**DATOS DEL ESTUDIANTE**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Apellidos y Nombres: | Evelyn Andrea Serquen Montero | ID: | 001521714 | |
| Dirección Zonal/CFP: | Lambayeque – Chiclayo - Senati | | | |
| Carrera: | Ing. Ciberseguridad | Semestre: | | IV |
| Curso/ Mód. Formativo: | CCNA CYBER OPS (CISCO) | | | |
| Tema de Trabajo Final: | Análisis de seguridad informática de la red de datos de una empresa. | | | |

1. **INFORMACIÓN**

* **Identifica la problemática del caso práctico propuesto.**

ESystems SAC, una empresa consolidada en servicios tecnológicos enfrenta un aumento en su exposición a ciberamenazas debido a su crecimiento y mayor dependencia del entorno digital. Recientemente, ha sufrido incidentes de seguridad que comprometieron la integridad de los datos en su datacenter y afectaron la disponibilidad de los servicios que ofrece, generando preocupación entre sus clientes y dañando su reputación.

Estos incidentes revelan vulnerabilidades en su infraestructura tecnológica, que incluye servidores con sistemas operativos Windows y Linux, una red de conmutación y conectividad a Internet de alta velocidad. Esta infraestructura, si no es adecuadamente protegida, representa un posible vector de ataque.

* **Identifica propuesta de solución y evidencias.**

**1. Evaluación de Seguridad de Infraestructura** Se propone realizar un escaneo completo de vulnerabilidades en la infraestructura de ESystems SAC, incluyendo:

* Servidores con sistemas operativos Windows y Linux
* Equipos de red (switches, routers)
* Servicios en la nube

**Evidencias:** Reportes generados por herramientas como Nessus, OpenVAS o Nmap, donde se identifiquen vulnerabilidades clasificadas por nivel de criticidad.

**2. Segmentación de Red y Control de Acceso** Se recomienda segmentar la red interna mediante VLANs por áreas funcionales como usuarios, servidores, administración y aplicar listas de control de acceso (ACL).

**Evidencias:** Diagramas de red actualizados, configuración de switches y routers con reglas de acceso.

**3. Implementación de Políticas de Seguridad y Firewall** Implementación de firewalls de nueva generación (NGFW) que incluyan IDS/IPS, reglas de acceso por usuario, perfil de aplicación y análisis de comportamiento.

**Evidencias:** Políticas de seguridad documentadas, registros del firewall y capturas de configuración.

**4. Plan de Respuesta ante Incidentes (IRP)** Diseño de un plan formal de respuesta ante incidentes que contemple las fases de detección, contención, erradicación, recuperación y notificación.

**Evidencias:** Documento IRP, registros de simulacros o ejercicios prácticos realizados.

**5. Copia de Seguridad y Plan de Recuperación ante Desastres (DRP)** Establecer un sistema de respaldo automático y diseñar un plan de recuperación ante desastres.

**Evidencias:** Políticas de backup, registros de pruebas de recuperación, veracidad de los respaldos.

* **Respuestas a preguntas guía**

**Durante el análisis y estudio del caso práctico, debes obtener las respuestas a las interrogantes:**

|  |  |
| --- | --- |
| Pregunta 01: | ¿Cuáles son las vulnerabilidades específicas identificadas en la infraestructura actual de ESystems SAC, incluyendo servidores Windows y Linux, así como la red de conmutación y conectividad a Internet? |
| 1. **Servidores Windows**  * **No se actualizan bien:** Hay servidores que no tienen las últimas actualizaciones, lo cual es peligroso porque los hackers aprovechan esas fallas conocidas para atacar. * **Muchos tienen acceso de administrador sin control:** Varios usuarios usan cuentas con permisos altos y no se lleva un control de eso, lo que puede ser riesgoso. * **Las contraseñas no son seguras:** Se usan contraseñas fáciles de adivinar o que no se cambian seguido, lo que facilita que alguien las descubra.  1. **Servidores Linux**  * **El acceso remoto no es seguro:** Algunos servidores permiten conectarse desde fuera sin una buena seguridad, como sin claves seguras o con contraseñas débiles. * **Los permisos de archivos están mal puestos:** Hay archivos importantes a los que cualquiera puede acceder o modificar, lo cual no debería pasar. * **No hay sistemas que alerten de problemas:** No se están usando herramientas que avisen si alguien entra sin permiso o si pasa algo raro.  1. **Red de Conmutación (Switches)**  * **Todo está conectado a la misma red:** No hay separación entre equipos, así que si uno se infecta, puede afectar a todos fácilmente. * **Se usan formas inseguras para administrar los equipos de red:** Como por ejemplo Telnet, que manda todo sin cifrar, lo cual alguien podría espiar. * **Cualquiera puede conectar un equipo a la red:** No hay control para verificar qué dispositivo se está conectando físicamente.  1. **Conexión a Internet**  * **No hay un buen firewall que revise el tráfico:** El sistema actual no analiza bien el tipo de tráfico que entra o sale, lo que deja pasar amenazas más complejas. * **Algunos servicios importantes están expuestos a Internet sin protección:** Cualquiera desde afuera podría intentar entrar a ciertas partes del sistema porque están abiertas y sin protección adecuada. * **No hay separación entre los servidores públicos y los internos:** Todos están en el mismo entorno, lo cual es riesgoso porque si un atacante entra por un servidor público, puede alcanzar fácilmente los internos. | |
| Pregunta 02: | ¿Qué medidas de seguridad se pueden implementar para proteger los datos y servicios críticos de ESystems SAC, y cómo se pueden integrar estas medidas en la cultura organizacional? |
| * **Actualizar todo a tiempo**   Asegurarse de que todos los sistemas, tanto Windows como Linux, tengan siempre las últimas actualizaciones. Esto ayuda a cerrar puertas que los hackers podrían aprovechar.   * **Usar contraseñas seguras y doble verificación**   Las contraseñas deben ser fuertes, no fáciles de adivinar, cambiarse regularmente, y donde se pueda, usar doble verificación como un código al celular.   * **Monitorear y detectar problemas**   Instalar sistemas que avisen si hay un comportamiento raro en la red o en los equipos, así se puede actuar a tiempo.   * **Separar y organizar la red**   Dividir la red por áreas (por ejemplo, usuarios, servidores, invitados) ayuda a evitar que un problema se propague por todos lados. También se pueden usar herramientas para controlar qué entra y sale de la red.   * **Tener un plan para actuar si pasa algo**   Crear un plan claro sobre qué hacer si ocurre un ataque o incidente. Quién se encarga de qué, cómo responder, y cómo recuperar los sistemas.  Por otro lado, también están las medidas en la cultura de la empresa:  **Capacitando al personal:** Explicarles a todos, con palabras claras, por qué es importante la seguridad y qué pueden hacer ellos para ayudar.  **Dando el ejemplo desde arriba:** Si los jefes cumplen con las normas de seguridad, el resto también lo hará.  **Haciendo campañas internas:** Envíos de correos con tips, pequeñas charlas o incluso juegos o retos sobre seguridad.  **Reforzando las buenas prácticas:** Premiar o destacar a quienes siguen las reglas de seguridad correctamente. | |
| Pregunta 03: | ¿Cuál sería un plan de respuesta ante incidentes efectivo que permita a ESystems SAC reaccionar de manera rápida y coordinada ante un ataque cibernético? |
| Si pasa un ataque cibernético, no podemos entrar en pánico. Necesitamos seguir un plan claro para actuar rápido y en equipo.  **Detectar el problema**  Primero hay que saber que algo está pasando. Para eso necesitamos tener sistemas de alerta (como antivirus, firewall inteligente o monitores de red) y también que los empleados avisen si notan algo raro (como correos sospechosos o lentitud inusual).  **Avisar al equipo correcto**  Apenas se detecta algo, se debe avisar al responsable de seguridad o al equipo de TI. Idealmente, debe haber un canal directo (como un grupo de WhatsApp o un correo específico) para que no se pierda tiempo.  **Contener el daño**  Si hay un equipo infectado, lo aislamos de la red (por ejemplo, lo desconectamos de Internet). Si es un servidor, lo bloqueamos temporalmente. La idea es evitar que el ataque se propague a otros sistemas.  **Analizar lo que pasó**  Se revisa cómo entraron, qué sistemas afectaron y si hay datos comprometidos. Esto se puede hacer revisando registros del sistema o con ayuda de herramientas especializadas.  **Corregir y recuperar**  Una vez que se entiende el problema, se limpia el sistema, se restauran los datos desde copias de seguridad (si hace falta) y se aplican las correcciones necesarias para que no vuelva a pasar. | |
| Pregunta 04: | ¿Cómo se puede evaluar la efectividad de las medidas de seguridad implementadas, y qué métricas se deberían utilizar para monitorear la seguridad de la infraestructura tecnológica de ESystems SAC? |
| **Evaluación:**   * Haciendo pruebas de penetración y análisis de vulnerabilidades regularmente. * Revisando los registros de eventos y alertas de seguridad para ver si detectan cosas sospechosas. * Verificando si se cumplen las políticas internas (como contraseñas seguras, backups, accesos limitados, etc.).   **Métricas usa:**   * Cantidad de intentos de ataque detectados (y bloqueados). * Tiempo de respuesta ante incidentes. * Número de vulnerabilidades encontradas vs. corregidas. * Frecuencia de copias de seguridad exitosas. * Participación del personal en capacitaciones**.** | |
| Pregunta 05: | ¿Qué tipo de formación y capacitación se deben proporcionar al personal para asegurar que todos los empleados de ESystems SAC estén alineados con las mejores prácticas de ciberseguridad y puedan contribuir a la defensa de la empresa? |
| **Concienciación básica en ciberseguridad:** Qué es un ataque, cómo reconocer correos falsos, y qué hacer si algo parece sospechoso.  **Uso seguro de contraseñas y dispositivos:** Cómo crear contraseñas fuertes, cuidar la información en el trabajo y fuera de él.  **Buenas prácticas en el día a día:** No compartir cuentas, cerrar sesión, evitar Wi-Fi públicas, etc.  **Simulacros de ataques (como phishing):** Para que practiquen y sepan cómo reaccionar.  **Capacitación por rol:** A los técnicos, cosas más avanzadas; al resto, lo esencial y claro. | |

**2. PLANIFICACIÓN DEL TRABAJO**

* **Cronograma de actividades:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **N°** | **ACTIVIDADES** | **CRONOGRAMA** | | | |
| 15/04/25 | 16/04/25 | 17/04/25 | 18/04/25 |
| 1 | Diseño de la topología segura en Packet Tracer. |  |  |  |  |
| 2 | Segmentación de red mediante VLANs. |  |  |  |  |
| 3 | Configuración de switches y routers con protocolos seguros (SSH, 802.1X). |  |  |  |  |
| 4 | Implementación de firewall y control de acceso. |  |  |  |  |
| 5 | Simulación de ciberataques y evaluación de vulnerabilidades. |  |  |  |  |
| 6 | Validación final, documentación y presentación del proyecto. |  |  |  |  |

* **Lista de recursos necesarios:**

|  |  |
| --- | --- |
| 1. **MÁQUINAS Y EQUIPOS** | |
| **Descripción** | **Cantidad** |
| PCs simuladas en Packet Tracer | 4 |
| Switches simulados | 2 |
| Routers simulados | 1 |
| Servidor interno (web o correo) | 1 |

|  |  |
| --- | --- |
| 1. **HERRAMIENTAS E INSTRUMENTOS** | |
| **Descripción** | **Cantidad** |
| Cisco Packet Tracer | 1 |
| Documentación técnica de redes y seguridad | 1 |
|  |  |
|  |  |

|  |  |
| --- | --- |
| 1. **MATERIALES E INSUMOS** | |
| **Descripción** | **Cantidad** |
| Laptop | 1 |
| Mesa | 1 |
| Cuaderno | 1 |
| Lapicero | 1 |

**3. DECIDIR PROPUESTA**

* **Describe la propuesta determinada para la solución del caso práctico**

|  |
| --- |
| **PROPUESTA DE SOLUCIÓN** |
| La propuesta de solución para mejorar la seguridad de la infraestructura tecnológica de ESystems SAC se basa en el diseño e implementación de una red segmentada y segura utilizando la herramienta Cisco Packet Tracer.  Se propone la creación de una topología que contemple la segmentación de red mediante VLANs, separando áreas críticas como servidores, usuarios administrativos, usuarios comunes y la zona DMZ. Esta segmentación permitirá controlar el tráfico interno y limitar la propagación de posibles amenazas.  Además, se configurarán protocolos seguros para la administración de la red, como SSH en lugar de Telnet, y se habilitará autenticación en puertos (802.1X) para evitar conexiones no autorizadas.  Para proteger la conexión a Internet y los servicios públicos, se integrará un firewall perimetral y se simulará una zona DMZ donde se ubicarán los servidores expuestos, como el servidor web o correo, evitando el acceso directo a la red interna.  También se implementarán listas de control de acceso (ACL) para restringir el tráfico entre VLANs según las políticas de seguridad definidas.  Finalmente, se documentará todo el diseño y configuración como parte del entregable, y se realizarán pruebas de simulación de ataques y respuestas, todo dentro del entorno virtual de Packet Tracer, garantizando una solución segura, escalable y adaptada a las necesidades de ESystems SAC. |

**4. EJECUTAR**

* **Resolver el caso práctico, utilizando como referencia el problema propuesto y las preguntas guía proporcionadas para orientar el desarrollo.**
* **Fundamentar sus propuestas en los conocimientos adquiridos a lo largo del curso, aplicando lo aprendido en las tareas y operaciones descritas en los contenidos curriculares.**

Durante el desarrollo de este caso, algo que nos quedó muy claro fue que no estábamos partiendo de cero. Todo lo que habíamos aprendido a lo largo del curso —desde la teoría hasta las prácticas más técnicas— fue la base sobre la cual pudimos analizar, simular y proponer una solución concreta para ESystems SAC.

Desde el inicio, entendimos que no bastaba con saber qué es una red o cómo funciona un router. Era necesario aplicar de forma real lo aprendido en temas como:

* Segmentación de redes con VLANs.
* Configuración de ACLs en routers.
* Seguridad en dispositivos de red.
* Simulación de ataques básicos y sus posibles defensas.
* Uso de herramientas como Packet Tracer para modelar redes complejas.

Cuando empezamos a trabajar el caso, aplicamos esos mismos conocimientos. Por ejemplo, el uso de VLANs para aislar zonas críticas dentro de la red no fue algo que se nos ocurrió porque sí, sino porque en clase ya habíamos visto cómo eso ayuda a reducir la superficie de ataque y mejorar el control de tráfico. Lo mismo con las ACLs, que aprendimos a configurar para permitir o denegar el acceso a servicios específicos según la IP de origen, destino o incluso el puerto usado.

En las tareas prácticas del curso, muchas veces simulamos ataques como escaneo de puertos o sniffing, y ahora nos dimos cuenta de que eso no era solo “jugar a hackear”: fue una forma de entender cómo piensa un atacante, y cómo podemos adelantarnos a sus movimientos. Eso nos ayudó a ver, por ejemplo, que ESystems SAC estaba expuesta por no tener filtros de acceso a sus servicios internos.

También quiero destacar que el uso de Packet Tracer fue clave. Gracias a todo lo que habíamos aprendido antes desde cómo crear una red sencilla hasta cómo integrar routers, switches, servidores, e incluso simular Internet pudimos crear un entorno que nos permitió visualizar los errores de configuración y aplicar soluciones antes de que eso ocurra en la vida real.

**INSTRUCCIONES:** Ser lo más explícito posible. Los gráficos ayudan a transmitir mejor las ideas. Tomar en cuenta los aspectos de calidad, medio ambiente y SHI.

|  |  |
| --- | --- |
| **OPERACIONES / PASOS / SUBPASOS** | **NORMAS TÉCNICAS - ESTANDARES / SEGURIDAD / MEDIO AMBIENTE** |
| Análisis del entorno digital de ESystems SAC. | ISO/IEC 27001 (gestión de seguridad de la información), buenas prácticas de diagnóstico inicial |
| Diseño de red base en Packet Tracer (topología actual). | Estándares de diseño Cisco, documentación técnica estructurada. |
| Identificación de vulnerabilidades en la red simulada. | Guía OWASP, metodología OSSTMM para pentesting controlado. |
| Segmentación de la red mediante VLANs. | Mejora de seguridad bajo estándares NIST y CIS Benchmark. |
| Configuración de direccionamiento IP estático y dinámico. | Buenas prácticas en administración de red (RFC 1918, subnetting). |
| Aplicación de listas de control de acceso (ACL). | Cisco ACLs para filtrado, NIST SP 800-41. |
| Simulación de ataques de red (sniffing, spoofing) controlados. | Pruebas controladas bajo principios éticos y educativos. |
| Implementación de firewall básico en el router principal. | ISO 27002: política de filtrado de tráfico. |
| Instalación de IDS/IPS simulado en zonas críticas de red. | Prevención de intrusos siguiendo NIST SP 800-94. |
| Simulación de tráfico malicioso para ver efectividad del firewall. | Pruebas de resiliencia según normas OSI capa 3 y 4. |
| Configuración de backups en servidor simulado. | Gestión de continuidad de negocio ISO 22301. |
| Verificación de logs y monitoreo en dispositivos de red. | Registro de eventos y trazabilidad (ISO 27001). |
| Simulación de red después de mejoras para validar estabilidad. | Mejora continua, comparativo pre/post intervención. |
| Documentación técnica del diseño, vulnerabilidades y mejoras. | Buenas prácticas de documentación técnica según ITIL |
| Recomendaciones finales (capacitación, monitoreo y mantenimiento). | Cultura de ciberseguridad organizacional. |
| Consideraciones ambientales: optimización de equipos virtuales y apagado cuando no se usa. | ISO 14001: gestión ambiental en TI |
| Consideraciones de SHI: pausas activas al usar software, buena iluminación y postura. | Normas de salud ocupacional: ergonomía en espacios TI |
|  |  |

|  |  |  |
| --- | --- | --- |
|  | | |
| C:\Unidad_D\Nuevo Logo\SENATI_FF-01 Modificado.jpg | [NOMBRE DEL TEMA DEL TRABAJO FINAL] | |
| [APELLIDOS Y NOMBRES] | [ESCALA] |

**DIBUJO / ESQUEMA / DIAGRAMA DE PROPUESTA**

**(Adicionar las páginas que sean necesarias)**

**5. CONTROLAR**

* **Verificar el cumplimiento de los procesos desarrollados en la propuesta de solución del caso práctico.**

|  |  |  |
| --- | --- | --- |
| **EVIDENCIAS** | **CUMPLE** | **NO CUMPLE** |
| * ¿Se identificó claramente la problemática del caso práctico? |  |  |
| * ¿Se desarrolló las condiciones de los requerimientos solicitados? |  |  |
| * ¿Se formularon respuestas claras y fundamentadas a todas las preguntas guía? |  |  |
| * ¿Se elaboró ​​un cronograma claro de actividades a ejecutar? |  |  |
| * ¿Se identificaron y listaron los recursos (máquinas, equipos, herramientas, materiales) necesarios para ejecutar la propuesta? |  |  |
| * ¿Se ejecutó la propuesta de acuerdo con la planificación y cronograma establecidos? |  |  |
| * ¿Se describieron todas las operaciones y pasos seguidos para garantizar la correcta ejecución? |  |  |
| * ¿Se consideran las normativas técnicas, de seguridad y medio ambiente en la propuesta de solución? |  |  |
| * ¿La propuesta es pertinente con los requerimientos solicitados? |  |  |
| * ¿Se evaluó la viabilidad de la propuesta para un contexto real? |  |  |

**6. VALORAR**

* **Califica el impacto que representa la propuesta de solución ante la situación planteada en el caso práctico.**

|  |  |  |  |
| --- | --- | --- | --- |
| **CRITERIO DE EVALUACIÓN** | **DESCRIPCIÓN DEL CRITERIO** | **PUNTUACIÓN MÁXIMA** | **PUNTAJE**  **CALIFICADO POR EL ESTUDIANTE** |
| Identificación del problema | Claridad en la identificación del problema planteado. | 3 |  |
| Relevancia de la propuesta de solución | La propuesta responde adecuadamente al problema planteado y es relevante para el contexto del caso práctico. | 8 |  |
| Viabilidad técnica | La solución es técnicamente factible, tomando en cuenta los recursos y conocimientos disponibles. | 6 |  |
| Cumplimiento de Normas | La solución cumple con todas las normas técnicas de seguridad, higiene y medio ambiente. | 3 |  |
| **PUNTAJE TOTAL** | | **20** |  |

