RETO FINAL

CIBERSEGURIDAD NIVEL EXPLORADOR

2025

Reto Práctico Final: "Fortaleciendo la Red de Empresa XYZ en 6 Horas"

Escenario

La Empresa XYZ es una compañía pequeña que ha detectado problemas de seguridad en su red interna. La red actual es plana, sin segmentación, y carece de controles básicos de seguridad, lo que la hace vulnerable a ataques y accesos no autorizados. Se te ha asignado el rol de consultor de ciberseguridad para evaluar, rediseñar y aplicar medidas de protección en un entorno simulado (por ejemplo, utilizando Cisco Packet Tracer, GNS3 o una herramienta similar).

Objetivos del Reto:

Los participantes deberán demostrar lo siguiente:

Conceptos Fundamentales y Modelos de Seguridad:Identificar y explicar la relevancia de la tríada CIA (Confidencialidad, Integridad y Disponibilidad) y otros modelos básicos de seguridad en la red.

Higiene Digital: Proponer y aplicar acciones de higiene digital (por ejemplo, gestión de contraseñas, actualizaciones, segmentación y respaldos) que protejan la información.

Análisis de Vulnerabilidades, Amenazas y Riesgos: Detectar y documentar al menos tres vulnerabilidades o riesgos presentes en la red actual.

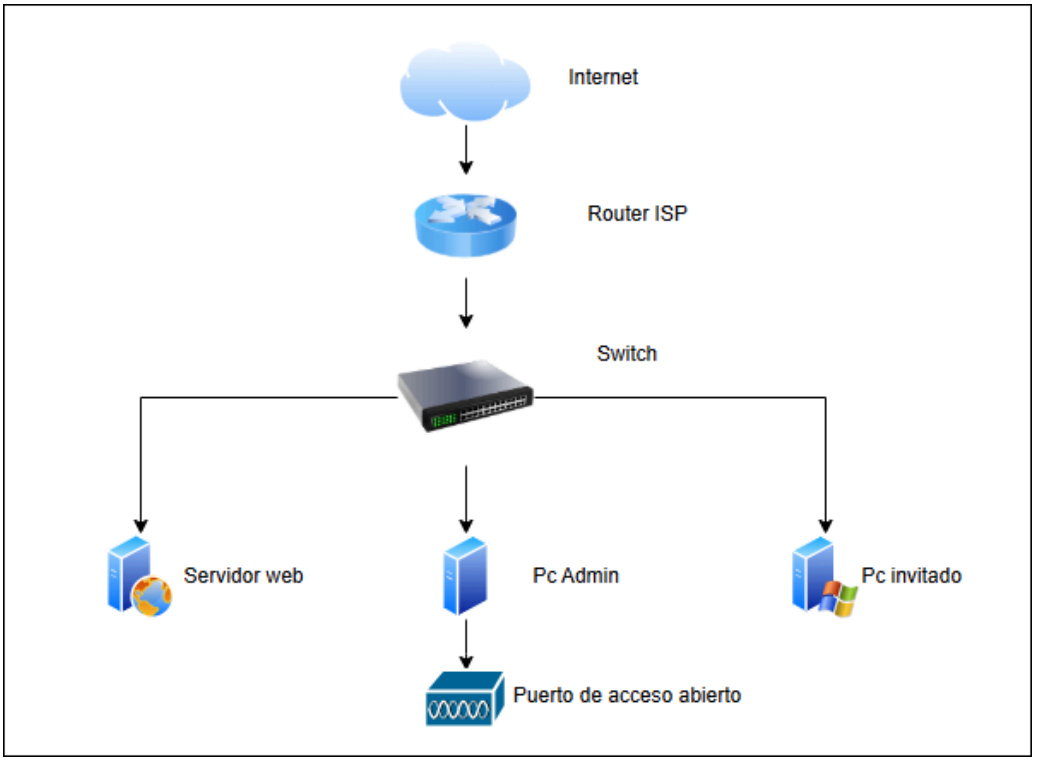
Medios de Transmisión y Autenticación: Reconocer y configurar mecanismos de autenticación y protocolos seguros para la transmisión de datos (por ejemplo, configuración de WPA2 en redes inalámbricas o autenticación en puertos).

Configuración de Redes LAN y VLAN: Diseñar y configurar una red LAN segmentada en al menos dos VLAN (por ejemplo, una para el área administrativa y otra para invitados) y definir reglas de acceso.

Política de Seguridad de la Información: Elaborar un documento breve que contenga las políticas, normas y procedimientos básicos para la protección de los recursos informáticos de la empresa.

Estructura y Cronograma:

Análisis y Evaluación de la Red Actual (1 Hora):



Tarea: Revisa el diagrama de red proporcionado y utiliza herramientas (simuladas o teóricas) para identificar vulnerabilidades, amenazas y riesgos.

Resultados:

- Un breve informe (1-2 páginas) que detalle al menos tres vulnerabilidades detectadas, explicando su impacto y riesgo potencial.

Rediseño y Configuración de la Red (2.5 Horas):

- Rediseña la topología de la red para implementar segmentación mediante VLAN (por ejemplo, separar la red en dos: administrativa y de invitados).
- Configura en el entorno simulado (Cisco Packet Tracer, GNS3, etc.) los dispositivos de red (switches y routers) para soportar las VLAN.
- Implementa mecanismos básicos de autenticación (por ejemplo, configuración de WPA2 en un punto de acceso o autenticación de puertos).
  Resultados:
  - Capturas de pantalla de la configuración de dispositivos.
  - Un diagrama actualizado de la red que muestre las VLAN y la segmentación aplicada.
  - Breve explicación de las configuraciones realizadas y los motivos de las decisiones tomadas.

Implementación de Medidas de Higiene Digital (1 Hora):

Tarea: Define y aplica (simulada o documentadamente) acciones de higiene digital, como políticas de contraseñas seguras, actualización de firmware/software y buenas prácticas de acceso.
Resultados:

- Un documento corto (1 página) que liste las medidas de higiene digital implementadas y cómo cada una contribuye a la seguridad de la red.

Desarrollo de una Política de Seguridad de la Información (1 Hora):

Tarea: Redacta una política de seguridad de la información básica para la Empresa XYZ, que incluya normas de uso de recursos, gestión de incidentes y responsabilidades del personal.
Resultados:

- Un documento (1-2 páginas) con la política de seguridad, argumentando brevemente cómo ayuda a mitigar los riesgos identificados.

Presentación y Justificación Final (30 Minutos):

Tarea: Prepara una presentación breve (puede ser en PowerPoint o similar) donde resumas el análisis, las configuraciones aplicadas y las políticas implementadas.
Justifica tus decisiones vinculándolas con los conceptos teóricos aprendidos.
Resultados:

- La presentación final y, si es posible, una grabación o exposición en vivo (según la dinámica del bootcamp).

Consideraciones Finales:

- El reto debe completarse en un máximo de 6 horas.
- Se evaluará tanto la correcta aplicación de los conceptos teóricos como la habilidad práctica para configurar y proteger una red.
- Este reto integrador está diseñado para que los campistas demuestren de manera práctica y efectiva el manejo de los criterios esenciales del bootcamp de ciberseguridad. ¡Buena suerte!