuarios.

EL ejercicio PKT lo estoy adjuntado desde un archivo RAR