

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

CARRERA DE TELECOMUNICACIONES

Tema:

TESTBED PARA EL APRENDIZAJE DE INFORMÁTICA FORENSE

Trabajo de titulación modalidad Proyecto de Investigación, presentado previo a la obtención del título de Ingeniero en Telecomunicaciones

ÁREA: Programación y redes

LÍNEA DE INVESTIGACIÓN: Tecnología de la información y Sistemas de control

AUTOR: Victor Guillermo Robalino Gavilanes

TUTOR: Ing. Víctor Santiago Manzano Villafuerte, Mg.

Ambato - Ecuador

febrero 2025

APROBACIÓN DEL TUTOR

En calidad de tutor del trabajo de titulación con el tema: TESTBED PARA EL APRENDIZAJE DE INFORMÁTICA FORENSE, desarrollado bajo la modalidad Proyecto de Investigación por el señor Victor Guillermo Robalino Gavilanes, estudiante de la Carrera de Telecomunicaciones, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, me permito indicar que el estudiante ha sido tutorado durante todo el desarrollo del trabajo hasta su conclusión, de acuerdo a lo dispuesto en el Artículo 17 del Reglamento para la Titulación de Grado en la Universidad Técnica de Ambato y el numeral 6.3 del instructivo del reglamento referido.

Ambato, febrero 2025.



Ing. Víctor Santiago Manzano Villafuerte, Mg.

TUTOR

AUTORÍA

El presente trabajo de titulación con el tema: TESTBED PARA EL APRENDIZAJE DE INFORMÁTICA FORENSE es absolutamente original, auténtico y personal y ha observado los preceptos establecidos en la Disposición General Quinta del Reglamento para la Titulación de Grado en la Universidad Técnica de Ambato. En tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato, febrero 2025.



Victor Guillermo Robalino Gavilanes

C.C. 1804927521

AUTOR

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato para que reproduzca total o parcialmente este trabajo de titulación dentro de las regulaciones legales e institucionales correspondientes. Además, cedo todos mis derechos de autor a favor de la institución con el propósito de su difusión pública, por lo tanto, autorizo su publicación en el repositorio virtual institucional como un documento disponible para la lectura y uso con fines académicos e investigativos de acuerdo con la Disposición General Cuarta del Reglamento para la Titulación de Grado en la Universidad Técnica de Ambato.

Ambato, febrero 2025.



Victor Guillermo Robalino Gavilanes

C.C. 1804927521

AUTOR

APROBACIÓN DEL TRIBUNAL DE GRADO

En calidad de par calificador del informe final del trabajo de titulación presentado por el señor Victor Guillermo Robalino Gavilanes, estudiante de la Carrera de Telecomunicaciones, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, bajo la Modalidad Proyecto de Investigación, titulado TESTBED PARA EL APRENDIZAJE DE INFORMÁTICA FORENSE, nos permitimos informar que el trabajo ha sido revisado y calificado de acuerdo al Artículo 19 del Reglamento para la Titulación de Grado en la Universidad Técnica de Ambato y el numeral 6.4 del instructivo del reglamento referido. Para cuya constancia suscribimos, conjuntamente con el señor Presidente del Tribunal.

Ambato, febrero 2025.

Firmado electrónicamente por:
FRANKLIN OSWALDO
MAYORGA MAYORGA

Ing. Franklin Oswaldo Mayorga Mayorga, Mg.
PRESIDENTE DEL TRIBUNAL

Firmado electrónicamente por:
JOSE VICENTE
MORALES LOZADA

Ing. Jose Morales Lozada, PhD.
PROFESOR CALIFICADOR

Firmado electrónicamente por:
SANTIAGO MAURICIO
ALTAMIRANO MELENDEZ

Ing. Santiago Altamirano Meléndez, Mg
PROFESOR CALIFICADOR

DEDICATORIA

Dedico este trabajo a Dios, quien ha sido mi luz en la oscuridad, mi fortaleza en los momentos difíciles y mi guía constante en este camino.

Dedico este trabajo principalmente a mi padre, quien ha sido el pilar fundamental en mi vida. Su apoyo incondicional, su preocupación por mi bienestar y futuro, sus valiosas enseñanzas y su esfuerzo constante me han permitido alcanzar mis metas tanto en la vida como en lo académico. Todo lo que soy y lo que he logrado se lo debo a él.

También dedico esta tesis a mi hermano, quien me acompañó gran parte de mi vida inculcándome buenos hábitos y enseñanzas que forjaron el camino hacia un buen futuro.

Finalmente, a mi compañera y amor de mi vida, Sharon López, por estar siempre a mi lado y apoyarme durante todo este proceso, brindándome motivación y fortaleza en los momentos más desafiantes.

AGRADECIMIENTO

Agradezco profundamente a mi padre por darme la oportunidad de estudiar, por preocuparse siempre por mi bienestar y enseñarme con su ejemplo el valor del esfuerzo y la dedicación. Su apoyo ha sido indispensable en mi camino hacia este logro.

Agradezco profundamente a Dios por darme la vida, la salud y las oportunidades que me permitieron alcanzar esta meta.

A mi hermano, por ser una guía constante y ayudarme a forjar un futuro mejor.

A mis amigos de la universidad, Darío Chuquitarco, Flavio Jerez y Byron Aman, por su inestimable apoyo y compañía. Su ayuda y colaboración fueron clave para completar este trabajo.

A mi tutor, ingeniero Santiago Manzano, por su guía y orientación profesional, que fueron cruciales para el desarrollo de este proyecto.

Finalmente, agradezco a mis amigos del colegio, Bryan Peña, Sebastián Guerrero y Nicolás coronel, por los momentos compartidos, las risas y las anécdotas que siempre recordaré. Ustedes me enseñaron que el equilibrio entre el esfuerzo y la diversión es esencial para vivir plenamente.

ÍNDICE GENERAL DE CONTENIDOS

PORTADA ..... **i**

APROBACIÓN DEL TUTOR ..... **ii**

AUTORÍA ..... **iii**

DERECHOS DE AUTOR ..... **iv**

APROBACIÓN DEL TRIBUNAL DE GRADO ..... **v**

DEDICATORIA ..... **vi**

AGRADECIMIENTO ..... **vii**

ÍNDICE DE TABLAS ..... **xii**

ÍNDICE DE FIGURAS ..... **xiii**

ÍNDICE DE ANEXOS ..... **xv**

RESUMEN EJECUTIVO ..... **xvi**

ABSTRACT ..... **xvii**

CAPÍTULO I. MARCO TEÓRICO **1**

1.1 Tema de investigación 1

1.1.1 Planteamiento del problema 1

1.2 Antecedentes investigativos 3

1.3 Fundamentación teórica 7

1.3.1 La informática forense 7

1.3.2 Análisis forense digital..... 9

1.3.3 IDIP…… 11

1.3.4 Perito Judicial o Perito Forense..... 12

1.3.5 Topología de Red 13

1.3.6 Objetivos de un laboratorio forense 14

1.3.7 Herramientas de análisis forense..... 14

1.3.8 Herramientas de Análisis de Particiones y Sistemas de Archivos 16

1.3.9 Metodologías de análisis forense 20

1.3.10 Infraestructura Cloud 25

1.4 Objetivos 29

1.4.1 Objetivo general..... 29

1.4.2 Objetivos específicos 29

CAPÍTULO II. METODOLOGÍA 30

2.1 Materiales..... 30

2.2 Métodos..... 30

2.2.1 Modalidad de la investigación 30

2.2.2 Recolección de información..... 31

2.2.3 Procesamiento y análisis de datos 32

CAPÍTULO III. RESULTADOS Y DISCUSIÓN..... 33

3.1 Introducción 33

3.2 Requisitos de Hardware para el Laboratorio Forense 34

3.3 Metodología utilizada para el laboratorio forense 34

3.4 Arquitectura general del laboratorio forense 35

3.4.1 Análisis de escenarios 37

3.4.2 Recolección de Evidencia 38

3.4.3 Transferencia y almacenamiento seguro de datos 41

3.4.4 Análisis en la Nube 43

3.5 Cadena de custodia por AWS 43

3.6 Desarrollo de las prácticas de laboratorio 44

3.6.1 Práctica 1: Denegación de servicios 44

3.6.2 Práctica 2: Ataque de tipo Man in the Middle (MITM) Attack 46

3.6.3 Práctica 3: Ataque con Exploit en VSFTPD (Metasploitable 2) 49

3.6.4 Práctica 4: Análisis forense de tráfico SMTP. 51

3.6.5 Práctica 5: DNS Spoofing 55

3.6.6 Práctica 6: Escalado de privilegios 57

3.6.7 Práctica 7: Análisis de archivos de celular Android 10 59

3.7 Evaluación de conocimientos en prácticas forenses 61

3.7.1 Resultados de la Evaluación 63

3.8 Costos 64

3.8.1 Insumos del proyecto 64

3.8.2 Costo del desarrollo técnico 64

3.8.3 Costo total 65

3.9 Discusión 65

CAPÍTULO IV. CONCLUSIONES Y RECOMENDACIONES 67

4.1 Conclusiones 67

4.2 Recomendaciones 67

REFERENCIAS BIBLIOGRÁFICAS 69

ANEXOS 73

ÍNDICE DE TABLAS

Tabla 1. Estándares de aplicación nacional e internacional. 9

Tabla 2. Tipos de análisis forense digital. 10

Tabla 3. Comparación entre dd y dcfldd 19

Tabla 4. Resumen de las metodologías de análisis forense 25

Tabla 5. Modelos de infraestructura Cloud. 26

Tabla 6. Criterios de recolección de información. 32

Tabla 7. Resumen de Credenciales y Comandos SMTP. 52

Tabla 8. Registro de HASSH de la evidencia. 57

Tabla 9. Costos del proyecto 64

Tabla 10. Costos de desarrollo técnico 64

ÍNDICE DE FIGURAS

Figura 1. Proceso forense digital 10

Figura 2. Metodología del desarrollo del proyecto. 34

Figura 3. Esquema general del laboratorio forense digital. 36

Figura 4. Suspensión del sistema comprometido. 38

Figura 5. Agregar nuevo disco duro a una maquina Kali Linux. 39

Figura 6. Nuevo disco agregado al sistema. 39

Figura 7. Información de particiones de discos del sistema. 40

Figura 8. Copia del disco sdb. 40

Figura 9. Integridad de los datos con SHA-256. 40

Figura 10. Instalación de ASW CLI. 41

Figura 11. Configuración de Roles AWS. 41

Figura 12. Generación de clave de acceso. 42

Figura 13. Transferencia de archivos al bucket S3. 42

Figura 14. Análisis del uso de la memoria por el comando htop. 45

Figura 15. Registros de acceso (.log). 45

Figura 16. Solicitudes de acceso de la IP atacante. 45

Figura 17. Tabla arp de la víctima. 46

Figura 18. Solicitudes http registradas en Wireshark. 47

Figura 19. Extracto del log de autenticación con la ip sospechosa. 47

Figura 20. Solicitudes realizadas desde la dirección IP de la máquina víctima. 48

Figura 21. Archivo credentials.txt en el servidor con cambios. 48

Figura 22. Análisis de puertos abiertos en la maquina víctima. 49

Figura 23. Accesos realizados al puerto vsftpd.log. 50

Figura 24. Conexiones establecidas del puerto TCP. 50

Figura 25. Conexiones establecidas a Shell con privilegios root. 50

Figura 26. Trafico capturado en wireshark. 51

Figura 27. Reconstrucción de eventos de ataque a SMTP por Wireshark. 52

Figura 28. Respuesta de tráfico DNS manipulada con Wireshark. 55

Figura 29. Servidores DNS configurados. 56

Figura 30. Ejecución del comando nslookup del domino victordoc.com. 56

Figura 31. Ejecución del comando dig del domino victordoc.com. 56

Figura 32. Clave SSH maliciosa ingresada. 58

Figura 33. Intento de ingreso exitoso de una ip maliciosa por SSH. 58

Figura 34. Numero de celular móvil de registro de WhatsApp. 60

Figura 35. Bases de datos almacenadas en wa-db. 60

Figura 36. Información de contactos extraída. 61

Figura 37. Promedio por categorías de las preguntas evaluadas. 63

ÍNDICE DE ANEXOS

Anexo A.: Informe Técnico – Guía Práctica 1 – Denegación de servicio (DoS) 73

Anexo B: Informe Técnico – Guía Práctica 2 - Man-in-the-Middle (MITM) 79

Anexo C: Informe Técnico – Guía Práctica 3 - Ataque con Exploit de VSFTPD. 86

Anexo D. Informe Técnico – Guía Práctica 4 – Análisis forense de tráfico SMTP .. 92

Anexo E. Informe Técnico – Guía Práctica 5 – DNS Spoofing..... 103

Anexo F. Informe Técnico – Guía Práctica 6 – Escala de privilegios 111

Anexo G. Informe Técnico – Guía Práctica 7 – Android 10 119

RESUMEN EJECUTIVO

La investigación aborta la brecha de talento de ciberseguridad en América Latina y en el campo de informática forense, se identifican problemas y desafíos como la escasez de recursos y capacitación, esta investigación expresa la necesidad de un fortalecimiento de la Estrategia Nacional de Ciberseguridad de Ecuador a través de inversiones y educación. Como principal objetivo de implementar un entorno de prueba para aprendizaje de la informática forense.

El enfoque metodológico combinará un entorno local y una nube de recursos para maximizar las capacidades de análisis y preservar la integridad de la evidencia, ofreciendo así un sistema integral para la educación informática forense.

En este trabajo se han presentado, como resultados, los pasos del proceso práctico de análisis forense realizado en la investigación, desde la configuración de escenarios de ataque controlados en máquinas virtuales locales hasta el análisis avanzado en la nube a través de los servicios de AWS. A través de guías prácticas, se explicaron los pasos-clave, incluyendo la recolección de evidencia, la posterior transferencia asegurando la integridad a través de los valores hash y su procesamiento en las instancias EC2.

Como se ha desarrollado una simulación y una experimentación usando las plataformas en la nube, fueron integradas las herramientas y tecnologías implementables tanto en los entornos en la cloud como en los locales, creando las guías prácticas para abordar la adquisición de habilidades de análisis forense digital, para las audiencias académicas y profesionales.

Palabras clave: Informática forense, análisis digital, escenarios de ataque, AWS, ciberseguridad.

ABSTRACT

The research addresses the cybersecurity talent gap in Latin America and in the field of computer forensics, problems and challenges are identified as the shortage of resources and training, this research expresses the need for a strengthening of the National Cybersecurity Strategy of Ecuador through investment and education. As a main objective to implement a test environment for learning computer forensics.

The methodological approach will combine a local environment and a cloud of resources to maximize analysis capabilities and preserve the integrity of evidence, thus providing a comprehensive system for computer forensics education.

In this paper, the steps of the practical forensic analysis process performed in the research, from the configuration of controlled attack scenarios on local virtual machines to advanced analysis in the cloud through AWS services, have been presented as results. Through practical guides, the key-steps were explained, including evidence collection, subsequent transfer ensuring integrity through hash values and its processing on EC2 instances.

As simulation and experimentation using cloud platforms was developed, tools and technologies deployable in both cloud and on-premises environments were integrated, creating practical guidelines to address the acquisition of digital forensics skills for both academic and professional audiences.

Keywords: Computer forensics, digital analysis, attack scenarios, AWS, cybersecurity.

CAPÍTULO I. MARCO TEÓRICO

1.1 Tema de investigación

TESTBED PARA EL APRENDIZAJE DE INFORMÁTICA FORENSE

1.1.1 Planteamiento del problema

El problema se analiza en la documentación que describe que la región de América Latina y el Caribe enfrenta un futuro sombrío en ciberseguridad, caracterizado por una creciente demanda de trabajadores con talento y una grave escasez de talento. La brecha actual varía entre 515,000 y 701,000 trabajadores y, con muchos factores que la empeoran, el envejecimiento de la población trabajadora, la tasa de desempleo juvenil y la falta de conciencia de las oportunidades de ciberseguridad son algunos de estos ejemplos [1].

Varios desafíos enfrentan la informática forense en América latina accionados por la falta de recursos y capacitación. A ello, la región carece de legislación específica en ciberdelincuencia, y hay poco espacio para la cooperación policial. La informática forense no es una prioridad para los países latinoamericanos, ya que la ven como una ciencia costosa y con pocas competencias a su alcance. La falta de dinero no permite a las entidades desarrollar habilidades avanzadas y comprar herramientas necesarias para investigar crímenes cibernéticos. A la vez, la ciberdelincuencia carece de los fundamentos jurídicos específicos, lo que impide la persecución efectiva de criminales y deja a las partes interesadas sin ninguna directriz a seguir.

La informática forense se enfrenta a varios desafíos en América latina debido a la falta de recursos y capacitación, esto causa una ausencia de legislación específica sobre la ciberdelincuencia y la escasa cooperación entre las fuerzas del orden y el sector privado. En lo que respecta a la cibernética, la falta de presupuesto y capacitación adecuada evita que las organizaciones adquieran la capacidad de desarrollar habilidades avanzadas y adquirir herramientas que sean importantes para desarrollar investigaciones significativas en el proceso de eliminación.

Una cooperación limitada entre las fuerzas de seguridad y el sector privado agrava la situación, y aunque el problema a menudo proviene del intercambio pobre de información y la falta de colaboración, los informáticos forenses también ven una oportunidad para liderar la capacitación y la educación contra la ciberdelincuencia y abogar por una mejor liderazgo de políticas y alianzas en la región [2].

Ecuador ha desarrollado la Estrategia Nacional de Ciberseguridad. Este hecho es significativo para asegurar de manera práctica que la infraestructura de información y comunicación del país está bien protegida y para garantizar a los ciudadanos que sus datos personales están seguros. Sin embargo, para cada uno de esos objetivos, es decisivo abordar un gran número de desafíos que se encuentran en el camino, como la ausencia de financiamiento, el déficit de empleados calificados y la falta de fortaleza institucional. La inversión en ciberseguridad, un enfoque más valioso para enseñar y capacitar y el aumento de la calidad de la cooperación interinstitucional son medidas centrales para avanzar en dirección a los fines indicados [3].

Dada la falta de conciencia sobre la importancia de la informática forense en muchas organizaciones, esto impide la implementación de medidas de seguridad adecuadas, dejando así a las empresas vulnerables a ataques cibernéticos causando una falta de medidas de seguridad que dificulta la contratación y retención de expertos en informática forense, este impacto lleva a crear una escasez de profesionales capacitados para proteger los datos digitales y limita la capacidad de las organizaciones para responder eficazmente a incidentes de seguridad perpetuando un ciclo de desinformación y vulnerabilidad. De forma, que la fomentación de la educación y el conocimiento sobre informática forense en las empresas puede ayudar a las organizaciones a comprender la necesidad de la gestión de ciberseguridad e invertir encontrando la solución de mitigación de riesgo de seguridad antes de que sea extremadamente costoso.

Dado el caso se puede tener un fracaso en la gestión de riesgo de ciberseguridad por la falta de condiciones laborales y el reconocimiento profesional de la gestión de riesgo de ciberseguridad por no permitir a las organizaciones contratar a un especialista informático forense. La falta de gestión de riesgo de ciberseguridad es causada por la inhabilidad de la organización de manejar el riesgo que el tema de la seguridad

informática puede comprometer la integridad de los datos digitales y la reputación organizacional. Es fundamental que las empresas implementen estrategias robustas de gestión de riesgos cibernéticos para atraer y retener talento especializado en informática forense.

La incapacidad de las empresas para proteger sus datos digitales y responder eficazmente a los incidentes de seguridad cibernética ha resultado en una escasez de expertos en informática forense. A la luz del reducido personal capacitado, es prácticamente imposible para las empresas identificar, comprender y mitigar las amenazas cibernéticas, lo que se traduce en un tiempo de respuesta más largo a los incidentes y en graves daños financieros y de reputación. La escasez de recursos capacitados ha impedido a las organizaciones implementar estrategias de seguridad cibernética proactivas o conducir auditorías de seguridad cibernética. Por consiguiente, estas empresas se encuentran en alto riesgo de sufrir ataques cibernéticos. Del mismo modo, pueden enfrentar la interrupción de las operaciones y la pérdida de con fianza de los clientes.

El alto costo de la formación para los profesionales de la informática forense disminuye la inversión empresarial en formación. Afecta a la disponibilidad de conocimientos especializados. Por ende, las empresas no pueden implementar estrategias de seguridad adecuadas ni actualizar sus instalaciones de protección. Tal circunstancia, por lo tanto, las pone más en riesgo de sufrir amenazas cibernéticas. Si las inversiones no se realizan, el nivel de integridad de los datos, la continuidad operativa y la reputación se comprometerán.

1.2 Antecedentes investigativos

Tras realizar la investigación bibliográfica en repositorios y en distintas publicaciones de revistas de artículos científicos se encuentran los siguientes antecedentes similares, sirviendo como referencia a la investigación.

La investigación titulada "CloudMe Forensics: A Case of Big-Data Investigation", realizada por Yee-Yang Teing, Ali Dehghantanha y Kim-Kwang Raymond Choo, realizada en el 2018 aborda los desafíos de la informática forense en entornos de

almacenamiento en la nube, específicamente en el servicio CloudMe. El estudio se centró en identificar y analizar los artefactos residuales generados por las actividades de los usuarios en dispositivos de escritorio y móviles, como la instalación, sincronización y eliminación de archivos. Para ello, se implementaron entornos experimentales que incluían máquinas virtuales con sistemas operativos Windows, Ubuntu y MacOS, así como dispositivos móviles con Android y iOS. Se emplearon herramientas forenses como Volatility, SQLite Browser y Autopsy para analizar bases de datos, registros y cachés generados por la aplicación CloudMe. Los resultados demostraron la importancia de los artefactos como la base de datos de caché (cache.db) y los registros web en la reconstrucción de actividades del usuario. Se destaca la relevancia de desarrollar metodologías específicas para la investigación forense en servicios de nube habilitados para big data y propone futuras líneas de investigación orientadas a la reducción de datos y la integración de técnicas avanzadas de minería de datos en el análisis forense digital [4].

En 2019, Miguel Fernández Mata llevó a cabo el proyecto "Laboratorio de Pentesting basado en tecnología de contenedores" en la Universidad de Cantabria. En este trabajo, se utilizó la tecnología de contenedores, específicamente Docker, para implementar un entorno de red virtual con dos máquinas virtuales sobre las cuales se realizó un proceso típico de pentesting. Además, se comparó este enfoque basado en contenedores con el uso de máquinas virtuales a través de la herramienta VirtualBox. La metodología empleada consistió primero en implementar un escenario de referencia basado en máquinas virtuales y luego un escenario objetivo basado en contenedores. Se realizaron pruebas relacionadas con el hacking ético, específicamente la ejecución de una prueba de penetración en ambos entornos. Entre los resultados más relevantes, se destacó la comparación de rendimiento entre las máquinas anfitrionas al utilizar Docker frente a las máquinas virtuales, observándose un rendimiento más eficiente y una mayor capacidad para soportar un mayor número de servicios. Asimismo, se demostró la viabilidad de la tecnología de contenedores para competir con las máquinas virtuales en la realización de funciones de pentesting, destacándose la alta portabilidad y flexibilidad de los contenedores Docker, lo que facilitaba su despliegue en diversos entornos, incluidos los académicos [5].

La investigación titulada "Estructura de un laboratorio de Informática Forense para la Dirección de Seguridad Informática", realizada por Oscar Lázaro Garcés Pérez, publicada en la *Revista Cubana de Ciencias Informáticas* (2022), presenta un diseño general para la implementación de un laboratorio de informática forense con el objetivo de mejorar el análisis y manejo de evidencias digitales durante incidentes de seguridad informática. El trabajo destaca la importancia de contar con un laboratorio especializado que garantice la preservación, integridad y análisis riguroso de evidencias digitales mediante procedimientos y herramientas científicas. La propuesta incluye la creación de seis áreas funcionales: seguridad de datos, recuperación de archivos borrados, análisis de memoria RAM, análisis de red, análisis de aplicaciones instaladas y un departamento legal. Como resultado, este diseño busca fortalecer las capacidades investigativas en delitos informáticos dentro de la institución, asegurando una respuesta eficiente ante incidentes de seguridad y contribuyendo a la formación académica en informática forense [6]

El proyecto titulado "La importancia del cómputo forense en la actualidad", desarrollado por Yeiny Romero Hernández y colaboradores en 2023 en la Benemérita Universidad Autónoma de Puebla, se enfoca en la implementación de un laboratorio de cómputo forense para abordar delitos cibernéticos y fortalecer la educación en ciberseguridad. La investigación utiliza herramientas como NMAP, OWASP ZAP y Bulk-Extractor, integradas en un entorno basado en Kali Linux, para realizar auditorías de seguridad, identificar vulnerabilidades en redes y aplicaciones, y analizar datos en dispositivos comprometidos. La metodología incluyó pruebas prácticas en un laboratorio configurado con hardware y software especializados, permitiendo el análisis detallado de casos de pérdida de datos y ataques informáticos. Entre los resultados más destacados está la identificación precisa de vulnerabilidades en redes y sitios web, así como la recuperación eficiente de información de memorias RAM. Este proyecto no solo contribuye a la investigación en ciberseguridad, sino que también tiene un impacto educativo significativo, al proporcionar un entorno práctico para el aprendizaje de técnicas de informática forense y fortaleciendo la formación de estudiantes en el área [7].

La investigación con el título de "Análisis forense digital en dispositivos móviles", fue realizada por Arnulfo Alemán Ariza y publicada en la revista *Cathedra* en 2024,

aborda los retos y avances en la disciplina del análisis forense digital aplicado a dispositivos móviles. Este trabajo examina las metodologías y herramientas disponibles para la extracción y análisis de evidencia digital en dispositivos con sistemas operativos Android y iOS, destacando los desafíos técnicos y legales que enfrenta esta especialidad. El estudio subraya la importancia de garantizar la integridad de la evidencia mediante la aplicación de procedimientos rigurosos y herramientas especializadas, como Cellebrite y Oxygen Forensic Detective, utilizadas tanto para extracciones lógicas como físicas. Además, se abordan cuestiones éticas y legales relacionadas con la privacidad y la proporcionalidad en el manejo de la información extraída. El análisis resalta la necesidad de actualización continua de los profesionales forenses para mantenerse al día con las tecnologías emergentes y los marcos legales vigentes. Los hallazgos de esta investigación proporcionan una base sólida para la mejora de los procesos de extracción y análisis en dispositivos móviles, contribuyendo a la profesionalización y eficacia de esta disciplina en contextos legales y administrativos [8].

El trabajo titulado "Análisis Forense de Evidencias Digitales en Entornos iCloud", desarrollado por Carlos Adrián Pita Vera en 2024 en la Universidad Estatal Península de Santa Elena, aborda la creciente necesidad de estudiar las vulnerabilidades y desafíos asociados con el servicio de almacenamiento en la nube iCloud. Este proyecto implementa laboratorios forenses utilizando herramientas de código abierto y máquinas virtuales para analizar evidencias digitales en entornos controlados. A través de tres escenarios experimentales, se diseñaron y ejecutaron ciberataques específicos, incluyendo casos de denegación de servicios, infección de malware y defacement, aplicando normas como la ISO 27037:2012 para garantizar la integridad de las evidencias. El estudio emplea una metodología descriptiva y exploratoria que incluye la identificación de amenazas cibernéticas comunes, el análisis de implicaciones legales y la elaboración de un informe detallado con recomendaciones de ciberseguridad. Los resultados destacan la importancia de las técnicas forenses para extraer y preservar evidencias digitales en entornos Cloud, clasificando amenazas y proponiendo estrategias para minimizar riesgos. Este trabajo no solo contribuye al avance de la informática forense en servicios de nube, sino que también ofrece

herramientas prácticas para la formación académica y profesional en tecnologías de la información [9].

1.3 Fundamentación teórica

1.3.1 La informática forense

La informática forense es una rama especializada que se centra en el uso de métodos científicos y de investigación para recopilar, analizar y preservar pruebas digitales y que sirvan por sí solas para ser utilizadas como evidencia en eventos legales. Además, la informática forense implica descubrir, recuperar y presentar no sólo datos evidentes, sino también elementos ocultos que pueden haber sido gestionados u obliterados, una parte sustancial de la exploración de la criminalidad informática, el engaño, la verificación y la recopilación de información perdida por la caída del sistema o la eliminación accidental [10].

Los profesionales de la informática forense emplean tecnologías avanzadas para examinar una amplia gama de dispositivos electrónicos, como discos duros, memorias extraíbles y correos electrónicos, asegurando que la integridad de los datos se mantenga intacta durante el proceso. Esto es crucial, ya que la evidencia digital es sumamente delicada y puede alterarse fácilmente. La informática forense, por tanto, permite obtener, analizar y presentar pruebas en un formato aceptable legalmente, aportando respuestas técnicas que asisten a tribunales o partes involucradas en litigios civiles y penales [11].

a. Fases en el proceso de informática forense

El proceso de peritaje en informática forense se puede definir en tres etapas fundamentales (adquisición, análisis y presentación), este proceso conlleva a un desglose de cinco fases más detalladas que aseguran un enfoque metódico y preciso. A continuación, se describen cada una de estas fases [11]:

- ***Preparación.*** Este ocurre antes de que surja un incidente, los profesionales de la informática forense se aseguran de contar con la formación adecuada, el mantenimiento de los equipos y los recursos necesarios para la investigación.

- ***Adquisición.*** Fase en la que se recopilan los datos que serán objeto de análisis. Esta recopilación puede realizarse directamente en la escena del incidente o en un laboratorio especializado, se debe asegurar la integridad de los datos, lo que implica utilizar técnicas que garanticen que la evidencia no sea alterada ni comprometida.

- ***Análisis.*** Organización de la información recopilada, para extraer los datos relevantes para su investigación. Esto incluye la indexación de los datos, la identificación de patrones y la comprensión de los hechos clave que puedan apoyar o refutar una teoría del caso.

- ***Identificación de Evidencias.*** Se selecciona, entre toda la información adquirida y analizada, aquellos elementos que sean pertinentes para el caso específico.

- ***Informe de Conclusiones.*** Se detallan todas las actividades realizadas durante la investigación, desde la adquisición de datos hasta el análisis y la identificación de evidencias.

b. Pautas y normas de referencia para la pericia forense en entornos digitales

En 2012, la Organización Internacional de Normalización y la Comisión Electrotécnica Internacional publicaron el estándar ISO/IEC 27037: Guidelines for Identification, Collection, Acquisition, and Preservation of Digital Evidence, que similmente establece pautas claras para el manejo inicial de evidencia digital. Estos lineamientos buscan armonizar las prácticas en el tratamiento de la evidencia digital a nivel internacional, asegurando su validez en contextos legales y su correcta manipulación desde la identificación hasta la preservación. Se describen las fases como Identificación, recopilación, adquisición y preservación. Cuatro fases clave propuestas por este estándar para el manejo de la evidencia digital [12].

Se describen otras fases como el análisis y la elaboración de informes de conclusiones, donde el propósito del análisis es determinar si la evidencia digital es pertinente para el caso, ya sea para confirmar o refutar hechos clave bajo investigación. Respecto al informe, se intenta ser exhaustivo en el registro de toda la información relevante acerca

del proceso de investigación, incluyendo los pasos, procedimientos y resultados para todos ellos. Finalmente, en la Tabla 1 se presenta la síntesis de la normativa, tanto de aplicación nacional como internacional, relacionada con la investigación forense digital [13].

Tabla 1. Estándares de aplicación nacional e internacional [13].

Norma	**Descripción**	**Tipo**
UNE 197010:2015	Criterios para la elaboración de dictámenes e informes periciales sobre tecnologías de la información y comunicación.	Nacional (España)
UNE 71505:2013	Incluye vocabulario, principios generales y buenas prácticas en la gestión de evidencias electrónicas, así como formatos y mecanismos técnicos.	Nacional (España)
UNE 71506:2013	Establece procesos de análisis forense dentro del ciclo de gestión de evidencias informáticas.	Nacional (España)
ISO/IEC 27037:2012	Guías para la identificación, recolección, adquisición y preservación de evidencias digitales.	Internacional
ISO/IEC 27042:2015	Guías para el análisis e interpretación de evidencias digitales.	Internacional

1.3.2 Análisis forense digital

Análisis forense digital es una rama de la ciencia forense que se ocupa de la recuperación e investigación de datos en dispositivos digitales en relación con los delitos cibernéticos. Con una tasa creciente de delincuencia en el ámbito digital, la especialidad se vuelve más significativa no solo con respecto a los crímenes cibernéticos, sino también con respecto a actividades en operaciones personales y empresariales que implica participación en la presentación de datos digitales [12].

Las fases del análisis forense digital se ven a continuación en la Figura 1. Dicha metodología posibilita un enfoque sistemático hacia cada fase del análisis y asegura que la validez e integridad de los datos no serán comprometidos. La tecnología ha avanzado en una creciente era de digitalización por lo que el análisis forense digital se ha convertido en una herramienta esencial para resolver delitos informáticos y protección de información sensible en diversas industrias [14].



Figura 1. Proceso forense digital [14].

El análisis forense digital evalúa diferentes evidencias digitales que pueden tener múltiples datos, estos se pueden dar en eventos como el ransomware, la violación de red o incluso archivos corrompidos activos.

a. Categorías del análisis forense digital

La ciencia forense digital se puede clasificar en función de la fuente de la evidencia digital obtenida. El conjunto de artefactos digitales contenidos en el dispositivo informático de destino, que se pueden utilizar como prueba en un tribunal, se denomina evidencia digital, como se muestra en la Tabla 2 [15].

Tabla 2. Tipos de análisis forense digital [15].

Grafico				
Características	**Informática forense**	**Informática forense móvil**	**Informática forense de redes**	**Informática forense de bases de datos**
Descripción	Este es el tipo más común de análisis forense digital. Se trata de investigar evidencias en dispositivos como computadoras portátiles, de escritorio y dispositivos de almacenamiento.	Subconjunto de la informática forense digital que se especializa en recopilar datos de dispositivos móviles como teléfonos, tabletas y dispositivos portátiles.	Vigila el tráfico de red a través de monitoreo y análisis y obtenga Pruebas de ello para determinar el culpable de una violación de seguridad de la red o posible intrusión	Enfocada en el análisis de los datos almacenados en sistemas de bases de datos para determinar accesos no autorizados y detectar comportamientos maliciosos.

Características	Informática forense	Informática forense móvil	Informática forense de redes	Informática forense de bases de datos
Dispositivos o elementos investigados	Computadoras, discos duros, USB, tarjetas SD, memoria RAM, sistemas operativos y aplicaciones.	Teléfonos, tabletas, relojes inteligentes, dispositivos portátiles.	Tráfico de red, routers, switches, firewalls, logs de red.	Bases de datos como SQL Server, Oracle, MySQL.
Objetivo Principal	Recuperar datos eliminados o corruptos y analizar rastros digitales para encontrar pruebas de actividades ilegales o fraudulentas.	Obtener evidencia digital de dispositivos móviles, como registros de llamadas, mensajes, datos de aplicaciones y ubicación GPS.	Identificar intrusiones, rastrear el origen de ciberataques y analizar el tráfico de red en tiempo real o almacenado para detectar actividades sospechosas.	Analizar accesos a bases de datos, detectar modificaciones no autorizadas o comportamientos inusuales en los datos almacenados.
Métodos y Herramientas	Software de recuperación de datos (EnCase, FTK), herramientas de análisis de discos duros y recuperación de archivos eliminados.	Herramientas como Cellebrite, XRY, UFED, análisis de aplicaciones móviles y recuperación de datos de almacenamiento móvil.	Herramientas como Wireshark, tcpdump, IDS/IPS (Snort), análisis de logs de red, packet sniffers, sistemas de monitorización de red.	Herramientas como ApexSQL, DB Audit, análisis de logs de bases de datos, auditorías de seguridad de bases de datos.

1.3.3 IDIP

El IDIP (Proceso Integrado de Investigación Digital) adapta las técnicas de investigación convencionales usadas en las escenas de crímenes a la computadora, como si de una escena de crimen más se tratara. A través de la utilización de los métodos tradicionales en el entorno digital mediante este sistema que estructura el proceso en 5 etapas: preparación, despliegue, investigación de la escena física, investigación de la escena digital y presentación de hallazgos [10].

De esta manera, se asegura la cobertura completa y multidimensional de un caso, lo que brinda una perspectiva más detallada de los crímenes del mundo real en un mundo donde los aspectos digitales y físicos se conectan [10].

1.3.4 Perito Judicial o Perito Forense

Un perito judicial o perito informático forense es un experto con conocimientos especializados reconocidos, ya sea por formación académica o experiencia profesional, cuya labor es proporcionar información técnica fundamentada o emitir opiniones expertas que contribuyan al esclarecimiento de hechos en un proceso judicial. Este profesional actúa como un nexo entre los aspectos técnicos y el sistema judicial, aportando análisis y evaluaciones detalladas que son clave para la toma de decisiones en un caso [16].

El trabajo del perito incluye la recolección, preservación y análisis de evidencias digitales utilizando métodos científicos, asegurando en todo momento el cumplimiento de la cadena de custodia. Estos procedimientos garantizan que las evidencias sean válidas y admisibles ante los tribunales, desempeñando un rol fundamental en la administración de justicia. Además, los peritos pueden ser designados por las autoridades judiciales o propuestos por las partes interesadas, dependiendo de la naturaleza del caso [16].

a. Funciones de un perito informático

El perito informático cumple un rol fundamental en la investigación de incidentes relacionados con tecnologías de la información, desempeñando funciones especializadas que abarcan múltiples áreas de acción como [16]:

- Localización y recuperación de evidencias digitales, como archivos eliminados o alterados, que puedan ser relevantes en procesos legales.
- Auditorías y pruebas de penetración para evaluar y reforzar la seguridad informática en sistemas y redes.
- Recuperación de datos perdidos o dañados con herramientas avanzadas
- Valoración y tasación de equipos tecnológicos, así como de la certificación y homologación de software y hardware, asegurando que cumplan con los estándares establecidos.

- Asesoramiento técnico en casos de cibercrimen, ofreciendo soporte para identificar y mitigar ataques de malware o brechas de seguridad.

- Formación y capacitación de profesionales en áreas relacionadas con la informática forense, incluyendo a miembros de fuerzas de seguridad y del ámbito jurídico.

- Análisis forense de contenido multimedia, como videos, imágenes y audios, y el seguimiento de actividades sospechosas, como correos electrónicos anónimos o publicaciones digitales. También es responsable de garantizar la correcta preservación y manejo de la cadena de custodia de las evidencias digitales, asegurando su validez y admisibilidad en procesos judiciales.

Estas funciones destacan la importancia de un enfoque técnico y ético riguroso, que permita al perito informático actuar como un puente entre los aspectos tecnológicos y las exigencias del sistema judicial, contribuyendo de manera decisiva a la resolución de casos complejos en el ámbito digital.

1.3.5 Topología de Red

Es la estructura física o lógica en la que los nodos de una red están interconectados para facilitar el intercambio de datos. Se identifican varios componentes esenciales, como routers, switches, placas de red, estaciones de trabajo y medios de transmisión, incluyendo conexiones alámbricas e inalámbricas. Además, las herramientas como firewalls y sistemas de detección de intrusos (IDS) juegan un papel fundamental para monitorear y asegurar la integridad de la red [16].

a. Identificación de Componentes de Red

La identificación precisa de los componentes de una red es esencial en la informática forense para determinar los puntos clave de adquisición de datos. Esto incluye el registro de información de routers, switches, y estaciones de trabajo, así como la obtención de registros (logs) desde firewalls y sistemas IDS [16]. Estos datos permiten establecer patrones de comunicación y detectar posibles irregularidades o intrusiones

b. Protocolos de Captura y Adquisición de Datos

La fase de captura/adquisición sigue un protocolo riguroso para garantizar la autenticidad e integridad de la evidencia. Este incluye la documentación detallada de cada acción realizada, como la obtención de logs, tablas de enrutamiento, y registros de memoria volátil. Además, se recomienda el uso de herramientas que generen firmas hash (MD5 o SHA1) para asegurar la integridad de los datos adquiridos [16].

1.3.6 Objetivos de un laboratorio forense

El laboratorio forense debe proporcionar un entorno controlado para analizar, experimentar, validar herramientas y técnicas de análisis forense digital. Tener un laboratorio fundamenta la necesidad de garantizar la integridad de los datos o evidencia digital, para permitir realizar pruebas de análisis forense para proporcionar una base confiable en la capacitación de incidentes de seguridad cibernética [17].

Entre los objetivos de un laboratorio forense se incluyen [18]:

- **Custodia de evidencias digital:** Garantiza la captura de datos sin comprometer la integridad de estos.
- **Creación de entornos simulados:** Recrea escenarios reales para desarrollar habilidades técnicas y metodológicas.
- **Validación de herramientas forenses:** Probar y comparar herramientas para elegir las más efectivas en contextos específicos.

1.3.7 Herramientas de análisis forense

Existen una gran cantidad de aplicaciones dedicadas al análisis forense que abordan diferentes aspectos, como la memoria, los discos de almacenamiento, los protocolos de red y las aplicaciones. Para realizar un análisis forense digital se requiere herramientas específicas que permitan la extracción, preservación y análisis de evidencias en entornos controlados. Algunas de estas herramientas pueden clasificarse según su función, desde el análisis de memoria volátil hasta el monitoreo de sistemas

y redes. Se presenta las herramientas de un laboratorio forense con sus características y aplicaciones [14].

a. Análisis de Memoria Volátil

En la memoria RAM se puede identificar procesos activos como conexiones de red y datos almacenados temporalmente. Algunas herramientas como Volatility y Rekall son dos ejemplares para esta categoría. Volatility permite la extracción detallada de procesos, registros del sistema y conexiones activas, soportando múltiples sistemas operativos como Windows, Linux y MacOS. Rekall tiene la capacidad de automatizar análisis avanzados con su velocidad, siendo muy útil en la detección de malware persistente [14].

b. Recuperación de Datos

La recuperación de datos puede realizarse en Autopsy y Sleuth. Autopsy permite dicha tarea a través de su interfaz gráfica que ayuda a recuperar archivos borrados y a realizar el análisis de sistemas de archivos, mientras que Sleuth Kit, a través de la línea de comandos, proporciona al investigador un control más detallado, por ejemplo, cuando se examinan particiones y volúmenes dañados [14].

c. Análisis de Red

La escucha y el análisis del tráfico de la red son actividades fundamentales para detectar actividades sospechosas y ataques. En este sentido, Wireshark y Tcpdump son opciones que se destacan. La primera constituye una interfaz gráfica que permite realizar la captura y el análisis de paquetes utilizando filtros avanzados, lo que permite la detección de anomalías en protocolos específicos. Tcpdump, por su parte, se trata de una herramienta de línea que captura paquetes en tiempo real y es más sencilla de manejar en comparación con Wireshark., si bien se pregunta sobre “paquete” Tut-pad está ofreciendo la descripción básica de Tcpdump. Dado que se trata de una herramienta de línea que se puede correr en un entorno de consola completa mediante SSH [14].

d. Monitoreo del Sistema

Para un laboratorio forense se requiere de la capacidad de monitorear procesos, conexiones y cambios en el sistema en tiempo real. Las herramientas que ofrece el paquete SysInternals Suite para sistemas Windows incluyen Process Explorer, que examina procesos activos, y Autoruns, que explora la configuración de inicio automático [14].

En cuanto a los comandos nativos, lsof, que significa listado de archivos abiertos por procesos, strace, que realiza un rastreo de llamadas al sistema y sar, que es un monitoreo de estadísticas del sistema, son vitales para observar el comportamiento del sistema en sistemas Linux.

e. Herramientas Complementarias

Además de las herramientas principales, se dispone de soluciones complementarias como FTK Imager y EnCase. FTK Imager permite crear imágenes forenses de discos y realizar extracciones de datos sin alterar la evidencia original, además de la herramienta, EnCase, con su enfoque profesional, integra análisis forense y generación de reportes en una sola plataforma, siendo ampliamente utilizada en entornos legales [14].

1.3.8 Herramientas de Análisis de Particiones y Sistemas de Archivos

En el análisis forense digital, el uso de herramientas especializadas permite identificar, extraer y analizar información contenida en discos duros e imágenes de disco. Este apartado detalla el empleo de algunas herramientas fundamentales explicando su funcionamiento, utilidad y relevancia en el ámbito de la informática forense [19].

a. MMLS

Este comando *mmls* se utiliza para analizar la estructura de particiones de un disco físico o una imagen de disco. La función principal del comando mmls es listar las particiones existentes junto con las áreas de espacio no asignado. Esta información es utilizada para comprender la manera en que se organiza el disco y encontrar posiciones

donde el espacio almacene residentes lógicamente los datos que han sido eliminados, pero se conservan [20].

El comando *mmls* cuando se ejecutado, va a dar alrededor detallado sobre el comienzo y el final de cada partición junto con la presencia de los respectivos sistemas de archivos y las áreas que no fueron asignadas. El resultado muestra Meta Slot, que es una primera tabla de partición en un disco, se llama la Guía de Tabla Partición o Máster Boot Record, esta tabla contiene información crítica sobre cómo están organizadas las particiones en el disco, lo que facilita la reconstrucción de su estructura en escenarios donde existan alteraciones o daños [21].

El uso de *mmls* es clave en procesos forenses para identificar [21]:

- La ubicación exacta de particiones activas e inactivas.
- Sectores no asignados que pueden contener evidencia residual.
- Estructuras de partición que han sido manipuladas o eliminadas.

b. FSSTAT

El comando *fsstat* complementa la información recuperada por el comando mmls, proporcionando información y metadatos de sistema de archivos específicos relacionados con un sistema de archivos en una partición en particular [22]. Por lo tanto, dado los informes proporcionados por *mmls*, el comando *fsstat* examina el sistema de archivos en partición seleccionada y brinda información crítica en el análisis forense [23].

Algunos de los datos recuperados por el comando *fsstat* incluyen [22]:

- Características del sistema de archivos, por ejemplo, NTFS, FAT32, entre otros
- El número único asignado al volumen del sistema de archivos
- Los datos de la MFT en sistemas NTFS, que contiene la cantidad de registros y el tamaño de los inicios y finales de los índices, en número de sectores.

- Información general sobre el directorio raíz y la estructura general del sistema de archivos.

El uso de *fsstat* es facilita la comprensión de cómo se organiza la información dentro de una partición, permitiendo [23]:

- La recuperación de datos eliminados o dañados.
- La detección de posibles alteraciones en la estructura del sistema de archivos.
- La documentación precisa del estado del sistema en el momento del análisis.

c. FDISK

La gestión de particiones en discos duros usualmente es manejada por *fdisk*, aunque no está específicamente diseñada para análisis forense, su capacidad permite mostrar y manipular particiones la convierte en una herramienta útil en este contexto [24].

fdisk permite:

- Listar todas las particiones de un disco, incluyendo información sobre su tipo, tamaño y punto de inicio.
- Detectar particiones ocultas o no montadas.
- Exportar información básica sobre la estructura del disco para análisis posterior.

Para un caso de análisis forense digital, *fdisk* se puede utilizar principalmente para obtener una visión inicial del disco y confirmar la integridad de las particiones visibles antes de proceder con análisis más avanzados [24].

d. PARTED

Otra herramienta versátil para la gestión de particiones, *parted* es muy similar a *fdisk*, pero tiene soporte para discos más grandes y sistemas de particiones modernos, como GPT. Se utiliza en el análisis forense para visualizar la tabla de particiones en un formato comprensible, identificar particiones dañadas y cualquier otra inconsistencia

en la estructura de sus discos y realizar operaciones más avanzadas, como redimensionar o copiar particiones, en entornos controlados. También puede detectar posibles particiones manipuladas y trabajar con discos modernos que no son compatibles con una herramienta más antigua [25].

e. Herramientas de duplicación de discos

En el campo de la informática forense, es esencial utilizar herramientas que permitan la copia precisa de datos mientras se garantiza su integridad. Dos de las herramientas más utilizadas para esta tarea son *dd* y *dcfldd.* Aunque ambas se basan en la misma funcionalidad básica de copiar datos a bajo nivel, *dcfldd* incluye características adicionales que la hacen más adecuada para aplicaciones forenses. A continuación, en la Tabla 3 se presenta una tabla comparativa para resaltar sus diferencias clave. [26], [27], [28].

Tabla 3. Comparación entre dd y dcfldd [26], [27], [28].

	dcfldd	**dd**
Definición	Una herramienta mejorada basada en dd, diseñada específicamente para aplicaciones forenses y seguridad de datos.	Una herramienta de Unix/Linux para copiar y convertir datos a bajo nivel, ampliamente utilizada para duplicar discos o particiones.
Enfoque Principal	Creada para análisis forense, con características que aseguran la integridad y verificación de los datos copiados.	Generalmente utilizada para copias y conversiones de datos sin un enfoque específico en la seguridad o la integridad.
Características Clave	- Genera automáticamente resúmenes hash (como MD5 y SHA1) para verificar la integridad de los datos. - Permite dividir imágenes de disco en partes más pequeñas. - Ofrece registro detallado del proceso.	- Copia datos byte a byte de forma simple. - Es versátil, pero carece de funciones especializadas como generación de hashes o registro detallado.
Uso en Informática Forense	Ideal para entornos forenses debido a sus funciones de verificación y trazabilidad.	Se puede usar, pero requiere pasos adicionales para cumplir con estándares forenses.
Facilidad de Uso	Similar a dd, pero con comandos adicionales que simplifican el trabajo en aplicaciones específicas.	Más genérico y directo, pero requiere herramientas adicionales para funcionalidades avanzadas.
Limitaciones	Puede ser menos conocido que dd, por lo que algunos usuarios pueden necesitar capacitación básica.	No incluye herramientas integradas de validación o partición, lo que puede aumentar el riesgo de errores en entornos forenses.

1.3.9 Metodologías de análisis forense

a. ISO/IEC 27037: Directrices para la recolección y preservación de evidencia digital

La norma ISO/IEC 27037:2012, establece directrices esenciales para garantizar que la evidencia digital sea manejada de forma adecuada desde su identificación hasta su preservación. Este es un estándar internacional que contiene procesos que abordan la integridad, autenticidad y validez de la evidencia digital de manera que sea admisible en un procedimiento legal o administrativo [29]. Los principios en los que se basa esta norma son los siguientes:

- **Auditable**: Implica que todo el proceso se documente de manera que el tercero pueda verificar las acciones y los resultados obtenidos. Se puede reproducir el análisis utilizando las mismas herramientas y técnicas, y la misma data original [30].

- **Reproducible**: Requiere que la metodología empleada sea tal que otro especialista, usando el mismo proceso y diferencia sustancial en la data de entrada, obtenga los mismos resultados. Implica la validez de la evidencia para un tribunal. Requiere que aunque el proceso en su conjunto no pueda reproducirse, siguiendo los mismos procedimientos se obtiene el mismo resultado [30].

- **Defendible**: Requiere que las herramientas y las técnicas utilizadas sean justificables y aceptables en un contexto técnico y legal. Asegura que la evidencia pueda defenderse en una situación de revisión crítica [30].

Además, esta norma define las pautas de herramientas forenses y exige que las herramientas sean validadas con anticipación para errores de minimización en la adquisición y análisis de datos. De igual forma, fija las pautas sobre cómo conservar adecuadamente la cadena de custodia de la evidencia y la capacidad debido a que se asegura la existencia de un archivo completo de cada acción que se haga con los datos digitales. Este estándar es aplicable a ambientes físicos como laboratorios forenses y ambientes lógicos virtuales como se mencionó, teniendo en cuenta que hoy en día

plataformas basadas en la nube y dispositivos móviles. Se puede concluir que es una guía imprescindible para cualquier profesional de campo forense o de investigación de seguridad de incidentes digitales.

b. ISO/IEC 27042:2015

La norma ISO/IEC 27042:2015, es una descripción específica del análisis e interpretación de evidencia digital en la administración de justicia y procedimientos judiciales. El propósito de esta norma es garantizar la calidad del trabajo analítico en procesos técnicamente sólidos, reproducibles y legalmente defendibles. Proporciona un marco para la toma de decisiones informada para incidentes de seguridad e infracciones relacionadas con las TIC [31].

En este sentido, esta norma incluirá los conceptos de integridad, continuidad y validez referidos al análisis de la evidencia, a través de los siguientes puntos:

- **Procedimientos estructurados:** establecimiento de los pasos a seguir de forma clara para la realización del análisis de la evidencia digital, desde el inicio del proceso hasta la presentación de los resultados. Incluyendo la validación de las herramientas utilizadas y la documentación del análisis [32].

- **Diferentes interpretaciones:** promoción de la revelación de los datos con el menor sesgo posible, para que la conclusión tenga relación con el análisis de la evidencia [32].

- **Reproducción/repetibilidad:** se documentará la secuencia de pasos para que otro analista, independientemente, pueda llegar a una conclusión similar. Este último punto es importante para la validez jurídica y técnica [32].

La normativa ofrece pautas sobre la presentación de informes periciales. Esto incluye la obligatoriedad de contingencia en el criterio de debida clasificación de analistas, objetivos de la investigación, herramientas en uso, procedimientos desplegados y limitaciones encontradas mientras se realizaba el procesamiento [32]. Asimismo, la ISO/IEC 27042: 2015 enfatiza la necesidad de interpretar contextualmente la evidencia, lo que significa tomar en cuenta las condiciones bajo las cuales los datos fueron recolectados para desarrollar posibles factores influenciadores posibles en un

análisis [33]. Este enfoque integral es esencial para evitar la falla de inferir o inferir conclusiones erróneamente. Dada su amplia cobertura, los profesionales en informática forense encuentran esta valiosa norma de uso. Ayuda a garantizar que los expertos procesen evidencia digital aprobada que cumplen con los estándares para garantizar que tal información pueda usarse adecuadamente en procesos legales [32].

c. Forensic Examination of Digital Evidence: A Guide for Law Enforcement

Esta guía esta desarrollada por el National Institute of Justice (NIJ) de Estados Unidos, diseñada para proporcionar a las agencias encargadas de hacer cumplir la ley un conjunto de procedimientos y protocolos para el examen de evidencia digital [34].

- Su propósito es garantizar que el manejo de la evidencia digital sea realizado de manera sistemática, asegurando su integridad y validez para su admisión en procedimientos legales. Entre los aspectos clave que aborda, se incluyen [34]:

- Se ofrece pautas para cada paso del proceso forense que van desde la identificación y recolección de la evidencia digital hasta su posterior análisis y presentación en un tribunal. Esta evidencia incluiría la preservación de la escena digital, la creación de imágenes forenses sólidas de los dispositivos electrónicos comprometidos, y la documentación de las acciones realizadas para conservar la cadena de custodia [34].

- Se enfatiza la importancia de utilizar solo las herramientas probadas previamente para asegurarse de que los resultados sean fiables y reproducibles [34].

- Los análisis deben ser lo más objetivos posible, basados en los hechos verificables y sin especulaciones o sesgos de ninguna forma [34].

- Reconoce que el campo de la informática forense está en constante evolución debido a los avances tecnológicos. Por lo tanto, la guía se actualiza regularmente para incorporar nuevas técnicas y herramientas relevantes [34].

d. Manual de manejo de evidencias digitales y Entornos informáticos de la organización de los Estados Americanos – OAS

Es una guía diseñada para apoyar a profesionales en el campo de la informática forense, particularmente a policías judiciales, fiscales y peritos informáticos. Establece estándares claros y procedimientos adecuados para la recolección, preservación, análisis y presentación de evidencia digital, asegurando que se mantenga su integridad y validez en contextos legales [35].

Se enfatiza seis principios básicos que deben guiar todo procedimiento relacionado con el manejo de evidencia digital [35]:

- **Documentación:** Cada acción debe ser registrada minuciosamente para mantener un registro completo del proceso.
- **Objetividad**: El análisis debe ser imparcial y basado únicamente en hechos verificables.
- **Inalterabilidad**: La evidencia debe mantenerse en su estado original para evitar cuestionamientos sobre su autenticidad.
- **Conservación**: Las condiciones de almacenamiento deben garantizar la preservación de la evidencia a largo plazo.
- **Autenticidad**: La procedencia de la evidencia debe ser verificable y rastreable.
- **Idoneidad**: Los procedimientos y herramientas utilizados deben ser técnicamente apropiados para el tipo de evidencia.

e. UNE 71505 – Sistema de Gestión de Evidencias Electrónicas (2013)

La norma **UNE 71505:2013**, publicada por la Asociación Española de Normalización y Certificación (AENOR), establece un marco para la gestión de evidencias electrónicas, asegurando su autenticidad, integridad y disponibilidad durante todo su ciclo de vida, proporciona directrices que permitan el manejo adecuado de las evidencias digitales, manteniendo su valor probatorio en procesos legales y administrativos. Maneja la importancia de preservar la autenticidad de los datos,

garantizando que permanezcan en su estado original, y la integridad, evitando cualquier alteración o pérdida [36].

f. RFC 3227 – Guía para recolectar y archivar evidencia

La RFC 3227 fue publicada en 2002 por la Internet Engineering Task Force (IETF), es una guía práctica que tenga como objetivo estandarizar la recolección y archivo de evidencia digital en investigaciones de delitos informáticos. Por razones específicas, el documento incluirá directrices que deban seguirse para garantizar la integridad, autenticidad y validez de la evidencia desde el momento de la recolección hasta donde sea posible su presentación en procedimientos legales. En relación con la integridad, el uso de la cadena de custodia será aplicable para el significado de garantizar que se ha realizado un documento para la interacción con la evidencia en curso. Por otro lado, las prácticas recomendadas de almacenamiento y transporte estarán claramente explicadas, así como la necesidad de usar herramientas y técnicas para asegurar la evidencia y minimizar las potenciales alteraciones [37].

- **Orden de Volatilidad:** La evidencia debe recolectarse siguiendo un orden que priorice los datos más efímeros. Por ejemplo, primero se captura la memoria RAM y conexiones de red activas, y posteriormente se accede a archivos almacenados en disco.

- **Preservación de la Cadena de Custodia:** Cada acción realizada con la evidencia debe ser documentada, especificando quién tuvo acceso, qué herramientas se utilizaron y en qué condiciones se manejó la información.

- **Integridad de la Evidencia:** La integridad de los datos debe verificarse mediante algoritmos hash como SHA-256 o MD5, asegurando que la evidencia no ha sido alterada.

- **Almacenamiento y Transporte Seguro:** Se deben implementar medidas para proteger la evidencia contra daños o accesos no autorizados durante su traslado o almacenamiento.

En la Tabla 4 se presenta un resumen de las metodologías presentadas de análisis forense investigadas.

Tabla 4. Resumen de las metodologías de análisis forense [29].

Norma/Guía	Propósito Principal	Características Clave	Aplicación Destacada
ISO/IEC 27037:2012	Directrices para la recolección y preservación de evidencia digital.	Auditable, reproducible, defendible, cadena de custodia, herramientas validadas.	Guía imprescindible para garantizar evidencia digital válida en procedimientos legales.
ISO/IEC 27042:2015	Análisis e interpretación de evidencia digital en procesos legales.	Procedimientos estructurados, interpretaciones objetivas, reproducibilidad, informes periciales.	Establece un marco técnico y legal para análisis de evidencia digital.
Forensic Examination of Digital Evidence (NIJ)	Procedimientos y protocolos para el examen de evidencia digital.	Preservación de cadena de custodia, herramientas validadas, interpretación objetiva, actualización constante.	Diseñada para agencias de cumplimiento de la ley en manejo de evidencia digital.
Manual OAS	Normas claras para recolección, análisis y presentación de evidencia digital.	Documentación, objetividad, inalterabilidad, conservación, autenticidad, idoneidad.	Apoyo para fiscales, peritos y policías judiciales en procedimientos forenses.
UNE 71505:2013	Gestión de evidencias electrónicas con autenticidad e integridad.	Autenticidad, integridad, disponibilidad, manejo adecuado de evidencias digitales.	Gestión adecuada de evidencias en procesos legales y administrativos.
RFC 3227	Estandarizar recolección y archivo de evidencia digital.	Orden de volatilidad, preservación de cadena de custodia, integridad con algoritmos hash, almacenamiento seguro.	Guía para preservar y transportar evidencia en investigaciones de delitos.

1.3.10 Infraestructura Cloud

Un modelo Cloud se basa en un área tecnológica que permite a los proveedores ofrecer servicios informáticos a través de internet, impulsado por el crecimiento de las comunicaciones en línea. En lugar de adquirir hardware o software costoso, los usuarios y las empresas pueden almacenar datos y acceder a aplicaciones en la nube por un costo reducido. Los proveedores de la nube se encargan de manera eficiente de administrar y proteger los datos, lo que mejora la seguridad y la eficiencia. Las empresas utilizan también el modelo para minimizar el gasto en infraestructura de TI al pagar por la utilización del software según la demanda, lo que resulta más barato que las instalaciones locales. Hay también varios modelos de computación en la nube que combinan con las necesidades empresariales descritas en la Tabla 5 [38].

Tabla 5. Modelos de infraestructura Cloud [38].

Modelos de infraestructura Cloud	**IaaS**	**SaaS**	**PaaS**
Definición	Ofrece recursos como servidores virtuales y almacenamiento a través de la nube. Es como alquilar infraestructura física pero gestionada por el proveedor de servicios.	Proporciona aplicaciones listas para usar directamente desde la nube, sin necesidad de instalarlas o configurarlas. Ejemplo: correo electrónico o herramientas de oficina en línea.	Ofrece una plataforma para desarrollar, ejecutar y gestionar aplicaciones sin preocuparse por la infraestructura subyacente.
Ventajas	- Permite crear servidores en la nube según las necesidades. - Ofrece flexibilidad para gestionar recursos con herramientas específicas (API).	- Facilita el uso de aplicaciones sin instalaciones. - Ideal para soluciones completas como software empresarial (ERP).	- Es fácil de usar y acelera el desarrollo de aplicaciones web. - Paga solo por los recursos utilizados.
Desventajas	- Puede ser complejo de administrar si no se tiene experiencia. - El mantenimiento recae parcialmente en el usuario.	- No permite personalizar o modificar el software más allá de lo permitido por el proveedor.	- Genera dependencia del proveedor, lo que puede limitar la flexibilidad de integración con otros sistemas.

a. SaaS

En el caso de este modelo, el usuario compra una cuenta de computación en la nube y selecciona las aplicaciones que desea instalar. No realiza ninguna tarea en una máquina local, sino en un servidor remoto que existe en la nube. Google Apps for Education y Microsoft Office 365 son dos ejemplos de servicios basados en la nube [38].

- ***Nube Pública (Public Cloud)***

En este modelo, la infraestructura es gestionada por proveedores externos como Amazon Web Services (AWS), Google Cloud, o Microsoft Azure. Las aplicaciones SaaS se ejecutan en servidores compartidos y los usuarios acceden a ellas a través de internet [38].

- ***Nube Privada (Private Cloud)***

En una nube privada, la infraestructura está dedicada exclusivamente a una organización, lo que proporciona mayor control y personalización. Algunas empresas

prefieren este enfoque para garantizar el cumplimiento de normativas o mejorar la seguridad [38].

- ***Nube Híbrida (Hybrid Cloud)***

Combina infraestructura de nube pública y privada. Las aplicaciones SaaS pueden utilizar este modelo cuando las empresas quieren mantener ciertos datos o aplicaciones sensibles en una nube privada mientras aprovechan los beneficios de la nube pública para otros servicios [38].

b. IaaS

IaaS (Infraestructura como Servicio) es un modelo de computación en la nube donde un proveedor alquila recursos de infraestructura como servidores, almacenamiento y redes a través de internet. Los clientes pueden utilizar estos recursos para instalar sus propios sistemas operativos, aplicaciones y configurar su entorno sin tener que gestionar el hardware físico [38].

c. PaaS

El modelo PaaS (Plataforma como Servicio), el cliente, como una empresa de desarrollo web, paga por una cuenta con un proveedor de servicios en la nube que ofrece un entorno personalizado según sus necesidades específicas como la instalación de herramientas de desarrollo web necesarias, la configuración del entorno de desarrollo y pruebas, entre otros [38].

1.3.11 Seguridad y Custodia de Archivos en Infraestructura Cloud

La gestión de archivos digitales en la nube es fundamental para garantizar la seguridad y la integridad de los datos, especialmente en entornos forenses. En este contexto, Amazon Web Services (AWS) ofrece una infraestructura robusta y segura para el almacenamiento, protección y gestión eficiente de datos [39].

a. Servicios de almacenamiento en AWS

Existen servicios de almacenamiento en AWS han demostrado ser esenciales para la preservación y gestión de evidencias digitales. Por ejemplo:

- **Amazon S3 (Simple Storage Service):** Este servicio se utilizó para almacenar imágenes forenses de discos duros y registros de actividades capturados durante las simulaciones de ciberataques. La alta disponibilidad y durabilidad de S3 garantizaron que las evidencias permanecieran íntegras y accesibles para el análisis posterior [39].

- **AWS Backup:** Se utilizó para automatizar la creación de copias de seguridad de los buckets de S3 donde se almacenaban los datos críticos, permitiendo restaurar evidencias en caso de fallas o pérdidas accidentales. Este servicio también facilita la retención de datos durante el tiempo requerido por normativas legales o procedimientos judiciales [40].

b. Prácticas de seguridad

El modelo de seguridad de AWS se basa en un enfoque de responsabilidad compartida:

- **AWS:** Garantiza la seguridad de la infraestructura subyacente.

- **Cliente:** Es responsable de la configuración segura de sus datos y aplicaciones [40].

Para proteger la información, AWS recomienda:

- **Cifrado de datos:** Tanto en reposo como en tránsito, utilizando herramientas como AWS Key Management Service (KMS) [41].

- **Gestión de accesos:** Implementar políticas de acceso mediante AWS Identity and Access Management (IAM) y habilitar autenticación multifactor (MFA) [41] .

- **Monitoreo y auditoría:** Utilizar servicios como AWS CloudTrail para rastrear cambios y actividades [42].

AWS Backup fue implementado para automatizar la retención de copias de seguridad de imágenes forenses, permitiendo a los investigadores restaurar datos críticos de manera rápida y eficiente durante procedimientos legales. AWS puede ser una

plataforma esencial para cumplir con los altos estándares de seguridad, escalabilidad y eficiencia requeridos en investigaciones forenses [42].

El uso de AWS en contexto forense permite:

- Garantizar la integridad y seguridad de las evidencias digitales.
- Facilitar el escalado de recursos según las necesidades del análisis.
- Implementar mecanismos avanzados de control de acceso y auditoría.

1.4 Objetivos

1.4.1 Objetivo general

Implementar un Testbed para el aprendizaje de informática forense.

1.4.2 Objetivos específicos

- Analizar las técnicas y metodologías actuales utilizadas en el análisis de informática forense.
- Implementar una infraestructura Cloud para los laboratorios de análisis forense.
- Elaborar prácticas con procedimientos y recomendaciones detalladas para la ejecución efectiva del análisis forense en una red virtual.

CAPÍTULO II. METODOLOGÍA

2.1 Materiales

Para el desarrollo del proyecto, se emplearon diversas tecnologías y herramientas especializadas que permitieron replicar escenarios cibernéticos, recolectar evidencia digital y realizar un análisis. Entre estas herramientas destacan Slowloris, y Bettercap, utilizadas para simular ataques como fuerza bruta DoS y MITM. Además, se emplearon Wireshark para la captura de tráfico de red. En la etapa de almacenamiento y transferencia de datos, se utilizó Amazon S3, junto con algoritmos de hash como SHA-256 para garantizar la integridad de la evidencia.

El laboratorio forense se diseñó utilizando capacidades de virtualización en un entorno local, ejecutado en un único equipo con recursos suficientes para gestionar múltiples máquinas virtuales. Se configuraron entornos específicos con sistemas operativos Ubuntu y Kali Linux, los cuales se ejecutaron sobre plataformas de virtualización como VMware Workstation. La elección de este entorno permitió crear simulaciones controladas y reproducibles, optimizando el uso de recursos y asegurando un control preciso de las variables experimentales. Además, la integración con servicios en la nube como AWS amplió las capacidades del laboratorio, permitiendo escalabilidad y un análisis más robusto en entornos de alta disponibilidad.

2.2 Métodos

2.2.1 Modalidad de la investigación

El proyecto adoptó un enfoque aplicado mediante el diseño e implementación de un laboratorio forense que operó en un entorno local, utilizando un equipo con capacidades de virtualización. Este laboratorio permitió replicar escenarios de ataques cibernéticos y recolectar evidencia digital utilizando tecnologías accesibles y configuraciones reproducibles. Durante el desarrollo, se configuraron máquinas virtuales con sistemas operativos Ubuntu y Kali Linux, donde se simularon ataques como fuerza bruta como DoS y MITM, empleando herramientas especializadas como

slowloris y bettercap. Posteriormente, la evidencia recolectada, incluyendo tráfico de red y discos comprometidos, fue transferida a Amazon S3, garantizando su integridad mediante el uso de hashes SHA-256. Finalmente, los datos fueron procesados en instancias de Amazon EC2, permitiendo un análisis avanzado que facilitó la detección de patrones y la reconstrucción de eventos.

Se llevó a cabo una revisión exhaustiva de literatura académica, informes técnicos y estudios de caso previos relacionados con la informática forense y la ciberseguridad. Esta revisión permitió identificar metodologías, herramientas y mejores prácticas que resultaron esenciales para la recolección y el análisis de evidencia digital. Los resultados de esta investigación bibliográfica sirvieron como base para el diseño del laboratorio, asegurando que se siguieran estándares reconocidos en la simulación de ataques y el análisis forense. Además, se consideraron investigaciones recientes sobre el uso de servicios en la nube y herramientas escalables, lo que enriqueció el enfoque y validó la integración de tecnologías modernas en el proyecto.

El enfoque experimental se centró en replicar incidentes cibernéticos en un entorno controlado para analizar variables críticas relacionadas con la recolección y el procesamiento de evidencia digital. Se configuraron escenarios específicos que incluyeron la captura de tráfico de red durante los ataques y la generación de imágenes forenses de discos comprometidos, utilizando herramientas como Wireshark. La transferencia de los datos recolectados a Amazon S3 fue evaluada para garantizar la seguridad y la integridad mediante procedimientos de verificación con algoritmos de hash. Mediante las instancias que proporciona Amazon EC2, se realizaron los análisis detallados dando un enfoque experimental que permitió validar la funcionalidad del laboratorio y asegurar que las soluciones implementadas fueran aplicables a escenarios reales.

2.2.2 Recolección de información

Con el propósito de diseñar escenarios de ataque, se llevaron a cabo actividades centradas en la simulación de ataques y la experimentación con datos en un entorno controlado. Esto permitió obtener información relevante y replicable para analizar

casos típicos de investigación forense, utilizando herramientas especializadas que garantizaron la calidad y la integridad de los datos.

Tabla 6. Criterios de recolección de información.

Criterio	**Descripción**
¿Para qué?	Para recolectar evidencia y realizar análisis forense que permitan evaluar riesgos y desarrollar soluciones prácticas.
¿De qué personas u objetos?	Sistemas y dispositivos virtuales que incluyen máquinas virtuales
¿Cómo?	Mediante simulaciones y la experimentación de datos en entornos controlados.
¿Con qué?	Con herramientas que permitan el análisis forense y la evaluación de riesgos en escenarios replicables.
¿Cuándo?	Durante el periodo de septiembre de 2024 a febrero de 2025.
¿Dónde?	En la ciudad de Ambato.

2.2.3 Procesamiento y análisis de datos

La información recabada en la investigación fue procesada y analizada para la obtención de resultados claros y concisos, por ello se preconizaron acorde a lo siguiente:

- Analizar la información compilada.
- Depurar la información.
- Procesar la información.
- Elaborar una arquitectura esquematizada.
- Presentación de resultados de acuerdo con los objetivos planteados.

CAPÍTULO III. RESULTADOS Y DISCUSIÓN

3.1 Introducción

En la actualidad, la creciente sofisticación de los ciberataques requiere enfoques innovadores para su análisis y comprensión. La informática forense se posiciona como una herramienta clave para identificar las tácticas, técnicas y procedimientos utilizados por atacantes, así como para preservar y analizar evidencias digitales que puedan ser útiles en procesos legales y en la mejora de la seguridad. Este trabajo propone la creación de un laboratorio forense diseñado para simular ataques cibernéticos en un entorno controlado, recolectar evidencia digital y realizar análisis forense en la nube.

Para la implementación, se ha adoptado la metodología de la RFC 3227: Guidelines for Evidence Collection and Archiving, que proporciona directrices claras para la recolección, preservación, transferencia y análisis de evidencia digital. Esta metodología se eligió debido a su énfasis en la integridad de los datos y la trazabilidad del manejo de las evidencias, garantizando que los resultados sean reproducibles y admitidos en un contexto legal o administrativo.

El laboratorio se implementa en una máquina local equipada con capacidades de virtualización, lo que permite la ejecución de múltiples máquinas virtuales (VMs). Estas VMs desempeñan roles diferenciados: unas como sistemas comprometidos que simulan ciberataques, y otras como estaciones forenses responsables de recolectar y analizar las evidencias digitales. Durante la recolección, se emplearon herramientas específicas como Wireshark para la captura de tráfico de red y comandos *dcfldd* para la creación de imágenes forenses de discos. Una vez recolectada, la evidencia se transfiere a la nube de AWS (Amazon Web Services), donde se realizan análisis más profundos y se garantiza el almacenamiento seguro mediante Amazon S3.

Este capítulo detalla la infraestructura utilizada, las herramientas seleccionadas y las etapas seguidas en la implementación del laboratorio. Asimismo, se describen los escenarios simulados y la metodología aplicada para realizar la captura, análisis y reporte de evidencias digitales.

3.2 Requisitos de Hardware para el Laboratorio Forense

El hardware del laboratorio debe estar alineado con las necesidades de procesamiento y almacenamiento exigidas por las herramientas forenses. Los requisitos mínimos incluyen:

- **Procesadores**: Multinúcleo con capacidad para manejar cargas intensivas.
- **Memoria RAM**: Al menos 16 GB para ejecutar simultáneamente varias máquinas virtuales.
- **Almacenamiento SSD**: Crucial para el análisis rápido de grandes volúmenes de datos.

Estos componentes aseguran un rendimiento óptimo en tareas como la creación de imágenes de discos, el análisis de memoria volátil y el procesamiento de paquetes de red.

3.3 Metodología utilizada para el laboratorio forense

Se ha decidido usar el modelo RFC 3227 donde se centra en proporcionar un marco lógico para la realización de análisis forense digital. Este modelo se puede integrar con la metodología práctica de un laboratorio forense, asegurando que cada etapa respete principios clave de integridad y trazabilidad.

El laboratorio forense fue diseñado para operar en un entorno local, utilizando un único equipo con capacidades de virtualización. Este laboratorio tiene como propósito replicar escenarios de ataques cibernéticos y recolección de evidencia, empleando tecnologías accesibles y configuraciones que sean reproducibles por estudiantes y profesionales detallada en la Figura 2.

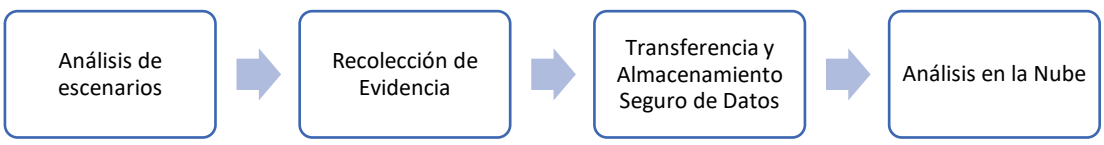


Figura 2. Metodología del desarrollo del proyecto.

Se describe cómo implementar cada fase del modelo en el laboratorio de análisis forense:

a. Análisis de Escenarios

Durante esta etapa, la RFC 3227 se utilizó para identificar las fuentes de evidencia digital en los escenarios de ataque simulados. Se definió un orden de recolección priorizando los datos más volátiles, como las conexiones de red activas y los registros temporales, asegurando que estos fueran capturados antes de ser sobrescritos.

b. Recolección de Evidencia

En esta etapa, la metodología estableció cómo preservar la evidencia utilizando herramientas forenses como dd para crear imágenes exactas de los discos. Se capturaron paquetes de red con herramientas como Wireshark, siguiendo las recomendaciones para minimizar alteraciones en los datos originales. Además, se documentaron de manera rigurosa todas las acciones realizadas para garantizar la trazabilidad.

c. Transferencia y Almacenamiento Seguro de Datos

La RFC 3227 proporcionó directrices para la transferencia y almacenamiento seguro de los datos recolectados. Se generaron hashes (SHA-256 y MD5) antes y después de la transferencia para verificar la integridad de los datos, y se utilizó encriptación para proteger la evidencia durante su traslado a Amazon S3.

d. Análisis en la Nube

Aunque la RFC 3227 no abordó técnicas avanzadas de análisis, su énfasis en la preservación de la evidencia permitió que los datos procesados en las instancias EC2 fueran fiables. Esto facilitó la reconstrucción de eventos y la detección de patrones en el tráfico de red, asegurando la validez de los hallazgos.

3.4 Arquitectura general del laboratorio forense

El presente proyecto se desarrolla en cuatro etapas principales, como se muestra en la Figura 3. En la primera etapa, **Análisis de Escenarios**, se configura un entorno de

prueba para simular ataques informáticos utilizando máquinas virtuales locales (Ubuntu y Kali Linux). Durante esta etapa se define el objetivo del ataque y se preparan las condiciones necesarias para recolectar evidencias digitales relevantes.

En la segunda etapa, **Recolección de Evidencia**, se capturan datos críticos como el tráfico de red, empleando herramientas como Wireshark, y se crean imágenes forenses de discos comprometidos utilizando comandos como `dcfldd`. Estos datos se almacenan temporalmente en entornos locales mientras se verifica su integridad y se documenta el proceso para preservar la cadena de custodia.

La tercera etapa, **Preservación y Transferencia**, asegura que la evidencia sea transferida a un entorno seguro en la nube, específicamente utilizando el servicio Amazon S3. Durante esta fase se generan valores hash (SHA-256 o MD5) para verificar la integridad de los datos antes y después de la transferencia, garantizando que no hayan sufrido alteraciones durante el proceso.

La cuarta etapa, **Análisis en la Nube**, la evidencia digital es procesada en instancias escalables de Amazon EC2. En esta fase se utilizan herramientas avanzadas para realizar análisis forense, como la detección de patrones en el tráfico de red y la reconstrucción de eventos, permitiendo extraer hallazgos clave y atribuir responsabilidades.

La Figura 3 destaca la relación entre cada etapa del proceso y cómo interactúan para garantizar un manejo riguroso de la evidencia digital, desde su captura inicial hasta su análisis avanzado.

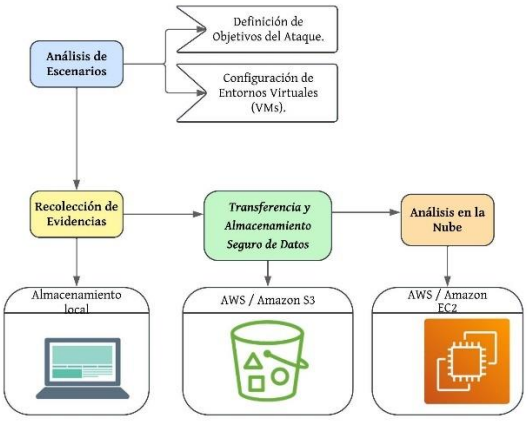


Figura 3. Esquema general del laboratorio forense digital.

3.4.1 Análisis de escenarios

El proceso inicia con la configuración de un entorno controlado que permita la simulación de diversos tipos de ciberataques. Este entorno se desarrolló tanto en máquinas virtuales locales como en instancias de Amazon Web Services (AWS). Se utilizaron sistemas operativos como Ubuntu y Kali Linux, distribuciones reconocidas en el ámbito de la seguridad informática por su robustez y adaptabilidad.

Los ataques implementados incluyen técnicas ampliamente documentadas, como ataques de fuerza bruta y simulaciones de denegación de servicio distribuida (DoS). Para su ejecución, se emplearon herramientas especializadas como Hydra (para pruebas de autenticación) y slowloris (generación de tráfico malicioso). Estas simulaciones buscan reproducir condiciones reales en las que las infraestructuras pueden verse comprometidas, generando evidencia auténtica y contextual para el análisis.

Esta etapa se diseñó con el objetivo de obtener datos relevantes en condiciones reproducibles, siguiendo un enfoque metodológico que permite estudiar los impactos de las amenazas sin comprometer la seguridad de los sistemas reales.

El diseño y operación del laboratorio forense requiere un conjunto de herramientas especializadas, tanto para la simulación de ataques como para la recolección y análisis de evidencia digital. Estas herramientas se clasifican según su función principal dentro del laboratorio:

e. Instalación de sistemas operativos

En esta sección se detalla la selección e instalación de los sistemas operativos utilizados en el desarrollo del laboratorio de pruebas de ciberseguridad, especificando sus propósitos en el contexto del proyecto:

- **Kali Linux**: Se implementó este sistema operativo especializado para la realización de pruebas de penetración y simulaciones de ataques cibernéticos. Su amplio conjunto de herramientas contribuyó a evaluar vulnerabilidades y realizar análisis de seguridad.

- **Ubuntu Server**: Este sistema se configuró como servidor víctima, proporcionando un entorno controlado para el análisis de intrusiones. Además, se utilizó para recolectar registros de actividad, facilitando la identificación de patrones de ataque y pruebas de respuesta.

3.4.2 Recolección de Evidencia

Una vez descritos y analizados los distintos tipos de escenarios, se procedió a la recolección de evidencia digital. Esta etapa incluye la captura de tráfico de red generado durante las simulaciones y la creación de imágenes forenses de los discos de las máquinas comprometidas.

a. Captura de tráfico de red

La captura de tráfico se realizó mediante Wireshark, una herramienta ampliamente utilizada en el análisis de redes que permite identificar patrones sospechosos, conexiones no autorizadas y posibles transferencias de datos maliciosos.

b. Recolección de evidencia de discos duro

La recolección de evidencia de discos duros se llevó a cabo empleando técnicas de imagen forense, siguiendo las mejores prácticas de la disciplina para garantizar la integridad de los datos. Este proceso se realizó en las máquinas virtuales comprometidas, alojadas en VMware Workstation, mediante los siguientes pasos:

- Se suspende la ejecución de la máquina virtual afectada para preservar el estado exacto del sistema en el momento del incidente indicado en la Figura 4.

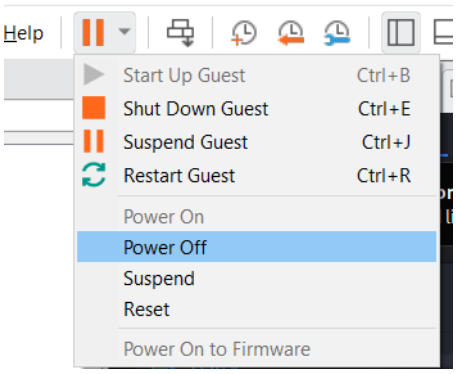


Figura 4. Suspensión del sistema comprometido.

- Realizar la copia de los discos virtuales de las maquinas comprometidas almacenados en formato VMDK (Virtual Machine Disk), que contiene la información del sistema. Este punto se realiza agregando un nuevo disco a otra Maquina como se observa en la Figura 5.

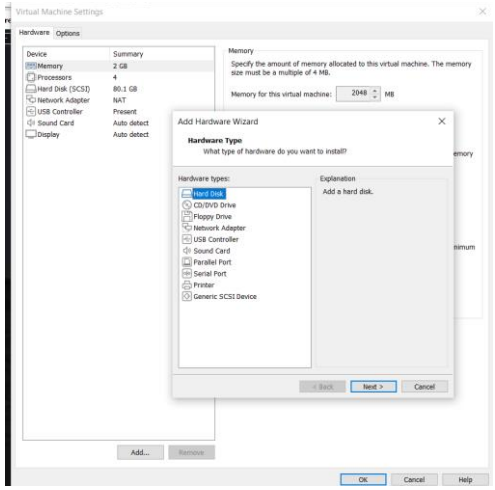


Figura 5. Agregar nuevo disco duro a una maquina Kali Linux.

Este disco debe ser agregado como un disco virtual existente ya que la máquina virtual comprometida genera discos VMDK el cual se almacena información de lo que ha pasado en el sistema. Al momento de agregar el disco existente es importante mantener el formato existente como se muestra en la Figura 6 ya que podría dañar el sistema actual

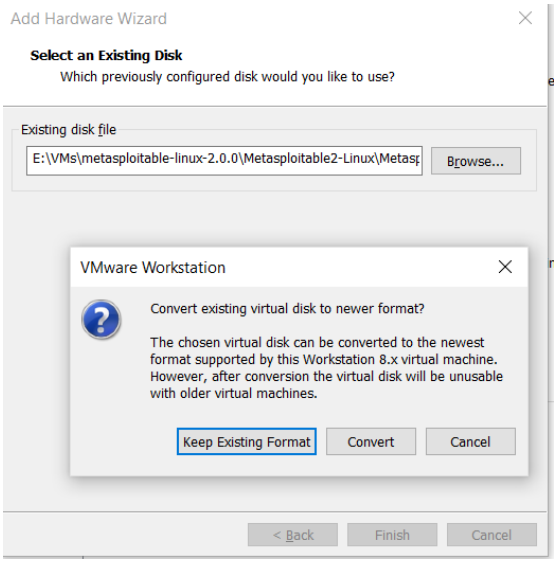


Figura 6. Nuevo disco agregado al sistema.

Una vez agregado el disco se enciente la máquina virtual y se verifica que se encuentre en el sistema con el comando *lsblk*. Se puede observar en la Figura 7 que el sistema actual es representado por el disco sda1 el cual tiene un punto montado como "/" donde indica que es el sistema instalado en la máquina virtual, mientras que el disco *sdb* pertenece al disco recién agregado del sistema comprometido.

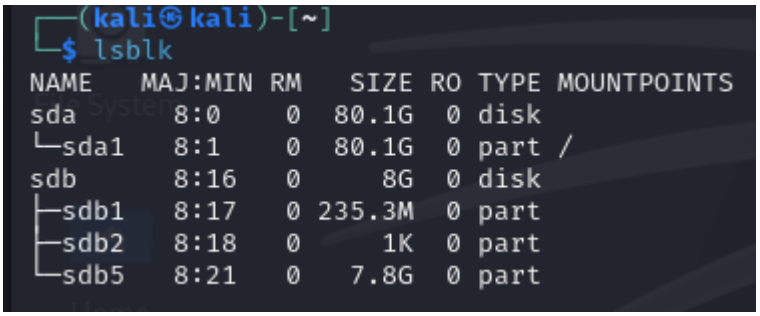


Figura 7. Información de particiones de discos del sistema.

El disco sdb tiene que someterse a una copia de seguridad para poder trabajar con él y no comprometer la evidencia original por lo que se realiza una copia del disco con el comando dcfldd mostrado en la Figura 8, agregando el destino y nombre de la copia del disco y además se agrega un documento de texto que me indique hash de tipo SHA-256 para su integridad de datos como corresponde en un análisis forense.



Figura 8. Copia del disco sdb.

Cada evidencia recolectada fue etiquetada y preservada siguiendo principios de cadena de custodia digital indicado en la Figura 9, lo que asegura su autenticidad y fiabilidad para análisis posteriores. El objetivo de esta etapa fue garantizar la obtención de datos íntegros y completos, indispensables para realizar un análisis forense riguroso y documentado.



Figura 9. Integridad de los datos con SHA-256.

3.4.3 Transferencia y almacenamiento seguro de datos

Con las evidencias recolectadas, se procedió a su transferencia a un entorno seguro en la nube, utilizando Amazon S3 como repositorio centralizado. La transferencia se realizó mediante el uso de AWS CLI, su instalación se realiza en la máquina virtual local como se indica en la Figura 10. Esta herramienta permitió una operación controlada en la cadena de custodia aplicada a los archivos y cada archivo se verifico su integridad mediante el uso de algoritmos de hash SHA-256 para calcular valores de integridad antes y después del traslado.



Figura 10. Instalación de ASW CLI.

Los datos transferidos se almacenaron dentro del bucket S3 configurado con políticas de acceso basadas en roles IAM (Identify and Access Management), esta configuración se basó en agregar políticas de permisos como *AmazonS3FullAccess* indicado en la Figura 11 permitiendo así una restricción de acceso a usuarios autorizados. Este enfoque asegura que los archivos permanecieran protegidos en casos de acceso no autorizado.

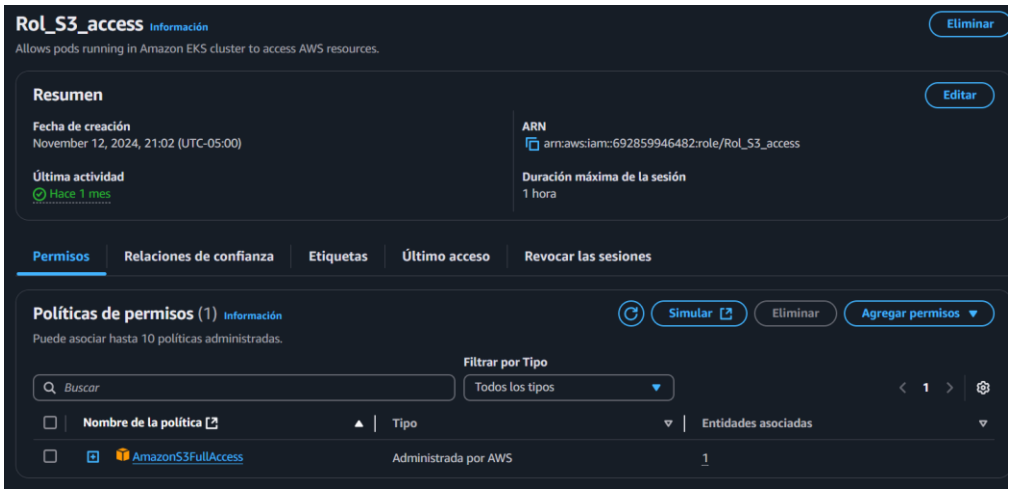


Figura 11. Configuración de Roles AWS.

Desde la maquina local (Kali Linux) donde se encuentren las evidencias, se configura el entorno de aws para poder enviar archivos a la nube, en este caso es el bucket S3. Para esto se realiza una configuración por consola con el comando *aws configure*, el cual solicita algunos parámetros como:

- AWS Access key ID: Esta es una ID de una clave de acceso que tiene la cuenta AWS, se puede crear una en "credenciales de seguridad" > "claves de acceso" el cual únicamente se genera un ID y una clave, indicado en la Figura 12.
- AWS Secret Access Key: Es la clave asociada con el Access Key ID generado.
- Default región name: Es la región en la que se encuentra la cuenta de AWS, en este caso, *us-east-1*.
- Default output format: Define el formato de la salida de comandos, se configuro como "text".

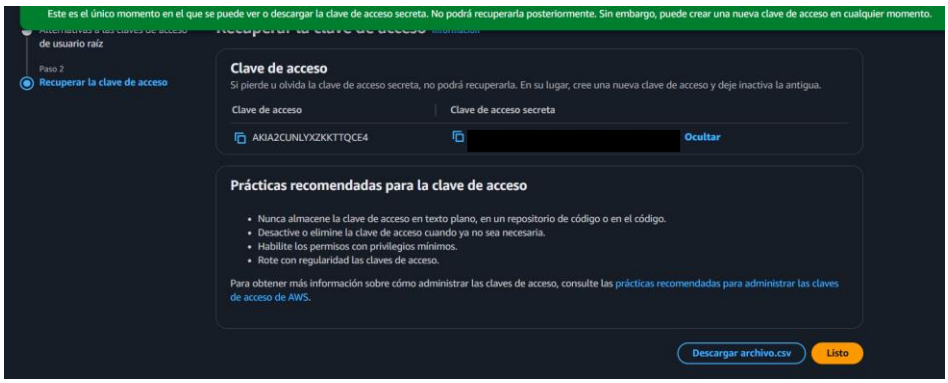


Figura 12. Generación de clave de acceso.

La transferencia de archivos desde una maquina local virtual al bucket S3 se realiza mediante comandos de AWS CLI indicado en la Figura 13.

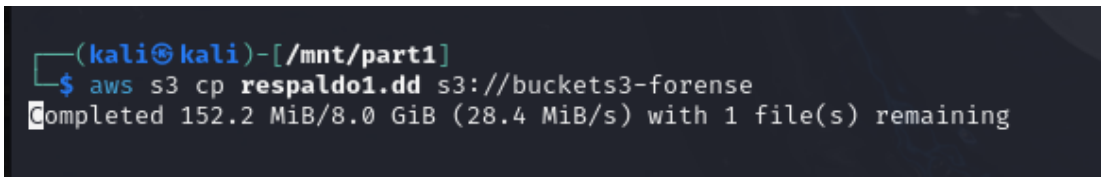


Figura 13. Transferencia de archivos al bucket S3.

Desde el bucket S3, los datos han sido descargados a una instancia de análisis en AWS EC2, la cual está configurada con un sistema operativo Kali Linux. La transferencia

de realizo mediante el uso de AWS CLI, manteniendo el protocolo HTTPS/TLS como medida de seguridad de tránsito.

3.4.4 Análisis en la Nube

La última etapa consistió en el procesamiento y análisis avanzado de las evidencias en instancias configuradas en Amazon EC2. Estas instancias fueron adaptadas para ejecutar herramientas y comandos esenciales como: dd, dcfldd, y mmls, utilizadas para procesar imágenes de disco, identificar particiones y analizar estructuras de sistemas de archivos. También se emplearon comandos como file y mount para verificar tipos de sistemas de archivos y montar imágenes para su exploración detallada.

El análisis permitió identificar indicadores de compromiso, como registros de procesos sospechosos y patrones en el tráfico de red. Además, facilitó la reconstrucción de eventos cronológicos de los ataques y la extracción de información clave almacenada en las imágenes de disco.

El uso de la nube permitió escalar los recursos según la demanda y aseguró un entorno seguro para el almacenamiento y procesamiento de la evidencia. Este enfoque maximizó la eficiencia del análisis y contribuyó al desarrollo de reportes técnicos documentados, útiles en procedimientos legales, auditorías o proyectos educativos futuros.

3.5 Cadena de custodia por AWS

Para facilitar el análisis avanzado en un entorno seguro, la imagen forense se transfirió a Amazon S3 utilizando el comando *aws s3 cp*. Esto aseguró el cifrado en tránsito (TLS/SSL).

La creación y transferencia de la copia forense garantizaron la preservación de la evidencia original, permitiendo realizar análisis detallados en entornos controlados sin comprometer la integridad de los datos. Este proceso es fundamental para cualquier investigación forense profesional.

3.6 Desarrollo de las prácticas de laboratorio

Se realizaron siete prácticas enfocadas en el análisis forense digital, diseñadas para replicar escenarios reales y fortalecer las habilidades técnicas de los participantes. Estas prácticas abarcaron desde la recolección de evidencia hasta su análisis avanzado, proporcionando un enfoque integral y aplicado al aprendizaje en entornos controlados.

3.6.1 Práctica 1: Denegación de servicios

En este ejercicio práctico, se investigó un ataque de Denegación de Servicio (DoS) llevado a cabo contra un servidor Ubuntu. El ataque, originado desde una máquina atacante con Kali Linux, tenía como objetivo saturar los recursos del servidor víctima mediante múltiples solicitudes simultáneas, imposibilitando el acceso de usuarios legítimos al servicio.

El análisis forense se realizó para identificar las técnicas empleadas por el atacante, evaluar el impacto en los recursos del servidor y proponer medidas para mitigar futuros incidentes de este tipo.

a. Objetivo

Desarrollar un procedimiento forense para identificar evidencia de un ataque de Denegación de Servicio (DoS) y determinar su impacto en un sistema Linux.

b. Metodología

El análisis forense se desarrolló siguiendo un enfoque estructurado para preservar la integridad de la evidencia y obtener información detallada sobre el ataque. Los pasos realizados incluyeron la recolección de datos, análisis de logs y validación de la configuración del sistema.

- ***Monitoreo de Recursos Afectados***

Durante el ataque, se ejecutaron comandos de monitoreo en tiempo real para evaluar el impacto en los recursos del sistema. Herramientas como *htop* permitieron observar el consumo inusual de CPU, memoria y ancho de banda de red en la Figura 14.

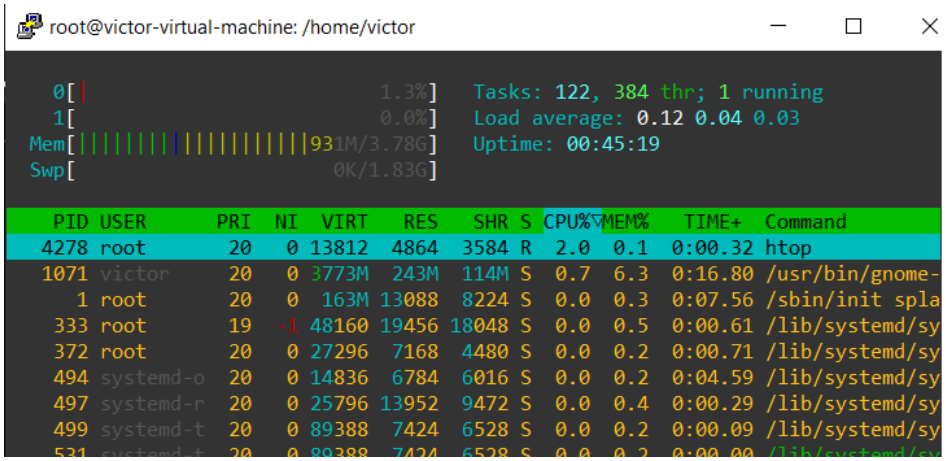


Figura 14. Análisis del uso de la memoria por el comando htop.

- ***Análisis de Logs del Servidor***

Se revisaron los registros de acceso del servidor web (/var/log/apache2/access.log) para identificar patrones inusuales en las solicitudes. Se detectaron múltiples peticiones repetitivas desde una única dirección IP (192.168.80.167), lo que indica un ataque de tipo Flood.

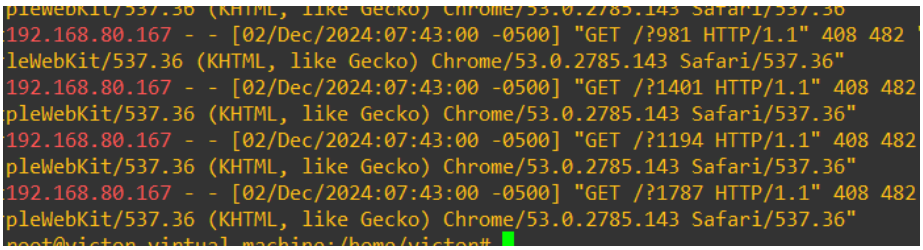


Figura 15. Registros de acceso (.log).

La dirección IP atacante realizó miles de solicitudes en un corto período de tiempo, sobrecargando al servidor, esto indica un ataque de tipo DoS (Denial of Service).

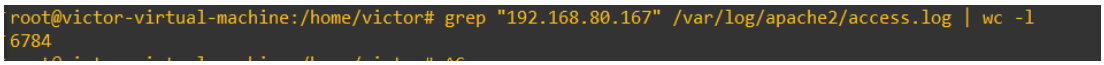


Figura 16. Solicitudes de acceso de la IP atacante.

El resultado 6784 indica que la IP 192.168.80.167 aparece un total de 6,784 veces en los logs, lo que corresponde al número de solicitudes realizadas por esta dirección IP al servidor. Este alto volumen de solicitudes confirma un comportamiento anómalo y sugiere que la IP está participando en un ataque DoS o generando tráfico malicioso.

Una vez desarrollada o culminada la práctica, se presenta un informe técnico junto con la Guía Práctica de Análisis Forense en el ANEXO A, la cual detalla los pasos utilizados para realizar un análisis forense de este tipo de ataque.

3.6.2 Práctica 2: Ataque de tipo Man in the Middle (MITM) Attack

En este ejercicio práctico, se analizó un ataque de tipo Man-in-the-Middle (MITM) llevado a cabo desde una máquina atacante con Kali Linux hacia una máquina víctima Ubuntu. El ataque se diseñó para interceptar y analizar el tráfico de red con el objetivo de capturar información sensible debido a la falta de cifrado en el tráfico HTTP de la víctima. El análisis forense busca identificar los métodos empleados por el atacante, evaluar el impacto del ataque y proponer soluciones para mitigar futuros incidentes similares.

a. Objetivo

Realizar un análisis forense detallado de un ataque Man-in-the-Middle (MITM), utilizando herramientas específicas para identificar, preservar y analizar la evidencia digital obtenida durante el ataque.

b. Metodología

El proceso de análisis forense se desarrolló siguiendo las mejores prácticas para preservar la integridad de la evidencia y obtener información clave sobre las actividades del atacante. A continuación, se detallan los pasos realizados: Se ejecutó el comando *arp -a* en la máquina víctima para analizar posibles inconsistencias en la tabla ARP, representada en la Figura 17. Se encontró que la dirección IP de la puerta de enlace (192.168.80.1) estaba asociada incorrectamente con la dirección MAC de la máquina atacante (192.168.80.167), confirmando el envenenamiento ARP.

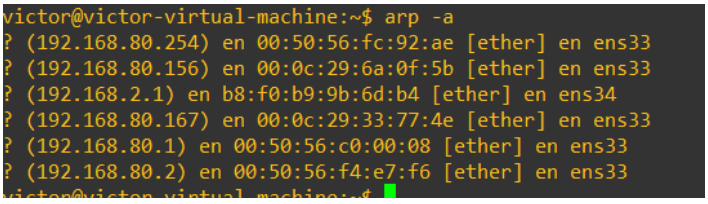


Figura 17. Tabla arp de la víctima.

Utilizando Wireshark, se capturó y analizó el tráfico ARP y HTTP de la máquina víctima. Al aplicar filtros para protocolos ARP y HTTP (arp || http), se identificaron paquetes que evidenciaron cómo el atacante redirigía el tráfico de la víctima hacia su máquina de la Figura 18. Esto permitió interceptar solicitudes HTTP, incluidas credenciales y datos sensibles.

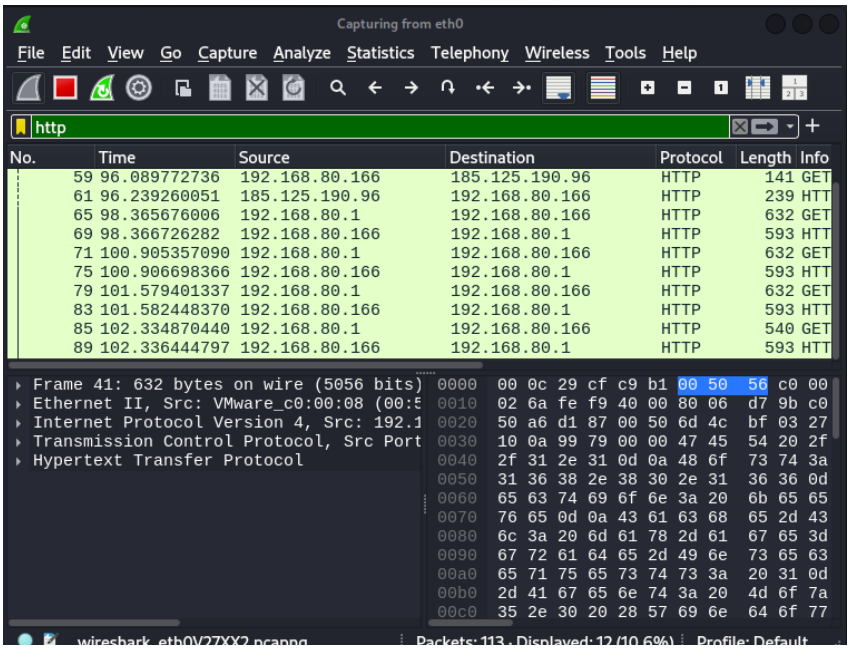


Figura 18. Solicitudes http registradas en Wireshark.

Como parte del análisis, se procedió a inspeccionar los logs de autenticación almacenados en la máquina víctima. Este paso fue fundamental para rastrear actividades relacionadas con la dirección IP identificada como sospechosa (192.168.80.167).

El análisis detallado de los registros de la Figura 19, permitió evidenciar intentos de conexión asociados al atacante, proporcionando una cronología de eventos relevantes para el ataque. Esto confirmó que la IP mencionada fue utilizada activamente durante el incidente.

```
victor@victor-virtual-machine:~$ grep "192.168.80.167" /var/log/auth.log
Dec  2 07:47:47 victor-virtual-machine sudo:     root : TTY=pts/2 ; PWD=/home/victo
r ; USER=root ; COMMAND=/usr/bin/tcpdump -i eth0 host 192.168.80.167
Dec  2 07:47:54 victor-virtual-machine sudo:     root : TTY=pts/2 ; PWD=/home/victo
r ; USER=root ; COMMAND=/usr/bin/tcpdump -i eth1 host 192.168.80.167
Dec  2 07:48:10 victor-virtual-machine sudo:     root : TTY=pts/2 ; PWD=/home/victo
r ; USER=root ; COMMAND=/usr/bin/tcpdump -i ens33 host 192.168.80.167
```

Figura 19. Extracto del log de autenticación con la ip sospechosa.

Adicionalmente, se revisaron los registros de acceso del servidor Apache, que actuó como uno de los puntos finales en la comunicación interceptada por el atacante. En los logs se observaron solicitudes provenientes de la máquina víctima (192.168.80.176), que correspondían a intentos de acceso realizados durante la ejecución del ataque.

En la Figura 20 se evidencia un análisis de estas solicitudes donde permitió identificar posibles interacciones dirigidas a recursos sensibles del servidor, evidenciando la manipulación del tráfico HTTP. Este hallazgo corroboró que el ataque tuvo un impacto directo sobre la seguridad y el funcionamiento del servidor.

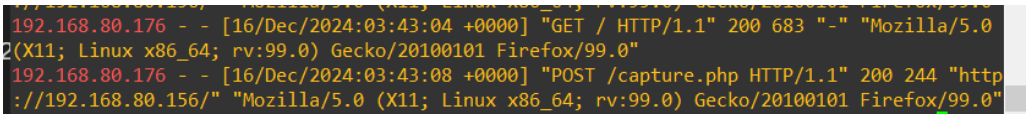


Figura 20. Solicitudes realizadas desde la dirección IP de la máquina víctima.

El último paso en el análisis incluyó la verificación de archivos críticos en el servidor, como el archivo credentials.txt ubicado en la Figura 21, que almacenaba información sensible. La revisión se centró en identificar modificaciones recientes que pudieran estar relacionadas con la actividad del atacante.

La inspección reveló que el archivo había sido accedido y posiblemente modificado durante el periodo en que se llevó a cabo el ataque. Este hallazgo refuerza la conclusión de que el atacante no solo interceptó tráfico de red, sino que también interactuó directamente con los recursos almacenados en el servidor.

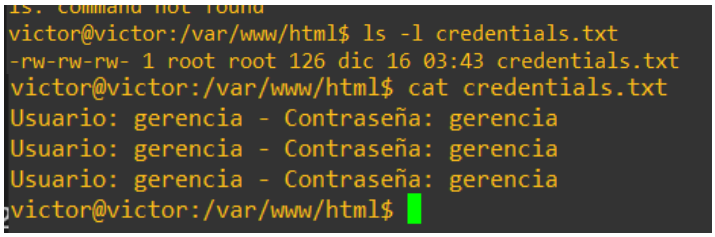


Figura 21. Archivo credentials.txt en el servidor con cambios.

Una vez desarrollada o culminada la práctica, se presenta un informe técnico junto con la Guía Práctica de Análisis Forense en el ANEXO B, la cual detalla los pasos utilizados para realizar un análisis forense de este tipo de ataque.

3.6.3 Práctica 3: Ataque con Exploit en VSFTPD (Metasploitable 2)

En este ejercicio práctico, se investigó un ataque realizado contra el servicio VSFTPD 2.3.4, un servidor FTP vulnerable que se encuentra en Metasploitable 2. El ataque fue ejecutado desde la herramienta Metasploit Framework (msfconsole), y el exploit utilizado permitió al atacante obtener acceso no autorizado al sistema con privilegios de root. Este análisis forense busca identificar las evidencias del ataque, comprender cómo se explotó la vulnerabilidad y proponer medidas de mitigación.

a. Objetivo

Realizar un análisis forense detallado de un ataque de explotación en el servicio VSFTPD en una máquina Metasploitable 2.

b. Metodología de Análisis Forense

El análisis forense se llevó a cabo siguiendo un enfoque estructurado para preservar la integridad del sistema comprometido, identificar rastros del exploit y evaluar su impacto.

- **Verificación de la Versión de VSFTPD**

La primera etapa del análisis consistió en confirmar que el servidor afectado estaba ejecutando una versión vulnerable de VSFTPD (2.3.4). Esto se logró mediante una exploración inicial con Nmap, con el comando *nmap* indicado en la Figura 22.

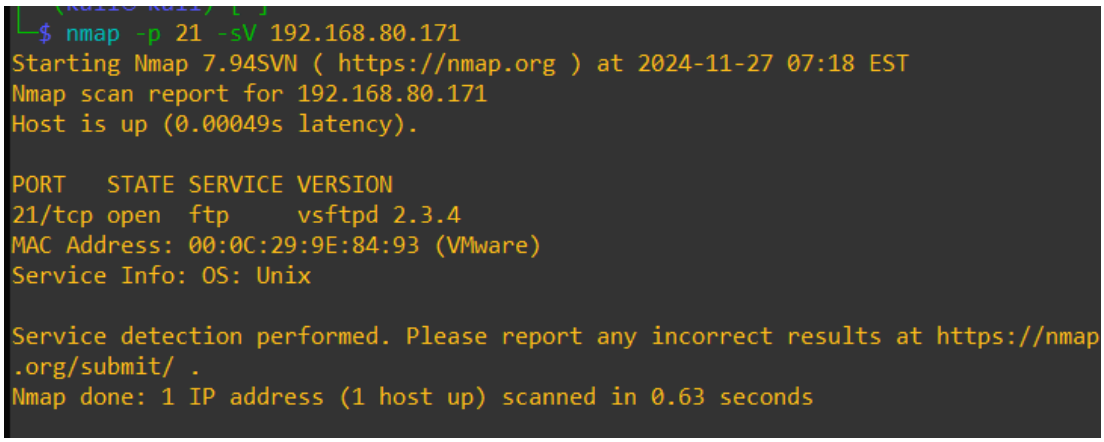


Figura 22. Análisis de puertos abiertos en la maquina víctima.

La versión 2.3.4 de VSFTPD tiene una vulnerabilidad conocida que permite al atacante abrir un backdoor y ejecutar comandos arbitrarios en el sistema.

- **Análisis de logs**

Se revisaron los registros del servicio FTP para identificar intentos de conexión sospechosos que podrían indicar el uso del exploit, para esto se debe buscar los logs que existen del servicio FTP, específicamente del vsftpd.log, este se le ve directamente en la Figura 23.

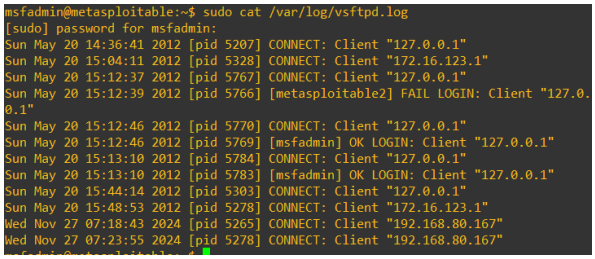


Figura 23. Accesos realizados al puerto vsftpd.log.

Durante el ataque, se identificaron conexiones inusuales con el comando netstat -antp indicado en Figura 24, esto despliega las conexiones y se puede verificar la máquina atacante (192.168.80.167) hacia un puerto TCP abierto dinámicamente en el servidor comprometido.

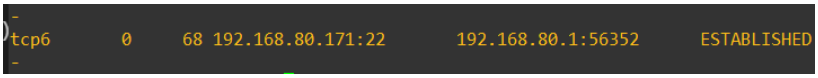


Figura 24. Conexiones establecidas del puerto TCP.

Se sabe que algunos procesos pueden ejecutar shells con privilegios de root en Figura 25, como puede ser el proceso, de esta manera se busca los procesos relacionados a este tipo de Shells.

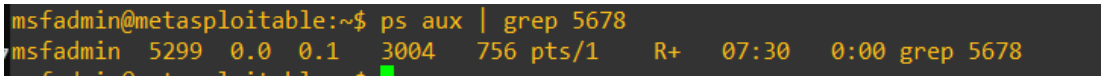


Figura 25. Conexiones establecidas a Shell con privilegios root.

Una vez desarrollada o culminada la práctica, se presenta un informe técnico junto con la Guía Práctica de Análisis Forense en el ANEXO C, la cual detalla los pasos utilizados para realizar un análisis forense de este tipo de ataque.

3.6.4 Práctica 4: Análisis forense de tráfico SMTP.

El análisis forense realizado en esta práctica se enfoca en un archivo pcap que contiene tráfico SMTP capturado durante la comunicación entre un cliente y un servidor. Este análisis tiene como objetivo identificar posibles vulnerabilidades en el servidor SMTP, reconstruir las acciones realizadas durante la conexión y evaluar la seguridad del entorno. La práctica es relevante en la detección de actividades no autorizadas, como el uso indebido de credenciales para el envío de correos electrónicos, y ofrece una visión integral sobre cómo abordar escenarios similares en entornos reales.

a. Objetivo

Analizar las acciones realizadas tras el acceso, incluyendo la autenticación y envío de correos

b. Metodología

El análisis se llevó a cabo en un entorno controlado utilizando herramientas especializadas como Wireshark. El flujo de trabajo se estructuró en las siguientes etapas:

- **Carga del archive pcap**: El archivo fue abierto en Wireshark para inspeccionar los paquetes capturados.
- **Aplicación de filtros de tráfico SMTP**: Se aplicaron los filtros tcp. port == 465 || tcp.port == 587 para aislar las conexiones relevantes del tráfico SMTP.
- **Decodificación y análisis de comandos SMTP:**

Se inspeccionaron comandos clave como AUTH LOGIN, MAIL FROM, RCPT TO y DATA como se indica en la Figura 26.

```
AUTH LOGIN
334 VXNlcm5hbWU6
User: Z3VycGFydGFwQHBhdHJpb3RzLmlu
334 UGFzc3dvcmQ6
Pass: cHVuamFiQDEyMw==
235 Authentication succeeded
```

Figura 26. Trafico capturado en wireshark.

Estas credenciales se decodificaron y se obtuvieron en texto plano, se presenta un resumen en la Tabla 7.

Tabla 7. Resumen de Credenciales y Comandos SMTP.

Comando	**Detalle**	**Observación**
AUTH LOGIN	Usuario y contraseña codificados en Base64	Credenciales interceptadas
MAIL FROM	gurpartap@patriots.in	Correo remitente validado
RCPT TO	raj_deol2002in@yahoo.co.in	Destinatario confirmado
DATA	Texto del mensaje y adjunto NEWS.txt	Contenido inspeccionado y reconstruido

Se reconstruyeron mensajes enviados y se analizó el flujo TCP reconstruido con el comando <Follow TCP Stream> en Wireshark en la Figura 27.



Figura 27. Reconstrucción de eventos de ataque a SMTP por Wireshark.

Se investigó el encabezado, cuerpo del correo y cualquier archivo adjunto incluido en los mensajes.

Hallazgos relevantes

- ***Credenciales Comprometidas***

Durante la conexión SMTP, se identificó el uso del comando AUTH LOGIN con un usuario y contraseña codificados en Base64. Al decodificar los datos, se detectaron las siguientes credenciales:

- Usuario: gurpartap@patriots.in.
- Contraseña: punjab@123

La falta de cifrado TLS permitió exponer las credenciales, facilitando su interceptación por actores malintencionados.

- ***Reconstrucción del trafico***

En el análisis realizado se reconstruyó el tráfico de un correo electrónico enviado desde la dirección **gurpartap@patriots.in** hacia **raj_deol2002in@yahoo.co.in**. El mensaje, en texto plano, incluía la siguiente frase: *"Hola, te envío un archivo pcap por SMTP. Busca el archivo adjunto."*. Adicionalmente, se identificó un archivo adjunto denominado **NEWS.txt**, el cual contenía información técnica sobre cambios en software.

Durante la transferencia del correo, se determinaron los siguientes aspectos técnicos clave:

- **Puerto del Cliente:** El cliente utilizó un puerto efímero, identificado como el 1470, para el envío.
- **Puerto y Protocolo del Servidor:** El servidor empleó el puerto estándar 25 del protocolo SMTP, sin implementar ningún tipo de cifrado en la comunicación.

Este análisis evidencia la ausencia de medidas de seguridad, como cifrado, en la transmisión del mensaje, lo que podría implicar riesgos de interceptación o alteración durante el proceso de envío.

- ***Análisis de encabezados del correo***

El análisis de los encabezados del correo electrónico permitió identificar detalles importantes sobre la estructura y el contexto del mensaje. El **Message-ID** asociado al

correo fue <000301ca4581$ef9e57f0$cedb07d0$@in>, un identificador único que permite rastrear y verificar el mensaje. Adicionalmente, se confirmó que el cliente utilizado para el envío fue **Microsoft Office Outlook 12.0**, como se especifica en el campo **X-Mailer**.

En cuanto a los horarios registrados, se observaron las siguientes marcas de tiempo:

- **Hora del Cliente:** lunes, 5 de octubre de 2009, 11:36:07 +0530.
- **Hora del Servidor:** lunes, 5 de octubre de 2009, 01:05:54 -0500.

Esto confirma que el mensaje fue enviado desde un cliente Outlook configurado correctamente, lo cual valida la legitimidad del origen del correo.

- **Evaluación de la Seguridad del Tráfico**

El análisis del tráfico reveló vulnerabilidades significativas en la transmisión:

- **Ausencia de Cifrado TLS:** La falta de implementación del protocolo de seguridad TLS expone los datos transmitidos a posibles ataques de interceptación o alteración.
- **Uso de Base64 para Autenticación:** Aunque Base64 es un método común de codificación, no proporciona un nivel adecuado de seguridad, lo que compromete la autenticación del servidor.

Por último, aunque el archivo adjunto **NEWS.txt** no contenía malware, su naturaleza podría facilitar la evasión de análisis en entornos más complejos o en situaciones con medidas de seguridad menos estrictas.

Una vez desarrollada o culminada la práctica, se presenta un informe técnico junto con la Guía Práctica de Análisis Forense en el ANEXO D, la cual detalla los pasos utilizados para realizar un análisis forense de este tipo de ataque.

3.6.5 Práctica 5: DNS Spoofing

La presente sección detalla el análisis forense realizado en un entorno controlado con el objetivo de identificar, confirmar y documentar un ataque de DNS Spoofing**.** La práctica permitió evidenciar cómo las respuestas DNS fueron manipuladas para redirigir un dominio legítimo hacia una IP maliciosa, utilizando diversas herramientas y técnicas forenses.

Este análisis tiene relevancia debido a la capacidad de los atacantes para redirigir el tráfico de red hacia servidores falsificados, lo que puede comprometer la integridad y confidencialidad de la información en sistemas vulnerables.

a. Objetivo

Desarrollar un procedimiento forense para identificar evidencia de un ataque de DNS Spoofing y determinar su impacto en un sistema Linux

b. Metodología

El análisis se llevó a cabo siguiendo un enfoque estructurado para la recopilación, verificación y análisis de la evidencia. Se utilizó la herramienta **tcpdump** para capturar tráfico DNS en la interfaz comprometida y generar un archivo pcap para su análisis.

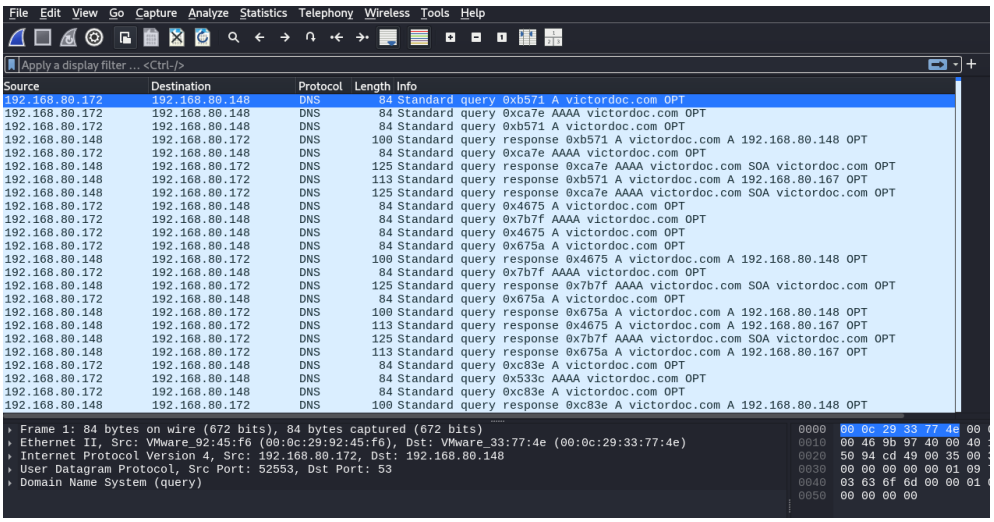


Figura 28. Respuesta de tráfico DNS manipulada con Wireshark.

La captura se analizó con Wireshark indicado en la Figura 28 donde se filtraron paquetes DNS (dns). Se compararon las solicitudes realizadas por la víctima con las respuestas recibidas, evidenciando redirecciones no autorizadas hacia la IP maliciosa **192.168.80.167**.

- ***Análisis relevantes a archivos y logs del sistema***

Se inspeccionó el archivo resolv.conf para determinar si los servidores DNS configurados eran legítimos en la Figura 29.

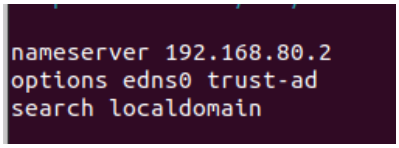


Figura 29. Servidores DNS configurados.

Los servidores DNS configurados en la interfaz ens33 correspondían a 192.168.80.2, lo cual permitió validar que las respuestas fueron interceptadas y manipuladas.

La resolución de dominios fue analizada en el momento del ataque, se utilizaron las herramientas <dig> y <nslookup> por comandos el cual se indicó una clara manipulación de redireccionamiento de ip del dominio indicado en Figura 30 y Figura 31.

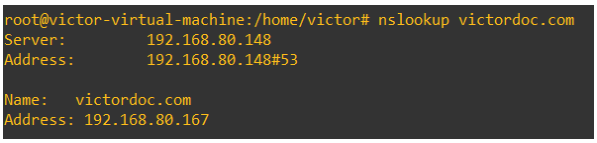


Figura 30. Ejecución del comando nslookup del domino victordoc.com.

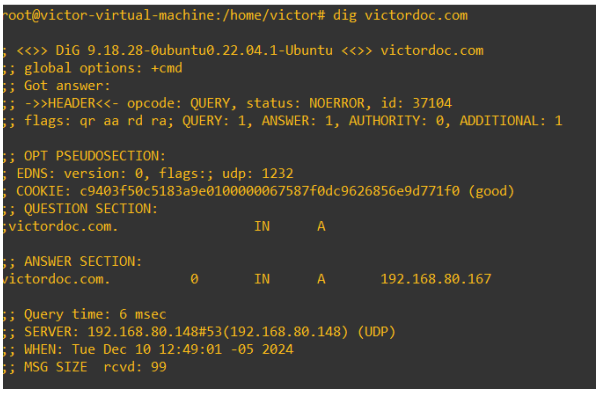


Figura 31. Ejecución del comando dig del domino victordoc.com.

Las consultas devolvieron la IP **192.168.80.167** en lugar de la IP legítima, confirmando que el tráfico DNS había sido redirigido. También se utilizó **resolvectl** para verificar los servidores DNS asociados a las interfaces de red y consultar las respuestas DNS para el dominio comprometido. La consulta a victordoc.com devolvió la IP maliciosa 192.168.80.167, confirmando el ataque de DNS Spoofing en la interfaz ens33.

Una vez desarrollada o culminada la práctica, se presenta un informe técnico junto con la Guía Práctica de Análisis Forense en el ANEXO E, la cual detalla los pasos utilizados para realizar un análisis forense de este tipo de ataque.

3.6.6 Práctica 6: Escalado de privilegios

El análisis realizado en esta práctica tiene como objetivo investigar un incidente de escalado de privilegios en un entorno controlado. El caso comenzó con la explotación de una vulnerabilidad en el protocolo FTP para subir archivos maliciosos, seguido de la utilización del exploit Dirty COW para obtener acceso privilegiado.

a. Objetivo

Profundizar en los archivos logs y registros del Sistema vulnerado con el fin de encontrar indicios de escalado de privilegios

b. Metodología

La adquisición de evidencia se realizó asegurando la integridad de los datos del disco comprometido. Para ello, se generó una copia forense del disco usando la herramienta **dcfldd,** acompañado de cálculos hash para garantizar que la imagen de disco replicaba fielmente la información del original, esta se evidencia indicado los hashes de los dos archivos en la Tabla 8.

Tabla 8. Registro de HASSH de la evidencia.

/dev/sdb	0039916915423492aab098d5dc70e0b50670dc3abc309847edac15c9b3ad86ce
File.dd	0039916915423492aab098d5dc70e0b50670dc3abc309847edac15c9b3ad86ce

Se inspeccionaron las particiones del disco utilizando herramientas como fdisk para identificar aquellas que contenían información relevante. La partición principal fue

montada de manera forense para su análisis detallado. En este análisis de disco se procedió a revisar archivos log para entender que cambios se han realizado.

- ***Análisis de logs.***

Se empezó analizando los archivos log registrados en /var/log/ de la Figura 32, aquí se encontró diferentes logs de acuerdo con el protocolo afectado como es FTP, lo que se observó fueron transferencias de archivos a la ruta /home/smbuser/. SSH, se evidencian claves SSH maliciosas de tipo 'ssh-rsa'.

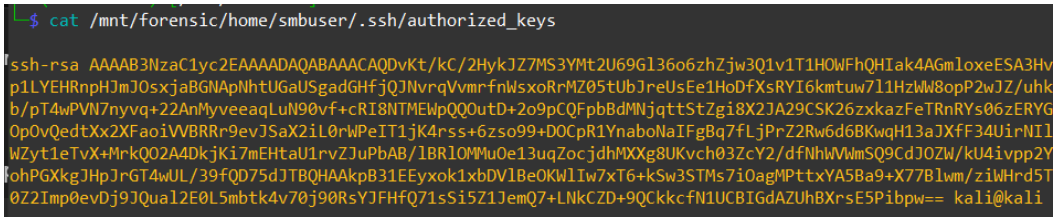


Figura 32. Clave SSH maliciosa ingresada.

En otro tipo de registro log 'secure -20241213' y con algunos parámetros adicionales para identificar acceso en el sistema, se encontró distintos intentos de ingreso por ssh de un ip desconocida indicado por la Figura 33, por este motivo se lo registra como la ip del atacante.

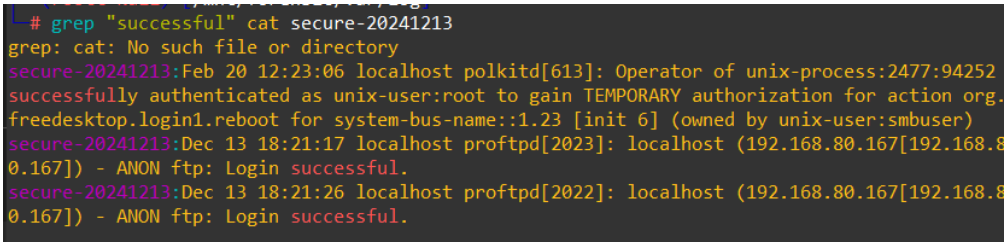


Figura 33. Intento de ingreso exitoso de una ip maliciosa por SSH.

- ***Evidencia de Escalado de Privilegios***

El análisis de archivos modificados recientemente reveló que el atacante utilizó el exploit Dirty COW para escalar privilegios. Esto fue confirmado al revisar marcas de tiempo y archivos alterados en el sistema, particularmente binarios críticos con permisos elevados. Se encontraron binarios y configuraciones alteradas en /usr/bin y /etc que correspondían a la actividad del exploit.

Una vez desarrollada o culminada la práctica, se presenta un informe técnico junto con la Guía Práctica de Análisis Forense en el ANEXO F, la cual detalla los pasos utilizados para realizar un análisis forense de este tipo de ataque.

3.6.7 Práctica 7: Análisis de archivos de celular Android 10

En este caso, se llevó a cabo un análisis forense centrado en archivos asociados a WhatsApp extraídos de un dispositivo con sistema operativo Android 10. Estos archivos, previamente obtenidos de un repositorio específico, proporcionaron un entorno controlado para el estudio. La investigación tuvo como objetivo identificar información crítica, como números de teléfono, contactos, mensajes y otros datos relevantes presentes en el sistema. Este enfoque no solo permitió simular un escenario realista de análisis forense, sino que también aseguró la validez de los hallazgos en un contexto controlado, brindando una base sólida para interpretar los resultados y establecer medidas de seguridad aplicables en casos similares.

a. Objetivo

Investigar un escenario relacionado a archivos de WhatsApp donde se almacenan diferentes archivos y presentar resultados de la investigación.

b. Metodología

Para garantizar la integridad de los datos, los archivos proporcionados en formato .zip fueron descomprimidos en un entorno controlado. La evidencia daba algunos archivos, entre los más importantes fue el directorio data, en este archivo se encontró subcarpetas que indican registros y datos de la aplicación WhatsApp.

Con el uso de la herramienta tree se pudo mapear la estructura de archivos y subdirectorios con el fin de ir encontrando la información necesaria a investigar, entre ellos fueron directorios como:

hared_prefs: Contenía configuraciones de la aplicación, incluido el número de registro del teléfono.

databases: Contain bases de datos relevantes, incluyendo la información de contactos.

- ***Identificación del número de registro de WhatsApp***

Dentro del directorio shared_prefs, se localizaron archivos .XML que almacenaban configuraciones y datos de registro de la aplicación. La revisión de estos archivos se realizó mediante herramientas estándar de Linux.

Se extrajo el número de teléfono asociado al registro de WhatsApp: **+9195794674**. Este número fue analizado para determinar su origen utilizando herramientas web como "AllAreaCodes".

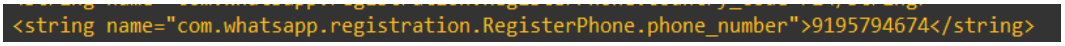


Figura 34. Numero de celular móvil de registro de WhatsApp.

- ***Análisis de contactos almacenados***

En el directorio databases, se identificaron varias bases de datos relacionadas con WhatsApp, incluidas wa.db y msgstore.db. Para el análisis, se centró la atención en wa.db, que almacena información sobre los contactos de WhatsApp. La visualización de estas bases de datos se realizó con el comando *sqlitebrowser* donde se usó para abrir las bases de datos internas de 'wa.db', este comando abrió una terminal grafica con una mejor visualización de la base de datos.

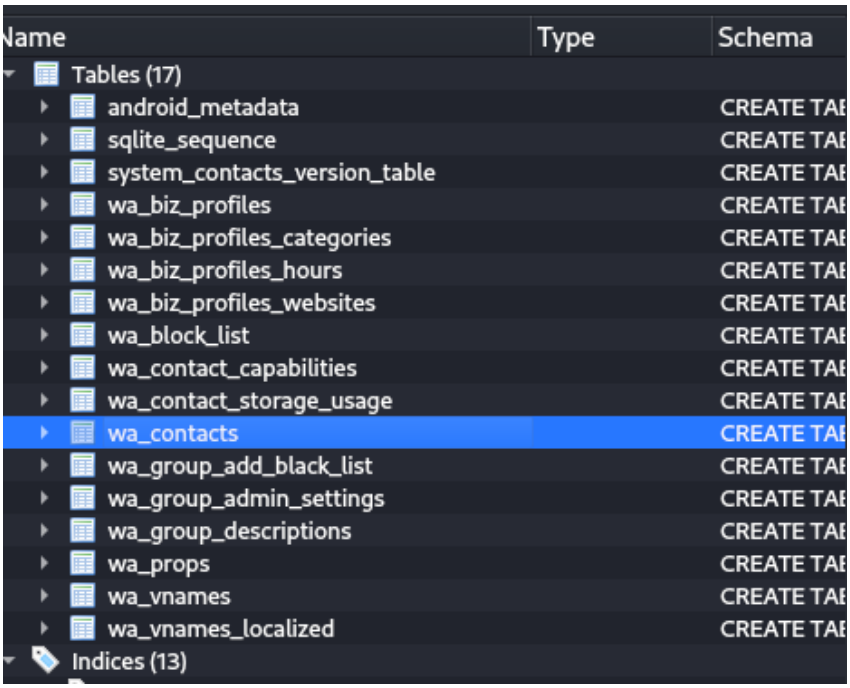


Figura 35. Bases de datos almacenadas en wa-db.

Se utilizó la función "Browser Database" de SQLite Browser para explorar las tablas de la base de datos. La base de datos contenía el id del contacto, estado del contacto y algunos nombres con números asociados.

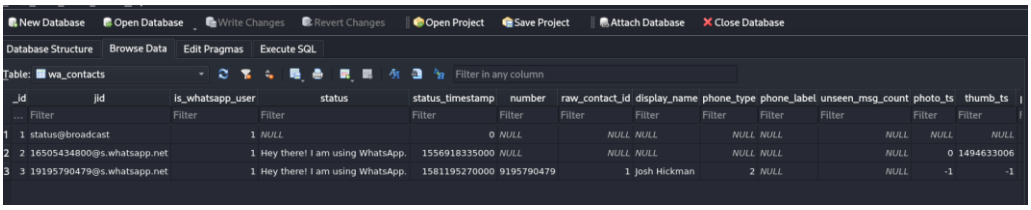


Figura 36. Información de contactos extraída.

Una vez desarrollada o culminada la práctica, se presenta un informe técnico junto con la Guía Práctica de Análisis Forense en el ANEXO G, la cual detalla los pasos utilizados para realizar un análisis forense de este tipo de ataque.

3.7 Evaluación de conocimientos en prácticas forenses

Las prácticas forenses diseñadas como parte de este proyecto fueron aplicadas a un grupo de 26 estudiantes de la carrera de Telecomunicaciones, cursando el séptimo semestre en la asignatura de Conmutación y Enrutamiento. Estas prácticas tuvieron como objetivo principal validar la efectividad de las guías forenses desarrolladas para la enseñanza de conceptos teóricos y prácticos en análisis forense digital.

Se diseñó un instrumento de evaluación con 10 preguntas que abarcan aspectos clave del análisis forense digital. Estas preguntas fueron seleccionadas y estructuradas para medir el nivel de conocimiento y comprensión de los estudiantes en relación con conceptos fundamentales, herramientas y comandos utilizados en las prácticas forenses. Las categorías evaluadas incluyen:

a. Conceptos básicos:

Preguntas enfocadas en evaluar el entendimiento de principios esenciales de la informática forense, tales como la identificación de directorios relevantes en un sistema operativo, el uso de valores hash para garantizar la integridad de la evidencia digital, y el propósito de realizar copias bit a bit en un análisis forense.

b. Herramientas y comandos prácticos

Este apartado incluyó preguntas sobre el manejo de herramientas y comandos forenses, como dd y dcfldd, para la creación de copias bit a bit de discos. Además, se evaluó el conocimiento del uso de comandos como *lsblk* para listar particiones, mmls para identificar estructuras en una imagen de disco, y *mount* para montar imágenes forenses en directorios específicos.

c. Aplicación técnica y análisis

Las preguntas abiertas de esta categoría buscaron medir la capacidad de los estudiantes para aplicar comandos en escenarios simulados y analizar los resultados obtenidos. Por ejemplo, se incluyó la identificación de particiones en una imagen de disco (mmls) y el uso de comandos como file para determinar el tipo de sistema de archivos presente.

d. Interpretación de resultados

En esta categoría se evaluó la habilidad de los estudiantes para interpretar datos derivados de análisis forenses, como estructuras de sistemas de archivos, resultados de hashes, y el propósito de comandos aplicados durante la práctica.

Cada una de estas categorías fue diseñada para reflejar un conocimiento progresivo, desde conceptos teóricos hasta la aplicación práctica en un entorno simulado. Este enfoque permitió identificar no solo el nivel de comprensión de los estudiantes, sino también áreas específicas que requieren refuerzo en futuras iteraciones de las guías prácticas.

La evaluación, calificada sobre un total de 3 puntos, consistió en 6 preguntas de opción múltiple y 4 preguntas abiertas diseñadas para medir el conocimiento teórico y práctico de los estudiantes en análisis forense digital. En la Figura 37 se muestra el promedio general obtenido por los estudiantes, así como la distribución de resultados en cada categoría evaluada.

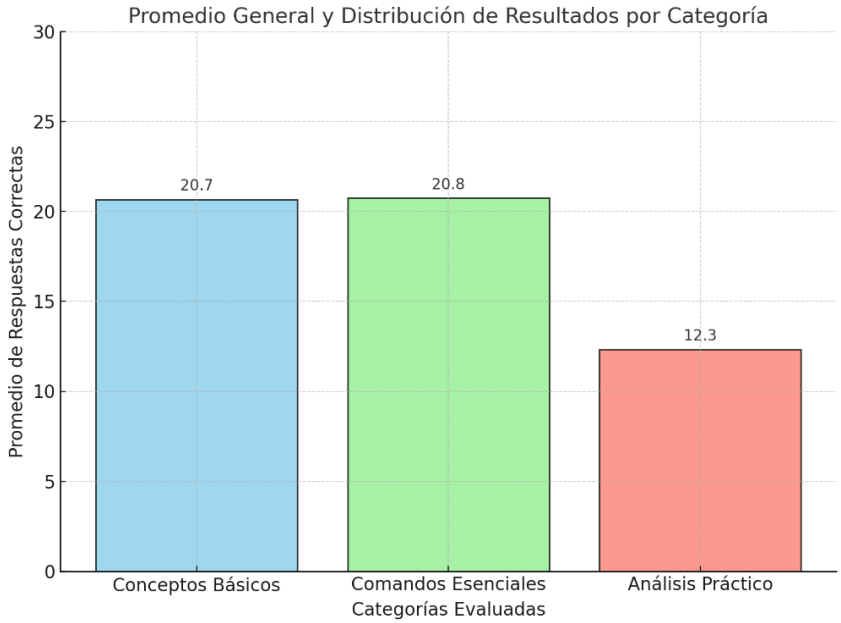


Figura 37. Promedio por categorías de las preguntas evaluadas.

3.7.1 Resultados de la Evaluación

El promedio general alcanzado fue de **2.11 puntos**, evidenciando que los estudiantes demostraron un buen dominio en las preguntas de opción múltiple, particularmente aquellas relacionadas con conceptos básicos como la utilización de valores hash para garantizar la integridad de la evidencia digital y la aplicación de comandos esenciales como dd y dcfldd. Estas preguntas reflejaron una adecuada comprensión de los fundamentos del análisis forense.

Sin embargo, las preguntas abiertas, enfocadas en habilidades prácticas como el análisis de particiones con mmls y la identificación de sistemas de archivos mediante file, fueron más desafiantes. Estas áreas presentaron un promedio más bajo, indicando la necesidad de fortalecer el aprendizaje práctico en temas relacionados con estructuras de sistemas de archivos y la interpretación de datos en escenarios simulados.

La evaluación permitió validar que las guías prácticas diseñadas son efectivas para transmitir conceptos fundamentales y habilidades básicas en análisis forense. Es necesario reforzar las prácticas con ejemplos aplicados que aborden escenarios más complejos, complementados con simulaciones detalladas que fortalezcan la capacidad de interpretación técnica.

3.8 Costos

3.8.1 Insumos del proyecto

Se presenta la Tabla 9 como los costos de insumos del proyecto.

Tabla 9. Costos del proyecto

ITEMS	CANTIDAD	COSTO UNITARIO	COSTO TOTAL
Computadora Principal	1	1800	$ 1800,00
Almacenamiento SSD 1 TB	1	120	$ 120,00
Amazon EC2	72 horas	0.40/hora	$ 28,00
Amazon S3	1 MES	2.30	$ 2,30
		Total	$ 1950

3.8.2 Costo del desarrollo técnico

En el desarrollo de proyectos técnico-científicos, es fundamental evaluar los recursos empleados, tanto humanos como económicos, para garantizar la viabilidad y eficiencia del proyecto. En este sentido, los valores presentados en la Tabla 10 detallan la relación entre las horas laborales invertidas y los costos asociados al desarrollo del testbed propuesto para el aprendizaje de informática forense.

Tabla 10. Costos de desarrollo técnico

Descripción	Tiempo ocupado
Desarrollo de las Prácticas	30 días
Desarrollo del análisis forense	60 días
Total	**90 días**
Horas laborales	8 horas
Horas totales	720 horas

El salario de un ingeniero en Telecomunicaciones según el Ministerio de Trabajo es de $494.51 en 2024 [43] . El salario mínimo por día es de $24.72, por ende, se gana $3.10 por hora. En base a la Tabla 10 de horas trabajadas se aplica la Ecuación (1)

$$\boldsymbol{Costo\ desarrollo\ técnico = Valor\ por\ hora * horas\ totales} \quad (1)$$

$$\boldsymbol{Costo\ desarrollo\ técnico = 3.10 * 720 = \$2.232}$$

3.8.3 Costo total

El costo total resulta de la suma del costo de desarrollo técnico y el costo de insumos como se muestra en la Ecuación (2).

$$\boldsymbol{Costo\ total = Costo\ de\ desarrollo\ tecnico + Costos\ de\ insumo} \quad (2)$$

El resultado final del costo total es:

$$\boldsymbol{Costo\ desarrolo\ técnico = \$\,2230.00 + \$\,1950.00 = \$\,4182,0(}$$

3.9 Discusión

Se revela una evolución significativa en el desarrollo de metodologías y herramientas aplicadas a la informática forense en diferentes contextos tecnológicos. Los estudios revisados contribuyen con enfoques específicos, que enriquecen el conocimiento actual y ofrecen perspectivas prácticas relevantes para la implementación de un testbed para el aprendizaje en esta área.

Según el estudio sobre CloudMe Forensics [4] subraya la importancia de identificar artefactos digitales residuales en entornos de almacenamiento en la nube, destacando la necesidad de adaptar herramientas tradicionales para contextos de big data. Esta experiencia resulta relevante para el presente trabajo, que busca integrar tecnologías de la nube, como AWS, para fortalecer el análisis forense digital.

Los aportes de investigaciones como la de Estructura de un laboratorio de informática forense y la de Análisis Forense de Evidencias Digitales en Entornos iCloud [6], [9] destacan la importancia de un diseño estructurado del laboratorio, incluyendo áreas funcionales clave y el uso de normas internacionales como la ISO 27037:2012. Estos elementos son fundamentales para garantizar la integridad de la evidencia y la validez de los procedimientos en el testbed, estableciendo un marco metodológico que refuerza la credibilidad de los resultados obtenidos.

Por otro lado, estudios más recientes, como el análisis forense en dispositivos móviles [8], subrayan la relevancia de herramientas avanzadas y actualizadas como Cellebrite y Oxygen Forensic Detective. Este punto resalta la necesidad de incorporar tecnologías

emergentes y marcos legales vigentes en la formación de futuros especialistas, un objetivo que el presente proyecto aborda al combinar escenarios controlados en entornos locales y su posterior análisis en la nube.

Las investigaciones reflejan un impacto educativo significativo, como es el caso del laboratorio de cómputo forense para ciberseguridad [7]. Este enfoque educativo refuerza la relevancia del testbed propuesto como una herramienta no solo para el aprendizaje técnico, sino también para la formación de competencias críticas en la identificación y análisis de riesgos cibernéticos.

CAPÍTULO IV. CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones

Se llevó a cabo una revisión de las metodologías y estándares internacionales, como la ISO/IEC 27037 y RFC 3227, que destacan la recolección, preservación y análisis de evidencia digital. Estas normativas fueron esenciales para garantizar la integridad de la evidencia en diversos entornos. Se implementaron herramientas como Wireshark y algoritmos hash para la captura y validación de evidencias digitales, consolidando un enfoque estructurado y confiable para el análisis forense.

Se implementó una infraestructura basada en Amazon Web Services (AWS), integrando servicios como Amazon S3 y Amazon EC2. Esto permitió garantizar escalabilidad, seguridad y alta disponibilidad en el manejo de evidencias digitales. La infraestructura implementada soportó la transferencia segura de datos y el análisis avanzado en la nube, optimizando los procesos forenses en entornos híbridos. El uso de AWS también validó su capacidad para cumplir con estándares internacionales y satisfacer las necesidades de análisis forense en grandes volúmenes de datos

Se desarrollaron ocho prácticas detalladas que abarcan desde la recolección hasta el análisis avanzado de evidencias digitales. Estas prácticas fueron validadas en escenarios controlados, incluyendo recomendaciones para preservar la cadena de custodia, realizar análisis en memoria volátil y procesar datos en entornos virtuales y en la nube. Las practicas aseguraron la replicabilidad y aplicabilidad educativa del laboratorio, contribuyendo a la formación de futuros especialistas en informática forense.

4.2 Recomendaciones

Se recomienda mantener una evaluación constante de las metodologías utilizadas en el análisis de informática forense, con énfasis en aquellas emergentes que respondan a las necesidades de entornos cloud y dispositivos IoT. Asimismo, es necesario complementar las normas aplicadas, como ISO/IEC 27037 y RFC 3227, con estudios de caso específicos que validen su efectividad en contextos prácticos. Además, se

sugiere ampliar la revisión bibliográfica para incluir estándares y herramientas internacionales de vanguardia, asegurando que el laboratorio esté alineado con las mejores prácticas globales.

Es fundamental considerar la evaluación de plataformas alternativas a AWS, como Google Cloud o Microsoft Azure, para analizar su compatibilidad con los procesos forenses y comparar sus costos y beneficios. También se recomienda fortalecer la capacitación del equipo técnico en el manejo de herramientas y servicios en la nube, maximizando la eficiencia operativa. Adicionalmente, se sugiere implementar políticas de seguridad avanzadas, como accesos jerárquicos y encriptación de extremo a extremo, para garantizar la integridad y confidencialidad de los datos gestionados en la infraestructura cloud.

Se recomienda actualizar periódicamente las guías prácticas para incluir nuevas herramientas y técnicas que respondan a las tendencias y desafíos actuales del análisis forense digital. También sería pertinente integrar escenarios adicionales que simulen ataques emergentes, como ransomware o compromisos en entornos IoT, ampliando el alcance y relevancia de las prácticas propuestas. Finalmente, se sugiere establecer un sistema de retroalimentación estructurada tras la ejecución de las prácticas, lo cual permitirá identificar oportunidades de mejora y reforzar el aprendizaje de los participantes.

REFERENCIAS BIBLIOGRÁFICAS

[1] O. de los Estados Americanos, “Reporte sobre el desarrollo de la Fuerza Laboral de Ciberseguridad en una era de escasez de talento y habilidades,” Organización de los Estados Americanos, 2023.

[2] E. Ferreyra, “La investigación forense informática en América Latina,” Asociación por los Derechos Civiles (ADC), Apr. 2018.

[3] M. de Telecomunicaciones y de la Sociedad de la Información, “Estrategia nacional de ciberseguridad del Ecuador,” Ministerio de Telecomunicaciones y Sociedad de la Información, Quito, 2022.

[4] Y.-Y. Teing, A. Dehghantanha, and K.-K. R. Choo, “CloudMe forensics: A case of big data forensic investigation,” Concurrency and Computation: Practice and Experience, vol. 30, no. 5, p. e4277, 2018.

[5] M. Fernández Mata, “Laboratorio de Pentesting basado en tecnología de contenedores.” 2019.

[6] O. L. G. Pérez, “Estructura de un laboratorio de Informática Forense para la Dirección de Seguridad Informática,” Revista Cubana de Ciencias Informáticas, vol. 16, no. 4, 2022.

[7] Y. Romero Hernández, M. del C. Santiago Díaz, J. Pérez Marcial, A. C. Zenteno Vázquez, G. Rubin Trinidad Linares, and R. Martínez Pérez, “La Importancia del Cómputo Forense en la Actualidad,” Tecnología Educativa Revista CONAIC, vol. 10, no. 1, 2023.

[8] A. Alemán Ariza, “ANÁLISIS FORENSE DIGITAL EN DISPOSITIVOS MÓVILES,” CATHEDRA, no. 21, pp. 45–64, May 2024.

[9] C. A. P. Vera, “Análisis forense de evidencias digitales en entornos iCloud.” Universidad Estatal Península de Santa Elena, La Libertad, Ecuador, Dec-2024.

[10] M. I. Romero Castro, M. A. Choez Chele, C. J. Álava Mero, V. F. Romero Castro, M. A. Castillo Merino, L. R. Murillo Quimiz, and H. B. Delgado Lucas, “LA INFORMÁTICA FORENSE DESDE UN ENFOQUE PRÁCTICO,” Sep. 2020.

[11] C. V. Gioia, “Metodología de análisis forense informático para la obtención de evidencia digital en Base de Datos.” Universidad Nacional de La Matanza, Buenos Aires, Argentina, Jun-2019.

[12] M. Lopéz Delgado, Análisis Forense Digital. CriptoRed, 2007.

[13] S. Roatta, M. E. Casco, and M. Fogliato, “El tratamiento de la evidencia digital y las normas ISO/IEC 27037:2012,” 2012.

[14] C. G. Rivas, “Metodología para un análisis forense.” Universitat Oberta de Catalunya, Dec-2014.

[15] A. Bhardwaj and K. Kaushik, Practical Digital Forensics: Forensic Lab Setup, Evidence Analysis, and Structured Investigation Across Windows, Mobile, Browser, HDD, and Memory, 1st ed. London: BPB Online, 2023.

[16] I. M. H. Cajo, B. G. H. Cajo, B. G. H. Olmedo, and N. B. L. Benalcázar, Informática Forense II: Prueba Indiciaria Informático Forense. Editorial Investigativa Latinoamericana, 2024.

[17] K. Hapuc López Molina and J. Carlos Vindell Olivas, “Laboratorio de computación forense para el departamento de criminalística de la Policía Nacional de Nicaragua,” Universidad Nacional Autónoma de Nicaragua, UNAN-Managua, 2011.

[18] D. Evidence, “The Basics of Digital Evidence.” 2025.

[19] The Sleuth Kit, “The Sleuth Kit and Autopsy.” 2025.

[20] The Sleuth Kit, “mmls - Display Partition Layouts.” 2025.

[21] Command Masters, “MMLS Command: Common Usage and Examples.” 2024.

[22] W. A. Villota Jimenez, A. Chavez, and others, “Análisis forense y sus herramientas,” 2018.

[23] The Sleuth Kit, “fsstat - Display general details of a file system.” 2025.

[24] D. Santo Orcero, Kali Linux. Ra-Ma Editorial, 2018.

[25] D. J. T. España, F. A. Salazar, and S. A. Hidrobo, “Informática Forense,” INNOVACIÓN TECNOLÓGICA, p. 262.

[26] J. S. Rueda-Rueda, D. Rico-Bautista, and C. D. Guerrero, “Guía práctica abierta para el análisis forense digital en dispositivos Android,” Revista Ibérica de Sistemas e Tecnologías de Informação, no. E18, pp. 442–457, 2019.

[27] SAHW, “Obtención de Imágenes Forenses Mediante Derivados Mejorados de DD: DCFLDD y DC3DD.” 2010.

[28] Y. S. Torres Torres, “Sistema Forense Auditor de Integridad y Recuperación de Soportes de Datos.” Universidad Autónoma del Estado de México, Valle de Chalco Solidaridad, México, 2017.

[29] R. Sánchez and F. Pérez, Peritaje Informático y Tecnológico, 1a ed. Madrid, España: Editorial X, 2013.

[30] ISO, “ISO/IEC 27037:2012 – Guidelines for identification, collection, acquisition and preservation of digital evidence.” 2012.

[31] ISO, “ISO/IEC 27042:2015 — Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence.” 2015.

[32] P. Informáticos, “ISO 27042: Perito Informático.” 2024.

[33] F. de Evidencias Electrónicas, “ISO 27037: Directrices de gestión de evidencias electrónicas.” 2024.

[34] N. I. of Justice, “Forensic Examination of Digital Evidence: A Guide for Law Enforcement.” U.S. Department of Justice, Apr-2004.

[35] S. Acurio Del Pino, “Manual de Manejo de Evidencias Digitales y Entornos Informáticos,” Fiscalía General del Estado, 2009.

[36] Govertis, “UNE 71505: Sistemas de gestión de evidencias electrónicas.” 2024.

[37] D. Brezinski and T. Killalea, “RFC 3227: Guidelines for Evidence Collection and Archiving.” 2002.

[38] N. I. of Justice, “Forensic Examination of Digital Evidence: A Guide for Law Enforcement.”

[39] AWS, “What is Cloud Storage?” 2025.

[40] Amazon Web Services, “AWS Backup - Automatización y gestión centralizada de copias de seguridad.” 2025.

[41] Amazon Web Services, “AWS Key Management Service (KMS) - Gestión de claves de cifrado escalable.” 2025.

[42] “AWS CloudTrail - Seguimiento de actividad en AWS.” 2025.

[43] A. Santos, “ANEXO 1: SALARIOS MÍNIMOS SECTORIALES Y TARIFAS,” 2024.

ANEXOS

Anexo A. Informe Técnico – Guía Práctica 1 – Denegación de servicio (DoS)

1. Introducción

El presente informe describe el análisis forense realizado a un servidor Linux que sufrió un ataque de Denegación de Servicio (DoS). Durante el ataque, el servidor presentó interrupciones frecuentes y fallos en la disponibilidad de sus servicios.

- **Objetivo del Análisis**:

Confirmar la existencia del ataque, identificar el alcance y las técnicas utilizadas, y proporcionar recomendaciones para evitar futuros incidentes similares.

---

2. Métodos y Herramientas Utilizadas

Métodos:

- Preservación de la evidencia mediante la copia bit a bit del disco afectado y capturas de red.
- Análisis de tráfico de red para identificar patrones de ataque.
- Revisión de logs del sistema y configuración del servidor para encontrar debilidades explotadas.

Herramientas:

- **Wireshark**: Captura y análisis de tráfico de red.
- **tcpdump**: Generación de capturas en formato. pcap.
- **Comandos Linux**: Validación (cat /etc/resolv.conf, dig, nslookup).
- **awk**, **grep** y **whois**: Análisis de logs e identificación del atacante.

3. Evidencia Recolectada

3.1. Capturas de Tráfico DNS en Wireshark

El análisis en Wireshark reveló múltiples conexiones HTTP incompletas (SYN flood) desde una IP específica.

3.2. Logs del servidor apache

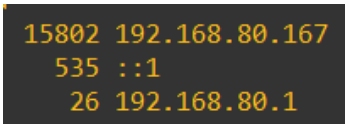


Figura A7. Contenido del archivo /var/log/apache2/access.log.

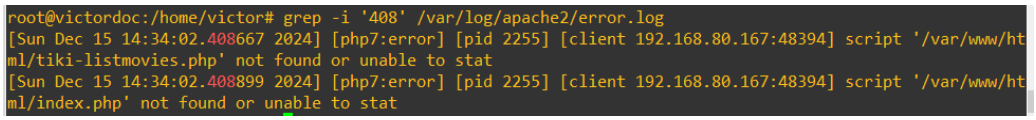


Figura A8. Conexiones fallidas y códigos de error HTTP 408 (Request Timeout).

3.3. Configuración del servidor Apache

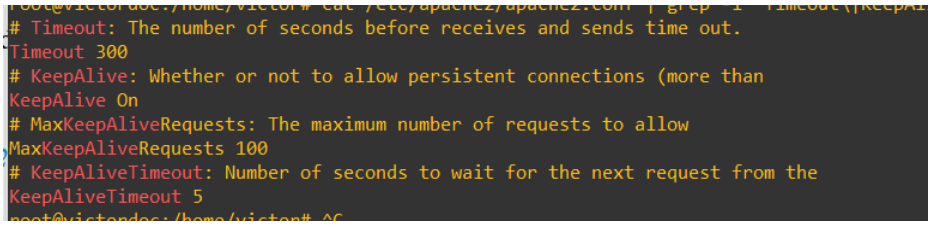


Figura A6. Configuración predeterminada encontrada en /etc/apache2/apache2.conf:

Estas configuraciones permitieron conexiones maliciosas persistentes durante largos períodos

4. Conclusiones

El análisis forense confirmó que el servidor fue víctima de un ataque DoS utilizando la técnica **Slowloris**, caracterizada por conexiones HTTP incompletas para saturar los recursos del servidor, efectivo contra configuraciones predeterminadas de Apache sin límites de conexión o tiempo de espera ajustados.

Se identificaron configuraciones inseguras en Apache que facilitaron el ataque, además de un uso crítico de recursos del sistema. Las medidas recomendadas permitirán mejorar la seguridad del servidor y prevenir incidentes similares en el futuro.

---

5. Recomendaciones

- Reconfiguración segura del servidor Apache.
- Uso de límites en conexiones por IP y tiempo de espera.
- Implementación de módulos como mod_reqtimeout y herramientas de balanceo de carga para prevenir saturaciones similares en el futuro.

Guía Practica 1

1. Tema:
Denegación de servicio (DoS)

2. Objetivo:
Desarrollar un procedimiento forense para identificar evidencia de un ataque de Denegación de Servicio (DoS) y determinar su impacto en un sistema Linux.

3. Instrucciones:
Un servidor Linux ha reportado interrupciones frecuentes y rendimiento degradado. Se sospecha de un ataque DoS. El objetivo es recolectar evidencia, identificar vectores de ataque y documentar el análisis.

4. Listado de equipos, materiales y recursos:
• Sistema Linux (servidor objetivo) • Tcpdump

- Grep
- Top
- Wireshark

5. Actividades por desarrollar:

Introducción

Esta guía práctica describe los pasos para realizar un análisis forense de un ataque de tipo Denegación de Servicios (DoS). En este ejercicio, un atacante genera un volumen masivo de solicitudes hacia un servidor Apache Linux, lo que provoca que los recursos del servidor se agoten y los usuarios legítimos no puedan acceder a los servicios.

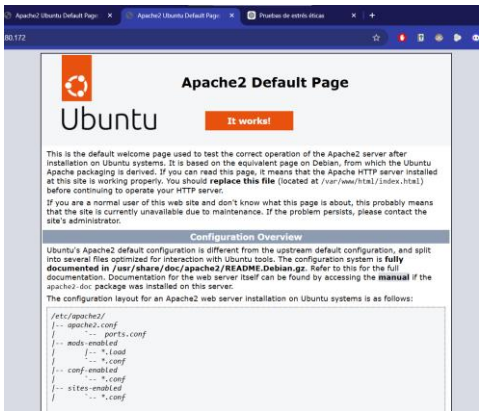


Figura A1. Página web predeterminada de Apache.

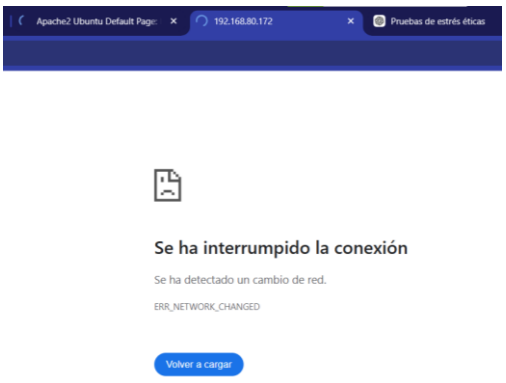


Figura A2. Denegación de servicio, el servidor dejó de responder.

Recolección de evidencia

Análisis de trafico de red

El primer paso en el análisis forense es recopilar evidencias del ataque. Esto incluye la captura de tráfico de red, la revisión de los registros del servidor Apache y el monitoreo de recursos del sistema durante el ataque.

Capturar tráfico de red en el servidor utilizando Tcpdump.

sudo tcpdump -i eth0 -w dos_attack. pcap

Este archivo se puede abrir en wireshark y agregar algunos filtros que permitan ser conexiones sospechosas.

Filtros útiles:

- *'tcp[tcpflags] == tcp-syn '*
- tcp. dstport == 80
- tcp.flags.syn == 1 and tcp.flags.ack == 0

Identificar al atacante con la herramienta whois <ip atacante>.

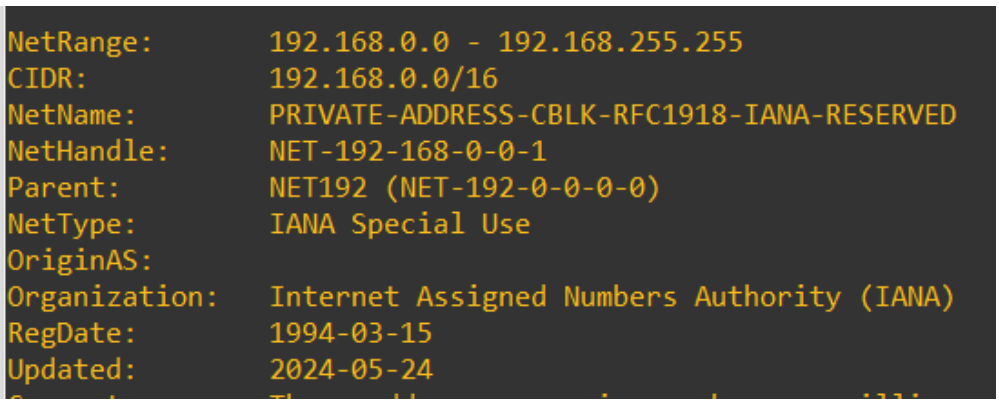


Figura A3. Uso de la herramienta whois para identificar al atacante a partir de su dirección IP.

Análisis de los logs del sistema

Buscar IPs con solicitudes excesivas en los logs de acceso de apache.

awk '{print $1}' /mnt/mounted_disk/var/log/apache2/access.log | sort | uniq -c | sort -nr | head

```
root@victordoc:/home/victor# awk '{print $1}' /var/log/apache2/access.log | sort | uniq
-c | sort -nr | head
  15802 192.168.80.167
    535 ::1
     25 192.168.80.1
```

Figura A4. Análisis de logs de Apache para identificar direcciones IP con solicitudes excesivas.

Verificar solicitudes repetidas desde la ip encontrada anteriormente.

grep "<IP_ATACANTE>" /var/log/apache2/access.log

```
192.168.80.167 - - [15/Dec/2024:16:43:53 +0000] "GET /?1021 HTTP/1.1" 400 487 "-" "Mozil
la/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome
/53.0.2785.143 Safari/537.36"
192.168.80.167 - - [15/Dec/2024:16:43:55 +0000] "GET /?1430 HTTP/1.1" 400 487 "-" "Mozil
la/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome
/53.0.2785.143 Safari/537.36"
192.168.80.167 - - [15/Dec/2024:16:43:53 +0000] "GET /?422 HTTP/1.1" 400 487 "-" "Mozill
a/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
53.0.2785.143 Safari/537.36"
192.168.80.167 - - [15/Dec/2024:16:43:55 +0000] "GET /?1673 HTTP/1.1" 400 487 "-" "Mozil
la/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome
```

Figura A5. Verificación de solicitudes repetidas desde la dirección IP identificada en los logs de acceso de Apache.

Análisis de archivos de la máquina virtual afectada.

El atacante utilizó un método básico de DoS enviando múltiples solicitudes HTTP al servidor Apache desde una única IP. Esto causó que el servidor devolviera un código HTTP 408 (Request Timeout) en múltiples ocasiones, debido a la incapacidad de procesar todas las conexiones simultáneamente.

Revisar la configuración de apache que está dada en el servidor. Se analiza valores altos de timeout y KeepAlive.

cat /etc/apache2/apache2.conf | grep -i 'Timeout\|KeepAlive'

```
# Timeout: The number of seconds before receives and sends time out.
Timeout 300
# KeepAlive: Whether or not to allow persistent connections (more than
KeepAlive On
# MaxKeepAliveRequests: The maximum number of requests to allow
MaxKeepAliveRequests 100
# KeepAliveTimeout: Number of seconds to wait for the next request from the
KeepAliveTimeout 5
```

Figura A6. Configuración predeterminada encontrada en /etc/apache2/apache2.conf:

La configuración actual de Apache presenta un Timeout de 300 segundos, lo cual es excesivo y permite que conexiones inactivas permanezcan abiertas por demasiado

tiempo, facilitando ataques de denegación de servicio (DoS) como Slowloris. Además, *KeepAlive On* con conexiones persistentes habilitadas multiplica el riesgo, ya que un atacante puede abrir múltiples conexiones simultáneas y agotar los recursos del servidor.

6. Recomendaciones

- Configurar límites de conexiones en Apache utilizando el módulo mod_reqtimeout.
- Bloquear direcciones IP maliciosas utilizando iptables o un firewall de aplicación.
- Implementar herramientas de detección de intrusos (IDS) como Fail2Ban para identificar y bloquear patrones maliciosos.
- Usar un balanceador de carga para distribuir el tráfico entre múltiples servidores.

Anexo B. Informe Técnico – Guía Práctica 2 - Man-in-the-Middle (MITM)

1. Introducción

El presente informe describe el análisis forense realizado tras un ataque de tipo Man-in-the-Middle (MITM) en un entorno de red interna. En este escenario, un atacante utilizando una máquina Kali Linux ejecutó un ataque de ARP Spoofing para interceptar el tráfico entre una máquina Ubuntu (víctima) y un servidor Apache.

- **Objetivo del análisis**

Confirmar la ejecución de un ataque MITM, identificar las evidencias asociadas, y proporcionar recomendaciones prácticas para prevenir incidentes similares en el futuro.

---

2. Métodos y Herramientas

- Validación de la tabla ARP para identificar inconsistencias en las relaciones IP-MAC.

- Revisión de logs del sistema y del servidor Apache.
- Inspección de archivos clave en el servidor para detectar actividad sospechosa.

Herramientas

- **Comandos de Linux**: Validación de logs y configuración de red (arp, grep, cat).
- **Hashing Tools**: Preservación de integridad en las evidencias recolectadas.

---

3. Evidencia Recolectada

3.1. Validación de la Tabla ARP

La tabla ARP de la máquina víctima mostró relaciones IP-MAC inconsistentes, lo que sugiere un ataque de envenenamiento ARP:

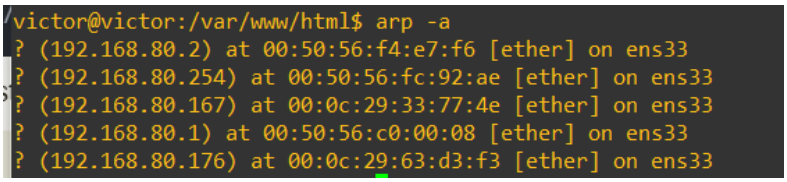


Figura B1: Tabla ARP con direcciones IP y MAC asociadas.

- Dirección IP del atacante: 192.168.80.167.
- Dirección MAC del atacante: 00:0c:29:33:77:4e.

3.2. Logs del Sistema

Se inspeccionaron los logs de autenticación en la máquina víctima para rastrear actividades relacionadas con la IP sospechosa:

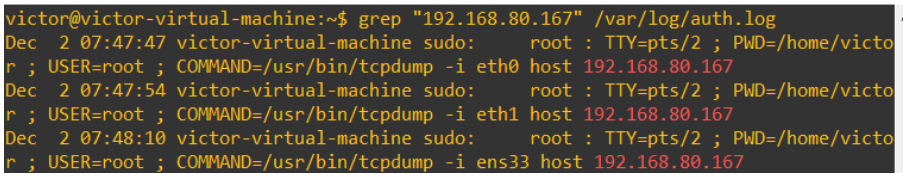


Figura B2. Extracto del log de autenticación mostrando conexiones relacionadas con la dirección IP del atacante.

3.3. Logs del Servidor Apache

Los registros de acceso del servidor Apache mostraron solicitudes provenientes de la máquina víctima (192.168.80.176):

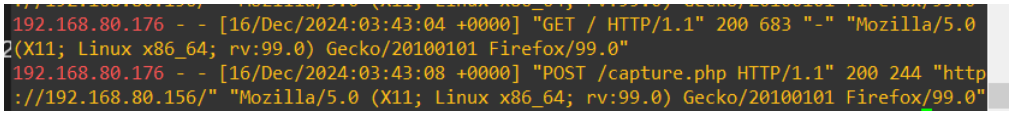


Figura B3. Análisis de logs de Apache para rastrear solicitudes realizadas desde la dirección IP sospechosa 192.168.80.176.

3.4. Inspección de Archivos Clave

Se verificaron posibles modificaciones en el archivo credentials.txt, que contenía información sensible:

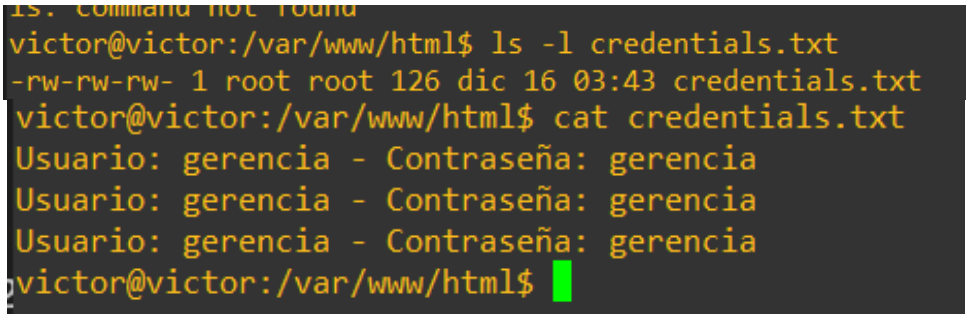


Figura B4. Verificación del archivo credentials.txt en el servidor.

---

4. Conclusión

El análisis forense confirmó la ejecución de un ataque MITM mediante ARP Spoofing, que comprometió la confidencialidad de las comunicaciones entre la máquina víctima y el servidor. Este tipo de ataque se vio facilitado por la falta de cifrado en el tráfico HTTP y configuraciones predeterminadas en la red. Las medidas recomendadas son esenciales para prevenir futuros incidentes similares, fortaleciendo la seguridad del entorno y protegiendo los datos sensibles.

5. Recomendaciones

- Implementar HTTPS en el servidor utilizando certificados digitales para asegurar el tráfico.

- Configurar el uso obligatorio de TLS en todos los servicios expuestos.
- Configurar tablas ARP estáticas en dispositivos críticos para evitar ataques de envenenamiento.
- Configurar una VPN para proteger las comunicaciones en redes públicas o inseguras.
- Realizar simulaciones de ataques MITM en un entorno controlado para identificar vulnerabilidades.

Guía Practica 2

1. Tema:
Man-in-the-Middle (MITM)

2. Objetivo:
En este escenario, una máquina Ubuntu ha sido víctima de un ataque Man-in-the-Middle (MITM) realizado desde una máquina Kali Linux.

3. Instrucciones:
• Detener cualquier actividad innecesaria en la máquina víctima para evitar alterar la evidencia. • Crear una instantánea de la máquina virtual o una copia forense del disco para poder trabajar en ella y no alterar información original.

4. Listado de equipos, materiales y recursos:
• VMware • Wireshark • Hashing Tools

5. Actividades por desarrollar:

Introducción

Esta guía práctica describe los pasos para realizar un análisis forense de un ataque de tipo Man-in-the-Middle (MITM). En este ejercicio, un atacante en una máquina con Kali Linux realiza un ataque de ARP Spoofing hacia una máquina víctima con Ubuntu. El objetivo es interceptar tráfico de red y analizar el impacto del ataque.

Preservación de la Evidencia

- Servidor (192.168.80.156)
- Máquina Víctima (192.168.80.176)
- Logs de la máquina víctima.
- Logs del servidor Apache.
- Archivos de configuración y el archivo de salida (capture.txt).

Recolección de Evidencia

Análisis de la maquina victima

Validar tabla arp en busca de inconsistencias IP– MAC que indiquen ataques spoofing.

```
victor@victor:/var/www/html$ arp -a
? (192.168.80.2) at 00:50:56:f4:e7:f6 [ether] on ens33
? (192.168.80.254) at 00:50:56:fc:92:ae [ether] on ens33
? (192.168.80.167) at 00:0c:29:33:77:4e [ether] on ens33
? (192.168.80.1) at 00:50:56:c0:00:08 [ether] on ens33
? (192.168.80.176) at 00:0c:29:63:d3:f3 [ether] on ens33
```

Figura B1. Tabla ARP con direcciones IP y MAC asociadas.

Se observa a una maquina tercera <192.168.80.167>, esta ip de la MAC <00:0c:29:33:77:4e > podría ser del atacante.

Identificar en los logs del sistema anomalías relacionadas con la ip encontrada en la red.

grep "192.168.80.167" /var/log/auth.log

```
victor@victor-virtual-machine:~$ grep "192.168.80.167" /var/log/auth.log
Dec  2 07:47:47 victor-virtual-machine sudo:     root : TTY=pts/2 ; PWD=/home/victo
r ; USER=root ; COMMAND=/usr/bin/tcpdump -i eth0 host 192.168.80.167
Dec  2 07:47:54 victor-virtual-machine sudo:     root : TTY=pts/2 ; PWD=/home/victo
r ; USER=root ; COMMAND=/usr/bin/tcpdump -i eth1 host 192.168.80.167
Dec  2 07:48:10 victor-virtual-machine sudo:     root : TTY=pts/2 ; PWD=/home/victo
r ; USER=root ; COMMAND=/usr/bin/tcpdump -i ens33 host 192.168.80.167
```

Figura B2. Identificación de anomalías relacionadas con la dirección IP sospechosa en los logs del sistema.

Se identifica que se hizo una captura de trafico de red por el comando <tcpdump> en dirección a las tarjetas de red de la máquina. Esto con el fin de poder interceptar datos relevantes como tráfico http y métodos GET y POST que puede contener información sensible.

Análisis del servidor

Revisar Logs de Acceso de Apache en busca las conexiones provenientes de la máquina víctima.

cat /var/log/apache2/access.log | grep "192.168.80.176"

```
192.168.80.176 - - [16/Dec/2024:03:43:04 +0000] "GET / HTTP/1.1" 200 683 "-" "Mozilla/5.0
(X11; Linux x86_64; rv:99.0) Gecko/20100101 Firefox/99.0"
192.168.80.176 - - [16/Dec/2024:03:43:08 +0000] "POST /capture.php HTTP/1.1" 200 244 "http
://192.168.80.156/" "Mozilla/5.0 (X11; Linux x86_64; rv:99.0) Gecko/20100101 Firefox/99.0"
```

Figura B3. Análisis de logs de Apache para rastrear solicitudes realizadas desde la dirección IP sospechosa 192.168.80.176.

Se verifica si se han registrado credenciales últimamente

ls -l credentials.txt

```
victor@victor:/var/www/html$ ls -l credentials.txt
-rw-rw-rw- 1 root root 126 dic 16 03:43 credentials.txt
victor@victor:/var/www/html$ cat credentials.txt
Usuario: gerencia - Contraseña: gerencia
Usuario: gerencia - Contraseña: gerencia
Usuario: gerencia - Contraseña: gerencia
victor@victor:/var/www/html$
```

Figura B4. Verificación del archivo credentials.txt en el servidor de posibles modificaciones recientemente.

Evaluación del impacto

Existe una tabla ARP para identificar envenenamiento, para esto se ejecuta el siguiente comando en la máquina víctima para listar la tabla ARP y buscar entradas incorrectas que asocien la dirección IP de la puerta de enlace (gateway) con la dirección MAC del atacante:

arp -a

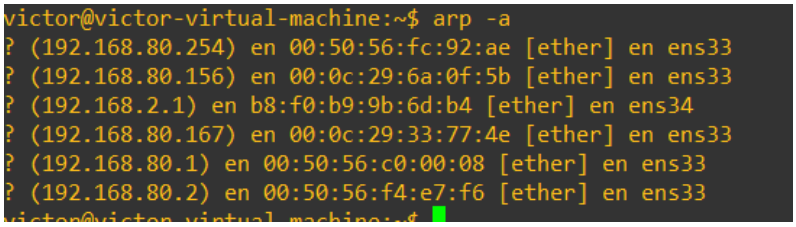


Figura B5. Tabla ARP con direcciones IP y MAC asociadas.

Se analiza la imagen que da Wireshark como evidencia que la maquina trato de recolectar información de la maquina victima por la falta de seguridad en el Puerto 80 y no tener activo el puesto https.

6. Recomendaciones

Para prevenir ataques similares en el futuro, se recomienda implementar las siguientes medidas:

- Usar HTTPS y TLS para cifrar el tráfico de red.
- Configurar tablas ARP estáticas para dispositivos críticos.
- Implementar una VPN para proteger el tráfico en redes públicas.
- Monitorear la red para detectar ataques de ARP Spoofing.

Anexo C. Informe Técnico – Guía Práctica 3 - Ataque con Exploit de VSFTPD.

1. Introducción

El presente informe documenta el análisis forense realizado tras un ataque exitoso que explotó una vulnerabilidad en el servicio vsftpd (vsFTPd v2.3.4) de la máquina intencionadamente vulnerable Metasploitable 2. Esta vulnerabilidad permitió al atacante obtener acceso a un shell con privilegios de root mediante un backdoor activado tras una autenticación manipulada.

2. Objetivos

Identificar las vulnerabilidades explotadas y las actividades maliciosas realizadas, recopilando evidencia clave que permita comprender el alcance del ataque y proponer medidas de mitigación.

---

3. Métodos y Herramientas

Métodos

- Exploración inicial de la máquina víctima para confirmar la existencia de la vulnerabilidad.
- Análisis de logs del sistema y servicio FTP para identificar actividades relacionadas con el ataque.
- Revisión de archivos y procesos recientes en busca de evidencia de actividad posterior.

Herramientas

- **Comandos Linux**: Para análisis de logs, revisión de procesos y archivos.
- **Hashing Tools**: Para preservar la integridad de las evidencias recolectadas.

4. Actividades Desarrolladas

4.1. Exploración Inicial

Se utilizó el comando nmap para confirmar la presencia del servicio vulnerable y obtener información de la versión:

El escaneo mostró que el puerto 21 estaba abierto y que el servicio vsftpd ejecutaba la versión 2.3.4, conocida por incluir un backdoor.

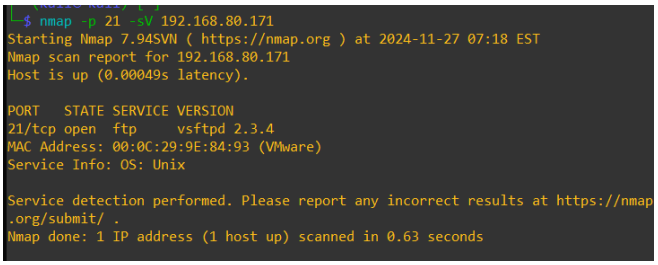


Figura C1. Escaneo del puerto 21 de la maquina víctima.

4.2. Revisión de Logs del Servicio FTP

El archivo vsftpd.log fue analizado para identificar conexiones sospechosas relacionadas con el ataque. Este análisis permitió identificar una conexión activa desde la dirección IP del atacante (192.168.80.167), establecida mediante el protocolo TCP.

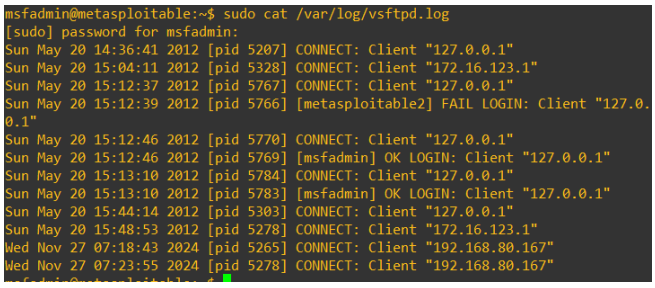


Figura C2. Revisión de archivos Logs de conexiones sospechosas por protocolo vsftpd.

4.4. Identificación de Archivos Modificados

Se utilizó el comando find para detectar cambios recientes en el sistema y se identificó la creación de un archivo sospechoso (nano.txt) en el directorio /home/msfadmin, lo que sugiere que el atacante manipuló el sistema tras obtener acceso.

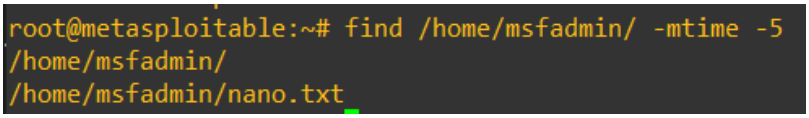


Figura C3. Identificación de archivos modificados recientemente en el directorio /home/msfadmin.

4.5. Análisis de Procesos Activos

- Se revisaron los procesos en ejecución en busca de actividad maliciosa o shells activos.
- Se detectó un proceso sospechoso que pudo haber sido utilizado para mantener el acceso persistente al sistema.

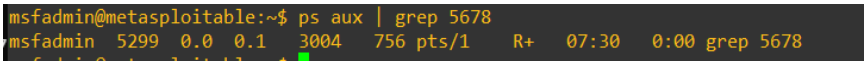


Figura C4. Identificación de proceso activo sospechoso.

---

5. Conclusión

El análisis realizado permitió identificar la explotación de una vulnerabilidad conocida en vsftpd v2.3.4, que otorgó al atacante acceso root al sistema. Las evidencias recolectadas destacan la importancia de mantener actualizados los servicios expuestos y configurar medidas de seguridad adecuadas para mitigar riesgos.

---

6. Recomendaciones

- Reemplazar vsftpd v2.3.4 por una versión segura o deshabilitar el servicio si no es esencial.
- Implementar reglas de firewall para restringir accesos externos al puerto 21.
- Realizar auditorías de seguridad para identificar y mitigar vulnerabilidades similares en otros servicios.

Guía Práctica 3

1. Tema:

Ataque con Exploit de VSFTPD

2. Objetivo:

- Identificar cómo ocurrió el ataque.
- Determinar si hubo actividad maliciosa posterior.
- Recopilar y analizar evidencia relacionada con el exploit y el acceso root.

3. Instrucciones:

Analizar la evidencia disponible de la maquina vulnerada como son los logs del sistema para cumplir los objetivos planteados.

4. Listado de equipos, materiales y recursos:

- VMware
- Wireshark
- Hashing Tools

5. Actividades por desarrollar:

Introducción

El sistema Metasploitable 2, una máquina intencionadamente vulnerable, ha sido explotado mediante una vulnerabilidad en el servicio vsftpd (vsFTPd v2.3.4), la cual permite obtener acceso a un shell con privilegios de root. Este exploit es conocido

por incluir un backdoor que otorga al atacante un shell tras una autenticación manipulada.

Análisis de archivos de la máquina virtual afectada.

La primera etapa del análisis consistió en confirmar que el servidor afectado estaba ejecutando una versión vulnerable de VSFTPD (2.3.4). Esto se logró mediante una exploración inicial con Nmap, con el comando:

nmap -p 21 -sV 192.168.80.171

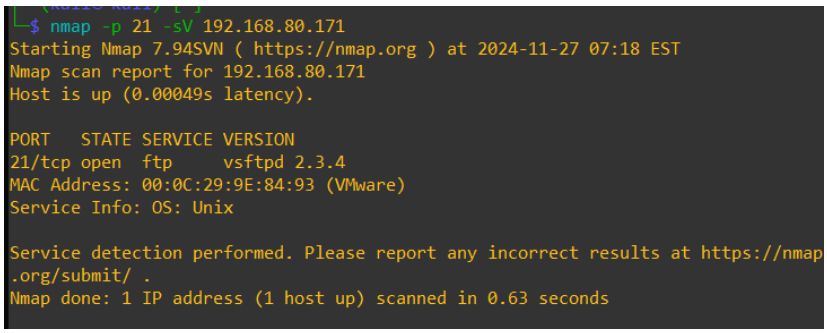


Figura C1. Escaneo del puerto 21 de la maquina víctima.

Análisis de los Registros (Logs)

Para identificar actividades sospechosas, se revisan los registros del servicio FTP. Específicamente, se examina el archivo vsftpd.log con el siguiente comando:

cat /var/log/vsftpd.log

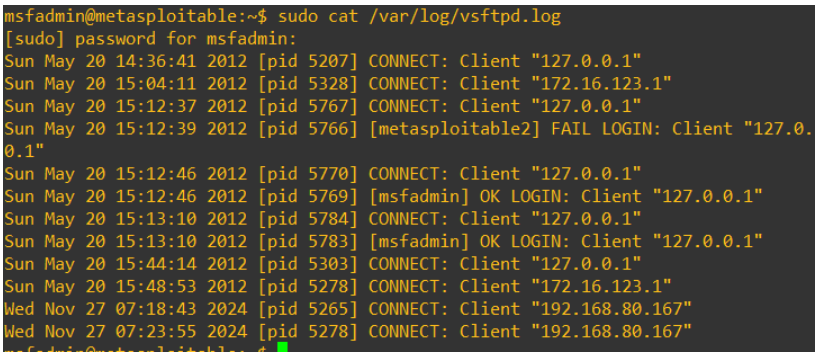


Figura C2. Revisión de archivos Logs de conexiones sospechosas por protocolo vsftpd.

Este comando muestra todas las conexiones activas. Se puede observar que la IP atacante (192.168.80.167) establece una conexión estable al protocolo TCP del servidor comprometido

Identificar archivos modificadores recientemente.

find -mtime -5

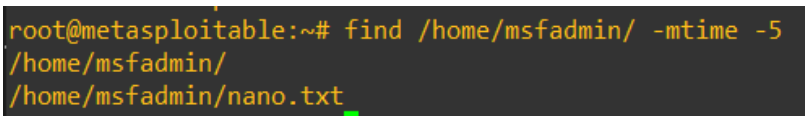


Figura C3. Identificación de archivos modificados recientemente en el directorio /home/msfadmin, detectando la creación de un archivo llamado nano.txt

Se observa creaciones de archivos en carpetas como /home/msfadmin

Se sabe que algunos procesos pueden ejecutar shells con privilegios de root, como puede ser el proceso, de esta manera se busca los procesos relacionados a este tipo de Shells.

ps aux | grep 5678

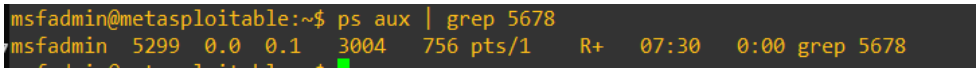


Figura C4. Identificación de proceso activo sospechoso.

6. Recomendaciones

- Desarrollar la capacidad de adaptación a nuevos retos dentro de las vulnerabilidades de Metasploitable
- Aplicar análisis forense de cada caso vulnerado o explotado de Metasploitable.

1. Introducción

El presente informe documenta el análisis forense realizado sobre un archivo pcap que contiene tráfico SMTP capturado, obtenido de un repositorio de Wireshark. Este archivo proporcionó un entorno controlado y representativo para examinar el tráfico de correo electrónico, facilitando la identificación de patrones y eventos relevantes en la comunicación a través del protocolo SMTP. El análisis permitió trabajar con datos auténticos que reflejan escenarios de interacción entre servidores y clientes de correo electrónico, asegurando la confiabilidad de las observaciones realizadas en este ejercicio.

- **Objetivo**

Analizar el tráfico SMTP capturado para identificar vulnerabilidades en la configuración del servidor, determinar el acceso y uso no autorizado de credenciales, y proponer medidas de seguridad para mitigar riesgos futuros.

---

2. Métodos y Herramientas

2.1. Métodos

Preparación del Entorno:

- Descarga del archivo pcap para análisis forense.
- Configuración de un entorno virtualizado para el análisis con herramientas específicas.

Análisis del Tráfico:

- Carga del archivo pcap en Wireshark para inspeccionar encabezados, comandos SMTP y contenidos MIME.
- Aplicación de filtros específicos para aislar el tráfico SMTP relevante.

Evidencia Forense:

- Decodificación de credenciales codificadas en Base64.
- Reconstrucción del contenido de correos electrónicos y análisis de encabezados.

2.2. Herramientas

- **VMware**: Para virtualizar el entorno de análisis.
- **Wireshark**: Captura y análisis del tráfico SMTP.
- **Comandos Linux**: Validación de la integridad de archivos y preservación de evidencia.

---

3. Actividades Desarrolladas

3.1. Descarga y Configuración Inicial

El archivo pcap fue descargado desde un repositorio público y cargado en Wireshark para su análisis. Se utilizaron filtros específicos como: *tcp.port == 465 || tcp.port == 587*

Esto permitió aislar el tráfico SMTP relacionado con conexiones cifradas, facilitando una inspección más clara.

3.2. Análisis de Sesiones SMTP

El análisis identificó que el cliente (10.10.1.4) inició conexiones con el servidor SMTP (74.53.140.153) utilizando el comando AUTH LOGIN. Las credenciales enviadas estaban codificadas en Base64 y fueron decodificadas utilizando las preferencias de protocolo de Wireshark.

Hallazgos:

- **Usuario**: gurpartap@patriots.in.

- **Contraseña**: Decodificada exitosamente, lo que sugiere la ausencia de cifrado TLS durante la transmisión.

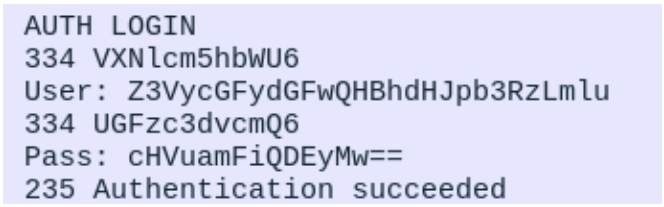


Figura D3. Trafico de red capturado en el archivo pcap.

3.3. Reconstrucción del Contenido del Correo

A través del comando DATA, se reconstruyó el contenido del correo electrónico enviado:

Encabezados:

- Message-ID: <000301ca4581$ef9e57f0$cedb07d0$@in>.
- Cliente de correo: Microsoft Office Outlook 12.0.

Cuerpo del Mensaje:

- Texto: "Hola, te envío un archivo pcap por SMTP. Busca el archivo adjunto."

Adjunto:

- Nombre: NEWS.txt.
- Contenido: Detalles técnicos relacionados con cambios de software.

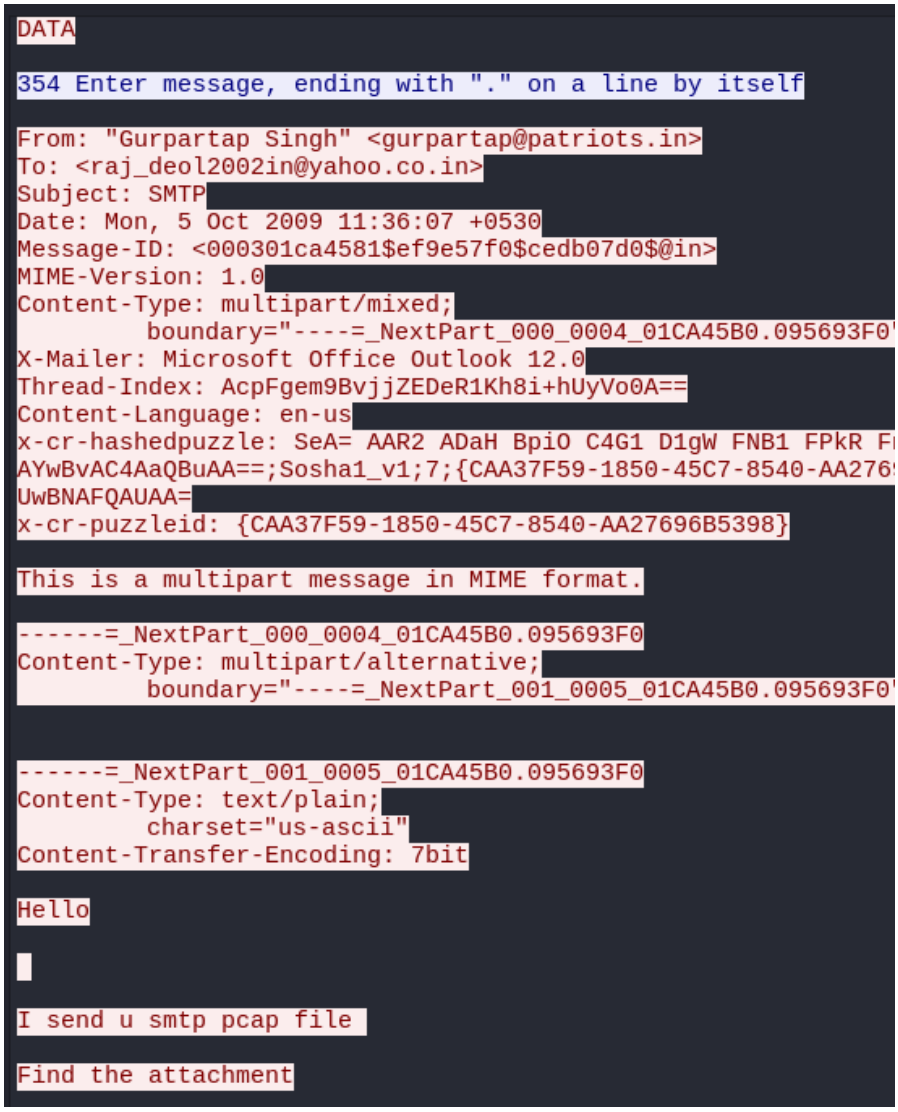


Figura D6. Contenido reconstruido de un correo electrónico capturado, mostrando detalles sensibles.

3.4. Análisis de Puertos y Direcciones

El análisis identificó las siguientes configuraciones técnicas:

Puertos Utilizados:

- Cliente: Puerto efímero 1470.
- Servidor: Puerto estándar SMTP 25.

Direcciones IP:

- Cliente: 10.10.1.4.

- Servidor: 74.53.140.153.

Direcciones MAC:

- Cliente: 3c:17:c2:00:e0:1c.
- Servidor: Dispositivo Netgear, identificado por los prefijos de hardware.

---

4. Conclusión

El análisis forense realizado evidenció la importancia del cifrado en las comunicaciones SMTP y de la implementación de configuraciones seguras para evitar accesos no autorizados. La ausencia de TLS permitió la interceptación de credenciales sensibles y podría facilitar el uso malicioso del servidor. Las medidas recomendadas son esenciales para proteger los datos y garantizar la seguridad del sistema en el futuro.

---

5. Recomendaciones

- Cambiar las credenciales comprometidas y verificar si otras cuentas han sido utilizadas de forma no autorizada.
- Auditar el servidor SMTP para detectar configuraciones inseguras.
- Implementar TLS obligatorio para todas las comunicaciones SMTP.
- Deshabilitar protocolos de autenticación no cifrados como AUTH LOGIN sin TLS.
- Requerir MFA para proteger cuentas críticas.

Guía Práctica 4

1. Tema:

Análisis forense de tráfico SMTP.

2. Objetivo:

- Identificar cómo se accedió al servidor SMTP.
- Analizar las acciones realizadas tras el acceso, incluyendo la autenticación y envío de correos.
- Determinar si se utilizaron credenciales comprometidas para envíos no autorizados.

3. Instrucciones:

Preparación:

- Descargar el archivo smtp.pcap que contiene tráfico SMTP para analizar.
- Configurar el entorno para análisis en una máquina virtual.

Ejecución:

- Abrir Wireshark y carga el archivo PCAP.
- Aplicar filtros y realiza un análisis de encabezados, autenticación y contenido MIME.

Resultados:

- Documentar los hallazgos, incluyendo posibles vulnerabilidades, análisis de reputación de IPs y contenido sospechoso.
- Generar un informe con las recomendaciones y acciones a implementar.

4. Listado de equipos, materiales y recursos:

- VMware
- Wireshark
- Archivo smtp.pcap para análisis

5. Actividades por Desarrollar

Introducción

El presente análisis forense se enfoca en un archivo pcap que contiene tráfico capturado del protocolo SMTP. El objetivo es investigar indicios de accesos no autorizados y posibles envíos de correos electrónicos no legítimos. El análisis busca identificar cómo se comprometió el servidor SMTP y determinar la naturaleza del tráfico capturado.

Además, el servidor SMTP no autoriza el uso del sistema para enviar correos electrónicos no solicitados (spam) ni correos en masa (bulk emails), lo cual es clave en el análisis de posibles abusos.

Preparación

- Adquirir el archivo de trafico de red pcap en el repositorio de wireshark, se puede descargar directamente con el comando:

Wget https://wiki.wireshark.org/uploads/__moin_import__/attachments/SampleCaptures/smtp.pcap

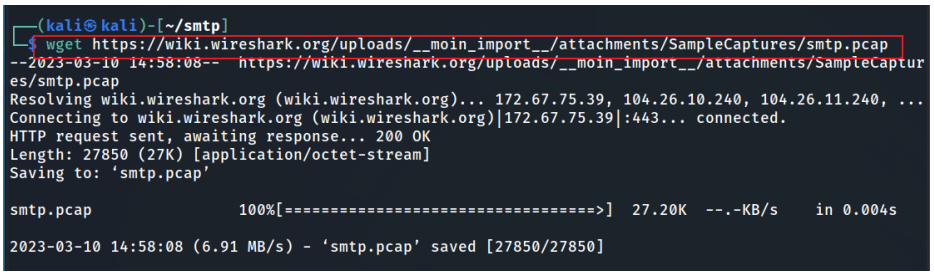


Figura D1. Descarga del archivo de trafico de red.

Análisis del archivo pcap

- Abrir Wireshark y cargar el archivo pcap (File > Open > smtp_traffic.pcap).

Para una mejor visualización del cifrado se usa el siguiente filtro:

tcp.port == 465 || tcp.port == 587

- Configurar las columnas de visualización necesarias (e.g., Fuente, Destino, Protocolo, Puerto).

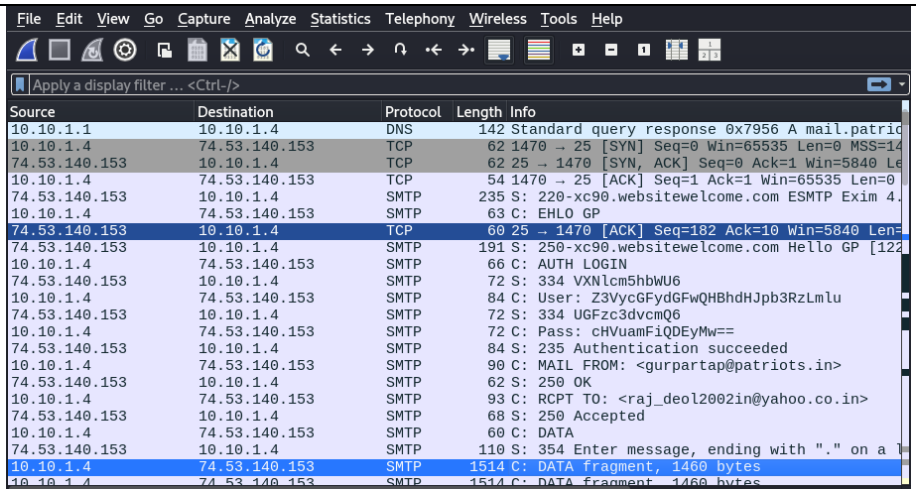


Figura D2. Examinación del archivo pcap en la herramienta Wireshark.

Identificar sesiones de autenticación (normalmente se describen con AUTH LOGIN) e indicios de envió de algún correo no autorizado dentro del tráfico de red.

- Observa las columnas de Source (origen) y Destination (destino). Identifica las direcciones IP involucradas en la comunicación:

Fuente: **10.10.1.4** parece ser el cliente que inicia la conexión.

Destino: **74.53.140.153**, que probablemente es el servidor SMTP.

- Observa que el protocolo SMTP aparece claramente en el tráfico, confirmando que se están transmitiendo datos relacionados con correos electrónicos.

Se identifica el comando AUTH LOGIN seguido de un username y password claramente codificados en base64

```
AUTH LOGIN
334 VXNlcm5hbWU6
User: Z3VycGFydGFwQHBhdHJpb3RzLmlu
334 UGFzc3dvcmQ6
Pass: cHVuamFiQDEyMw==
235 Authentication succeeded
```

Figura D3. Trafico de red capturado en el archivo pcap.

Decodificar las credenciales con la herramienta wireshark dando clic derecho a algún paquete visto y seleccionar “Protocol preferences >> SMTP >> decode base 64”.

```
AUTH LOGIN
334 Username:
User: gurpartap@patriots.in
334 Password:
Pass: punjab@123
235 Authentication succeeded
```

Figura D4. Credenciales desencriptadas por Wireshark.

Análisis de comandos SMTP

Observar los siguientes comandos y analizar sus implicaciones:

- **MAIL FROM:** gurpartap@patriots.in. Identifica el remitente del correo.
- **RCPT TO:** raj_deol2002in@yahoo.co.in. Es el destinatario.
- **DATA:** Aquí se transmite el contenido del correo.

Realizar un seguimiento del comando DATA para reconstruir el mensaje:

1. Haz clic derecho sobre el paquete relacionado con el comando DATA.
2. Selecciona **Follow TCP Stream** para visualizar el contenido completo del mensaje enviado.

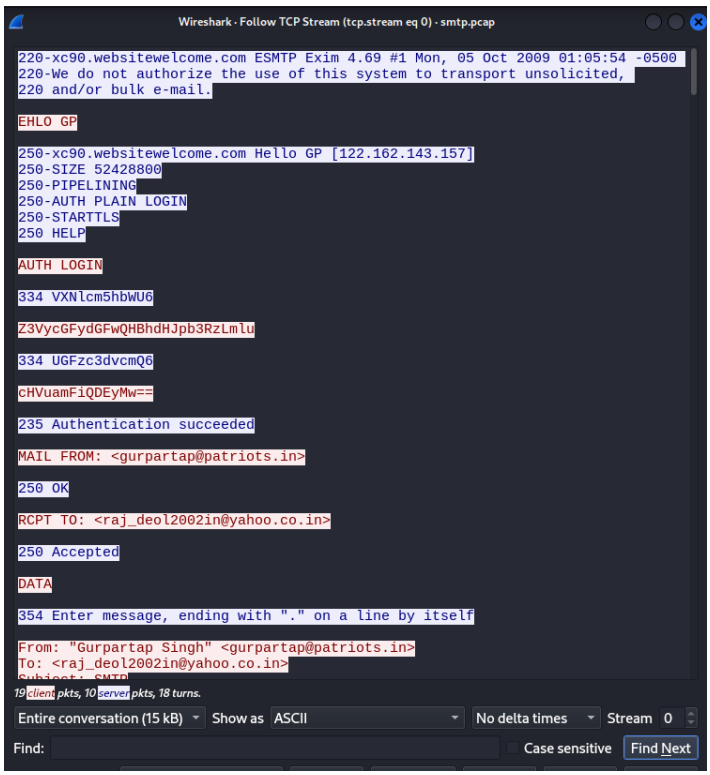


Figura D5. Análisis de tráfico SMTP en Wireshark para reconstruir contenido.

Análisis del Contenido del Correo

Encabezados del Correo:

El encabezado Message-ID es único: <000301ca4581$ef9e57f0$cedb07d0$@in>.

X-Mailer: Microsoft Office Outlook 12.0.

Cuerpo del Mensaje:

Texto simple: "Hello, I send u smtp pcap file. Find the attachment."

Archivo Adjunto:

Nombre: NEWS.txt.

- Contenido: Incluye información sobre versiones de software, lo que podría ser legítimo o una técnica para evadir análisis.

El seguimiento de cómo se accede y envía el correo se da en DATA, aquí se tiene la siguiente información:

La fecha y hora del correo electrónico son:

- lunes, 5 de octubre de 2009 11:36:07 +0530 (hora local del remitente).
- Fecha y hora del servidor: lunes, 5 de octubre de 2009 01:05:54 -0500.

El cliente de correo electrónico:

- El cliente utilizado para enviar el correo electrónico es Microsoft Office Outlook 12.0

El contenido del correo electrónico:

- El correo electrónico contiene contenido de varias partes, que incluye:
- Texto simple: "Hola, te envío un archivo pcap por SMTP. Busca el archivo adjunto".
- Una versión HTML del mensaje.
- Un archivo adjunto (NEWS.txt) con detalles del registro de cambios de un software.

Puertos utilizados:

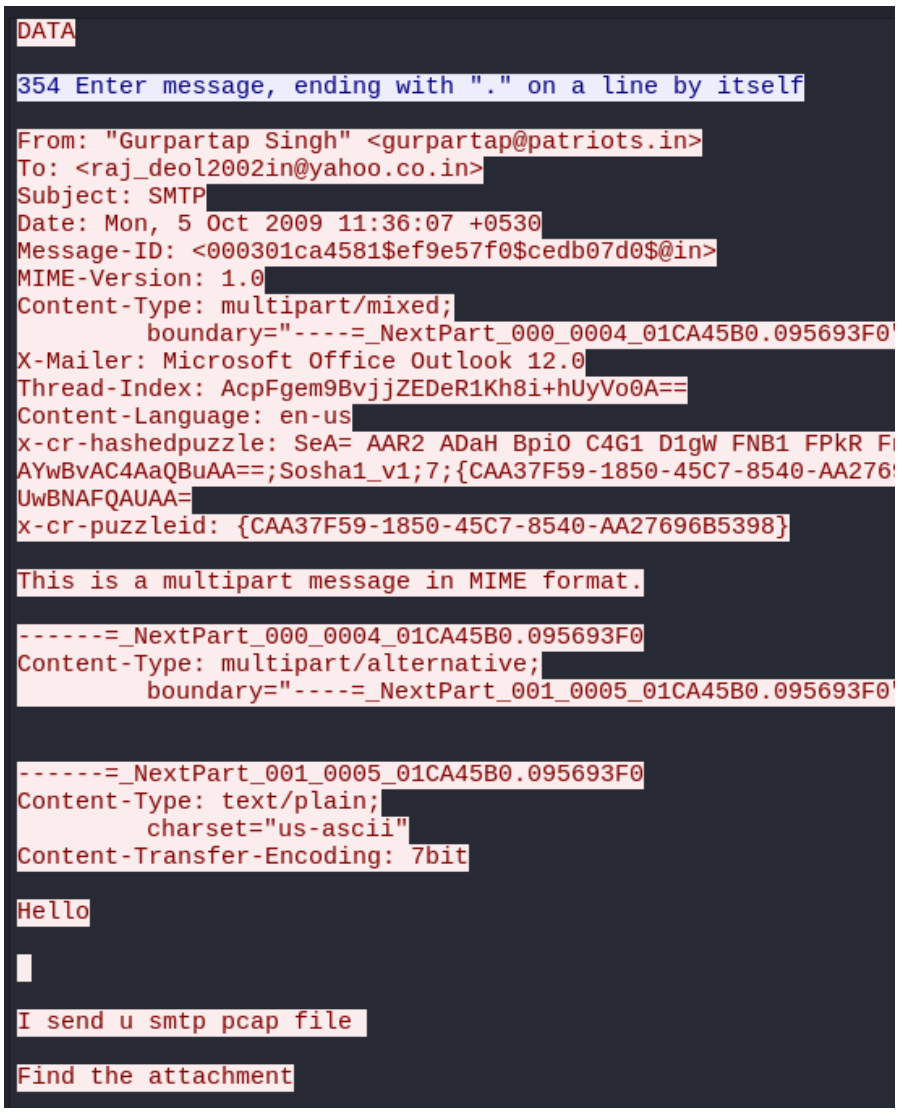
- El remitente utilizó el puerto 1470 (puerto efímero).
- El receptor (servidor SMTP) utilizó el puerto 25 para la comunicación.

Direcciones IP:

- IP del remitente: 10.10.1.4 (red interna).
- IP del receptor: 74.53.140.153 (servidor SMTP).

Direcciones MAC:

- MAC del remitente: 3c:17:c2:00:e0:1c (como se capturó en la red).
- MAC del receptor: dispositivo Netgear (como se deduce de los prefijos del proveedor de hardware).



```
DATA

354 Enter message, ending with "." on a line by itself

From: "Gurpartap Singh" <gurpartap@patriots.in>
To: <raj_deol2002in@yahoo.co.in>
Subject: SMTP
Date: Mon, 5 Oct 2009 11:36:07 +0530
Message-ID: <000301ca4581$ef9e57f0$cedb07d0$@in>
MIME-Version: 1.0
Content-Type: multipart/mixed;
        boundary="----=_NextPart_000_0004_01CA45B0.095693F0"
X-Mailer: Microsoft Office Outlook 12.0
Thread-Index: AcpFgem9BvjjZEDeR1Kh8i+hUyVo0A==
Content-Language: en-us
x-cr-hashedpuzzle: SeA= AAR2 ADaH BpiO C4G1 D1gW FNB1 FPkR F
AYwBvAC4AaQBuAA==;Sosha1_v1;7;{CAA37F59-1850-45C7-8540-AA276
UwBNAFQAUAA=
x-cr-puzzleid: {CAA37F59-1850-45C7-8540-AA27696B5398}

This is a multipart message in MIME format.

------=_NextPart_000_0004_01CA45B0.095693F0
Content-Type: multipart/alternative;
        boundary="----=_NextPart_001_0005_01CA45B0.095693F0"


------=_NextPart_001_0005_01CA45B0.095693F0
Content-Type: text/plain;
        charset="us-ascii"
Content-Transfer-Encoding: 7bit

Hello

I send u smtp pcap file

Find the attachment
```

Figura D6. Contenido reconstruido de un correo electrónico capturado, mostrando detalles sensibles.

6. Recomendaciones

Acción Inmediata:

- Si las credenciales fueron comprometidas, cámbialas inmediatamente.
- Investiga si otras cuentas en el servidor han sido utilizadas de forma similar.

Mejoras de Seguridad:

- Implementa autenticación multifactorial (MFA) para todos los usuarios del servidor SMTP.
- Habilita cifrado TLS obligatorio para todo el tráfico SMTP.

Monitoreo Continuo:

- Configura alertas en el servidor SMTP para detectar:
- Autenticaciones sospechosas.
- Envió masivo de correos no autorizados.

Anexo E. Informe Técnico – Guía Práctica 5 – DNS Spoofing

1. Introducción

Se identificaron comportamientos anómalos en el sistema, donde las solicitudes DNS legítimas parecían ser redirigidas a IPs sospechosas. El objetivo es determinar si se trata de un ataque de DNS Spoofing y documentar evidencia para la mitigación.

- **Objetivo**

Confirmar la existencia del ataque, identificar el alcance y las técnicas utilizadas, y proporcionar recomendaciones para evitar futuros incidentes similares.

---

2. Métodos y Herramientas Utilizadas

Métodos

- Preservación de evidencia (captura de tráfico, integridad de datos).
- Inspección del tráfico DNS mediante Wireshark.
- Validación de configuraciones DNS en el sistema.
- Comparación de registros DNS con herramientas como dig y nslookup.

Herramientas

- **Wireshark**: Captura y análisis de tráfico de red.

- **Comandos Linux**: Validación (cat /etc/resolv.conf, dig, nslookup).

---

3. Evidencia Recolectada

3.1. Capturas de Tráfico DNS en Wireshark

Se muestra cómo el dominio victordoc.com fue redirigido a la IP maliciosa 192.168.80.167.

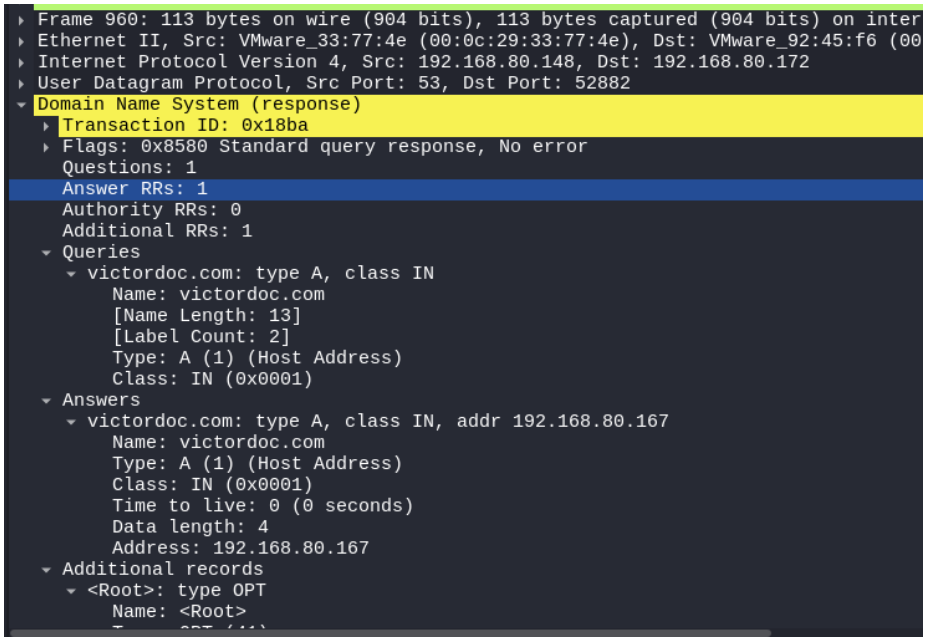


Figura E4. Análisis de tráfico DNS

3.2. Configuración DNS del Sistema

Contenido del archivo /etc/resolv.conf.

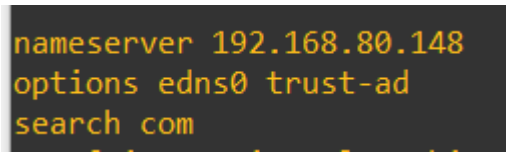


Figura E5. Contenido del archivo /etc/resolv.conf.

3.3. Validación con dig y nslookup

Respuesta correcta de un servidor DNS legítimo.



Figura E6. Resolución de DNS con el comando dig para el dominio victordoc.com.

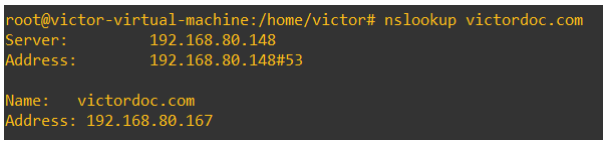


Figura E7. Resolución del dominio victordoc.com con ip maliciosa.

---

4. Conclusiones

El análisis forense confirmó la existencia de un ataque de DNS Spoofing, que redirigió tráfico legítimo hacia una IP maliciosa mediante manipulaciones en las respuestas DNS. Este ataque expuso datos sensibles y comprometió la confiabilidad de los servicios en la red afectada. Las medidas recomendadas son esenciales para prevenir futuros incidentes y fortalecer la seguridad del sistema DNS.

---

5. Recomendaciones

- Configurar servidores DNS seguros y evitar el uso de servidores no confiables.
- Implementar herramientas de monitoreo de red para detectar anomalías en el tráfico DNS.
- Actualizar regularmente el sistema operativo y aplicar parches de seguridad.
- Establecer registros completos de actividad para futuras investigaciones.
- Entrenar al equipo técnico en la identificación de comportamientos anómalos en la red.

Guía Práctica 5

1. Tema:

DNS Spoofing

2. Objetivo:

Desarrollar un procedimiento forense para identificar evidencia de un ataque de DNS Spoofing y determinar su impacto en un sistema Linux.

3. Instrucciones:

Un sistema Linux presenta indicios de redirecciones no autorizadas a dominios sospechosos. El administrador sospecha de un ataque de DNS Spoofing y necesita confirmar si se manipularon las respuestas DNS, identificar los posibles vectores de ataque, y documentar la evidencia recolectada para una posterior mitigación y reporte.

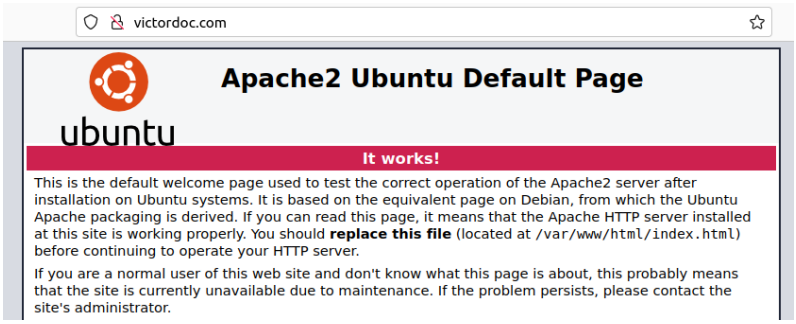


Figura E1. Página web apache del servidor

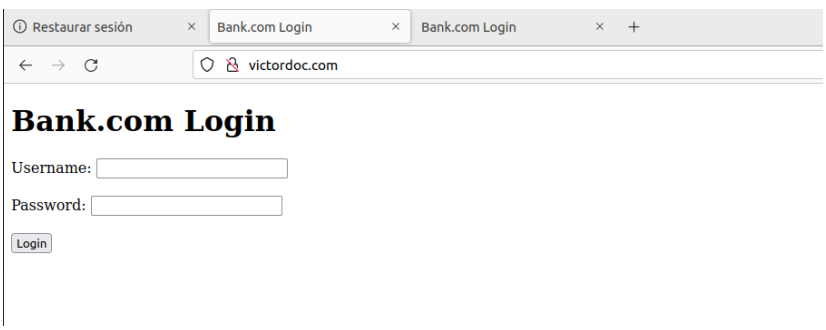


Figura E2. Cambio de página web del servidor por DNS spoofing.

4. Listado de equipos, materiales y recursos:

- VMware
- Sistema Linux
- Registros DNS
- Wireshark

5. Actividades por Desarrollar

Captura de tráfico de red

Iniciar la herramienta tcpdump para capturar tráfico DNS en la red:

sudo tcpdump -i <interfaz> port 53 -w dns_traffic.pcap

Analizar las solicitudes y respuestas DNS capturadas usando Wireshark.

- Filtrar los paquetes con “dns” y observar discrepancias en las respuestas de los servidores.

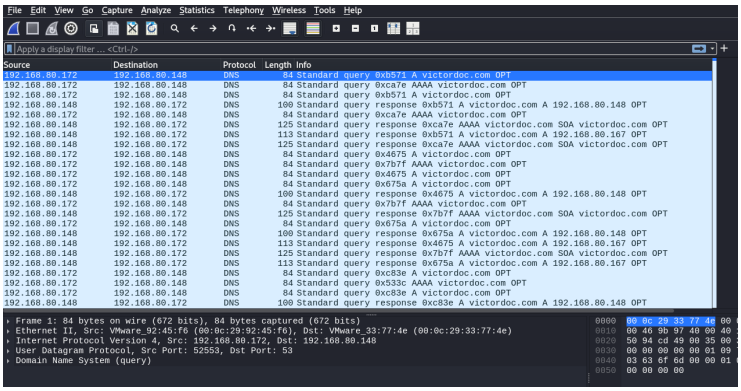


Figura E3. Captura de paquetes de red en tiempo real.

El ataque presentado modifica las respuestas DNS para redirigir dominios comunes a una IP maliciosa (192.168.80.167). Al analizar con Wireshark, estas manipulaciones serán visibles al comparar:

- **Dominio solicitado** (dns.qry.name): victordoc.com.
- **Respuesta maliciosa** (dns.a): 192.168.80.167.

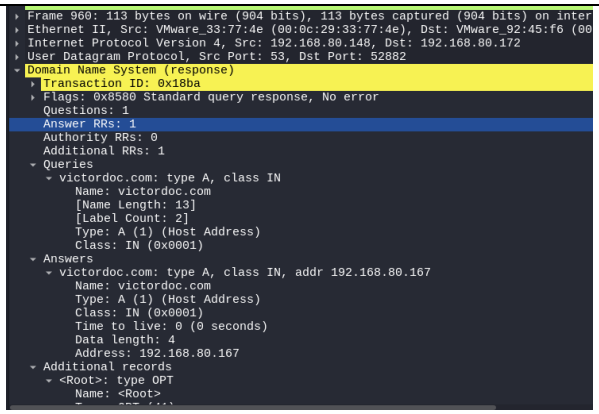


Figura E4. Análisis de tráfico DNS

Inspeccionar el archivo 'etc.resolv.conf' para verificar que apunta a servidores DNS confiables

cat /etc/resolv,conf

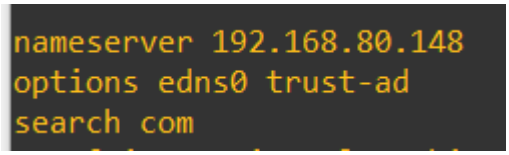


Figura E5. Contenido del archivo /etc/resolv.conf.

Determinar el alcance del ataque y los sistemas afectados, para esto se utiliza herramientas como `dig` y `nslookup` para validar la resolución de dominios sospechosos y confirmar si fueron redirigidos a IPs maliciosas.

dig victordoc.com

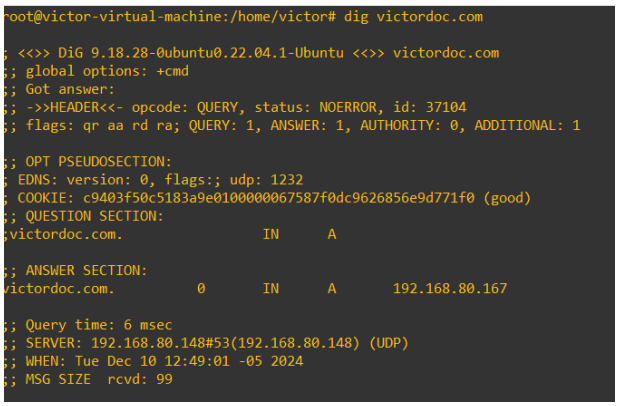


Figura E6. Resolución de DNS con el comando dig para el dominio victordoc.com.

Se observa como la ip del dominio establecido se ha redireccionado a otro, en este caso el atacante. De igual manera se puede visualizar con el comando nslookup

nslookup victordoc.com

```
root@victor-virtual-machine:/home/victor# nslookup victordoc.com
Server:         192.168.80.148
Address:        192.168.80.148#53

Name:   victordoc.com
Address: 192.168.80.167
```

Figura E7. Resolución del dominio victordoc.com con ip maliciosa.

Verificar el estado del dns del sistema y determinar si hubo manipulación, aquí se identifica servidores dns configurados como también interfaces de red afectadas.

resolvectl status

```
victor@victor-virtual-machine:~$ resolvectl status
Global
         Protocols: -LLMNR -mDNS -DNSOverTLS DNSSEC=no/unsupported
  resolv.conf mode: stub
Current DNS Server: 192.168.80.148
       DNS Servers: 192.168.80.148

Link 2 (ens33)
    Current Scopes: DNS
         Protocols: +DefaultRoute +LLMNR -mDNS -DNSOverTLS DNSSEC=no/unsupported
Current DNS Server: 192.168.80.2
       DNS Servers: 192.168.80.2
        DNS Domain: localdomain

Link 3 (ens34)
    Current Scopes: DNS
         Protocols: +DefaultRoute +LLMNR -mDNS -DNSOverTLS DNSSEC=no/unsupported
Current DNS Server: 192.168.1.1
       DNS Servers: 192.168.1.1 192.168.2.1
```

Figura E8. Verificación del estado del DNS del sistema utilizando el comando resolvectl status.

Se tiene DNS Servers asociados a la interfaz comprometida (ens33 en este caso).

Consultar el dominio afectado utilizando *resolvectl query* para verificar que dirección ip resuelve el dominio.

resolvectl query victordoc.com

```
victor@victor-virtual-machine:~$ resolvectl query amazon.com
amazon.com: ::ffff:192.168.80.167              -- link: ens33
            192.168.80.167                     -- link: ens33

-- Information acquired via protocol DNS in 22.9ms.
-- Data is authenticated: no; Data was acquired via local or encrypted transport: no
-- Data from: network
```

Figura E9. Consulta del dominio victordoc.com utilizando resolvectl query,

Se verifica una dirección ip redireccionada <192.168.80.167>, confirmando el dns spoofing.

Analizar tráfico http, en wireshark agregar un filtro “http” e inspeccionar los paquetes de trafico de red.

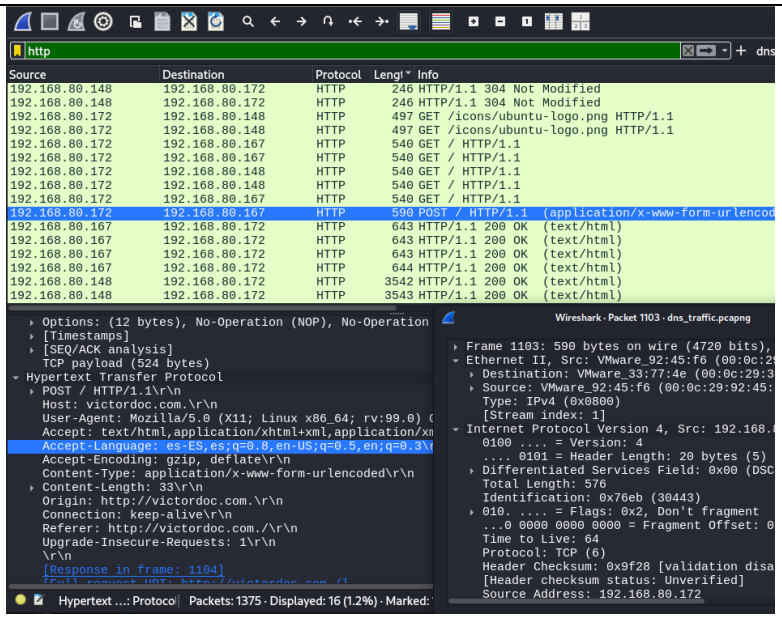


Figura E10. Análisis de tráfico HTTP en Wireshark utilizando un filtro.

En este apartado se puede identificar detalles de la víctima, algunos detalles son:

- User agent
- Sistema vulnerable por el protocolo http sin seguridad ssl
- Contenido enviado al server malicioso en un método POST
- Se tiene el Source Port (punto temporal: 40780) y el Destination Port (HTTP: 80)
- Confirmación de redirección de tráfico a una página HTML.

6. Recomendaciones

- Configurar servidores DNS seguros y evitar el uso de servidores no confiables.
- Implementar herramientas de monitoreo de red para detectar anomalías en el tráfico DNS.
- Actualizar regularmente el sistema operativo y aplicar parches de seguridad.
- Establecer registros completos de actividad para futuras investigaciones.
- Entrenar al equipo técnico en la identificación de comportamientos anómalos en la red.

Anexo F. Informe Técnico – Guía Práctica 6 – Escala de privilegios

1. Introducción

Este informe detalla el análisis forense realizado en una máquina denominada "Mi File Server 1", comprometida mediante una vulnerabilidad en el protocolo FTP. El atacante utilizó este punto de acceso para inyectar claves SSH y posteriormente ejecutar un escalamiento de privilegios mediante el exploit Dirty COW (CVE-2016-5195), que aprovecha vulnerabilidades en el kernel de Linux. El análisis busca identificar evidencia del ataque, evaluar su impacto, y proponer medidas para mitigar futuras amenazas.

- **Objetivo**

Determinar cómo se llevó a cabo el escalamiento de privilegios, identificar los indicios de actividad maliciosa en los registros del sistema, y recopilar evidencia técnica que permita implementar medidas de mitigación.

---

2. Métodos y Herramientas

Métodos

- Creación de una copia forense de la imagen del disco utilizando herramientas de hash para garantizar la integridad.
- Inspección de registros asociados al protocolo FTP y SSH.
- Identificación de archivos recientemente modificados o creados, destacando aquellos asociados con actividades del atacante.

Herramientas

- **VMware**: Virtualización del entorno de análisis.
- **dcfldd**: Creación de copias forenses de discos.

- **mmls**: Visualización de particiones.
- **Comandos Linux**: Revisión de registros y análisis de timestamps.
- **Wireshark**: Inspección de tráfico en redes comprometidas.

---

3. Actividades Desarrolladas

3.1. Preservación de la Evidencia

Se agregó el disco comprometido a un entorno de análisis en Kali Linux y se generó una copia forense utilizando dcfldd. Los hashes de la imagen del disco (sha256 y md5) confirmaron la integridad de los datos.



Figura F1. Custodia de la imagen forense y validación de su integridad.

3.2. Análisis de la Imagen del Disco

El contenido del disco fue visualizado con mmls, permitiendo identificar particiones relevantes. Posteriormente, se extrajo la partición del sistema raíz para su análisis:

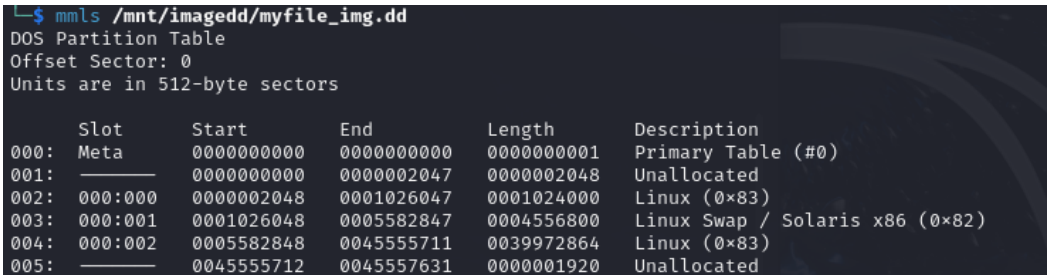


Figura F2. Contenido del disco .dd visualizado con mmls.

3.3. Revisión de Logs del Protocolo FTP

Los registros asociados al protocolo FTP fueron analizados para identificar actividades sospechosas. Si bien vsftpd.log no contenía información relevante, xferlog reveló que

archivos maliciosos fueron subidos al directorio /home/smbuser/.ssh/. La clave SSH incrustada (ssh-rsa) permitió al atacante establecer conexiones no autorizadas.

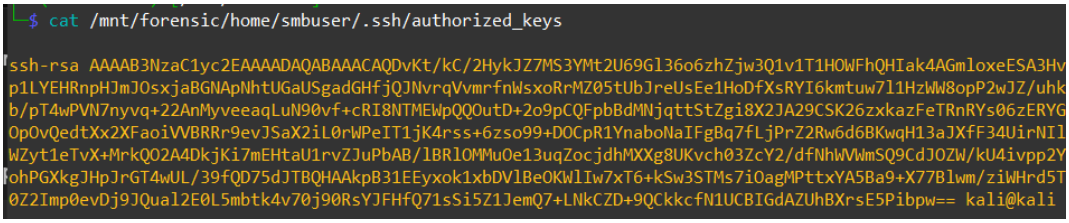


Figura F4. Clave maliciosa agregada a la maquina víctima.

3.4. Identificación de Archivos Modificados

Utilizando el comando find, se identificaron archivos recientemente modificados y en su análisis destacó el archivo authorized_keys como evidencia clave del ataque, junto con otros archivos sospechosos en el directorio /var/log.

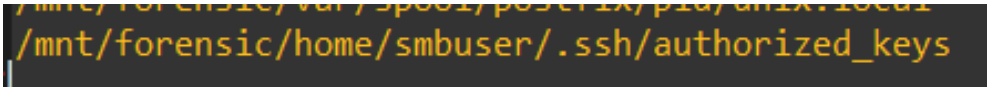


Figura F5. Uso del comando *find* para identificar archivos modificados recientemente en el sistema.

3.5. Análisis de Registros SSH

Revisando algunos archivos de logs se ha encontrado acciones realizadas, pero ha destacado el archivo de registros secure-20241213 ya que se identificaron intentos fallidos de conexión SSH desde la IP del atacante (192.168.80.167), así como un eventual acceso exitoso.

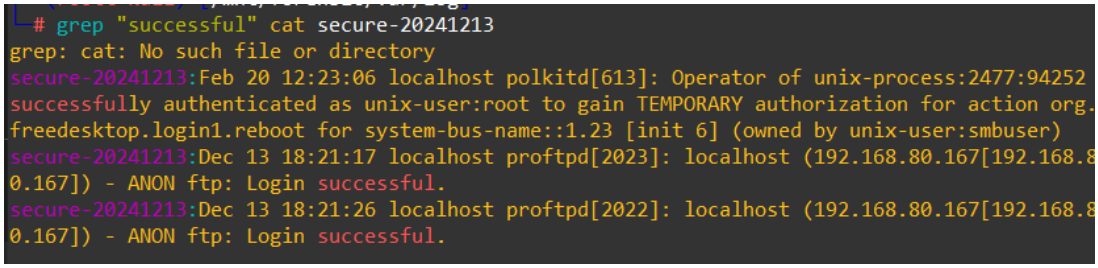


Figura F7. Análisis del archivo secure-20241213 en el directorio /var/log.

4. Conclusión

El análisis forense confirmó que la máquina "Mi File Server 1" fue comprometida mediante un ataque dirigido que combinó una vulnerabilidad en el protocolo FTP y un exploit de escalamiento de privilegios (Dirty COW). La actividad maliciosa incluyó la inyección de claves SSH y modificaciones en archivos críticos del sistema. Las medidas recomendadas buscan mitigar futuros ataques y fortalecer la seguridad de los sistemas vulnerables.

---

5. Recomendaciones

- Instalar parches de seguridad para el kernel y servicios vulnerables, eliminando la exposición a exploits como Dirty COW.
- Deshabilitar el servicio FTP si no es necesario y utilizar alternativas más seguras como SFTP.
- Implementar herramientas de monitoreo para detectar cambios no autorizados en archivos críticos y actividad sospechosa en la red.
- Capacitar al personal en respuesta a incidentes de seguridad y realizar auditorías periódicas para detectar configuraciones inseguras.

Guía Práctica 6

1. Tema:

Escala de privilegios

2. Objetivo:

Profundizar en los archivos logs y registros del Sistema vulnerado con el fin de encontrar indicios de escalado de privilegios.

3. Instrucciones:

Desarrollar el análisis de disco duro de una maquina vulnerada “mi file server 1” donde ha sido violentada por el protocolo ftp inyectando cables SSH para conseguir un escalado de privilegios de usuario con un exploit de kernel como el exploit de dirty cow.

4. Listado de equipos, materiales y recursos:

- VMware
- Sistema Linux
- Registros DNS
- Wireshark
- Archivo smtp pcap para análisis

5. Actividades por Desarrollar

Introducción

En el presente análisis forense se aborda el estudio de una máquina denominada "Mi File Server 1", que ha sido comprometida por medio de una vulnerabilidad en el protocolo FTP. El atacante utilizó este punto de acceso para inyectar claves SSH y obtener acceso no autorizado. Posteriormente, llevó a cabo un escalamiento de privilegios de usuario aprovechando una vulnerabilidad en el kernel mediante un exploit conocido, como el caso de Dirty COW (CVE-2016-5195).

Asegurar la evidencia

Agregar el disco duro de la maquina comprometida a Kali Linux y hacer una copia para su análisis.

sudo dcfldd if=/dev/sdb of=/mnt/imagedd/myfile_img.dd hash=sha256 hashlog=/mnt/imagedd/hashlog.txt



Figura F1. Custodia de la imagen forense y validación de su integridad.

Asegurar la integridad de los datos de la imagen de disco y la copia realizada

sudo sha256sum /dev/sdb

sudo sha256sum file.dd

/dev/sdb	0039916915423492aab098d5dc70e0b50670dc3abc309847edac15c9b3ad86ce
myfile_img.dd	0039916915423492aab098d5dc70e0b50670dc3abc309847edac15c9b3ad86ce

Visualizar el contenido del disco duro con <mmls>, esta muestra particiones del disco el cual se debe montar únicamente las que pueden dar datos relevantes.

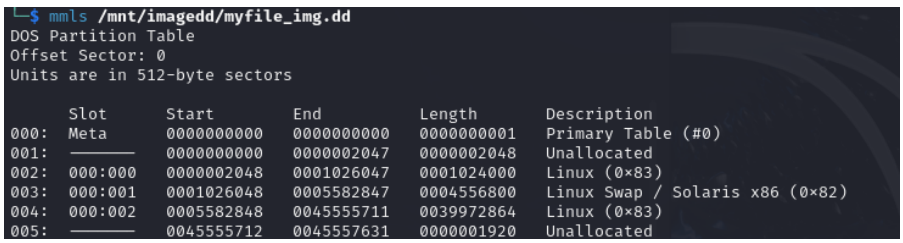


Figura F2. Contenido del disco .dd visualizado con mmls.

Se requiere extraer el disco con más información del Sistema "/", para esto se ejecuta el comando:

sudo dcfldd if=/ruta/a/la/imagen.dd of=/ruta/a/particion1.dd skip=2048 bs=512

- if: Archivo de entrada (imagen original).
- of: Archivo de salida (nombre del archivo extraído).
- bs=512: Tamaño del bloque (coincide con los sectores físicos).
- skip=1026048: Saltar los sectores iniciales antes de la partición.

Revisión de archivos Log del sistema

Principalmente se investiga los archivos logs del protocolo vulnerado FTP, en estos se encuentran las actividades que están sucediendo, se busca en /var/log/vsftpd.log y /var/log/xfer.log

cat /mnt/forensic/var/log/vsftpd.log

cat /mnt/forensic/var/log/xferlog

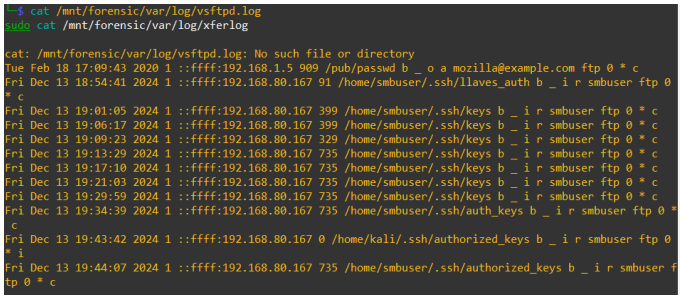


Figura F3. Análisis de los logs del protocolo FTP.

Los archivos log de vsftpd.log no se han registrado, sin embargo, los logs de 'xferlog' muestran que se han subido archivos a la carpeta /home/smbuser/.ssh/ por el protocolo ftp, lo que indica una vulnerabilidad en ftp y se accedió.

Revisar la carpeta mencionada donde se subieron los archivos, en esta se encontró una key de tipo 'ssh-rsa' para una conexión con Kali Linux.

cat /mnt/forensic/home/smbuser/.ssh/authorized_keys

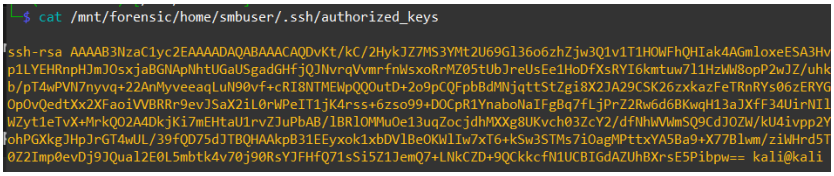


Figura F4. Clave maliciosa agregada a la maquina víctima.

Dicho esto, se busca más información en el sistema como archivos que pudo borrar el atacante usando timestamps recientes de archivos.

find /mnt/forensic -type f -mtime -30

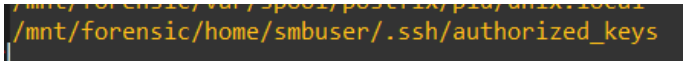


Figura F5. Uso del comando *find* para identificar archivos modificados recientemente en el sistema.

Se muestran múltiples archivos sospechosos pero el más destacado es el archivo 'autorized_keys'.

Revisando los logs del sistema ubicados en /var/log se encuentran algunos archivos modificados a una hora no concordante (Dec 13) por lo que se debería revisar los archivos uno a uno de ser necesario o si tiene conocimiento en el tema se revisa directamente archivos deseados, la mayoría son root por lo que deben verlos con privilegios root.

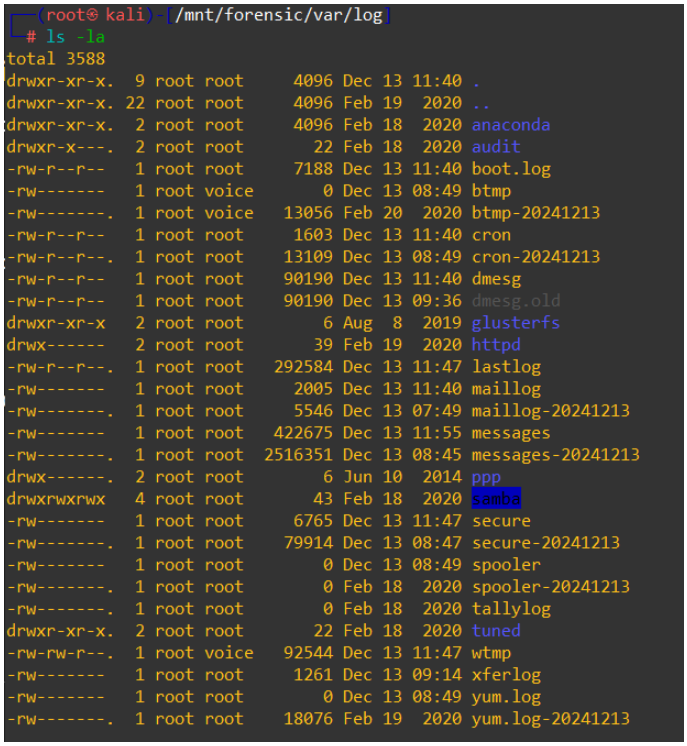


Figura F6. Exploración del directorio /var/log para identificar archivos de log modificados en fechas sospechosas.

Ingresando a un archivo llamado ‘secure-20241213’ se encuentran logs de una ip desconocida <192.168.80.167> tratando de ingresar por ssh, con intentos fallidos, pero a la larga se conecta al servidor.

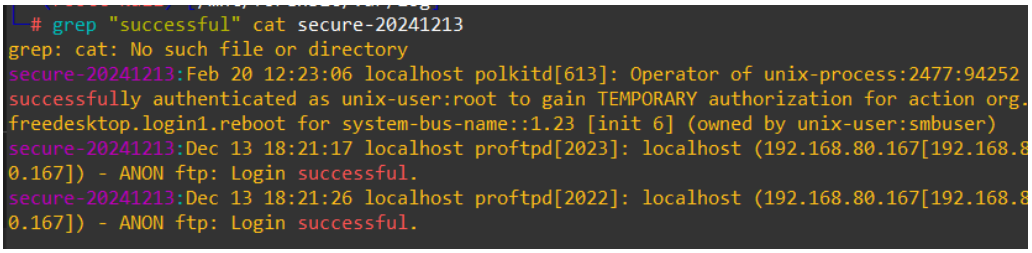


Figura F7. Análisis del archivo secure-20241213 en el directorio /var/log.

6.	Recomendaciones
	• Configurar servidores DNS seguros y evitar el uso de servidores no confiables. • Implementar herramientas de monitoreo de red para detectar anomalías en el tráfico DNS. • Actualizar regularmente el sistema operativo y aplicar parches de seguridad. • Establecer registros completos de actividad para futuras investigaciones. • Entrenar al equipo técnico en la identificación de comportamientos anómalos en la red.

Anexo G. Informe Técnico – Guía Práctica 7 – Android 10

1. Introducción

El presente informe documenta el análisis forense realizado sobre un conjunto de archivos extraídos de un dispositivo Android 10, enfocados en los datos generados por la aplicación WhatsApp. Este análisis permitió extraer información clave como el número de teléfono registrado en la aplicación, contactos almacenados, y datos relacionados con la estructura de las bases de datos utilizadas por WhatsApp.

- **Objetivo**

Investigar la estructura y contenido de los archivos de WhatsApp extraídos del dispositivo, identificando información relevante como números telefónicos, contactos, y otros datos almacenados en bases de datos y archivos asociados.

---

2. Métodos y Herramientas

Métodos

- Se utilizó el archivo comprimido Pixel 3.zip como fuente de datos para el análisis.

- Navegación por directorios para identificar archivos relevantes.

- Inspección de carpetas como shared_prefs y databases.
- Uso de SQLite para examinar la base de datos wa.db y extraer información de contactos almacenados.
- Revisión de archivos XML para obtener información como el número de teléfono asociado al dispositivo.

Herramientas

- **VMware**: Virtualización del entorno de análisis.
- **Linux Commands**: Navegación y análisis de directorios (tree, unzip).
- **SQLiteBrowser**: Análisis de bases de datos SQLite utilizadas por WhatsApp.
- **Web Tools**: Páginas como "AllAreaCodes" para investigar números telefónicos.

---

3. Actividades Desarrolladas

3.1. Descompresión y Montaje de Evidencia

Se descomprimió el archivo Pixel 3.zip para acceder a los datos almacenados en el dispositivo Android. Posteriormente, se utilizó el comando tree para visualizar la estructura de archivos dentro del directorio principal de WhatsApp.

Esto permitió identificar carpetas clave, como shared_prefs y databases.

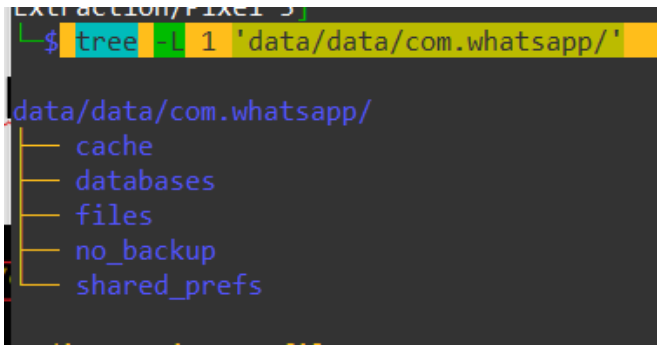


Figura G1. Visualización de la estructura de directorios de WhatsApp.

3.2. Número de Registro de WhatsApp

Se inspeccionó el contenido de la carpeta shared_prefs, donde se encontró un archivo XML que contenía información relevante, incluyendo el número de teléfono registrado en WhatsApp (9195794674). Este dato fue extraído y validado mediante herramientas web, confirmando la procedencia del número.

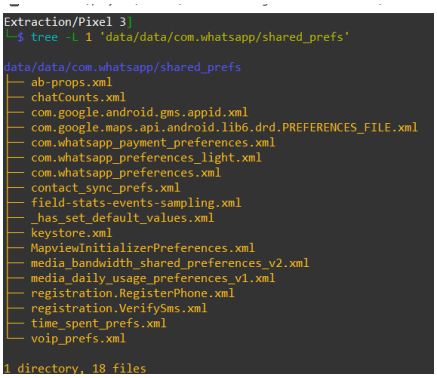


Figura G2. Exploración de la carpeta shared_prefs.

3.3. Análisis de Contactos en Bases de Datos

En el directorio databases, se identificaron varias bases de datos SQLite. Se utilizó sqlitebrowser para analizar el archivo wa.db, que contiene información sobre los contactos almacenados en WhatsApp. El análisis reveló datos organizados en tablas, específicamente en la tabla wa_contacts, que incluye:

- ID del contacto.
- Nombre del contacto.
- Estado del contacto (e.g., mensajes disponibles, última conexión).



Figura G3. Análisis del directorio databases dentro de los archivos de WhatsApp.

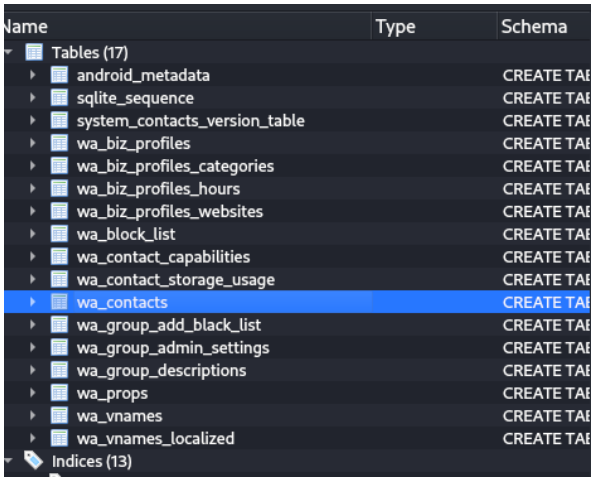


Figura G4. Vista general de las tablas contenidas en la base de datos wa.db.

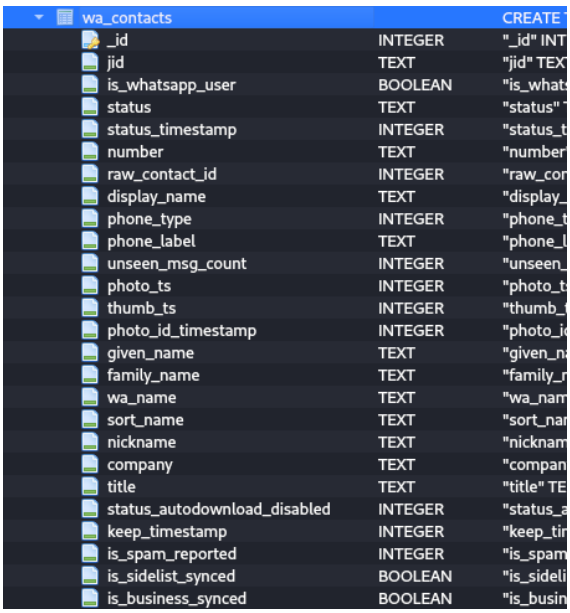


Figura G5. Detalle de la estructura de la tabla wa_contacts.

---

4. Conclusión

El análisis forense permitió extraer información significativa de los archivos de WhatsApp almacenados en un dispositivo Android 10. Este proceso evidenció la importancia de los archivos shared_prefs y databases en la recuperación de datos relevantes como números telefónicos y contactos. Las recomendaciones buscan ampliar el alcance del análisis y mejorar la eficiencia de futuros estudios forenses.

---

5. Recomendaciones

- Revisar otros archivos presentes en el archivo ZIP para identificar datos adicionales como historiales de mensajes o archivos multimedia.
- Utilizar herramientas específicas como Autopsy para analizar el contenido del dispositivo de forma más exhaustiva.
- Desarrollar scripts que permitan automatizar la extracción de datos clave en futuros análisis.

Guía Práctica 7

1. Tema:
Android 10

2. Objetivo:
Investigar un escenario relacionado a archivos de WhatsApp donde se almacenan diferentes archivos y presentar resultados de la investigación.

3. Instrucciones:
Descargar un zip donde encontrara diferentes archivos obtenidos de un celular para su análisis forense respectivo, montar cada evidencia y analizarla según corresponda.

4. Listado de equipos, materiales y recursos:
• Registros DNS • Wireshark • Archivo pcap para análisis • *Sqlitebrowser* • *tree*

5. Actividades por Desarrollar

Introducción

En este análisis forense se realizó un estudio de los archivos almacenados por la aplicación WhatsApp, enfocado en bases de datos y otros elementos relevantes. A partir del análisis, se logró extraer información clave, como el número de teléfono asociado al dispositivo, contactos almacenados y otros datos pertinentes.

Registro de evidencia

Obtener la documentación respectiva de un Android 10 en la nube para su análisis, este archivo se encontrará en el repositorio del informe.

Numero de registro de celular en WhatsApp

Analizar la estructura de los datos de WhatsApp, este se encuentra en el zip 'Pixel' recordando que debe descomprimirse.

unzip Pixel\ 3.zip

Analizar la estructura que tiene WhatsApp para poder observar los diferentes archivos que contiene el mismo.

tree -L 1 'data/data/com.whatsapp/'

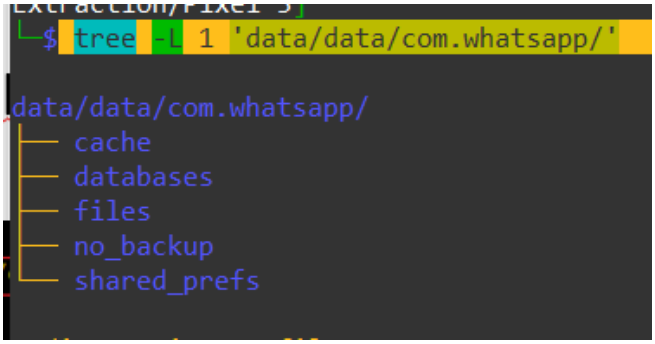


Figura G1. Visualización de la estructura de directorios de WhatsApp.

Revisando la carpeta de shared_prefs se encuentra información relevante al número de registro del teléfono.

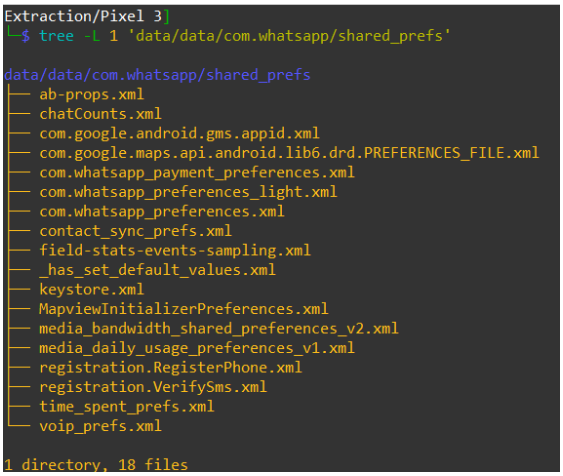


Figura G2. Exploración de la carpeta shared_prefs.

Navegando en los datos .XML se encuentra el número de teléfono <9195794674>

```
<string name="com.whatsapp.registration.RegisterPhone.phone_number">9195794674</string>
```

Se puede investigar de donde proviene el teléfono en una página web como "AllAreaCodes" con solo ingresar el número.

Contactos almacenados en WhatsApp

Como se observe anteriormente, existe un Directorio de databases en el Directorio data de WhatsApp, con el comando <tree -L 1>, se sigue visualizando esta información.

tree -L 1 'data/data/com.whatsapp/databases'

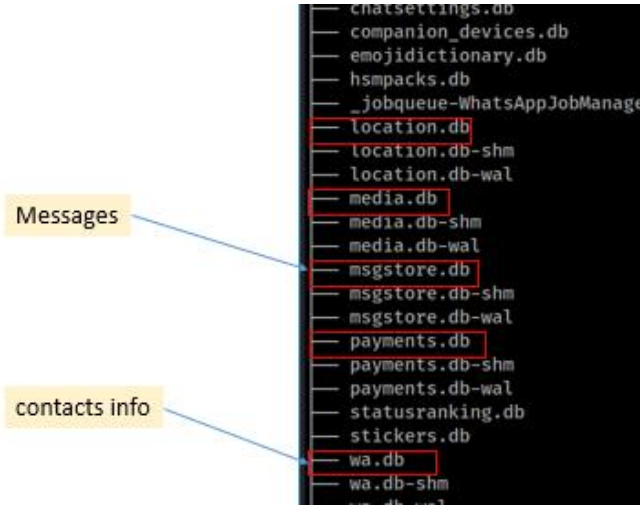


Figura G3. Análisis del directorio databases dentro de los archivos de WhatsApp.

Se despliegan varias bases de datos, por ahora se desea centra en los contactos, por lo que se visualiza los datos almacenados en wa.db. El comando se ejecuta directamente en la maquina Kali.

sqlitebrowser 'data/data/com.whatsapp/databases/wa.db'

En la base de datos se puede observar lista de números, nombres e información registrados en WhatsApp.

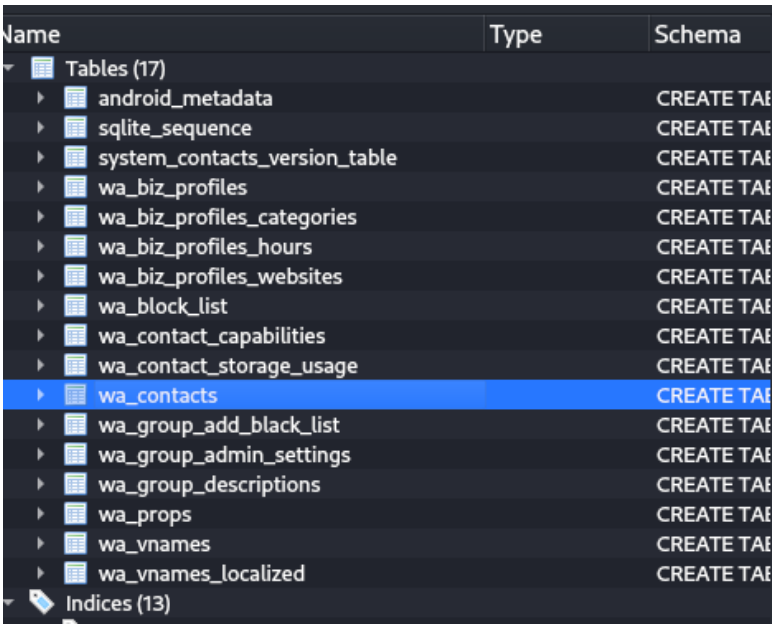


Figura G4. Vista general de las tablas contenidas en la base de datos wa.db.

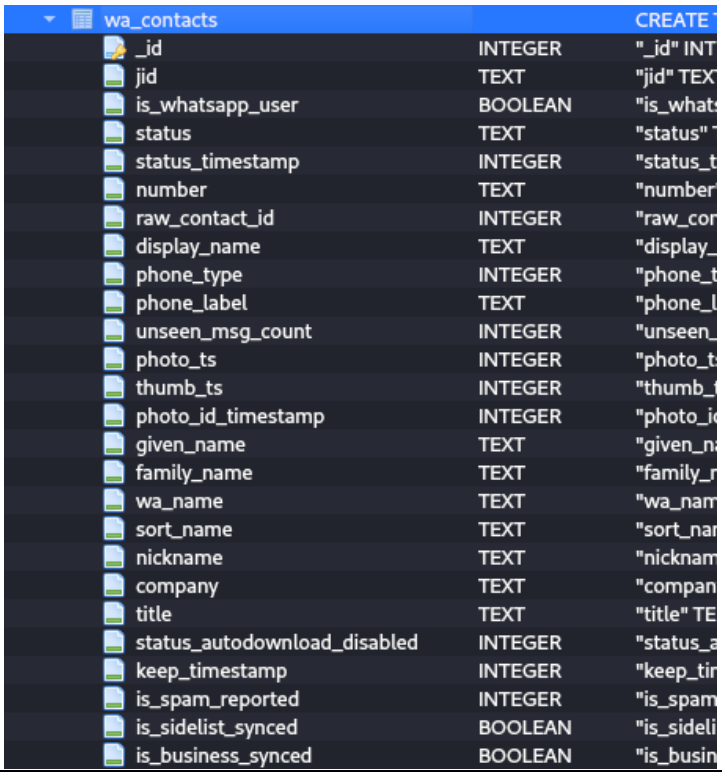


Figura G5. Detalle de la estructura de la tabla wa_contacts.

Seleccionar en ‘Browser database’ aquí seleccionar la base de datos indicada para visualizar la información de las tablas.

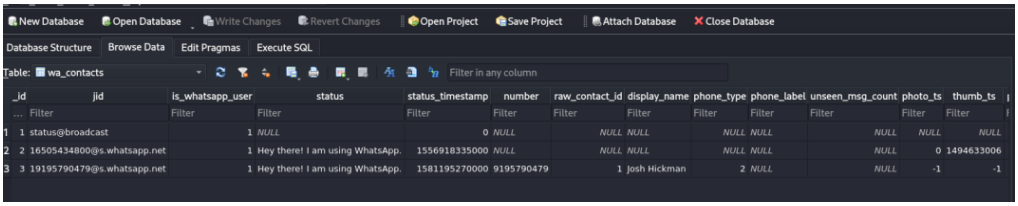


Figura G6. Vista de los datos almacenados en la tabla wa_contacts de la base de datos wa.db.

Principalmente se obtiene el ID del contacto, su estado y nombre de contacto.

6. Recomendaciones

- Investigar a fondo que otro tipo de archivos se encuentran en el zip y analizar con que herramientas puede visualizarse.