UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y COMUNICACIONES

Tema:

EVALUACIÓN DE SEGURIDAD DEL SISTEMA DE VIDEO VIGILANCIA DE LA EMPRESA ECUASEG

Trabajo de Titulación Modalidad: Proyecto de Investigación, presentado previo a la obtención del título de Ingeniero en Electrónica y Comunicaciones.

LINEA DE INVESTIGACIÓN: Tecnologías de la Información

AUTOR: Edwin Aníbal Velasteguí Vásquez

TUTOR: Ing. Andrea Patricia Sánchez Zumba, Mg.

Ambato – Ecuador

Septiembre - 2022

APROBACIÓN DEL TUTOR

En calidad de tutor del Trabajo de Titulación con el tema: EVALUACIÓN DE SEGURIDAD DEL SISTEMA DE VIDEO VIGILANCIA DE LA EMPRESA ECUASEG, desarrollado bajo la modalidad de Proyecto de investigación por el señor Edwin Aníbal Velasteguí Vásquez estudiante de la Carrera de Ingeniería en Electrónica y Comunicaciones, 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 15 del Reglamento para obtener el Título de Tercer Nivel, de Grado de la Universidad Técnica de Ambato, y el numeral 7.4 del respectivo instructivo.

Ambato, septiembre 2022

Firmado electrónicamente por:
ANDREA PATRICIA SANCHEZ ZUMBA

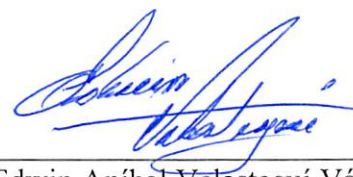
Ing. Andrea Patricia Sánchez Zumba, Mg.

TUTORA

AUTORÍA

El presente Proyecto de Investigación con título: EVALUACIÓN DE SEGURIDAD DEL SISTEMA DE VIDEO VIGILANCIA DE LA EMPRESA ECUASEG es absolutamente original, autentico y personal. En tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato, septiembre 2022



Edwin Aníbal Velasteguí Vásquez

CI: 1804490546

AUTOR

APROBACIÓN TRIBUNAL DE GRADO

En calidad de par calificador del Informe Final del Trabajo de Titulación presentado por el señor Edwin Aníbal Velasteguí Vásquez, estudiante de la Carrera de Ingeniería en Electrónica y Comunicaciones, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, bajo la Modalidad Proyecto de Investigación, titulado EVALUACIÓN DE SEGURIDAD DEL SISTEMA DE VIDEO VIGILANCIA DE LA EMPRESA ECUASEG, nos permitimos informar que el trabajo ha sido revisado y calificado de acuerdo al Artículo 17 del Reglamento para obtener el Título de Tercer Nivel, de Grado de la Universidad Técnica de Ambato, y al numeral 7.6 del respectivo instructivo. Para cuya constancia suscribimos, conjuntamente con la señora presidenta del Tribunal.

Ambato, septiembre 2022

Firmado electrónicamente por:
ELSA PILAR URRUTIA

Ing. Pilar Urrutia, Mg.

PRESIDENTA DEL TRIBUNAL

Firmado electrónicamente por:
VICTOR SANTIAGO MANZANO VILLAFUERTE

Ing. Santiago Manzano, Mg.

PROFESOR CALIFICADOR

Firmado electrónicamente por:
JOSE VICENTE MORALES LOZADA

Ing. Vicente Morales, Mg.

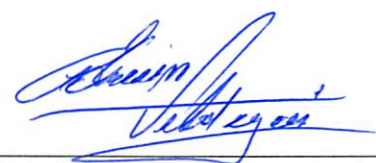
PROFESOR CALIFICADOR

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que use este Trabajo de Titulación como un documento disponible para la lectura, consulta y procesos de investigación-

Cedo los derechos de trabajo de titulación a favor de la Universidad Técnica de Ambato, con fines de difusión pública. Además, autorizo su reproducción total o parcial dentro de las respectivas regulaciones de la institución.

Ambato, septiembre 2022



Edwin Aníbal Velasteguí Vásquez

CI: 1804490546

AUTOR

DEDICATORIA

A mi amada familia, a mis padres, hermano y tíos que durante toda mi trayectoria universitario me han brindado su apoyo incondicional, a mis compañeros y amigos por su ánimo en todo momento.

Edwin Aníbal Velasteguí Vásquez

AGRADECIMIENTO

A mi amada familia, por su apoyo incondicional, a mis compañeros de facultad y amigos que colaboraron en todo momento y demás familiares que colaboraron de una u otra forma para la culminación de esta investigación.

Edwin Aníbal Velasteguí Vásquez

Índice General

APROBACIÓN DEL TUTOR I

AUTORÍA II

APROBACIÓN TRIBUNAL DE GRADO III

DERECHOS DE AUTOR IV

Autorizo a la Universidad Técnica de Ambato, para que use este Trabajo de Titulación como un documento disponible para la lectura, consulta y procesos de investigación- IV

Cedo los derechos de trabajo de titulación a favor de la Universidad Técnica de Ambato, con fines de difusión pública. Además, autorizo su reproducción total o parcial dentro de las respectivas regulaciones de la institución. IV

DEDICATORIA V

AGRADECIMIENTO VI

Índice General VII

Índice de Tablas IX

Índice de Figuras X

RESUMEN EJECUTIVO XIII

ABSTRACT XIV

CAPÍTULO I… 1

MARCO TEÓRICO 1

1.1 Antecedentes Investigativos 1

1.2 Contextualización del problema 4

1.3. Fundamentación teórica 6

1.3 Objetivos 21

CAPÍTULO II 22

METODOLOGÍA 22

2.1 Métodos 22

2.1.1 Modalidad de la Investigación 22

2.1.2 Recolección de Información 22

2.1.3 Procesamiento y Análisis de Datos 22

2.1.4 Desarrollo del proyecto 23
CAPÍTULO III 24
RESULTADOS Y DISCUSIÓN 24
3.1 Análisis y discusión de los resultados. 24
3.1.1 Desarrollo de la propuesta 24
3.1.1.1 Selección de los elementos para la implementación del laboratorio de Pentesting ……25
3.1.1.2 Diseño e Implementación del banco de pruebas del sistema de video vigilancia de gama baja basado en IP 25
4. Presupuesto 71
CAPÍTULO IV 73
CONCLUSIONES Y RECOMENDACIONES 73
4.1. Conclusiones 73
4.2. Recomendaciones 74
5. Bibliografía 75
Anexos ……78
Anexo A: Configuración de Virtual box 78
Anexo B instalación de Kali Linux 78
Anexo C informe Técnico 87
Anexo D informe ECUASEG 89

Índice de Tablas

Tabla 1. Software para el laboratorio de pentesting 25
Tabla 2. Vulnerabilidades de Hikvision expuestas por el navegador shodan 33
Tabla 3. Dispositivos conectados a la red ECUASEG_LOG 38
Tabla 4. Dispositivos conectados a la red ECUASEG_LOG 47
Tabla 5. Exploit CVE-2014-4880 61
Tabla 6. Exploit CVE-2021-36260 62
Tabla 7. Informe Ejecutivo 64
Tabla 8. Costos del proyecto 71
Tabla 9. Presupuesto 71

Índice de Figuras

Figura 1. Fases de Pentesting 24
Figura 2. Uso de google dorks 26
Figura 3. Uso intitle 26
Figura 4. Análisis de la página de Facebook de ECUASEG 27
Figura 5. Datos de la página Facebook de ECUASEG 27
Figura 6. Información de LinkedIn 28
Figura 7. Interfaz de Maltego 28
Figura 8. Hoja en blanco para el análisis de datos 29
Figura 9. Datos detectados por la Herramienta Maltego 29
Figura 10. Información relevante de la persona investigada 30
Figura 11. To Entities [IBM Watson] 30
Figura 12. Datos del transformer IBM Watson 31
Figura 13. Transformer mail 31
Figura 14. Navegador Shodan 32
Figura 15. Categorías mostradas por Shodan 32
Vulnerabilidades 33
Descripción 33
MS15-034 33
Figura 17. Situación de Hikvision en el Ecuador 34
Figura 18. Dispositivos Hikvision en la ciudad de Ambato 34
Figura 19. Top 10 de puertos utilizados en Hikvision 35
Figura 20. Organizaciones en donde se encuentran conectados dispositivos Hikvision 35
Figura 21. Dispositivos conectados a Telconet SA 36
Figura 22. Página de inicio de un DVR de la marca Hikvision 37
Figura 24. Tarjeta de red en modo monitor 37

Figura 25. Redes Wifi 38
Figura 26. Dispositivos conectados a la red ECUASEG_LOG 38
Figura 27. Desautentificación del dispositivo 1 39
Figura 28. Desautentificación del dispositivo 2 39
Figura 29. Desautentificación del dispositivo 3 40
Figura 30. WPA handshake del dispositivo 3 40
Figura 31. Primer Ataque de fuerza bruta 41
Figura 32. Creación de lista de numero con la herramienta Crunch 41
Figura 43. Segundo Ataque de fuerza bruta 42
Figura 34. Creación del diccionario 2 42
Figura 35. Tercer Ataque de fuerza bruta 43
Figura 36. Creación del diccionario 3 43
Figura 37. Cuarto Ataque con diccionario 44
Figura 38. Creación del 5 diccionario 44
Figura 39. Quinto Ataque con diccionario 45
Figura 40. Creación del sexto diccionario 45
Figura 41. Sexto Ataque con diccionario 46
Figura 42. Dispositivos conectados a la red ECUASEG_LOG 46
Figura 43. Archivo descargado de Nessus 47
Figura 44. Instalación Nessus 47
Figura 45. Configuración de herramienta Nessus 48
Figura 46. Configuración de la herramienta Nessus 48
Figura 47. Configuración de la cuenta en Nessus 49
Figura 48. Ingreso de código 49
Figura 49. Configuración de usuario y contraseña 50
Figura 50. Configuración Final 50
Figura 51. Inicialización de servicios 51

Figura 52. Ingreso a la interfaz 51
Figura 53. Creación de Escaneo en Nessus 52
Figura 54. Tipo de Escaneo 53
Figura 55. Inicio del Escaneo 53
Figura 56. Resultados del Escaneo 53
Figura 57. Descripción de la vulnerabilidad 54
Figura 58. Creación del escaneo 55
Figura 59. Selección de los puertos 55
Figura 60. Inicio del escaneo 56
Figura 61. Resultado del escaneo 56
Figura 62. Análisis de puertos con Nmap 57
Figura 63. Interfaz del DVR 57
Figura 64. Ejecución de Hydra 58
Figura 65. Ingreso al DVR 58
Figura 66. Visualización de las cámaras conectadas al DVR 58
Figura 67. Configuración del DVR 59
Figura 68. Configuración de la seguridad del DVR 60
Figura 69. Configuración de la Red 60
Figura 70. Configuración del Exploit 61
Figura 71. Ejecución del Exploit 62
Figura 72. Exploit CVE-2021-36260 63
Figura 73. Resultado del Exploit 63
Figura 74. Salario Mínimo Sectorial del 2022 [17] 71

RESUMEN EJECUTIVO

La conectividad en los últimos años ha aumentado, provocando que los dispositivos como cámaras, alarmas, porteros eléctricos estén conectados a internet para manipulación, visualización y control por parte del usuario, a pesar de las grandes prestaciones que brinda la conectividad deja brechas que los cibercriminales aprovechan para robar información y comprometer los equipos. Es por lo que, este proyecto está enfocado a realizar un análisis del sistema de video vigilancia de la empresa ECUASEG con el fin de determinar las vulnerabilidades del sistema por medio de las herramientas que brinda el hacking ético, con el fin de definir procedimientos para anticipar los posibles ataques que pueda sufrir la empresa. La investigación se enfocó en la detección de vulnerabilidades, amenazas y riesgos del sistema de video vigilancia en la empresa ECUASEG, por medio de 6 fases: reconocimiento, exploración, obtener acceso, mantener acceso, mantenerse oculto y reporte para evaluar la seguridad del sistema de video vigilancia donde se refleja la importancia de la ciberseguridad en los sistemas, infraestructura tecnológica, etc.

Descriptores: Hacking Ético, vulnerabilidades, KaliLinux, herramientas

ABSTRACT

Connectivity in recent years has increased, causing almost all devices such as cameras, alarms, electric intercoms are connected to the internet for user manipulation, viewing and control, Despite the great benefits that connectivity provides, it leaves gaps that cybercriminals take advantage of to steal information and compromise equipment. That is why, this project is focused on performing an analysis of the video surveillance system of the company ECUASEG in order to determine the vulnerabilities of the system through the tools provided by ethical hacking, in order to define guiding procedures to anticipate possible attacks on the company. Where the research focused on the detection of vulnerabilities, threats and risks of the video surveillance system in the company ECUASEG, through 6 phases: recognition, exploration, gaining access, maintaining access, keep hidden and report to evaluate the security of the video surveillance system where the importance of cybersecurity in systems, technological infrastructure, etc.

Keywords: Ethical Hacking, vulnerabilities, KaliLinux, tools

CAPÍTULO I

MARCO TEÓRICO

1.1 Antecedentes Investigativos

En el año 2016, Andrei Costion publica el artículo científico "**Security of CCTV and Video Surveillance Systems: Threats, Vulnerabilities, Attacks, and Mitigations**". En este artículo lleva a cabo una revisión sistemática de la amenazas nuevas y existentes en los sistemas de video vigilancia, circuito cerrado de tv y cámaras IP basada en datos. Para lo cual, se ha elegido 7 criterios para describir las amenazas, vulnerabilidades, ataques y mitigaciones para los sistemas de video vigilancia: (1) superficie de ataque, (2) tipo de ataque, (3) tipo de atacante, (4) componente directamente afectado, (5) complejidad de explotación, (6) mitigación y (7) complejidad de mitigación. Con base en datos disponibles públicamente y clasificaciones y taxonomías existentes, la revisión presentada información completa sobre cómo los sistemas de video vigilancia pueden ser atacados y protegidos en varios niveles. Este conocimiento estructurado, se utiliza para comprender e identificar mejor los riesgos de seguridad y privacidad asociados con el desarrollo, la implementación y el uso de estos sistemas. Finalmente, este documento presentó un conjunto de recomendaciones y mitigaciones que pueden mejorar los aspectos de seguridad y privacidad de los sistemas de video vigilancia.

En el año 2017, Brian Cusack y Zhuang Tian publican el artículo científico "**Evaluating IP surveillance camera vulnerabilities abilities**". Este artículo realizó una investigación en los sistemas de video vigilancia basado en IP, la investigación tiene seis fases. Estas fases incluyen la revisión de la literatura, la configuración del sistema, las pruebas piloto, la recopilación de datos, el análisis de los datos y su comparación con los resultados de investigaciones anteriores. En el análisis práctico del sistema se utilizaron las herramientas Angry IP Scanner y Nmap para recopilar información sobre el sistema de destino, como su dirección IP, dirección de control de acceso a medios, información del fabricante y del servidor.

Posteriormente, utilizan Wireshark en modo de monitorización y captura para autenticarse en la aplicación del sitio web del sistema de vigilancia de destino, con el fin de capturar el nombre de usuario y la contraseña en texto sin cifrar o en valores hash, debido a que con la herramienta Wireshark no se logró no capturó ningún paquete relacionado con el nombre de usuario y la contraseña se utilizaron dos técnicas de craqueo que son fuerza bruta y diccionario por medio de hydra el cual realizo 17 intentos con 22 posibles contraseñas; y se encontró un par de nombre de usuario y contraseña válidos. Cada uno de las pruebas realizadas con diferentes herramientas brindan un marco de referencia para identifica la vulnerabilidades y riegos en el sistema. Finalmente, esta investigación sugiere que las cámaras IP son vulnerables a la explotación y se aconseja una mayor urgencia en la distribución de contramedidas. La detección de actividad sospechosa requiere una constante vigilia para brindar muchas capas de protección que mitiguen al atacante y mantengan la integridad del sistema. De manera similar, la información crítica requiere encriptación, protección por túnel y complejidad criptográfica para confundir el análisis. La derrota a los cibercriminales se da con constantes controles de gestión de la red, auditorías comparativas en cada momento y la actualización periódica del software antivirus de las cámaras IP. [1]

En el año 2017, Reem Alshalawi, Turki Alghamdi publican el artículo científico "**Forensic Tool for Wireless Surveillance Camera**". En esta investigación presenta una nueva herramienta en red forense. Esta herramienta propuesta está diseñada en dos etapas. Primero, se crea un nuevo esquema de monitoreo para mantener la privacidad de los datos. En segundo lugar, se facilita el proceso de investigación que juega un papel importante para salvar la privacidad de los usuarios y los lugares altamente seguros que usan cámaras de vigilancia. Esta investigación se realiza utilizando un modelo que consta de una puerta de enlace predeterminada (G), una cámara de vigilancia IP, ambas con dirección IP estática y una PC de confianza. Para lo cual se tiene un enfoque que se basa en una configuración de hardware específica donde Wireshark se ejecuta en la puerta de enlace predeterminada para monitorear la cámara y el tráfico confiable de la PC y para preservar los datos. Luego, Se envía la copia de seguridad de los archivos de captura al servidor de respaldo.

El análisis de los archivos de captura comienza a filtrar los datos con el fin de determinar el tráfico perteneciente a la cámara de vigilancia. El segundo enfoque

consiste en encontrar el tiempo perdido de las transacciones de cámaras de vigilancia en las que cualquier paquete faltante indica que hay un ataque a la cámara de vigilancia. Los resultados tienen una puntuación de memoria del 100% y puntuaciones de precisión y exactitud del 99%. Esto facilita el seguimiento del tráfico entrante y saliente de la cámara de vigilancia por tiempo. [2]

En el año 2020, Noar Kalbo, Yisroel Mirsky, Asaf Shabtai y Yuval Elovici publicó el artículo científico "**The Security of IP-Based Video Surveillance Systems**". En este artículo, se revisa la ciberseguridad de los sistemas de vigilancia modernos. En donde se detalla la composición y topología de los sistemas de video vigilancia modernos. Aquí realizaron los siguientes ataques: inyección de código, observación del tráfico por medio de herramienta VideoJak, filtración de información por medio de malware contenido dentro de la red aislada puede hacer parpadear una luz LED a la vista de la cámara que está conectada a Internet. Modulando el patrón de parpadeo, el atacante puede extraer información robada a una ubicación remota, Inundaciones y perturbaciones al usar la herramienta hping3, una inundación TCP/SYN puede deshabilitar un servidor web, para el escaneo y reconocimiento se utilizó herramientas estándar como NMAP para mapear la red y revelar información sobre sus hosts. Para los ataques de fuerza bruta se utilizó la herramienta Hydra que permite revelar credenciales de usuario, Acceso físico para flashear el firmware de una cámara, obstruir la vista de la cámara o simplemente cortar un cable, etc. Finalmente, este estudio brinda resumen de las mejores prácticas y soluciones de seguridad que se pueden utilizar para mejorar la seguridad los sistemas de video vigilancia existentes y futuros. [3]

En el año 2020, Estefanía Briones publicó el trabajo: "**APLICACIÓN DE HACKING ÉTICO PARA LA DETERMINACIÓN DE AMENAZAS, RIESGOS Y VULNERABILIDADES EN LA RED DE LA UNIVERSIDAD ESTATAL DEL SUR DE MANABÍ**". Este proyecto presenta la aplicación hacking ético para detectar las amenazas, riegos y vulnerabilidades en la Universidad Estatal del Sur de Manabí en él que se establece un ambiente de pruebas para el evaluó del nivel de detección de vulnerabilidades. En donde se analizaron las principales técnicas de hacking ético las cuáles se aplicaron en el desarrollo de la investigación para evaluar el entorno de la red en un procedimiento necesario. Donde establecieron dos herramientas de pruebas para el análisis de la red y la determinación de amenazas,

e identificando los riesgos y vulnerabilidades que fueron detectados en la aplicación del hacking ético. La aplicación de hacking ético determinó las vulnerabilidades que existen en las redes wifi dentro de una institución y brindar una mejor seguridad a los dispositivos tecnológicos. [4]

1.2 Contextualización del problema

Los sistemas de video vigilancia han proliferado en empresas y hogares. Estos sistemas de video vigilancia son realmente económicos y proporcionan múltiples sensores que envían información a una estación centralizada y pantallas de monitoreo, los cuales se pueden encontrar en todas partes, están en las calles, en las estaciones de tren, en los lugares de trabajo, en las fábricas y en el hogar. [5] Las aplicaciones inteligentes han hecho que las grandes redes de vigilancia sean prácticas de administrar y utilizar. Por ejemplo, la tecnología de reconocimiento facial, identificación de amenazas, detección de eventos, seguimiento de objetos e investigación rápida de incidentes se puede escalar a miles de cámaras en grandes áreas geográficas. [6]

A nivel mundial cerca de 3.5 millones de cámaras de seguridad doméstica y empresariales corren riesgo de verse comprometidas por los ciberdelincuentes debido a fallas críticas de diseño y software. Por lo cual estos sistemas y sus componentes han sido objeto de numerosos ciberataques. Por ejemplo, han sido objeto de ataques de denegación de servicio distribuido DDoS, explotados para invadir la privacidad de los usuarios e incluso para minar Criptomonedas. Estos sistemas también han sido reclutados en botnets para realizar tareas nefastas. Por ejemplo, en 2014, la infame botnet Mira apuntó a los sistemas de vigilancia e infectó más de 600 000 dispositivos en todo el mundo. [3]

A través de consultas de Shodan.io y Censys.io de fabricantes conocidos, se encontró más de 1 millón de cámaras de vigilancia y más de 125 000 servidores de vigilancia expuestos a Internet. De estos dispositivos, el 90 % no tiene portales de inicio de sesión seguros utiliza HTTP y no HTTPS. Además, aproximadamente el 8 % tiene puertos SSH y Telnet abiertos, el 3 % tiene bases de datos MySQL expuestas y al menos el 1,7 % de estos dispositivos aún son vulnerables a la vulnerabilidad HeartBleed SSL descubierta en 2012. Incluso los grandes fabricantes de video vigilancia tienen productos expuestos. Por ejemplo, el servidor CCTV de Samsung

tiene al menos 83 035 dispositivos expuestos, donde el 86 % de ellos usa portales de inicio de sesión HTTP y 1604 tienen puertos ssh abiertos. Además, Hikvision, el fabricante de vigilancia con la mayor cuota de mercado del 24,7 %, tiene al menos 260.415 dispositivos expuestos, de los que solo 53 tenían habilitado HTTPS. pero con certificados auto firmados. En un estudio, se encontró que aproximadamente 73,000 cámaras de seguridad en 256 países son accesibles con contraseñas predeterminadas. Estas estadísticas enfatizan el mal estado de seguridad de los sistemas de vigilancia basados en IP. Además, estos sistemas son muy específicos. [6]

En América Latina, Argentina, México y Brasil estuvieron entre los cinco países con mayor porcentaje de usuarios de Internet en computadoras y dispositivos móviles afectados por malware en 2020. Aunque para muchos estos ataques pueden pasar casi desapercibidos, ciertas acciones ofensivas pueden suponen una grave amenaza para las empresas y organizaciones, dejando a su paso importantes perjuicios económicos. En 2019, Ecuador y Paraguay encabezaron la lista de países latinoamericanos donde las empresas sufrieron más incidentes de ciberseguridad. Según una encuesta, el 70 por ciento de los gerentes de TI de las empresas en estos dos países afirmaron tener este tipo de incidentes. Entre los principales incidentes reportados se encuentran las infecciones por malware, seguidas de los accesos no autorizados a aplicaciones y bases de datos. Aunque menos recurrente en la región, hasta el 65 por ciento de las organizaciones encuestadas en Brasil en 2020 informaron haber sufrido ataques de ransomware, frente al 44 por ciento tanto en México como en Colombia. [7]

Ecuador ha sido víctima del delito cibernético durante un período de tiempo considerable y cada vez es más evidente que esta amenaza supera las capacidades del país. El ciberdelito en Ecuador comenzó a ser tratado como una amenaza grave en el año 2009, se registraron 3.143 casos en los siguientes cinco años; sin embargo, se estima que el 80% de los ciberdelitos no son denunciados. El 17 de septiembre de 2019, el Gobierno de Ecuador anunció que había sido víctima de un ciberdelito ya que se filtraron los datos de seis entidades públicas por una brecha de seguridad. Según la BBC, un equipo de investigadores de VPNMentor, firma especializada en información sobre Redes Virtuales Piratas y privacidad en internet, descubrió que se había filtrado la información de unos veinte millones de ecuatorianos.

Esta cifra supera en cuatro millones a la población total de Ecuador, por lo que también se filtró información de personas fallecidas. Las características de la era

tecnológica moderna hacen que el ciberdelito sea considerado una amenaza asimétrica, especialmente para países poco desarrollados en materia técnica como Ecuador. [8]

Por lo cual, el objetivo de la investigación es la detección de vulnerabilidades, amenazas y riesgos del sistema de video vigilancia en la empresa ECUASEG, por medio de las 6 fases, reconocimiento, exploración, obtener acceso, mantener acceso, mantenerse oculto y reporte para evaluar la seguridad del sistema de video vigilancia.

1.3. Fundamentación teórica

1.3.1. Introducción al Hacking Ético

Piratear

Piratear se puede definir como el arte de explorar y explotar varias brechas de seguridad en un sistema o su red asociada. Internet se inventó para facilitar la vida de las personas, pero también proporcionó una plataforma en línea para que los delincuentes expandieran sus actividades delictivas. Los delincuentes comenzaron a utilizar canales en línea como el correo electrónico, los mensajeros en línea, etc. Para dirigirse a personas comunes desprevenidas y engañarlas para que proporcionen información sobre sus cuentas bancarias y tarjetas de crédito. A medida que avanzaba la tecnología, estos delincuentes comenzaron a desarrollar notorias aplicaciones informáticas para realizar su trabajo manual, y esto sentó las bases para el término hackear. [9]

Pirata

En un mundo simple, puede describir a un pirata como un adolescente antisocial e introvertido que solo siente curiosidad por las cosas. Sin embargo, hay varias formas de describir a un pirata en el mundo digital. Hay varias cosas que motivan a un pirata individual a ingresar a un sistema, y cada pirata emplea su propio conjunto de métodos y habilidades para hacerlo. La naturaleza común que une a todos los piratas informáticos es que tienen una mente aguda y curiosidad por aprender más sobre la tecnología. [9]

Hay dos significados para el término hacker.

- Hablando tradicionalmente, un pirata es alguien curioso por aprender cosas nuevas y, por lo tanto, le gusta profundizar en la tecnología para conocer su funcionamiento. Por lo general, les gusta jugar con la computadora y les gusta entender cómo funcionan las cosas electrónicamente.
- En los últimos tiempos, el término pirata ha adquirido un nuevo significado: alguien a quien le gusta ejecutar ataques maliciosos en los sistemas para beneficio personal. Técnicamente hablando, se les llama crackers, que es la abreviatura de hackers criminales. [9]

Los piratas informáticos criminales ingresan a los sistemas para obtener beneficios personales, popularidad o incluso venganza. Entran en un sistema para modificar, eliminar o robar información, haciendo miserable la vida de las personas al hacerlo. [9]

Tipos de piratas informáticos

Los piratas informáticos se clasifican en varias categorías según su función. Estos son algunos de los más comunes:

Pirata informático de sombrero blanco

Un pirata informático de sombrero blanco es alguien que se ocupa del hacking ético. Los piratas informáticos éticos son profesionales de la seguridad con conocimientos y habilidades sobre la piratería y las herramientas utilizadas para la piratería. Por lo general, son empleados por una organización para descubrir fallas de seguridad en sus sistemas e implementar medidas para reparar estas fallas antes del inicio de un ataque real. [9]

Los piratas informáticos de sombrero blanco también se conocen como probadores de penetración. Su enfoque principal es descubrir vulnerabilidades y parchearlas para brindar seguridad a los sistemas dentro de una organización. [9]

Pirata informático de sombrero negro

Un pirata informático de sombrero negro es alguien de naturaleza poco ética que se mete en los sistemas para obtener ganancias personales. Estos son delincuentes y crackers que emplean sus habilidades y conocimientos para obtener acceso a un

sistema con fines maliciosos o ilegales. A veces, simplemente son notorios y quieren violar la integridad de un sistema para molestar al propietario del sistema. [9]

Los piratas informáticos de sombrero negro también se conocen como piratas informáticos de seguridad o piratas informáticos poco éticos. Su intención principal es robar información para obtener beneficios monetarios. [9]

Pirata informático de sombrero gris

Un Pirata informático de sombrero gris, es alguien entre un pirata informático de sombrero blanco y un pirata informático de sombrero negro. Por lo general, no tienen intenciones de lastimar a nadie y no explotan los sistemas para obtener ningún beneficio personal, pero pueden cometer actos maliciosos, a sabiendas o sin saberlo, durante sus explotaciones. Los piratas de sombrero gris también se conocen como piratas híbridos que trabajan entre los unos piratas informáticos de sombrero blanco y los piratas informáticos de sombrero negro.

Los hackers de sombrero gris también se conocen como hackers híbridos que trabajan entre los hackers de sombrero blanco y los de sombrero negro.

Hacking Ético

El proceso autorizado de violar la seguridad de un sistema de información para identificar las debilidades y vulnerabilidades del sistema o su red asociada se conoce como hacking ético. El pirata ético o pirata de sombrero blanco obtiene autorización para ejecutar pruebas en los sistemas por parte de la organización propietaria del sistema. El hacker ético luego examina la configuración de seguridad de dicho sistema. La diferencia entre el pirata malicioso y el pirata ético es que este último es un ataque planificado y, por tanto, completamente legal.

El trabajo de un hacker ético es identificar las lagunas en un sistema de seguridad que un atacante malintencionado puede utilizar para obtener acceso al sistema. Los piratas informáticos éticos realizarán múltiples pruebas en un sistema de información para recopilar información sobre él y hacerlo más seguro. Por lo tanto, su objetivo final es garantizar que el sistema de información sea lo suficientemente fuerte como para dar un duro desafío a todos los ataques entrantes. Los hackers éticos utilizan la siguiente metodología para escanear un sistema en busca de lagunas. Sin embargo, el proceso de escaneo no se limita solo a los siguientes métodos.

- Incumplimiento de los mecanismos de autenticación de los sistemas.
- Exposición de datos críticos de la empresa.
- Modificaciones a la configuración de seguridad del sistema.
- Ataques de inyección.

Puntos de acceso de las redes y sistemas de la organización.

Reglas del Hacking Ético

Hay reglas y principios definidos para un hacker ético que deben seguirse en todo momento. Es común que estas reglas y principios se olviden o se ignoren cuando se realizan pruebas de piratería. Y el resultado de esto puede ser muy peligroso para la organización. Estos son algunos de los principales mandamientos de la piratería ética: [9]

Trabajar éticamente

El término ético significa trabajar con integridad y principios profesionales. Cuando realiza pruebas de piratería ética en los sistemas de una organización, debe asegurarse de que todas las pruebas hayan sido aprobadas y respalden el objetivo de la organización. A un hacker ético no se le permite tener agendas ocultas. La confianza es el factor más importante en el campo de la piratería ética. El hacker ético no debe conservar la información recuperada mientras realiza las pruebas para obtener ganancias personales, ya que eso es lo que separa a los piratas de sombrero blanco de los piratas de sombrero negro. [9]

Respeto a la privacidad

Un hacker ético obtiene acceso a una gran cantidad de información personal mientras realiza pruebas de penetración. Se espera que trate la información con respeto y no la utilice para beneficio personal. Toda la información recopilada durante las pruebas de penetración, desde la actividad de navegación web hasta las contraseñas, debe mantenerse privada. [9]

Asegurarse de que los sistemas no estén dañados

Los sistemas y la información que posee una organización son muy valiosos y no deben dañarse a ningún costo. Los hackers éticos deben leer toda la documentación disponible sobre la infraestructura digital de una organización para no obstaculizar el

sistema, incluso sin saberlo. Un sistema puede colapsar si termina ejecutando demasiadas pruebas simultáneamente. Si un sistema falla durante las horas de producción, puede generar enormes pérdidas de ingresos para la organización. [9]

Ejecutando el Plan

El tiempo y la paciencia son muy importantes en el campo del hacking ético. Debe tener mucho cuidado al realizar las pruebas y asegurarse de que ningún empleado no autorizado sepa lo que está haciendo. Habrá numerosos ojos sobre usted mientras realiza las pruebas, y no es prácticamente posible saber si un empleado de la organización desea dañarlo. Todo lo que puede hacer es asegurarse de realizar sus pruebas en silencio y de la manera más privada posible y no divulgar ninguna información a nadie, excepto a sus jefes, que lo ha contratado para el trabajo. [9]

Ciclo de vida de Pruebas de penetración

Un hacker ético también se conoce como probador de penetración en la industria. Los hackers éticos dominan el ciclo de vida de las pruebas de penetración. Una organización contrata a piratas informáticos éticos para que puedan realizar varias pruebas de penetración en la infraestructura digital de la organización con la aprobación de la gerencia y descubrir vulnerabilidades en el sistema para que puedan repararse antes de que un atacante real ataque el sistema. [9]

A lo largo de los años, se ha establecido un marco definido, que ha sido adoptado por los hackers éticos. Las primeras cinco etapas de este marco guían a un hacker ético para descubrir vulnerabilidades en un sistema y comprender hasta qué nivel se pueden explotar estas vulnerabilidades. En comparación, la etapa final termina documentando las acciones de las primeras cinco etapas en un informe ordenado que se presentará a la alta dirección de la organización. Este marco no solo ha creado una estructura adecuada de planificación y ejecución para un hacker ético. Aún sí, también ha demostrado ser muy eficiente para realizar pruebas de penetración en múltiples niveles de la infraestructura digital de una organización. [9]

Cada etapa reúne entradas de la etapa anterior y además proporciona entradas a la siguiente etapa. El proceso se ejecuta en una secuencia, pero no es raro que los piratas informáticos éticos regresen a una etapa anterior para analizar información previamente descubierta. [9]

1.3.2. Fases de prueba de penetración

La planificación garantiza que las pruebas de penetración sigan un orden secuencial de pasos para lograr el resultado deseado, que es identificar vulnerabilidades. Cada fase describe y describe lo que se requiere antes de pasar a los siguientes pasos. Esto garantiza que todos los detalles sobre el trabajo y el objetivo se recopilen de manera eficiente y que el probador de penetración tenga una comprensión clara de la tarea que tiene por delante. [11]

Las siguientes son las diferentes fases en las pruebas de penetración:

- Compromiso previo
- Recopilación de información
- Modelado de amenazas
- Análisis de vulnerabilidad
- Explotación
- Post-explotación
- Redacción de informes

Compromiso previo

Durante la fase previa al compromiso, se selecciona al personal clave. Estas personas son clave para proporcionar información, coordinar recursos y ayudar a los evaluadores a comprender el alcance, la amplitud y las reglas de participación en la evaluación. Esta fase también cubre los requisitos legales, que normalmente incluyen una Acuerdo de no divulgación (NDA) y un acuerdo de servicios de consultoría (CSA). [10]

Un NDA es un acuerdo legal que especifica que un probador de penetración no compartirá ni conservará ninguna información confidencial o patentada que se encuentre durante la evaluación. Las empresas suelen firmar estos acuerdos con empresas de ciberseguridad que, a su vez, lo firmarán con los empleados que trabajan en el proyecto. En algunos casos, las empresas firman estos acuerdos directamente con los probadores de penetración de la empresa que realiza el proyecto. [10]

Recopilación de información

La mayoría de los tipos de pruebas de penetración implican una fase de recopilación de información, que es vital para garantizar que los evaluadores tengan acceso a información clave que los ayudará a realizar su evaluación. La mayor parte de la recopilación de información se realiza para pruebas de penetración de aplicaciones basadas en la web, por lo que las preguntas involucradas generalmente están orientadas a las aplicaciones basadas en la web. [10]

Modelado de amenazas

El modelado de amenazas es un proceso que se utiliza para ayudar a los evaluadores y defensores a comprender mejor las amenazas que inspiraron la evaluación o las amenazas a las que la aplicación o la red son más propensas. Estos datos se utilizan luego para ayudar a los evaluadores de penetración a emular, evaluar y abordar las amenazas más comunes a las que se enfrenta la organización, la red o la aplicación.

Habiendo entendido las amenazas que enfrenta una organización, el siguiente paso es realizar una evaluación de vulnerabilidad en los activos para determinar aún más la clasificación y la gravedad del riesgo. [10]

Análisis de vulnerabilidad

El análisis de vulnerabilidad generalmente involucra a los asesores o evaluadores que ejecutan escaneos de vulnerabilidades o redes/puertos para comprender mejor qué servicios está ejecutando la red o la aplicación y si hay vulnerabilidades en los sistemas incluidos en el alcance de la evaluación. Este proceso a menudo incluye pruebas/descubrimiento de vulnerabilidades manuales, que suele ser la forma más precisa de análisis de vulnerabilidades o evaluación de vulnerabilidades. [10]

Explotación

La explotación es la parte más comúnmente ignorada o pasada por alto de las pruebas de penetración, y la realidad es que a los clientes y ejecutivos no les importan las vulnerabilidades a menos que entiendan por qué les importan. La explotación es la munición o evidencia que ayuda a articular por qué la vulnerabilidad es importante e ilustra el impacto que la vulnerabilidad podría tener en la organización. Además, sin explotación, la evaluación no es una prueba de penetración y no es más que una

evaluación de vulnerabilidad, que la mayoría de las empresas pueden realizar internamente mejor que un consultor externo. [10]

Post-explotación

La explotación es el proceso de obtener acceso a sistemas que pueden contener información confidencial. El proceso de post-explotación es la continuación de este paso, donde el punto de apoyo ganado se aprovecha para acceder a los datos o propagarse a otros sistemas dentro de la red. Durante la post-explotación, el objetivo principal suele ser demostrar el impacto que la vulnerabilidad y el acceso obtenido pueden tener para la organización. Este impacto ayuda a ayudar al liderazgo ejecutivo a comprender mejor las vulnerabilidades y el daño que podría causar a la organización. [10]

Reporte escrito

La redacción de informes es exactamente como suena y es uno de los elementos más importantes de cualquier prueba de penetración. Las pruebas de penetración pueden ser el servicio, pero la redacción de informes es el resultado que ve el cliente y es el único elemento tangible que se entrega al cliente al final de la evaluación. Los informes deben recibir tanta atención y cuidado como las pruebas. [10]

La redacción de informes implica mucho más que enumerar algunas vulnerabilidades descubiertas durante la evaluación. Es el medio en el que transmite el riesgo, el impacto comercial, resume sus hallazgos e incluye pasos de remediación. Un buen probador de penetración debe ser un buen redactor de informes, o los problemas que encuentre se perderán y es posible que el cliente que los contrató para realizar la evaluación nunca los entienda. [10]

Una vez completada esta sección, ahora puede describir cada fase de una prueba de penetración. Además, tiene una mejor idea de las expectativas de los probadores de penetración en la industria. [10]

1.3.3. Metodologías de pruebas de penetración

En el campo de las pruebas de penetración, existen muchas metodologías oficiales y estándar que se utilizan para realizar una prueba de penetración en un sistema o red de destino. [10]

OWASP

OWASP presenta proyecto de seguridad de aplicaciones web abiertas y proporciona metodologías, así como listas de las 10 mayores debilidades de seguridad presentes en las aplicaciones web. Esta lista es el marco de facto utilizado por los probadores de penetración de aplicaciones web y es lo que la mayoría de las empresas buscan cuando contratan probadores de penetración para probar sus aplicaciones web. Esta es también la forma más común y frecuente de pruebas de penetración. [9]

Este es uno de los marcos más populares, y cada probador de penetración debe tener una comprensión clara de él cuando se trata de pruebas de aplicaciones web. Sin embargo, es igualmente importante comprender a otros, como NIST. [9]

NIST

NIST representa el Instituto Nacional de Normas y Tecnología. NIST es una división del gobierno de EE. UU. y publica una serie de publicaciones especiales que definen las mejores prácticas, así como los estándares que las organizaciones deben emplear para mejorar su seguridad. Es importante comprender el NIST para asignar los hallazgos o las vulnerabilidades descubiertas a sus reglas apropiadas para ayudar a las organizaciones a comprender las implicaciones de cumplimiento de los problemas descubiertos durante la evaluación. [9]

A veces, una organización objetivo puede requerir pruebas de seguridad utilizando un marco o estándar específico. Estar familiarizado con OSSTMM puede ser útil para sus compromisos con la organización objetivo como probador de penetración. [9]

OSSTMM

OSSTMM representa el Manual de metodología de prueba de seguridad de código abierto. Este es un conjunto de estándares de prueba de seguridad impulsado por la comunidad, actualizado con frecuencia y revisado por pares que todo hacker ético debe conocer y mantenerse actualizado. Estos estándares tienden a cubrir una amplia gama de temas de prueba y son especialmente valiosos para aquellos que ingresan a la industria para ayudarlos a comprender mejor el proceso y las mejores prácticas de prueba. El conocimiento encontrado en OSSTMM será un gran activo como probador de penetración. [9]

SIN 25

SIN 25 es una lista de los 25 principales dominios de seguridad según la definición del Instituto SANS. Al realizar evaluaciones, es bueno estar familiarizado con esta lista y comprender cómo sus hallazgos se relacionan con la lista. Además, comprender los 25 dominios principales puede ayudar a aumentar la amplitud de su conocimiento de las vulnerabilidades de seguridad. Estos problemas generalmente se extienden mucho más allá de lo que se descubrirá a través de pruebas de intrusión, y comprender estos problemas puede incluso ayudarlo a identificar vulnerabilidades adicionales o tendencias de riesgo durante sus evaluaciones. [9]

1.3.4. Enfoques de prueba de penetración

Enfoques de prueba de penetración

Los siguientes son diferentes enfoques para realizar una prueba de penetración en una organización objetivo:

- Caja blanca
- Caja negra
- Caja gris

Caja blanca

Una evaluación de caja blanca es típica de las pruebas de aplicaciones web, pero puede extenderse a cualquier forma de prueba de penetración. La diferencia clave entre las pruebas de caja blanca, negra y gris es la cantidad de información proporcionada a los evaluadores antes del compromiso.

En una evaluación de caja blanca, el probador recibirá información completa sobre la aplicación y su tecnología, y generalmente se le otorgarán credenciales con diversos grados de acceso para identificar de manera rápida y completa las vulnerabilidades en las aplicaciones, sistemas o redes. [9]

Caja negra

Las evaluaciones de caja negra son la forma más común de evaluación de penetración de red y son más típicas entre las pruebas de penetración de red externa y las pruebas de penetración de ingeniería social. En una evaluación de caja negra, los probadores reciben muy poca o ninguna información sobre las redes o sistemas que están

probando. Esta forma particular de prueba es ineficiente para la mayoría de los tipos de pruebas de aplicaciones web debido a la necesidad de credenciales para probar vulnerabilidades autenticadas, como la escalada de privilegios lateral y vertical. [9]

Caja gris

Las evaluaciones de caja gris son un híbrido de pruebas de caja blanca y negra, y generalmente se usan para proporcionar un escenario de prueba realista al tiempo que brindan a los evaluadores de penetración suficiente información para reducir el tiempo necesario para realizar el reconocimiento y otras actividades de prueba de caja negra. Además de esto, es importante en cualquier evaluación asegurarse de que está probando todos los sistemas incluidos en el alcance. En una verdadera caja negra, es posible pasar por alto sistemas y, como resultado, dejarlos fuera de la evaluación. La caja gris suele ser la mejor forma de prueba de penetración de la red, ya que proporciona el mayor valor a los clientes. [9]

1.3.5. Tipos de pruebas de penetración

La vulnerabilidad y el escaneo de puertos no pueden identificar los problemas que pueden identificar las pruebas manuales, y esta es la razón por la que una organización contrata a probadores de penetración para realizar estas evaluaciones. Entregar escaneos en lugar de pruebas manuales es una forma de fraude y, en mi opinión, es muy poco ético. [9]

Pruebas de penetración de aplicaciones web

Pruebas de penetración de aplicaciones web, en lo sucesivo denominado WAPT, es la forma más común de prueba de penetración y probablemente sea el primer trabajo de prueba de penetración en el que participará la mayoría de las personas. WAPT es el acto de realizar piratería manual o pruebas de penetración contra una aplicación web para probar las vulnerabilidades que los escáneres ganaron no encontrar Con demasiada frecuencia, los evaluadores envían escaneos de vulnerabilidades de aplicaciones web en lugar de encontrar y verificar manualmente los problemas dentro de las aplicaciones web. [9]

Pruebas de penetración de aplicaciones móviles

Las pruebas de penetración de aplicaciones móviles son similares a las pruebas de penetración de aplicaciones web, pero son específicas de las aplicaciones móviles

que contienen sus propios vectores de ataque y amenazas. Esta es una forma creciente de pruebas de penetración con una gran oportunidad para aquellos que buscan ingresar a las pruebas de penetración y comprender el desarrollo de aplicaciones móviles. [9]

Pruebas de penetración de ingeniería social

La ingeniería social es el arte de manipular la psicología humana básica para encontrar las vulnerabilidades humanas y hacer que las personas hagan cosas que de otro modo no harían. Durante esta forma de prueba de penetración, es posible que se le pida que realice actividades como enviar correos electrónicos de phishing, hacer llamadas telefónicas de vishing o abrirse camino en instalaciones seguras para determinar qué podría lograr un atacante que se dirige a su personal. [9]

Pruebas de penetración de red

Las pruebas de penetración de red se centran en identificar las debilidades de seguridad en un entorno específico. Los objetivos de la prueba de penetración son identificar las fallas en los sistemas de la organización objetivo, sus redes alámbricas e inalámbricas y sus dispositivos de red, como conmutadores y enrutadores. [6]

Las siguientes son algunas tareas que se realizan mediante pruebas de penetración de red:

- Pasar por alto un Sistema de detección de intrusos (DNI)/Sistema de prevención de intrusiones (IPS)
- Eludir los dispositivos de cortafuegos
- Descifrado de contraseñas

Pruebas de penetración en la nube

Las pruebas de penetración en la nube implican realizar evaluaciones de seguridad y pruebas de penetración sobre los riesgos de las plataformas en la nube para descubrir cualquier vulnerabilidad que pueda exponer información confidencial a usuarios malintencionados. [9]

Antes de intentar contratar directamente una plataforma en la nube, asegúrese de tener el permiso legal del proveedor. Por ejemplo, si va a realizar pruebas de penetración en la plataforma Azure, necesitará el permiso legal de Microsoft. [9]

Pruebas de penetración física

Las pruebas de penetración física se centran en probar los sistemas de control de acceso de seguridad física existentes para proteger los datos de una organización. Existen controles de seguridad dentro de las oficinas y centros de datos para evitar que personas no autorizadas ingresen a las áreas seguras de una empresa. [9]

Los controles de seguridad física incluyen lo siguiente:

- Cámaras y sensores de seguridad: Las cámaras de seguridad se utilizan para monitorear acciones físicas dentro de un área.
- Sistemas de autenticación biométrica: La biometría se utiliza para garantizar que solo las personas autorizadas tengan acceso a un área.
- Puertas y cerraduras: Los sistemas de bloqueo se utilizan para evitar que personas no autorizadas entren en una habitación o área.
- Guardias de seguridad: Los guardias de seguridad son personas asignadas para proteger algo, alguien o un área.

1.3.6. Fases del Hacking Ético

Fases de pirateo

Durante cualquier entrenamiento de prueba de penetración, encontrará las cinco fases de la piratería.

Estas fases son las siguientes:

• Reconocimiento
• Escaneo
• Obtener acceso
• Mantenimiento del acceso
• Mantenerse oculto
• Reportar

Reconocimiento o recopilación de información.

La fase de reconocimiento o recopilación de información es donde el atacante se enfoca en adquirir información significativa sobre su objetivo. Esta es la fase más importante en la piratería: cuantos más detalles se conozcan sobre el objetivo, más fácil será comprometer una debilidad y explotarla. [9]

Las siguientes son técnicas utilizadas en la fase de reconocimiento:

- Uso de motores de búsqueda para recopilar información Uso de plataformas de redes sociales
- Realizar piratería de Google
- Realización de interrogación de DNS
- Ingeniería social

En esta fase, el objetivo es recopilar la mayor cantidad de información posible sobre el objetivo**.** [9]

Exploración

La segunda fase de la piratería es escanear. El escaneo implica el uso de un enfoque directo al atacar al objetivo para obtener información a la que no se puede acceder a través de la fase de reconocimiento. Esta fase implica perfilar la organización objetivo, sus sistemas y la infraestructura de red. [9]

Las siguientes son técnicas utilizadas en la fase de exploración:

- Comprobación de sistemas activos.
- Comprobación de cortafuegos y sus reglas.
- Comprobación de puertos de red abiertos.
- Comprobación de servicios en ejecución.
- Comprobación de vulnerabilidades de seguridad.
- Creación de una topología de red de la red de destino.

Esta fase es muy importante ya que ayuda a crear un perfil del target. La información encontrada en esta fase ayuda a pasar a realizar la explotación en el sistema o red de destino. [9]

Obtener acceso

En esta fase, el atacante utiliza la información obtenida de las fases anteriores para explotar el objetivo. Tras la explotación exitosa de las vulnerabilidades, el atacante puede ejecutar de forma remota un código malicioso en el objetivo y obtener acceso remoto al sistema comprometido. [9]

Lo siguiente puede ocurrir una vez que se obtiene el acceso:

- Descifrado de contraseñas

- Explotación de vulnerabilidades
- Escalada de privilegios
- Ocultar archivos
- Movimiento lateral

La fase de obtención de acceso a veces puede ser difícil, ya que las vulnerabilidades pueden funcionar en un sistema y no en otro. Una vez que un exploit tiene éxito y se adquiere el acceso al sistema, la siguiente fase es asegurarse de tener una conexión persistente con el objetivo. [9]

Mantenimiento del acceso

Después de explotar un sistema, el atacante generalmente debe asegurarse de poder acceder al sistema de la víctima en cualquier momento mientras el sistema esté en línea. Esto se hace creando un acceso de puerta trasera en el objetivo y configurando una conexión inversa o vinculante persistente entre las máquinas del atacante y el sistema de la víctima. [9]

Los objetivos de mantener el acceso son los siguientes:

- Movimiento lateral
- Ex filtración de datos
- Creación de puertas traseras y conexiones persistentes

Mantener el acceso es importante para garantizar que usted, el evaluador de penetración, siempre tenga acceso al sistema o red de destino. Una vez que se completa el aspecto técnico de la prueba de penetración, es hora de limpiar la red. [9]

Mantenerse Oculto

La última fase es cubrir las huellas. Esto asegura que no deje ningún rastro de su presencia en un sistema comprometido. A los probadores de penetración, gusta ser indetectables en la red de un objetivo, sin activar ninguna alerta mientras se elimina cualquier rastro residual de las acciones realizadas durante la prueba de penetración. [9]

Cubrir las pistas garantiza que no deje ningún rastro de su presencia en la red, ya que una prueba de penetración está diseñada para ser sigilosa y simular ataques del mundo real a una organización. [9]

1.3 Objetivos

1.3.1 Objetivo general

Evaluar la seguridad del sistema de video vigilancia de la empresa ECUASEG.

1.3.2 Objetivos específicos

- Analizar las principales técnicas de hacking ético y herramientas en sistemas de video vigilancia
- Implementar pruebas de penetración en el sistema de video vigilancia de la empresa ECUASEG aplicando hacking ético
- Definir una guía de referencia para procedimientos de seguridad en el sistema de video vigilancia de la empresa ECUASEG.

CAPÍTULO II

METODOLOGÍA

2.1 Métodos

2.1.1 Modalidad de la Investigación

El presente proyecto se fundamentó en una investigación aplicada, utilizando las siguientes modalidades:

- Investigación bibliográfica, debido a la obtención de información científica en base al tema de investigación se llevó a cabo consultando principalmente revistas científicas, artículos científicos, publicaciones y proyectos de titulación de repositorios públicos y privados desarrollados en los últimos años, cada uno relacionados y vinculados al hacking ético y sistema de video vigilancia.
- Investigación experimental, efectuando pruebas de vulnerabilidades, amenazas y riesgos aplicando hacking ético en el sistema de video vigilancia de la empresa ECUASEG.

2.1.2 Recolección de Información

Para la recolección de información se analizó arios artículos científicos, tesis, libros, así como guías prácticas y manuales por lo que se tomará en cuenta bases de datos confiables acerca de hacking ético sobre sistemas de video vigilancia

2.1.3 Procesamiento y Análisis de Datos

Para el procesamiento y análisis de datos se realizarán las siguientes actividades:

- Revisión de la información recopilada.
- Interpretación correcta la información recopilada.
- Estudio de las propuestas de solución planteada.
- Planteamiento de la propuesta de solución.
- Control y verificación de los datos obtenidos.

2.1.4 Desarrollo del proyecto

1. Análisis de los vulnerabilidades y ataques actuales que sufren los sistemas de video vigilancia.
2. Investigación de las principales técnicas de hacking en sistemas de video vigilancia.
3. Selección de herramientas de software para realizar el hacking ético. .
4. Identificación de los equipos y marcar utilizados en el sistema de video vigilancia de ECUASEG.
5. Búsqueda de las vulnerabilidades actuales de las marcas de los equipos de video vigilancia.
6. Implementación de pruebas de penetración en el sistema de video vigilancia de la empresa ECUASEG aplicando hacking ético.
7. Procesamiento de la información sobre las vulnerabilidades y ataques sobre el sistema de vigilancia auditado.
8. Desarrollo de una tabla resumen de las vulnerabilidades identificadas en la investigación y el software utilizado.
9. Diseño de una guía de referencia para procedimientos de seguridad en el sistema de video vigilancia de la empresa ECUASEG.
10. Elaboración del informe final.

CAPÍTULO III

RESULTADOS Y DISCUSIÓN

3.1 Análisis y discusión de los resultados.

3.1.1 Desarrollo de la propuesta

Para el presente proyecto se realizó una evaluación de vulnerabilidades del sistema de video vigilancia de la empresa ECUASEG aplicando hacking ético. El desarrollo de la investigación va dirigido a la detección de vulnerabilidades, amenazas y riesgos del sistema de video vigilancia en la empresa ECUASEG, por medio de las 6 fases establecidas como: reconocimiento, exploración, obtener acceso, mantener acceso, mantenerse oculto y reporte para evaluar la seguridad del sistema de video vigilancia.

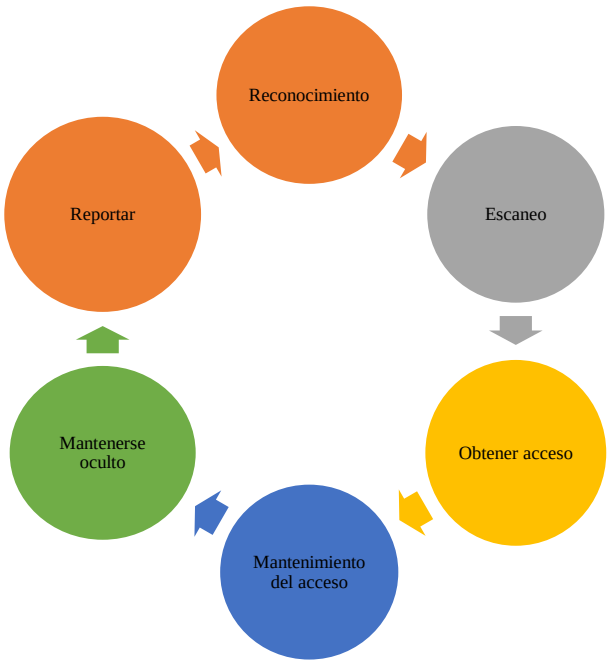


Figura 1. Fases de Pentesting

Fuente: Elaborado por el investigador

3.1.1.1 Selección de los elementos para la implementación del laboratorio de Pentesting

Tabla 1. Software para el laboratorio de pentesting

	Kali Linux	**Parrot Security OS**	**BackBox**
Sistema Operativo	Linux	Linux	Linux
Año	2004	2013	2010
Audiencia	Empresas e individuos que buscan una distribución de Linux de código abierto orientada a diversas tareas de seguridad de la información. [11]	Empresas e individuos que buscan una distribución de Linux de código abierto orientada a diversas tareas de seguridad de la información. [11]	Cualquiera que busque un sistema operativo gratuito que ofrezca herramientas de piratería ética y servicios de pruebas de penetración [11].
Software	Código Abierto	Código Abierto	Código abierto
Basado en	Debian	Debian	Debian
Arquitectura	armel, armhf, i386, x86_64	i386, x86_64, ARM	i386, x8E6_64, ARM
Paquetes	PGP	PGP	PGP
Personalizable	Si	Si	Si
Lenguaje	Multi-Lenguaje	Multi-Lenguaje	Multi-Lenguaje
Estado	Activo	Activo	Activado
Característica	Auditor de seguridad Forense	Forense	Auditoria de Seguridad
Herramientas	600	250	200

Elaborado por el investigador [11]

3.1.1.2 Diseño e Implementación del banco de pruebas del sistema de video vigilancia de gama baja basado en IP

Configuración del laboratorio de pentesting

1. Instalación de Virtual Box, ver anexo A.

2. Instalación de KaliLinux, ver anexo B.

Fase 1 Reconocimiento

Google Dorks. Para el reconocimiento de la empresa por medio de un buscador web en este caso se utilizó google dork para hacer más específica la búsqueda.

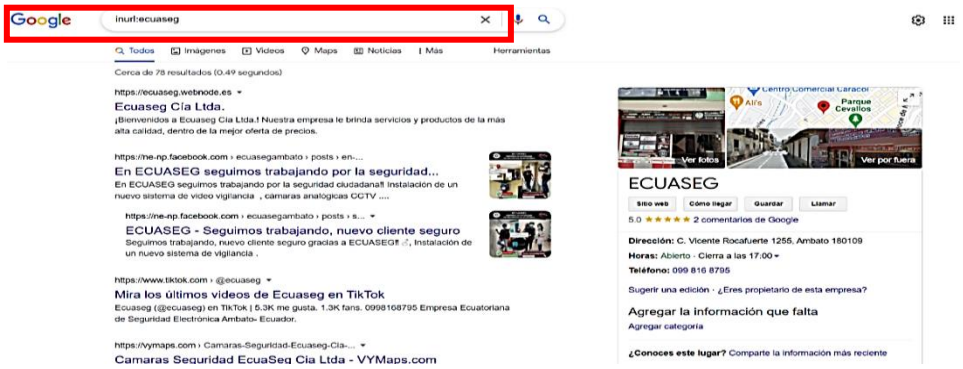


Figura 2. Uso de google dorks

Elaborado por el investigador

En la segunda búsqueda, se utiliza intitle para hacer una búsqueda de todas las páginas en donde aparezca la palabra ECUASEG.

En la figura 3, se destacaron las páginas de Facebook, Instagram, tiktok y LinkedIn de la Empresa ECUASEG y sus trabajadores.

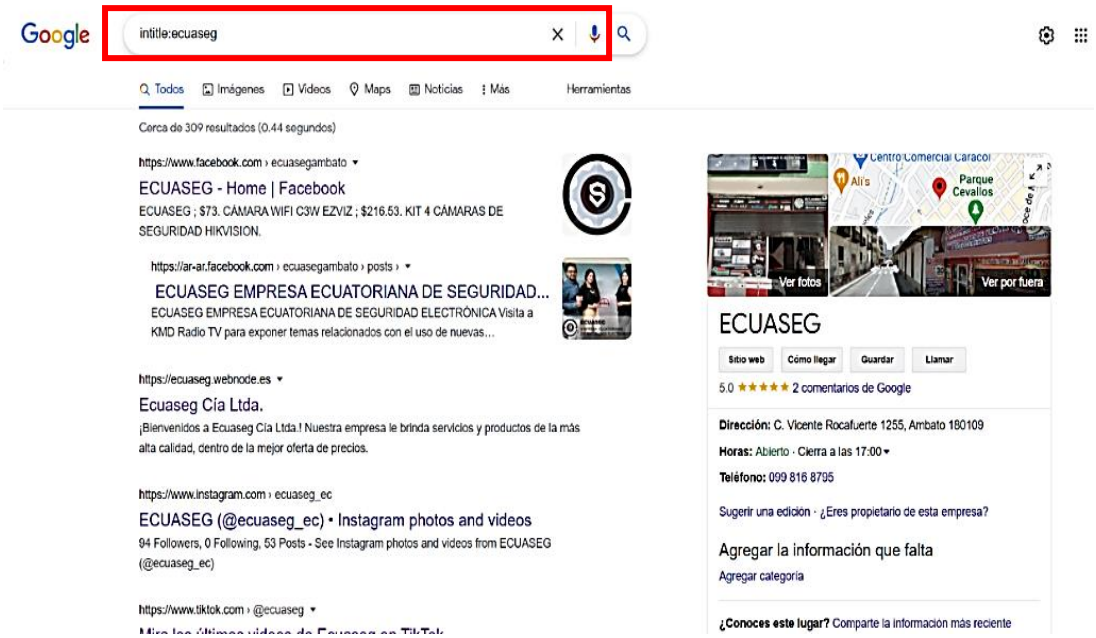


Figura 3. Uso intitle

Elaborado por el investigador

Facebook de ECUASEG. En la figura 4, se puede notar que las principales marcas con las que trabaja la empresa son Hikvison, Dawua, Ezviz.

Figura 4. Análisis de la página de Facebook de ECUASEG

Elaborado por el investigador

En la figura 5, se observó que en la página de Facebook de la empresa hay datos de teléfono, ubicación y correo electrónico.

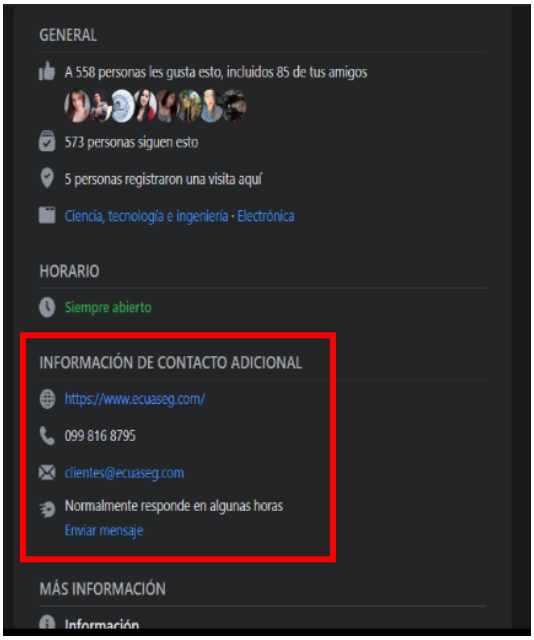


Figura 5. Datos de la página Facebook de ECUASEG

Elaborado por el investigador

LinkedIn de ECUASEG. En la página de LinkedIn del gerente de la empresa se observó la siguiente información, como se visualiza en la figura 6.

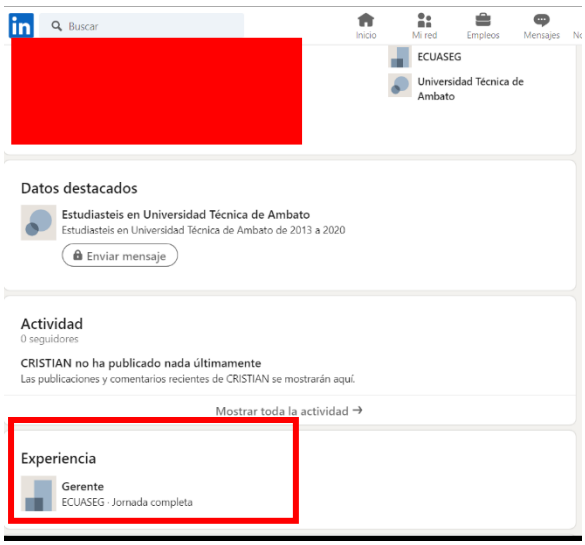


Figura 6. Información de LinkedIn

Elaborado por el investigador

Maltego. Es la herramienta para observar perfiles personales y empresariales en la que se realizó la búsqueda del dueño de la empresa ECUASEG.

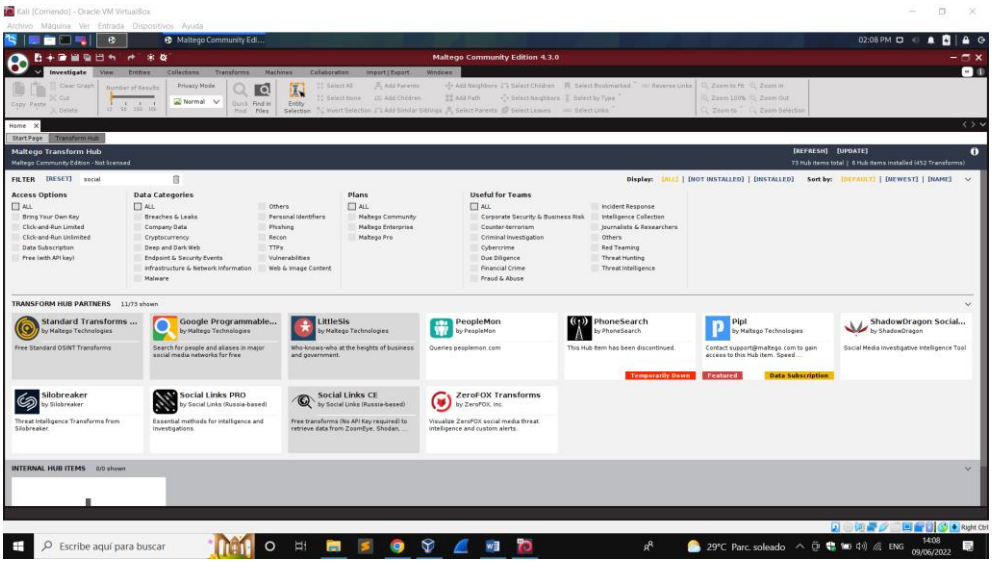


Figura 7. Interfaz de Maltego

Elaborado por el investigador

Después se creó una hoja en blanco para colocar los datos de la persona a investigar con una entidad de frase como punto de partida y cambiar el valor de entrada del valor predeterminado al alias de destino, "XXXXXXXXXXXXXXXXXXX" (Por políticas de confidencialidad se ocultó nombres personales).

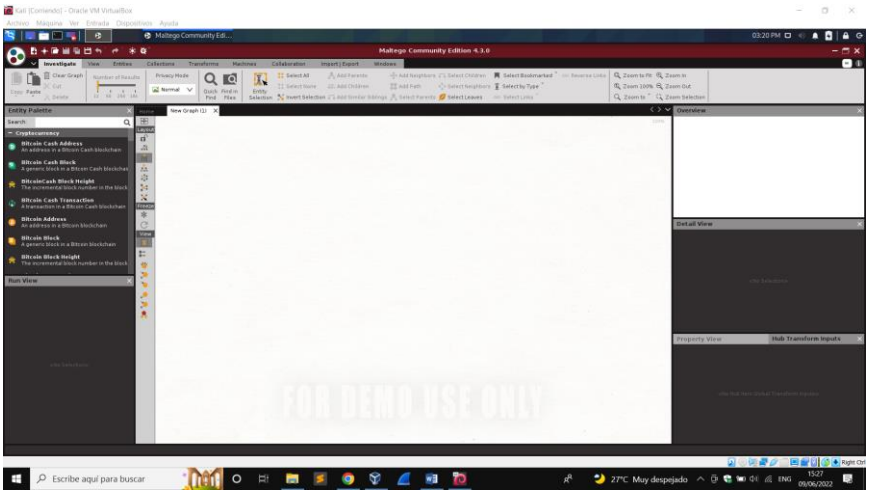


Figura 8. Hoja en blanco para el análisis de datos

Elaborado por el investigador

Se analizaron los sitios web que tengan el nombre de la persona que se está buscando. A continuación, se ejecuta la transformación a sitios web en esta entidad de frase. Esta transformación consulta el motor de búsqueda Bing, que devuelve todos los sitios web que mencionan nuestro término de búsqueda citado, XXXXXXXXXXXXXXXXXXX " (Por políticas de confidencialidad se ocultó nombres personales).

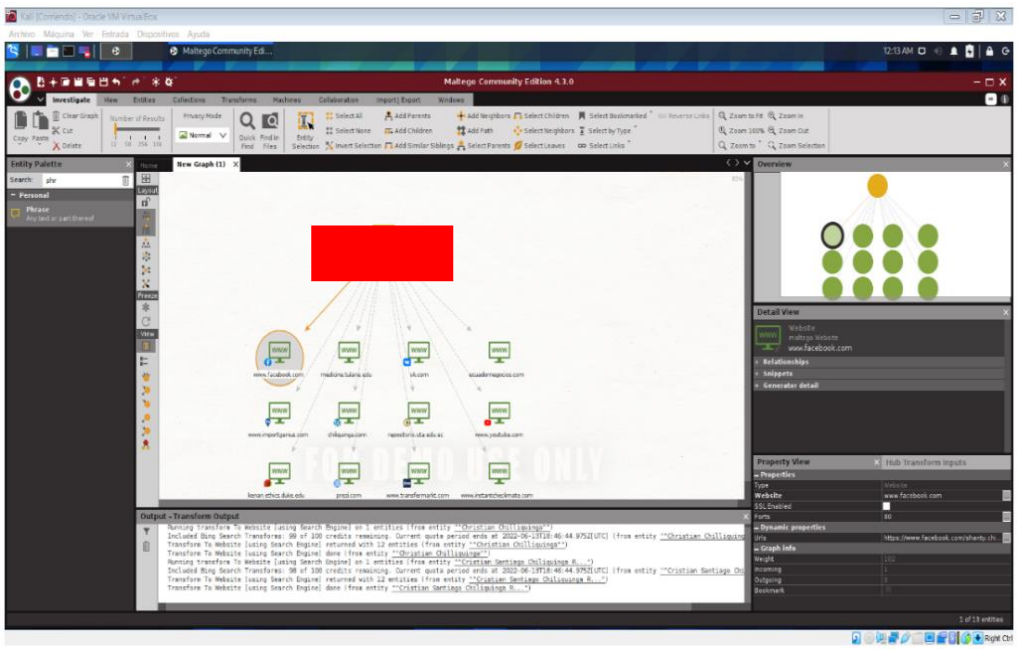


Figura 9. Datos detectados por la Herramienta Maltego

Elaborado por el investigador

Los datos más relevantes de la victimas en este caso la página de Facebook y la universidad en la cual realizó sus estudios.

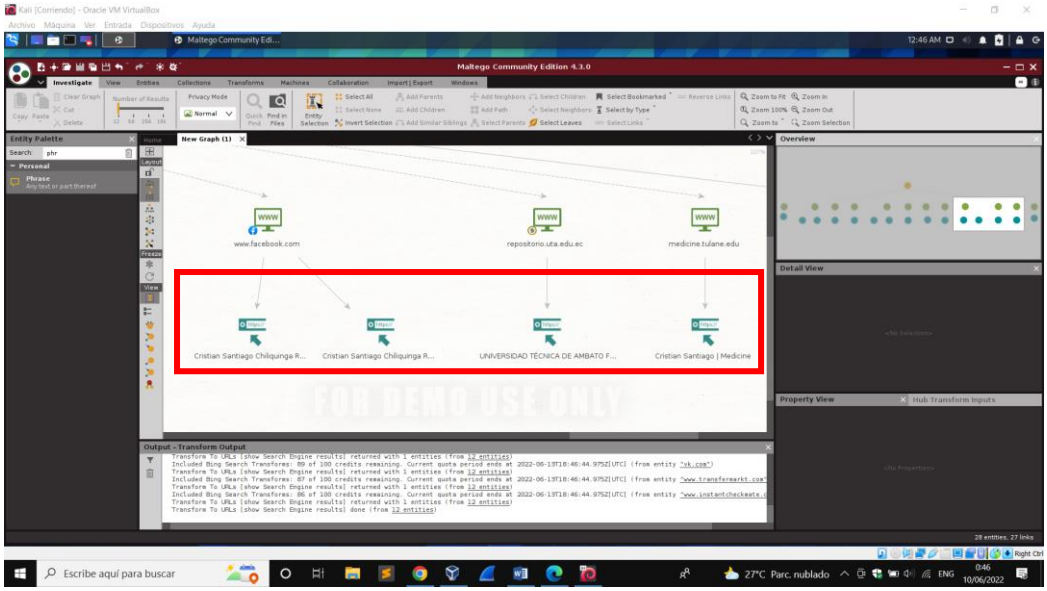


Figura 10. Información relevante de la persona investigada

Elaborado por el investigador

La herramienta arrojó 12 resultados y para profundizar la búsqueda en estos dos sitios web, se va a usar la transformación a direcciones URL [usando el motor de búsqueda] en estas entidades del sitio web para encontrar las direcciones URL relacionadas, como describe la figura 11.

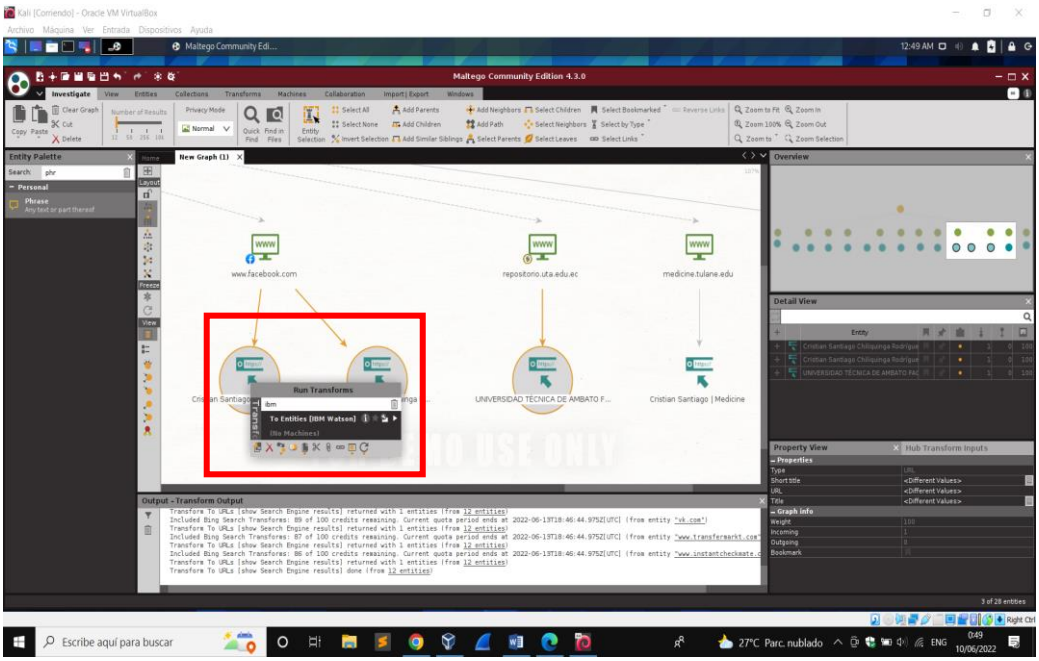


Figura 11. To Entities [IBM Watson]

Elaborado por el investigador

La ejecución de la transformación A entidades [IBM Watson], que extraerá entidades como organizaciones, ubicaciones, direcciones de correo electrónico, personas e imágenes que se encuentran en las páginas web.

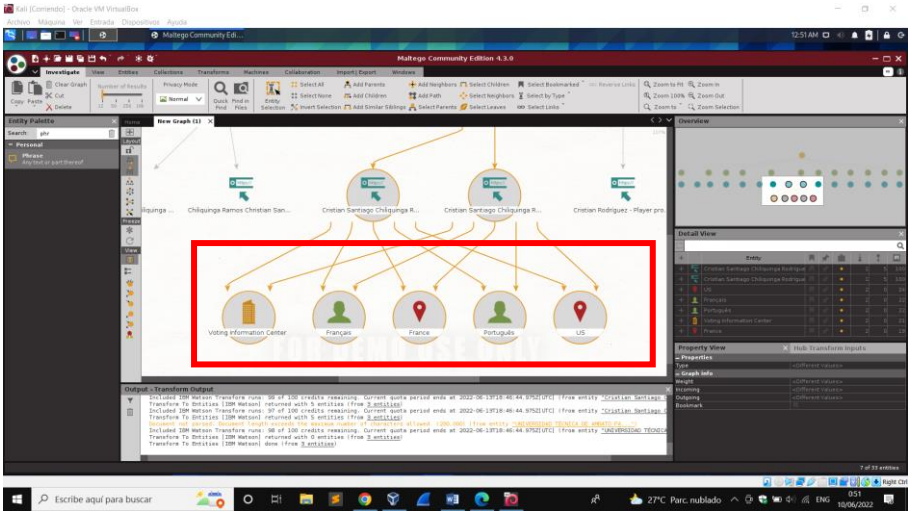


Figura 12. Datos del transformer IBM Watson

Elaborado por el investigador

De los datos encontrados se observa una URL, que dirige a una página en específico, como se observa en la figura 13.

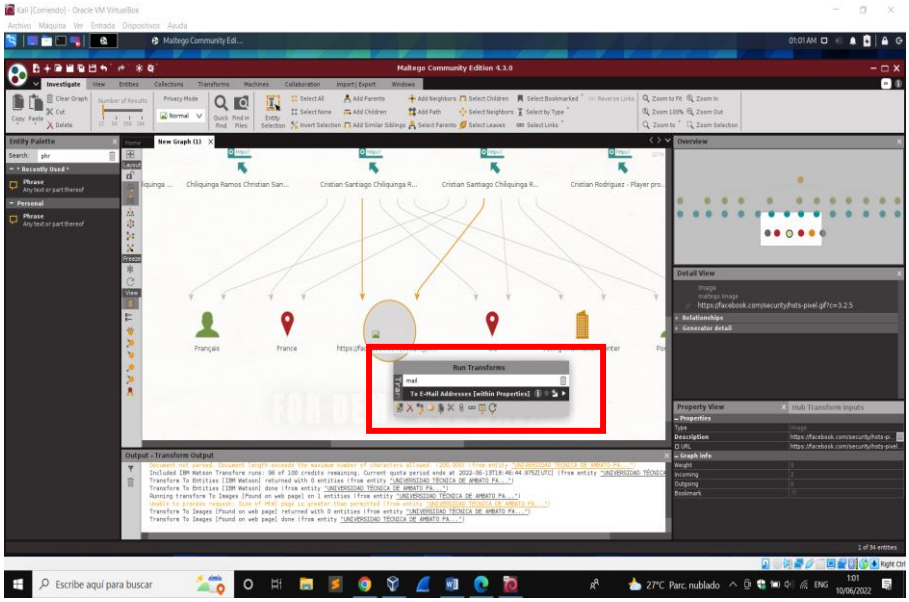


Figura 13. Transformer mail

Elaborado por el investigador

Al ejecutar la transformación a dirección de correo electrónico [Bing] en la entidad de persona permite obtener el correo electrónico del sujeto a investigar en este caso no se logró obtener más información relevante.

Recopilación o escaneo

Para el escaneo de vulnerabilidades se utiliza el navegador Shodan el cual permite detectar los dispositivos conectados a internet. En la figura 14, se observa los resultados de los equipos vulnerables alrededor del mundo de la marca Hikvision

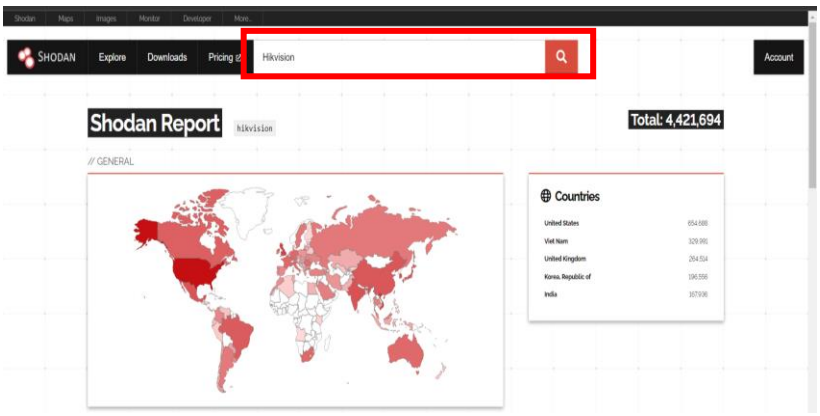


Figura 14. Navegador Shodan

Elaborado por el investigador

En la figura 15, se observó una serie de categorías que Shodan da a conocer, la situación de los equipos Hikvision, la categoría Vulnerabilities indica las vulnerabilidades que un hacker puede explotar.

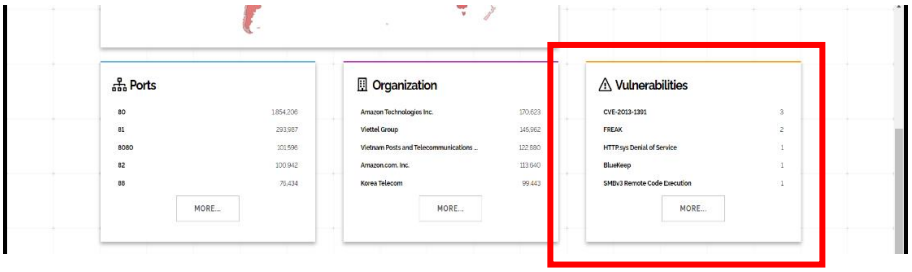


Figura 15. Categorías mostradas por Shodan

Elaborado por el investigador

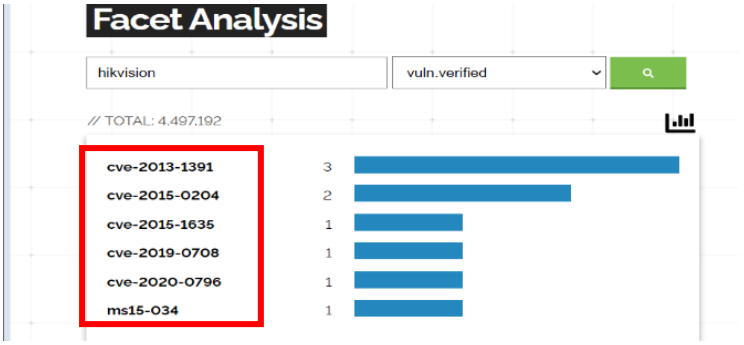


Figura 16. Vulnerabilidades de Shodan

Elaborado por el investigador

Tabla 2. Vulnerabilidades de Hikvision expuestas por el navegador shodan

Vulnerabilidades	**Descripción**
CVE-2019-0708	Existe una vulnerabilidad de ejecución remota de código en los Servicios de Escritorio Remoto, anteriormente conocidos como Servicios de Terminal Server, cuando un atacante no autenticado se conecta al sistema de destino mediante RDP y envía solicitudes especialmente diseñadas, también conocida como 'Vulnerabilidad de Ejecución Remota de Código de Servicios de Escritorio Remoto'. [11]
CVE-2020-0796	Existe una vulnerabilidad de ejecución remota de código en la forma en que el protocolo Microsoft Server Message Block 3.1.1 (SMBv3) maneja ciertas solicitudes, también conocida como "vulnerabilidad de ejecución remota de código cliente/servidor Windows SMBv3". [12]
MS15-034	La vulnerabilidad podría permitir la ejecución remota de código si un atacante envía una solicitud HTTP especialmente diseñada a un sistema Windows afectado. [13]

Elaborado por el investigador

Después, se realizó un análisis más profundo de los dispositivos en el Ecuador. Por medio del navegador se verifica la situación actual de seguridad en el país por medio de comando de Hikvision country:"Ec"

En la figura 17, se muestra 6,383 resultados de dispositivos conectados a internet de los cuales 130, se encontraron en la ciudad de Ambato con el comando: Hikvision country:"Ec" city:"Ambato"

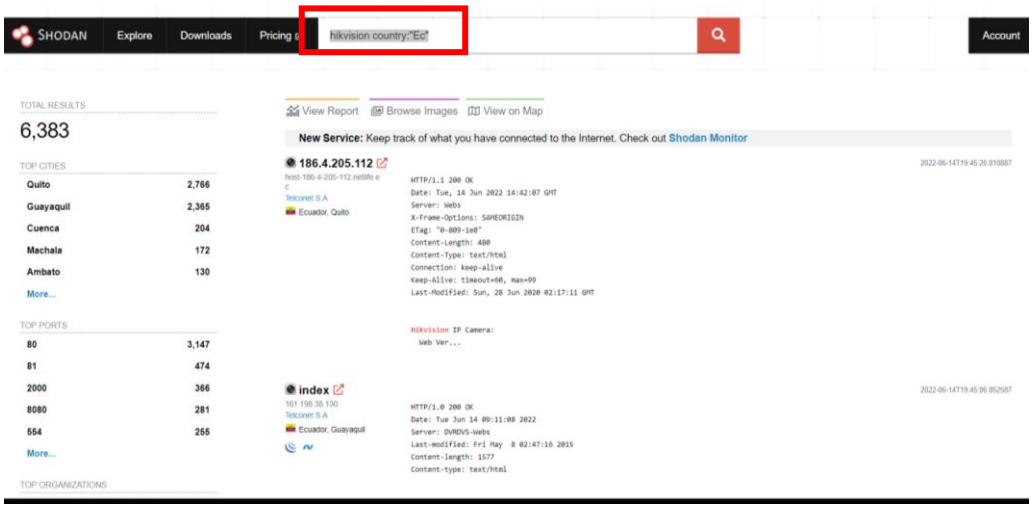


Figura 17. Situación de Hikvision en el Ecuador

Elaborado por el investigador

En la figura 18, se observó que el navegador shodan brinda información de los puertos más utilizados por las marcas y Hikvision y los proveedores de internet que tiene conectado algún equipo de dicha marca.

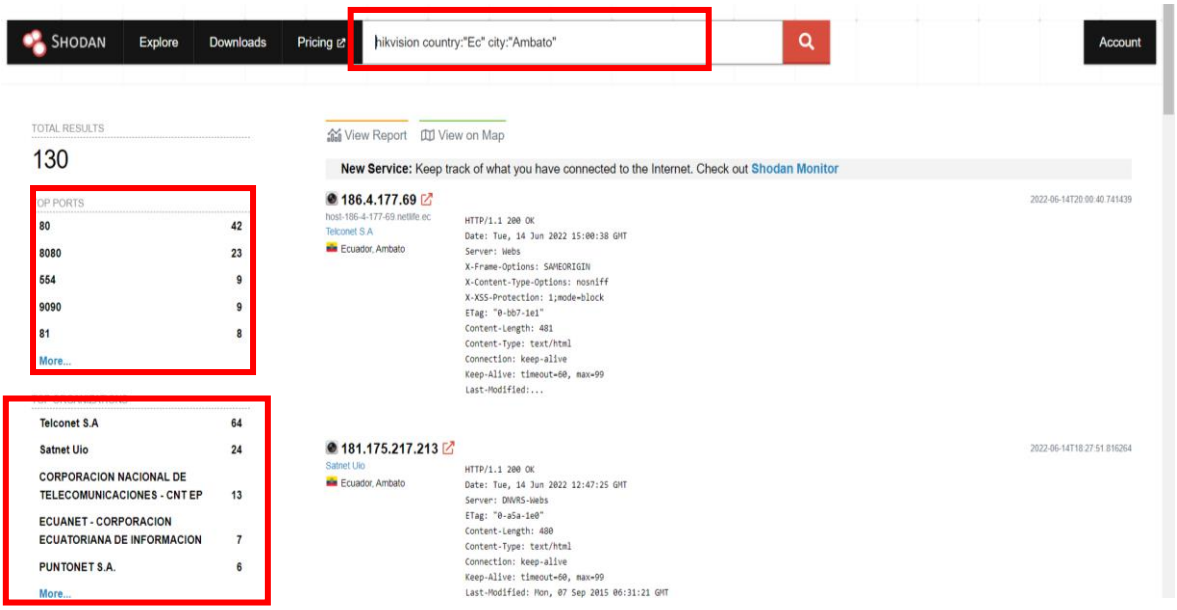


Figura 18. Dispositivos Hikvision en la ciudad de Ambato

Elaborado por el investigador

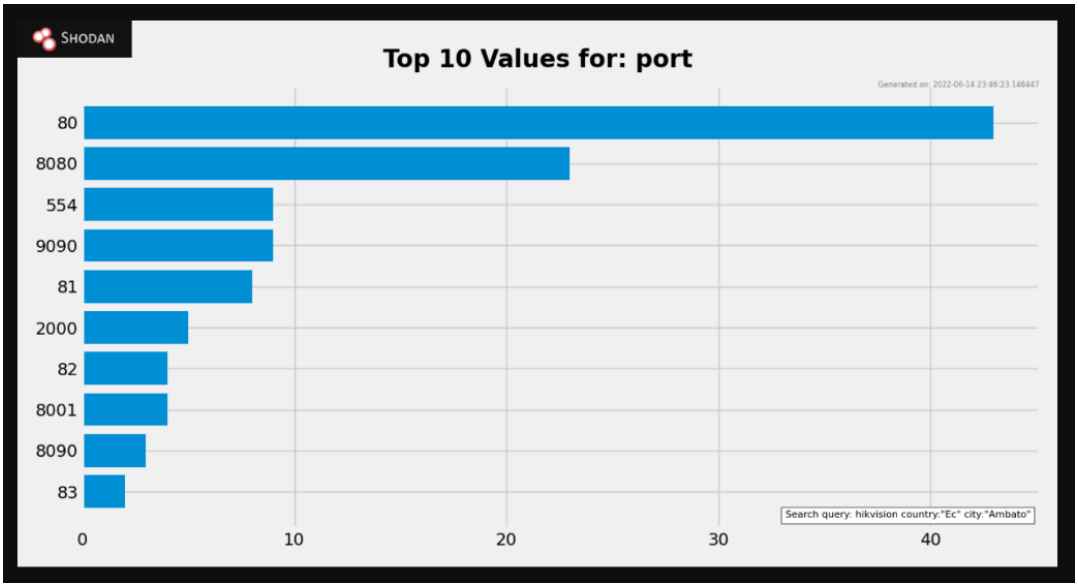


Figura 19. Top 10 de puertos utilizados en Hikvision

Elaborado por el investigador

En la ciudad de Ambato donde brinda los servicios la empresa ECUASEG se encontró varios equipos de la marca Hikvision conectados a internet, por medio de diferentes proveedores de internet, para especificar la búsqueda en la ciudad de Ambato se utilizó el comando: Hikvision country:"Ec" city:"Ambato" org:"Telconet S.A"

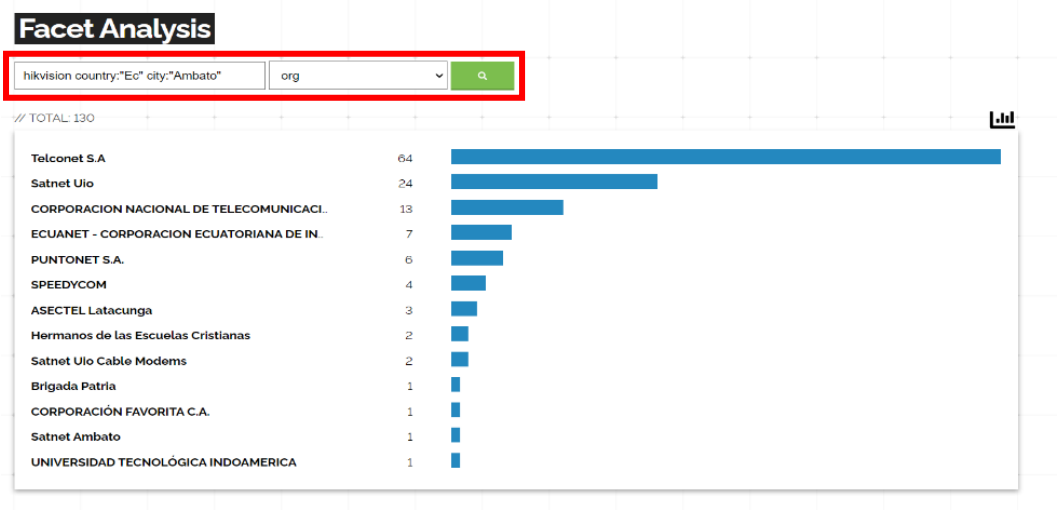


Figura 20. Organizaciones en donde se encuentran conectados dispositivos Hikvision

Elaborado por el investigador

En la figura 21, se muestran los dispositivos que están conectados a Telconet SA en este caso se ha encontrado a 64. A continuación, se selecciona uno al azar para analizar cómo se redirige a la página de inicio, en este caso de un DVR.

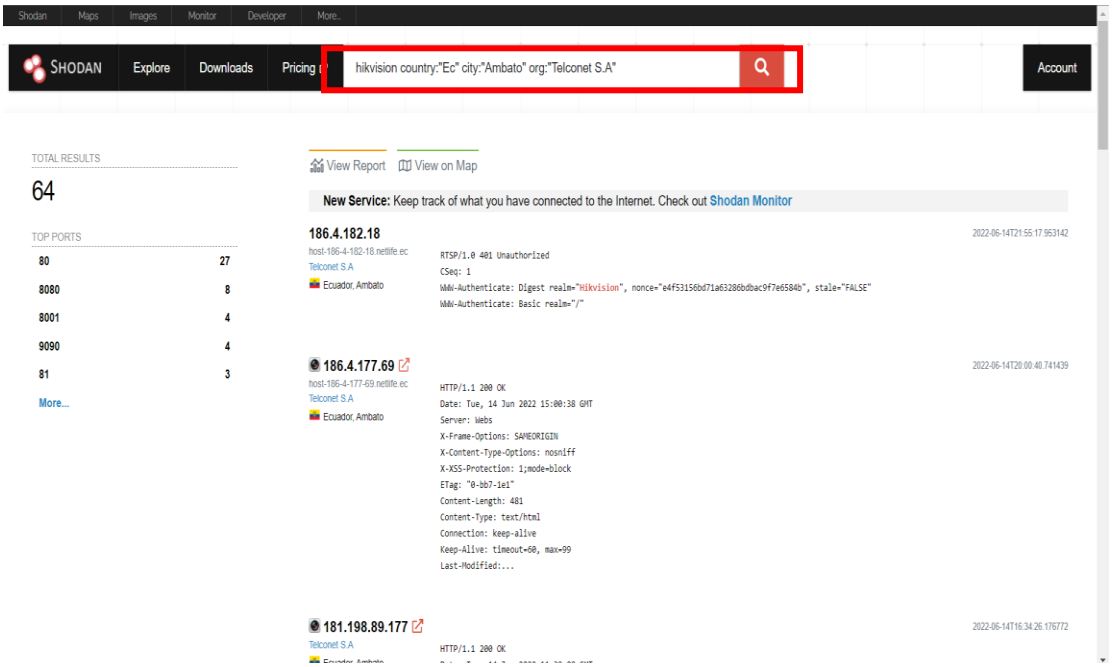


Figura 21. Dispositivos conectados a Telconet SA

Elaborado por el investigador

En la figura 22, se muestra que por medio de la herramienta shodan se obtuvo acceso a equipos Hikvision en la ciudad de Ambato mostrando lo fácil de detectar equipos conectados a la red.

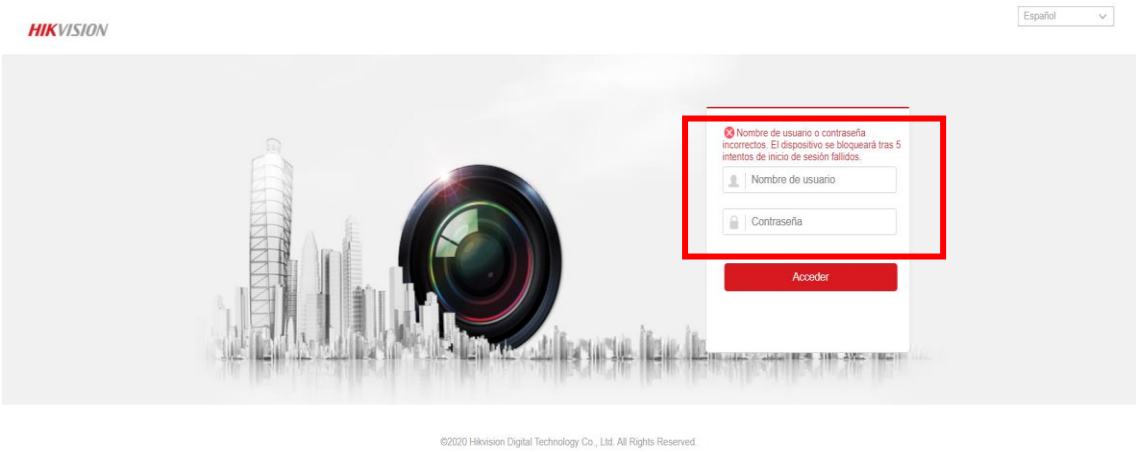


Figura 22. Página de inicio de un DVR de la marca Hikvision

Elaborado por Autor

Obteniendo Acceso

Ataque Wifi WPA/WPA2

Primero, se verificó que la tarjeta de red se encuentre activa, por medio del comando: iwconfig y para observar el estado del adaptador inalámbrico

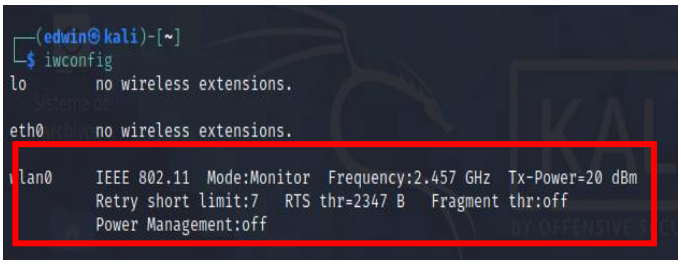


Figura 23. Verificación de tarjeta de red

Elaborado por el investigador

Segundo, se inició la tarjeta de red en modo monitor usando el comando: -airmon-ng iniciar wlan0 10

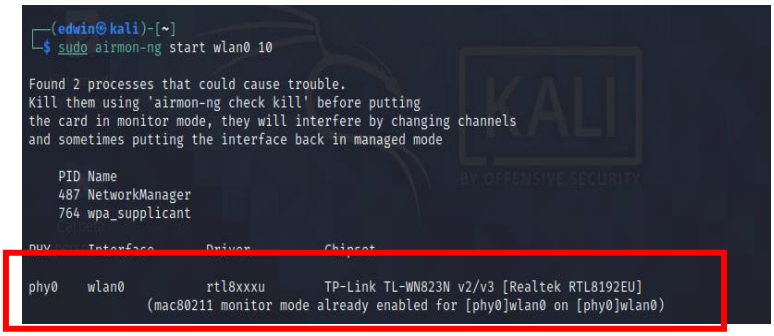


Figura 24. Tarjeta de red en modo monitor

Elaborado por Autor

Para observar todas las redes Wifi alrededor se utilizó la herramienta airodump-ng, con el comando: -airodump-ng wlan0

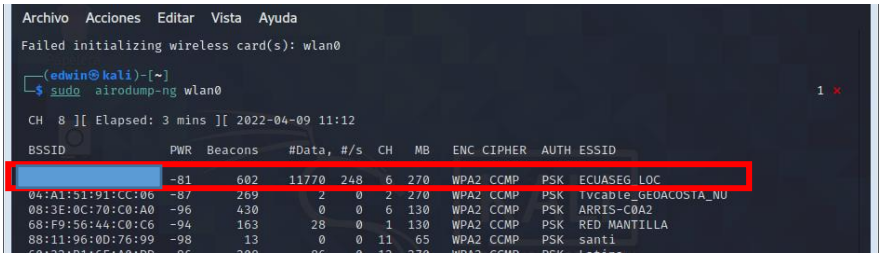


Figura 25. Redes Wifi

Elaborado por el investigador

En la figura 25, se observó la dirección MAC del AP de la empresa ECUASEG es: -&&:&&:&&:&&:&&:&& (Se remplazaron los caracteres hexadecimales de la MAC por políticas de seguridad empresarial).

Para la captura de los datos requerido de la red se utilizó el comando: airodump-ng --bssid &&:&&:&&:&&:&&:&& -c 6 wlan0 -w ECUASEG_hack

- &&:&&:&&:&&:&&:&& es el bssid de la red
- c 6 es el número de canal
- ECUASEG_hack es el archivo en el que se escribirá el tráfico capturado
- wlan0 es la red interfaz que se está monitoreando.

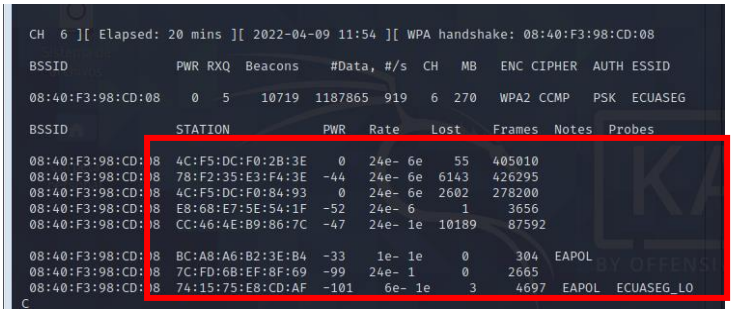


Figura 26. Dispositivos conectados a la red ECUASEG_LOG

Elaborado por el investigador

Por lo que se atacó a la red específica, para hacerlo se necesita capturar el tráfico en la red ECUASEG_LOG y comenzar a capturar el protocolo de enlace de 4 vías.

Tabla 3. Dispositivos conectados a la red ECUASEG_LOG

Dispositivo	**MAC**
AP (ECUASEGLOC)	&&:&&:&&:&&:&&:&&
Dispositivo 0	4C:F5:DC:F0:84:93
Dispositivo 1	E8:68:E7:5E:54:1F
Dispositivo 2	78:F2:35:E3:F4:3E
Dispositivo 3	BC:AB:A6:B2:3E:B4
Dispositivo 4	CC:46:4E:B9:86:7C

Dispositivo 5	78:F2:35:E3:F4:3E
Dispositivo 6	4C:F5:DC:F0:2B:3E

Elaborado por el investigador

Para desautenticar al cliente del Access Point se utilizó el comando: - aireplay-ng.

Dispositivo 1

-sudo aireplay-ng -0 5 -a &&:&&:&&:&&:&&:&& -c 4C:F5:DC:F0:84:93 wlan0

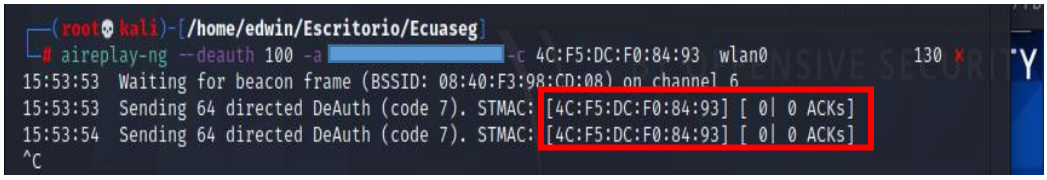


Figura 27. Desautentificación del dispositivo 1

Elaborado por el investigador

El dispositivo 1 no se desautentificó como se observa en la figura 27, no se obtiene captura del protocolo de 4 vías.

Dispositivo 2

-sudo aireplay-ng -0 5 -a &&:&&:&&:&&:&&:&& -c E8:68:E7:5E:54:1F wlan0

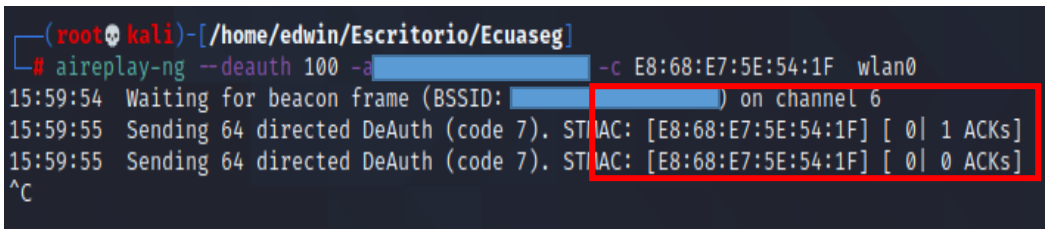


Figura 28. Desautentificación del dispositivo 2

Elaborado por el investigador

El dispositivo 2 no se desautentificó del AP, como se observa en la figura 28, no se obtiene el protocolo de 4 vías.

Dispositivo 3

-sudo aireplay-ng -0 5 -a &&:&&:&&:&&:&&:&& -c BC:A8:A6:B2:3E:B4 wlan0

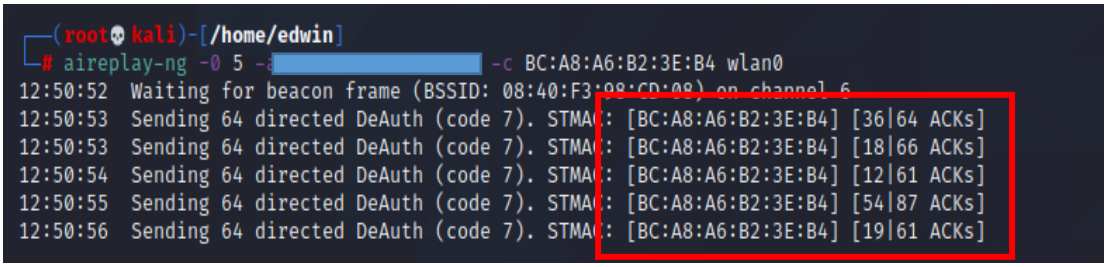


Figura 29. Desautentificación del dispositivo 3

Elaborado por el investigador

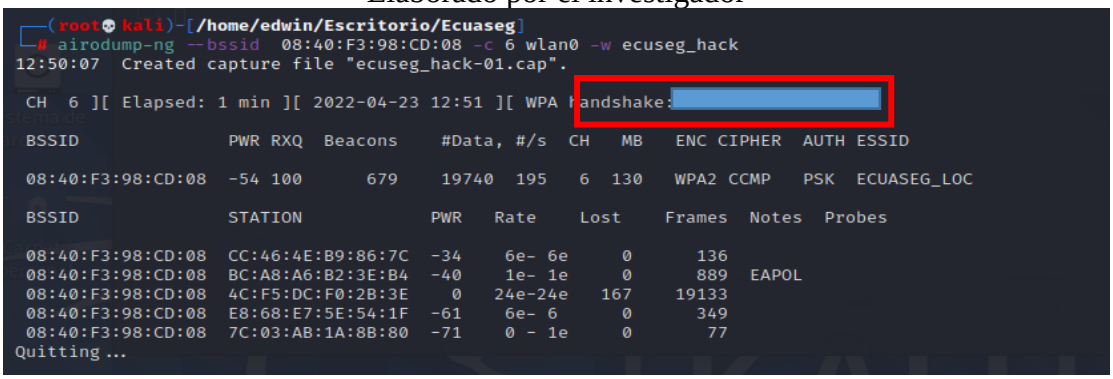


Figura 30. WPA handshake del dispositivo 3

Elaborado por el investigador

Una vez obtenido el protocolo de 4 vía, se procede a detener el monitoreo de la interfaz Wi-Fi. Se ingresa el comando para dejar de monitorear la interfaz Wi-Fi: airmon-ng stop wlan0.

Para descifrar la contraseña del archivo de protocolo de enlace capturado, se utilizó un ataque de fuerza bruta, en donde se necesitó una lista de palabras y el archivo de protocolo de enlace.

Prueba 1

Para la primera prueba de fuerza bruta se utilizó el diccionario “rockyou.txt” que se encuentra en KaliLinux, y es un listado de claves muy utilizado en ciberseguridad, a través del comando:

```
aircrack-ng -a2 -b &&:&&:&&:&&:&&:&&-w /usr/share/wordlists/
rockyou.txt/home/edwin/Escritorio/ECUASEG/*.cap
```

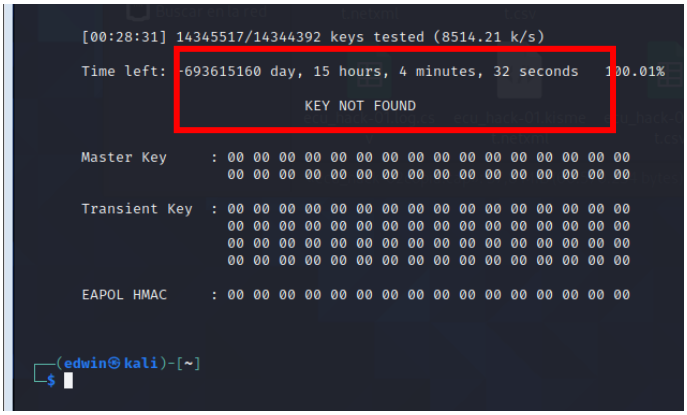


Figura 31. Primer Ataque de fuerza bruta

Elaborado por el investigador

Prueba 2

Para la creación de una lista se utilizó la herramienta Crunch, la cual genera una lista acorde a las especificaciones requeridas. Se creó un diccionario con números aleatorios para detectar la clave, este listado tiene 8 números, número mínimo que debe tener una clave Wifi.

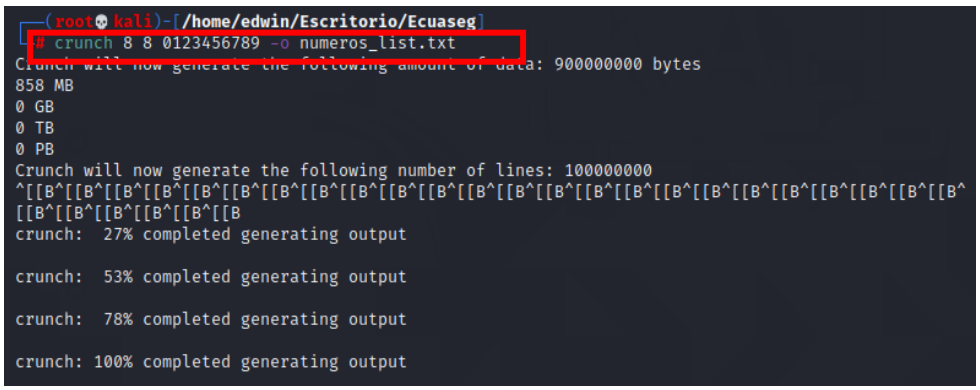


Figura 32. Creación de lista de numero con la herramienta Crunch

Elaborado por el investigador

Para el segundo ataque, se utilizó un nuevo diccionario creado con la herramienta Crunch: `aircrack-ng -a2 -b &&:&&:&&:&&:&&:&& -w numero_list.txt ecuseg_hack-01.cap`

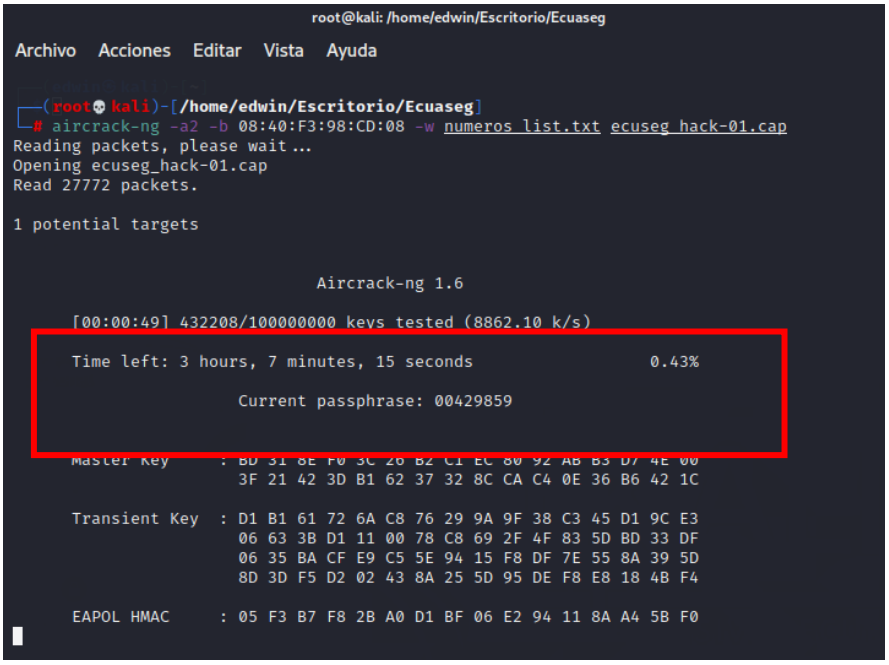


Figura 43. Segundo Ataque de fuerza bruta

Elaborado por el investigador

Prueba 3

Para la prueba 3, se creó una lista con 9 caracteres en la cual se combina la palabra ECUASEG con un listado de números.

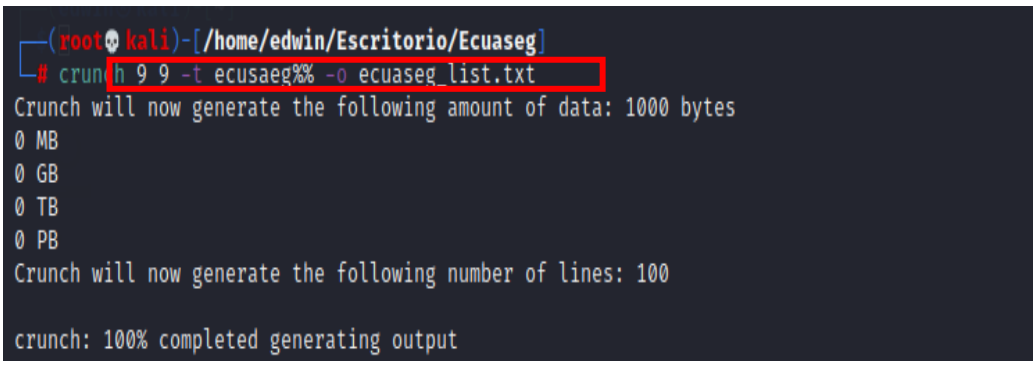


Figura 34. Creación del diccionario 2

Elaborado por el investigador

Después de la creación del diccionario se ejecutó el comando:

`-aircrack-ng -a2 -b &&:&&:&&:&&:&&:&& -w ECUASEG_list.txt ecuseg_hack-01.cap`

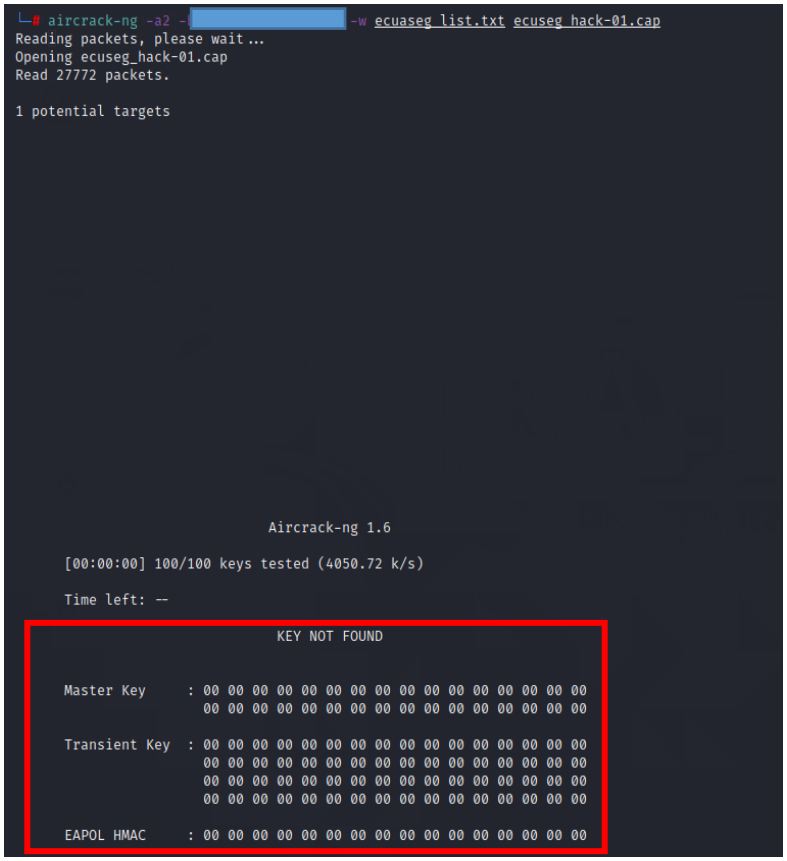


Figura 35. Tercer Ataque de fuerza bruta

Elaborado por el investigador

Prueba 4

Para la prueba número 4, se creó un diccionario con combinaciones de 10 caracteres, con la palabra ECUASEG y un conjunto de números y símbolos.

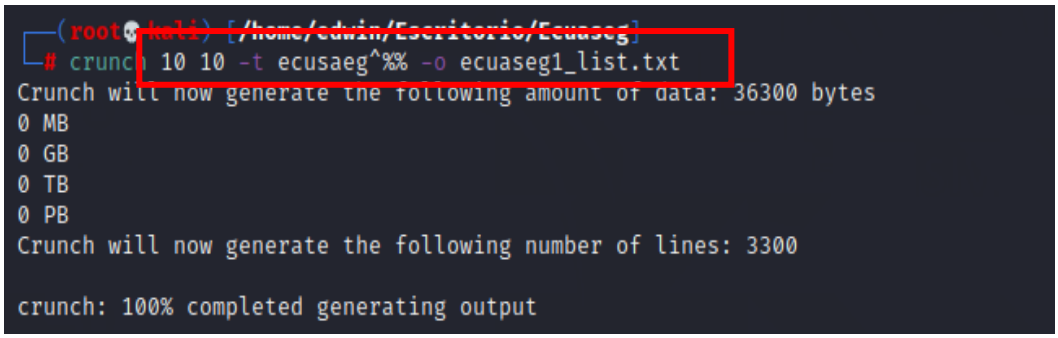


Figura 36. Creación del diccionario 3

Elaborado por el investigador

Para la cuarta prueba se utilizó el nuevo diccionario, creado con el comando:

`-aircrack-ng -a2 -b &&:&&:&&:&&:&&:&& -w ECUASEG1_list.txt ecuseg_hack-01.cap`

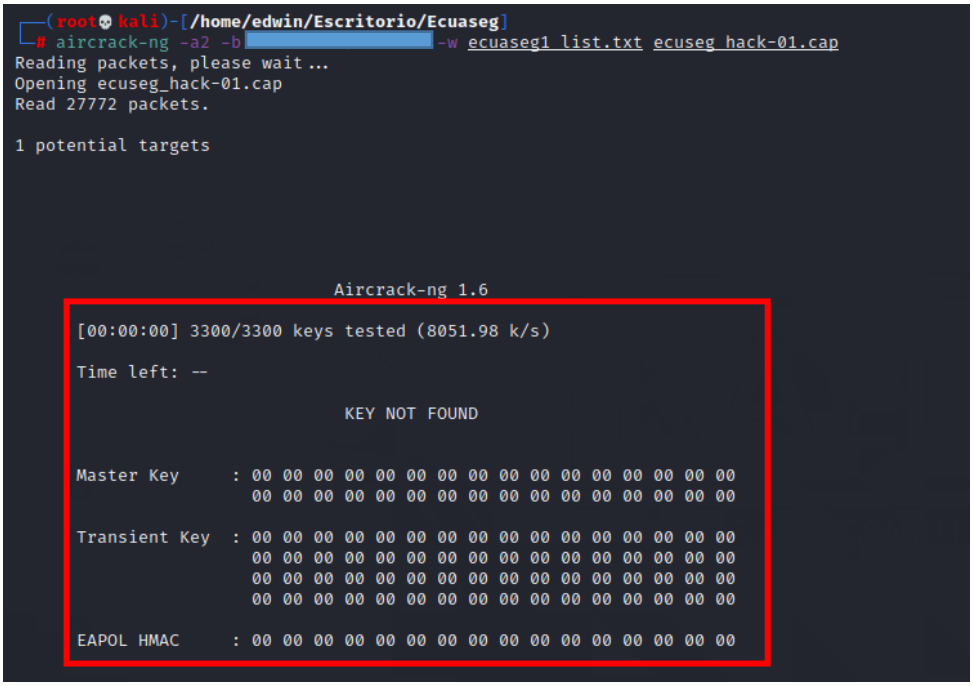


Figura 37. Cuarto Ataque con diccionario

Elaborado por el investigador

Prueba 5

Para la quinta prueba, se creó un diccionario con 11 caracteres con la palabra ECUASEG y un conjunto de símbolos y números.

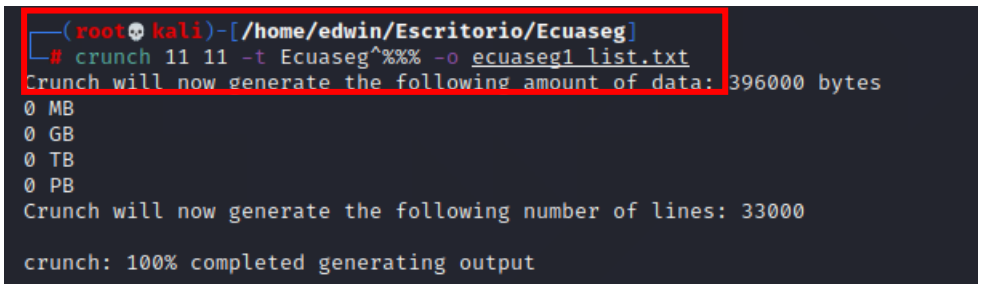


Figura 38. Creación del 5 diccionario

Elaborado por el investigador

En la quinta prueba, se utilizó un diccionario con 11 caracteres con el siguiente comando:

`-aircrack-ng -a2 -b &&:&&:&&:&&:&&:&& -w ECUASEG1_list.txt ecuseg_hack-01.cap`

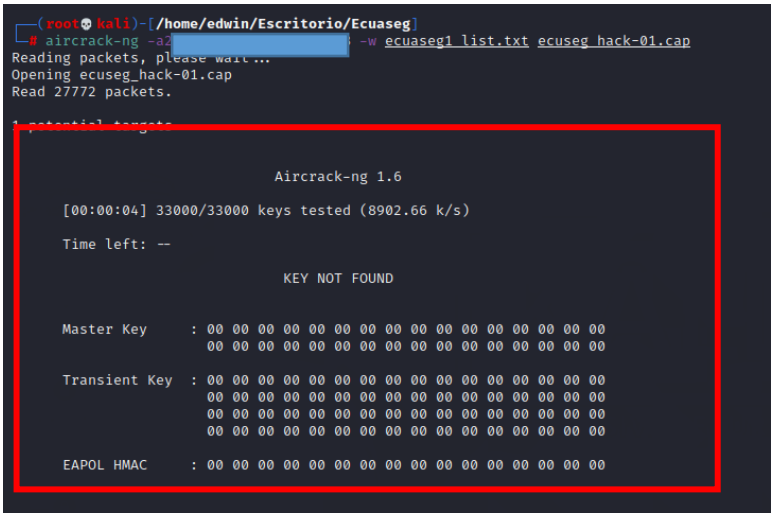


Figura 39. Quinto Ataque con diccionario

Elaborado por el investigador

Prueba 6

Para la sexta prueba, se creó un diccionario con 12 caracteres con la palabra ECUASEG y conjunto de números y símbolos.

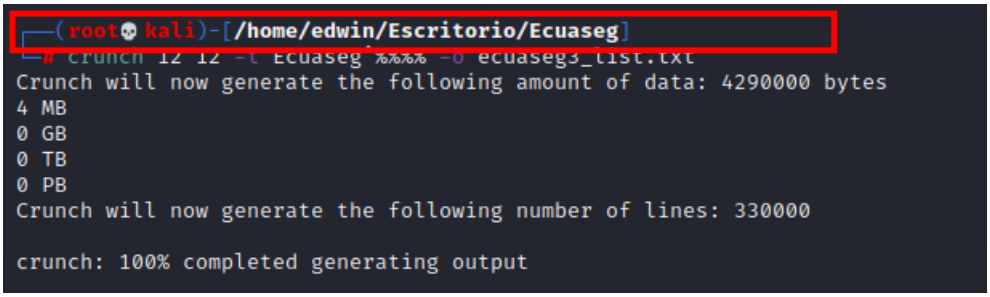


Figura 40. Creación del sexto diccionario

Elaborado por el investigador

Se utilizó un diccionario con longitud de 12 caracteres con el siguiente comando:

`-aircrack-ng -a2 -b &&:&&:&&:&&:&&:&& -w ECUASEG3_list.txt ecuseg_hack-01.cap`

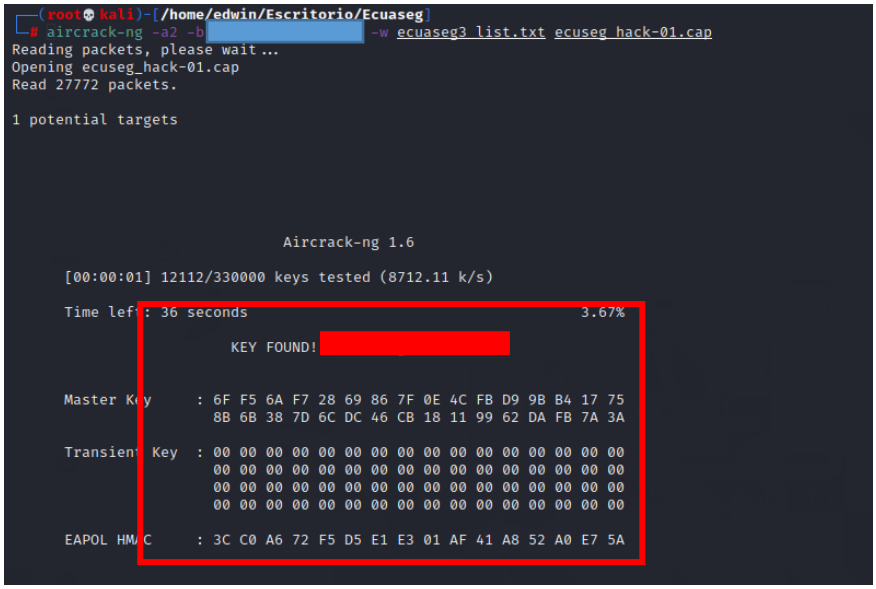


Figura 41. Sexto Ataque con diccionario

Elaborado por el investigador

En la prueba número 6, se logró capturar la contraseña de la red inalámbrica de la empresa auditada como se mostró en la figura 41, en un tiempo de 36 segundos en un diccionario con más 330000 líneas de claves posibles.

Mantener Acceso

Primero, se realizó un escaneo de los dispositivos de la empresa con la app FING.

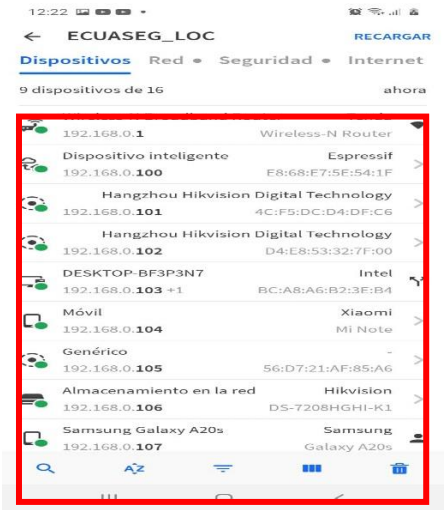


Figura 42. Dispositivos conectados a la red ECUASEG_LOG

Elaborado por el investigador

Tabla 4. Dispositivos conectados a la red ECUASEG_LOG

Dispositivo	Dirección IP
AP	192.168.0.1
DVR(DS-7208HGHI-KI)	192.168.0.106
CÁMARA (HANGZHOU HIKVISION DIGITAL TECHNOLOGY)	192.168.0.101
CÁMARA (HANGZHOU HIKVISION DIGITAL TECHNOLOGY)	192.168.0.102

Elaborado por el investigador

Una vez obtenida la información de los dispositivos, se realizó el análisis de los dispositivos conectados a la red con la herramienta Nessus, para lo cual se debe instalar previamente.

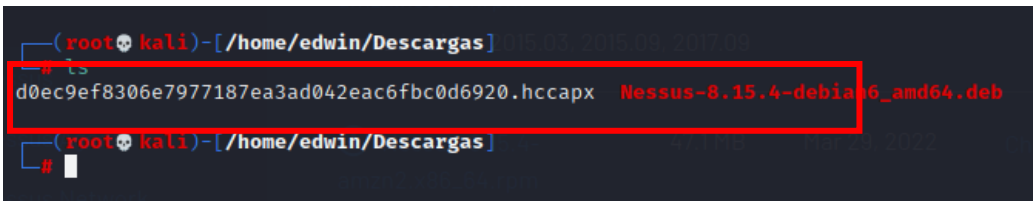


Figura 43. Archivo descargado de Nessus

Elaborado por el investigador

Después de descargarlo, se usó el comando `dpkg` para instalar Nessus

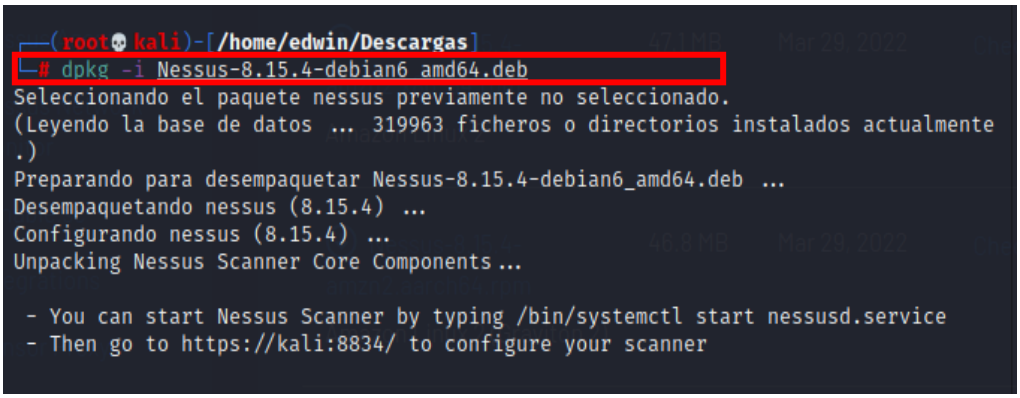


Figura 44. Instalación Nessus

Elaborado por el investigador

Para ejecutar la herramienta se utiliza el comando:

```
systemctl start nessusd.service
```

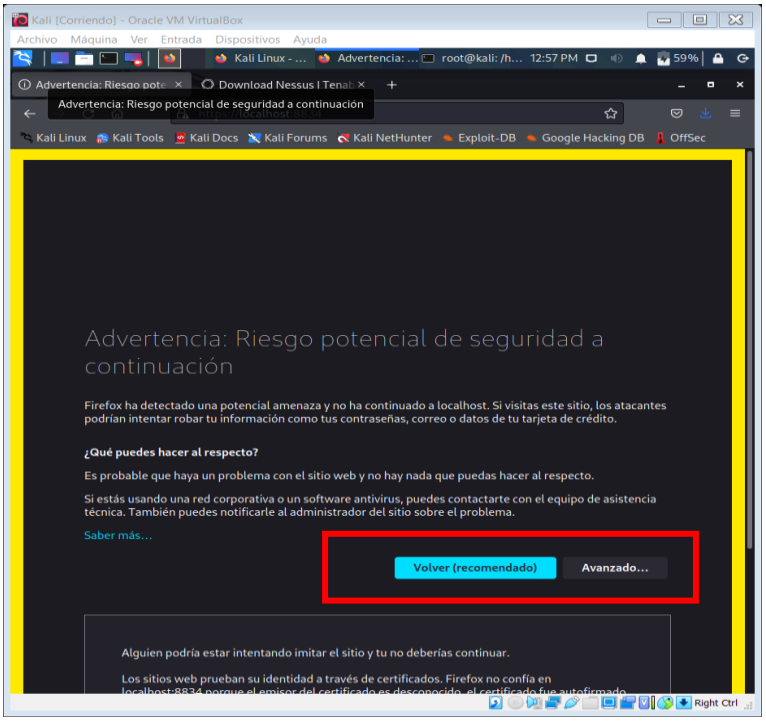


Figura 45. Configuración de herramienta Nessus

Elaborado por el investigador

En la figura 46, se realizó la selección del producto Nessus que se desea implementar. Selección “Nessus Essentials” y hacer clic en “Continuar”.

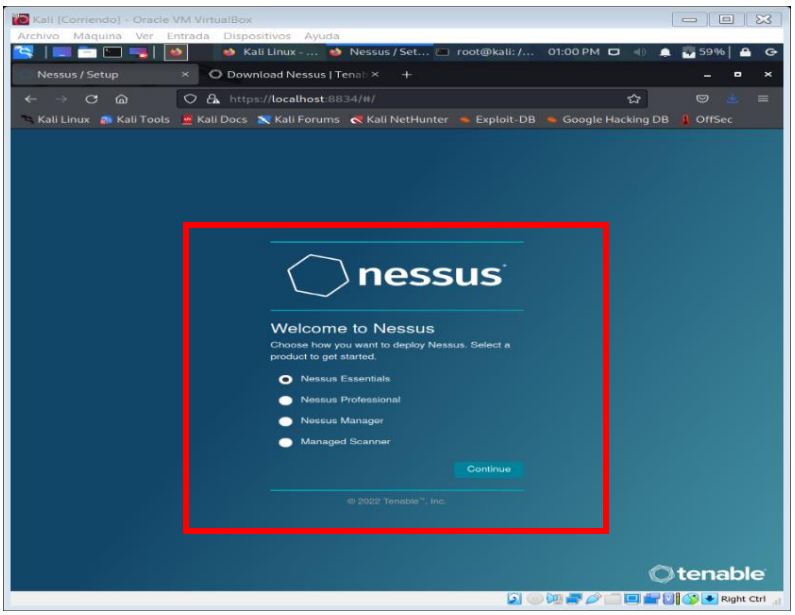


Figura 46. Configuración de la herramienta Nessus

Elaborado por el investigador

En la figura 47, se visualiza la interfaz de Nessus Essentials y se debe colocar el código de activación enviado previamente al correo electrónico. Revisar la bandeja de entrada para el código de activación. Finalmente copiar e ingresar el código y posteriormente clic en "Continuar" para avanzar acorde a las figuras 48 y 49.

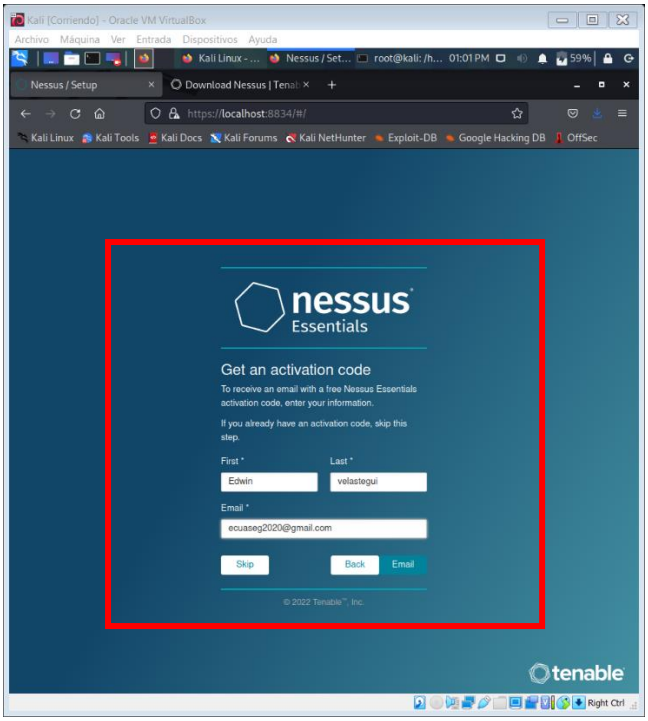


Figura 47. Configuración de la cuenta en Nessus

Elaborado por el investigador

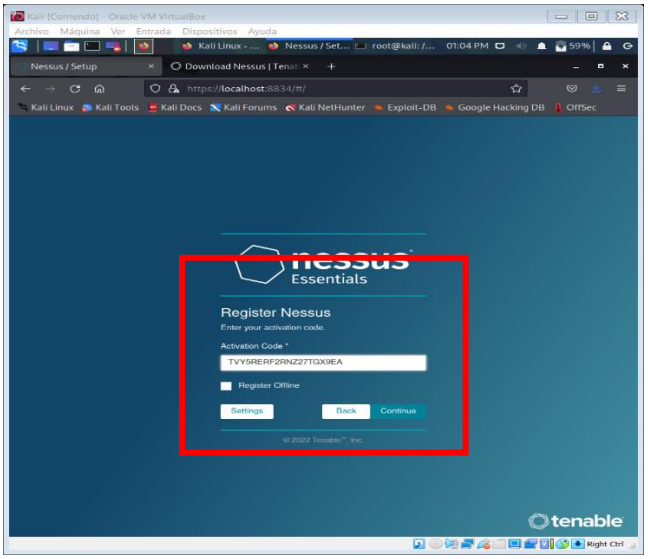


Figura 48. Ingreso de código

Elaborado por el investigador

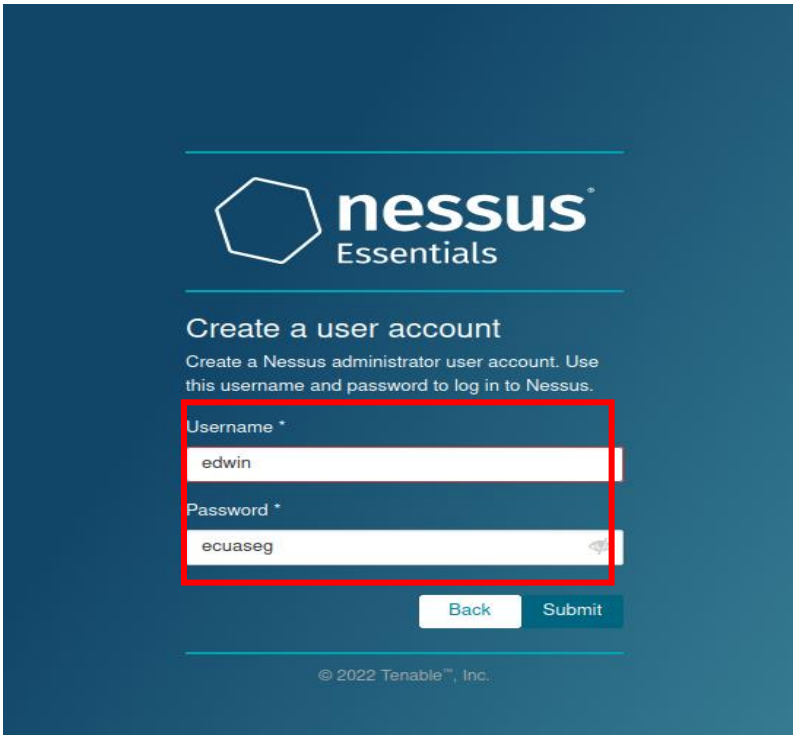


Figura 49. Configuración de usuario y contraseña

Elaborado por el investigador

Finalmente, se inicia la descarga y se obtiene la herramienta configurada

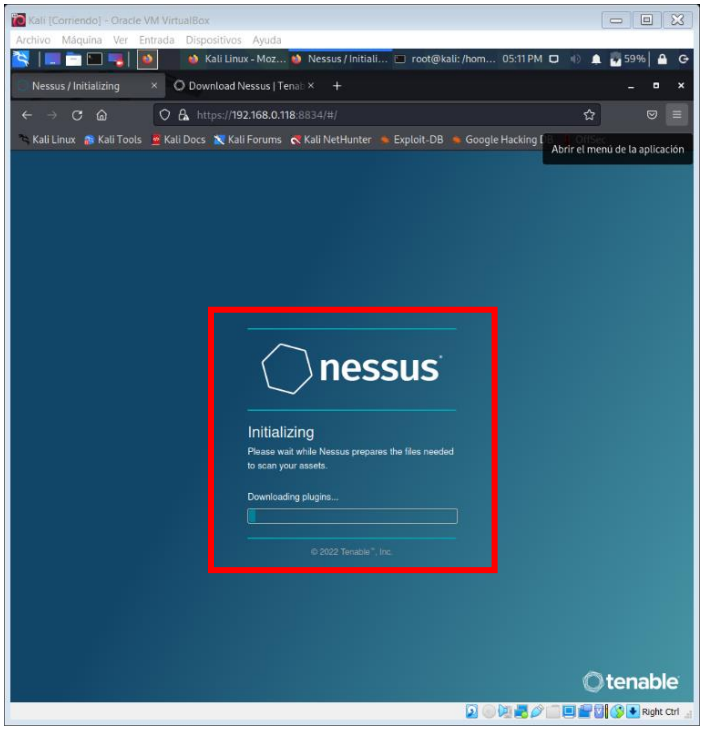


Figura 50. Configuración Final

Elaborado por el investigador

Para comenzar con el escaneo de vulnerabilidades con Nessus, se inicia sesión en Nessus en la máquina Kali Linux; en primer lugar, deberá habilitar el servicio Nessus utilizando el siguiente comando dentro de una ventana de Terminal:

```
-systemctl start nessusd.service
```

Figura 51. Inicialización de servicios

Elaborado por Autor

Una vez que el servicio se haya habilitado con éxito, abrir el navegador web en Kali Linux, e ingrese la URL https://localhost:8834 dentro de la barra de direcciones y presione ingresar.

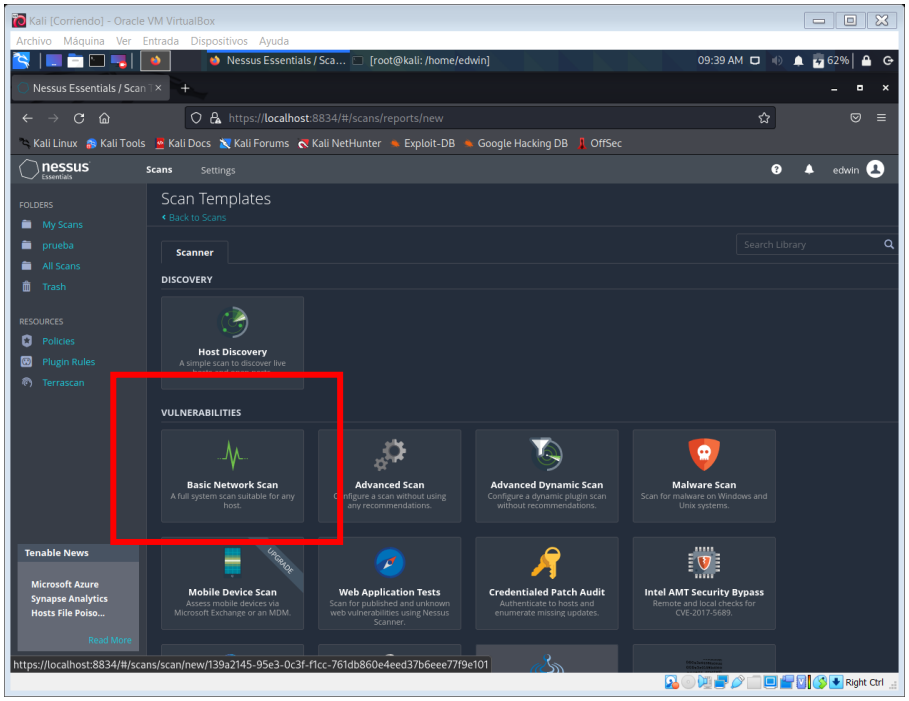


Figura 52. Ingreso a la interfaz

Elaborado por el investigador

Primero, se analizaron los dispositivos conectados a la Red de la empresa ECUASEG, se analizó la vulnerabilidad del Access Point que tiene la dirección

192.168.0.1, para iniciar el escaneo se debe rellenar la plantilla con un nombre que describa el objetivo, una IP y descripción breve del escaneo a realizar como se observa en la figura 53.

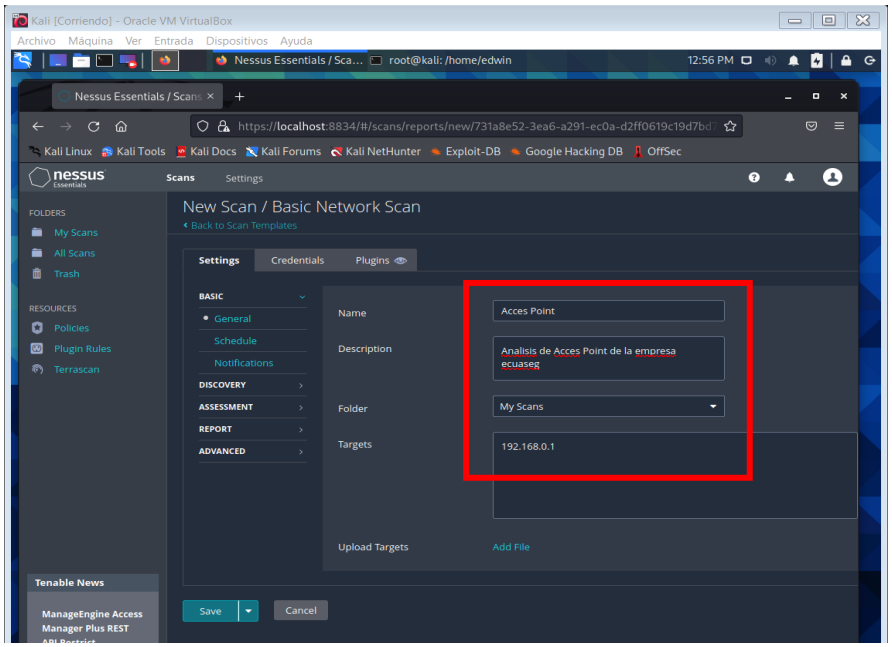


Figura 53. Creación de Escaneo en Nessus

Elaborado por el investigador

Se elige un escaneo de todos los puertos que el dispositivo tenga abierto como se observa en la figura 54.

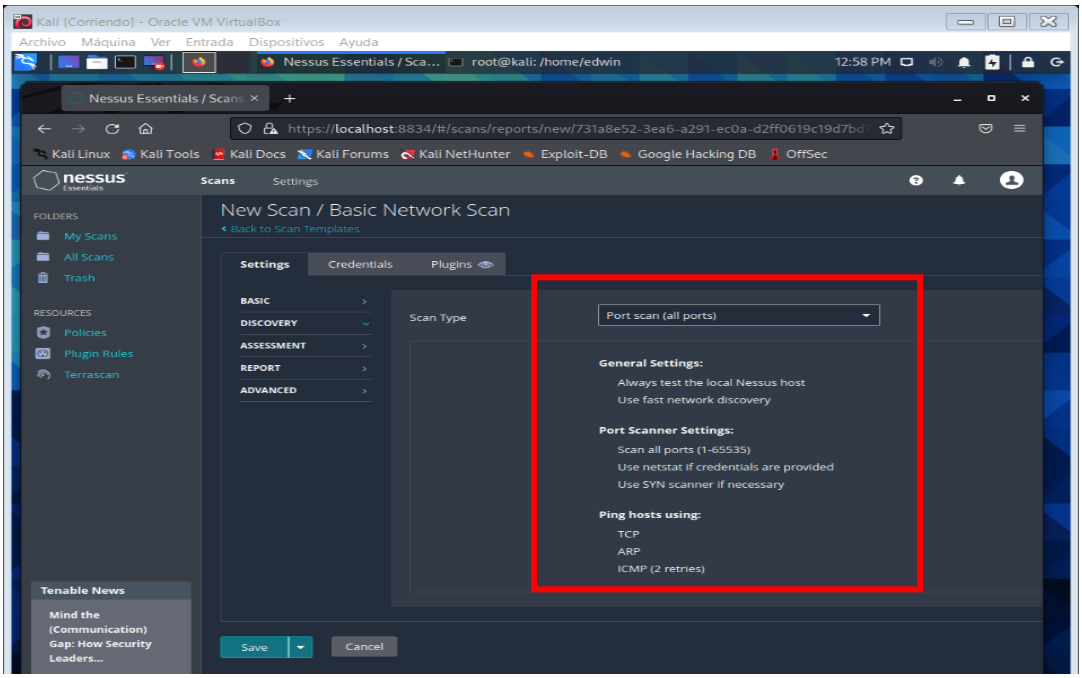


Figura 54. Tipo de Escaneo

Elaborado por el investigador

Se ejecutó el escaneo de los puertos de Access Point ECUASEG, como se visualiza en la figura 55.

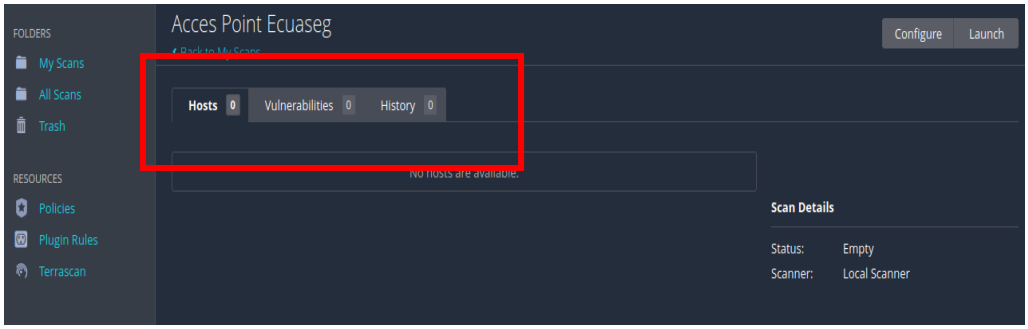


Figura 55. Inicio del Escaneo

Elaborado por el investigador

Una vez finalizado, se muestra el resultado en donde las vulnerabilidades van en forma descendente, el color rojo significa más crítico y el color azul es informativo como se observa en la figura 56.

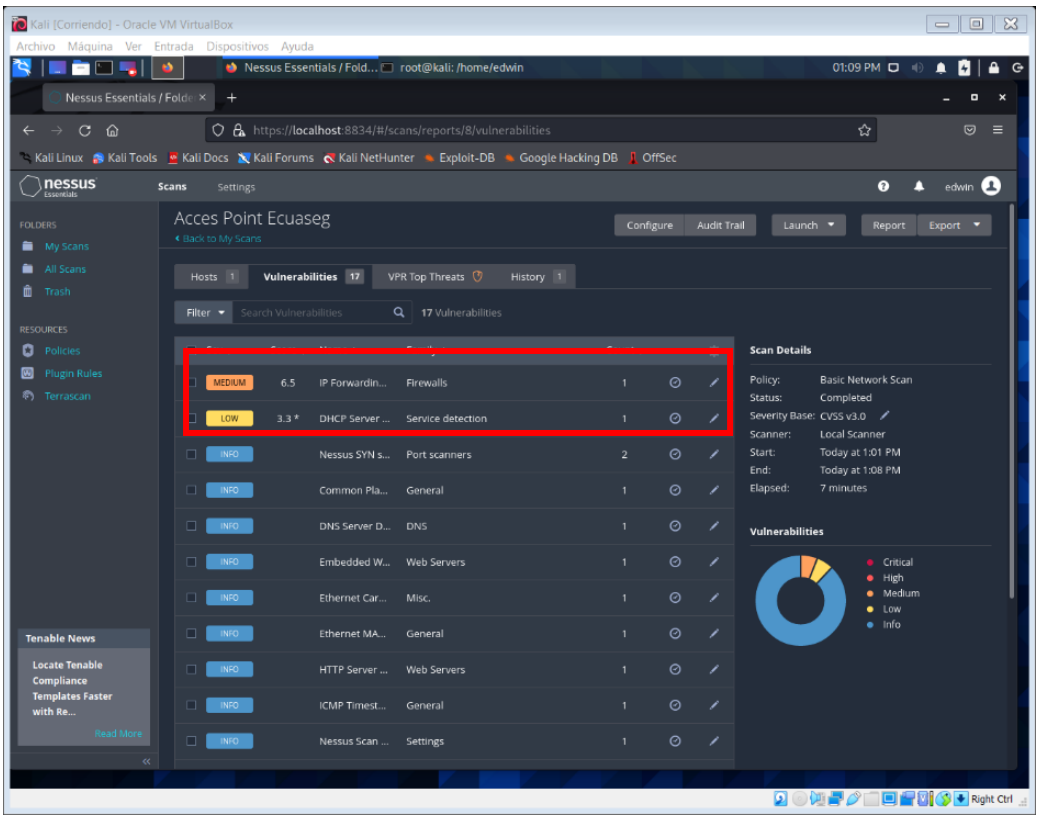


Figura 56. Resultados del Escaneo

Elaborado por el investigador

Se obtuvieron 17 resultados, de los cuales solo uno es de nivel medio el cual fue analizado para identificar el tipo de vulnerabilidad que afecta al dispositivo.

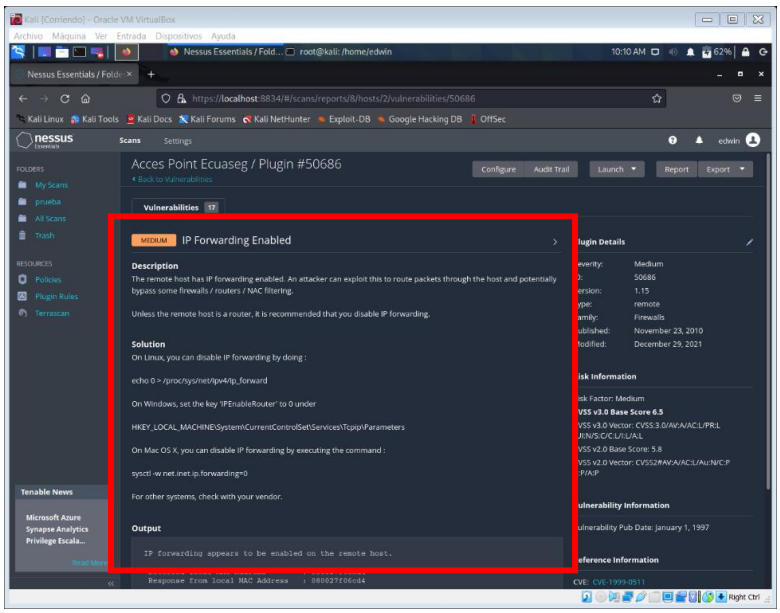


Figura 57. Descripción de la vulnerabilidad

Elaborado por el investigador

Se describe que el host remoto tiene activado el reenvío de IP. Un atacante puede explotar esto para enrutar paquetes a través del host y potencialmente eludir algunos cortafuegos/enrutadores/filtrado NAC.

El segundo análisis, se realizó a la dirección IP del DVR, para identificar que vulnerabilidades se pueden explotar en el siguiente ataque.

Se coloca el nombre del escaneo, una descripción y la dirección IP 192.168.0.106 como se muestra en la figura 57.

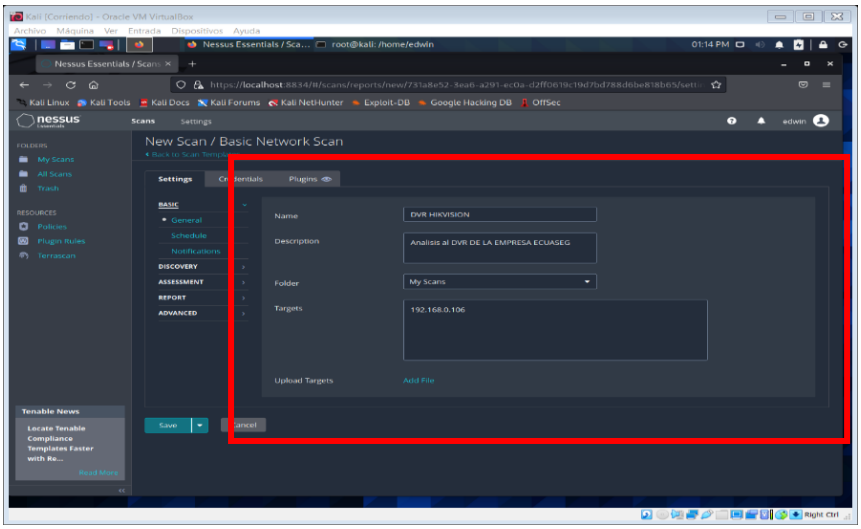


Figura 58. Creación del escaneo

Elaborado por el investigador

Seleccionar todos los puertos, para tener una amplia inspección del DVR como se muestra en la figura 59.

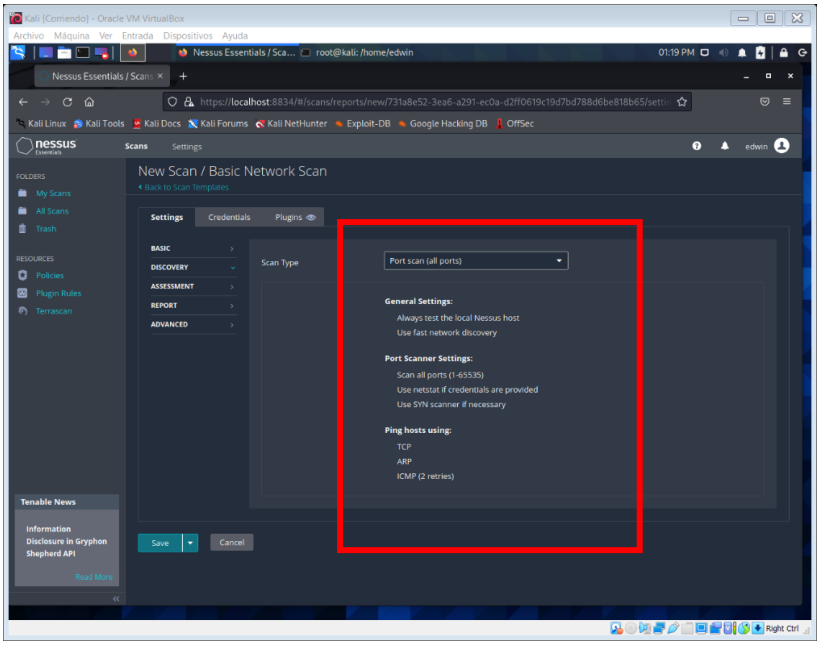


Figura 59. Selección de los puertos

Elaborado por el investigador

Iniciado el escaneo, el tiempo de espera dependerá de la cantidad de vulnerabilidades que encuentre la herramienta, como se observa en la figura 60.

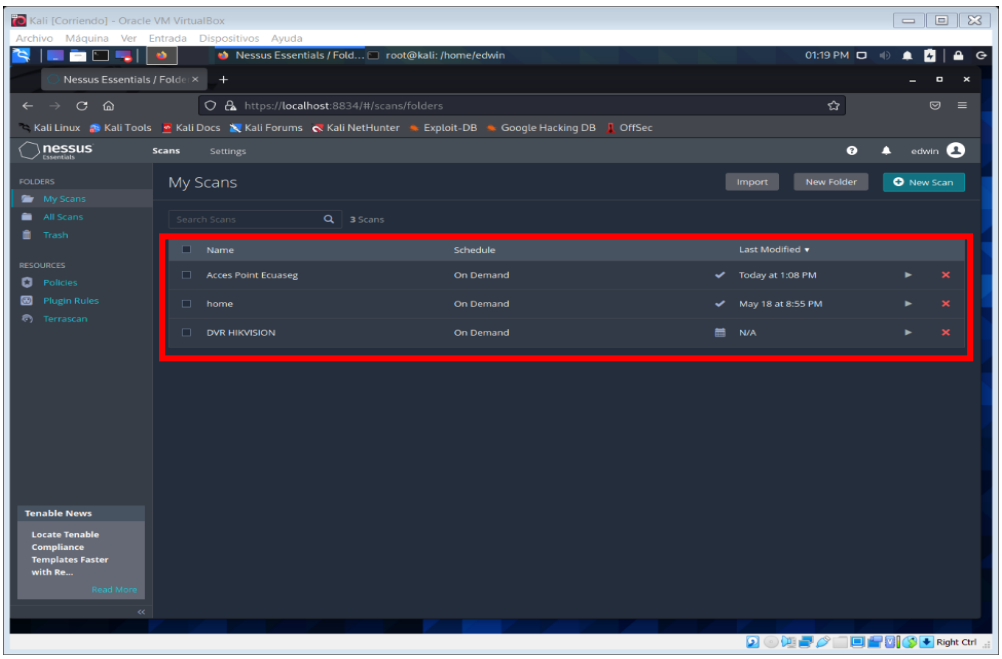


Figura 60. Inicio del escaneo

Elaborado por el investigador

En la figura 61, se identifican 12 resultados, en este caso la mayoría son de nivel leve o informativo.

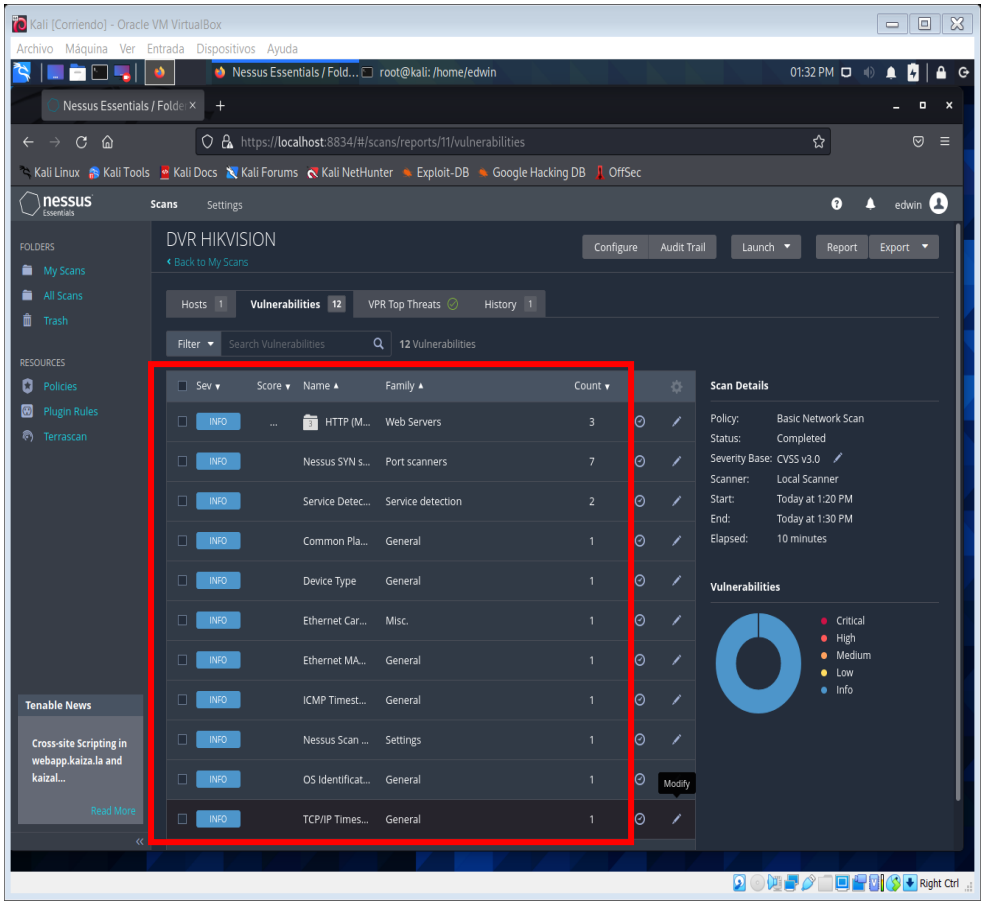


Figura 61. Resultado del escaneo

Elaborado por el investigador

Hydra

Después del análisis de las vulnerabilidades de los dispositivos más críticos conectados a la red, se procede a realizar un ataque de fuerza bruta con la herramienta Hydra. Antes de continuar con el ataque, se realizó un análisis con la herramienta Nmap para identificar los puertos abiertos del objetivo.

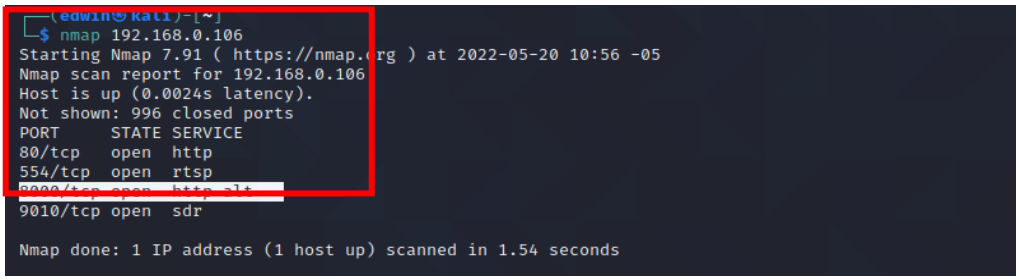


Figura 62. Análisis de puertos con Nmap

Elaborado por el investigador

Se obtuvieron los parámetros del formulario web, para acceder se debe determinar los parámetros de la página de inicio de sesión del formulario web y cómo responde el formulario a los inicios de sesión incorrectos o fallidos. Los parámetros clave a identificar son los siguientes:

- Dirección IP del sitio web
- URL

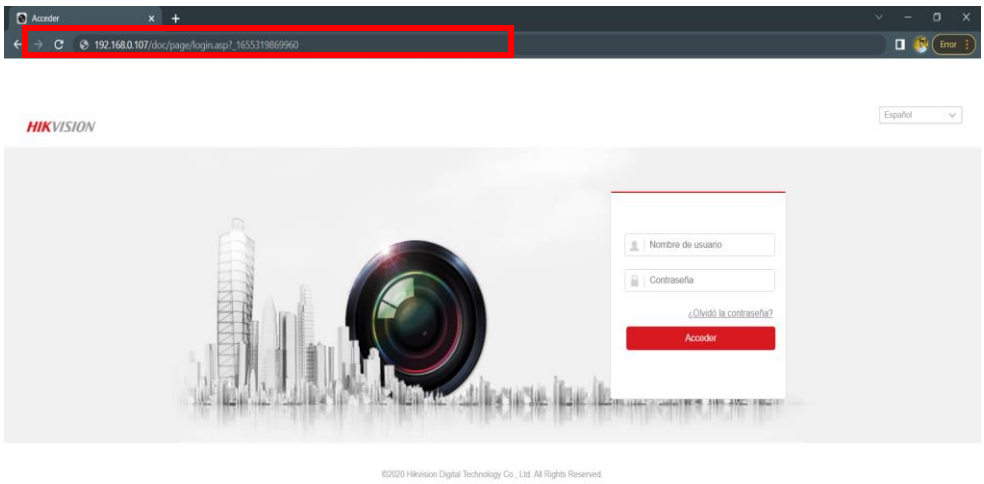


Figura 63. Interfaz del DVR

Elaborado por Autor

Se colocan los parámetros con el siguiente comando:

`-TCH Hydra; hydra -l admin -P /usr/share/wordlists/rockyou.txt 192.168.0.107 http-get /doc/page/login.asp? _1653492574781`

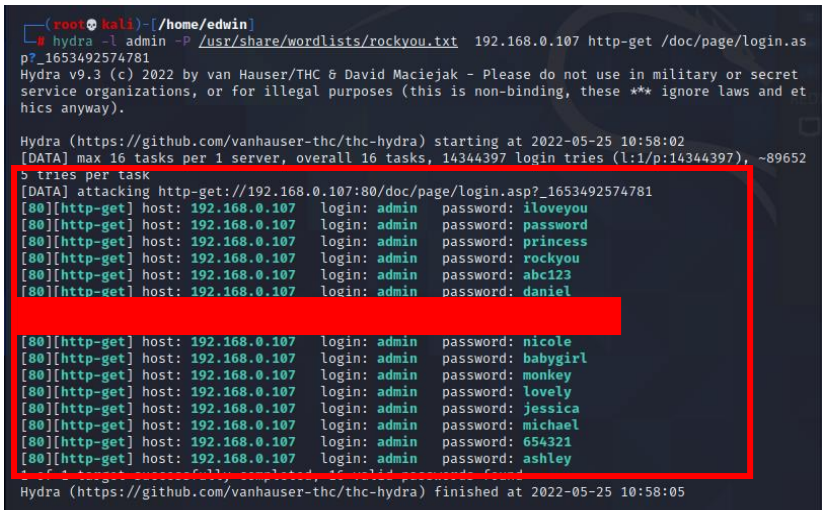


Figura 64. Ejecución de Hydra

Elaborado por el investigador

Se ingresó cada una de las claves sugeridas por la herramienta Hydra en el navegador para identificar cual es la verdadera, como se muestra en la figura 65.

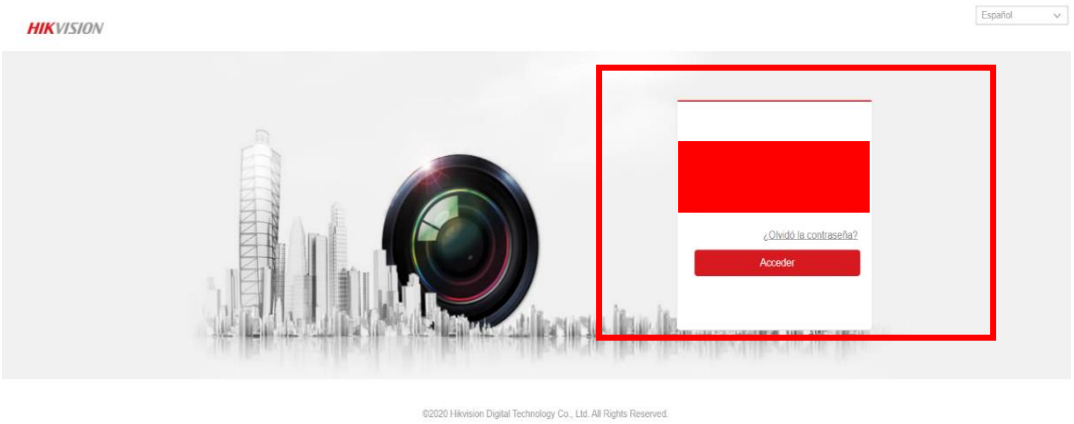


Figura 65. Ingreso al DVR

Elaborado por el investigador

Después de 7 intentos se encontró la contraseña correcta del dispositivo donde el usuario es [redacted] y la contraseña es [redacted].

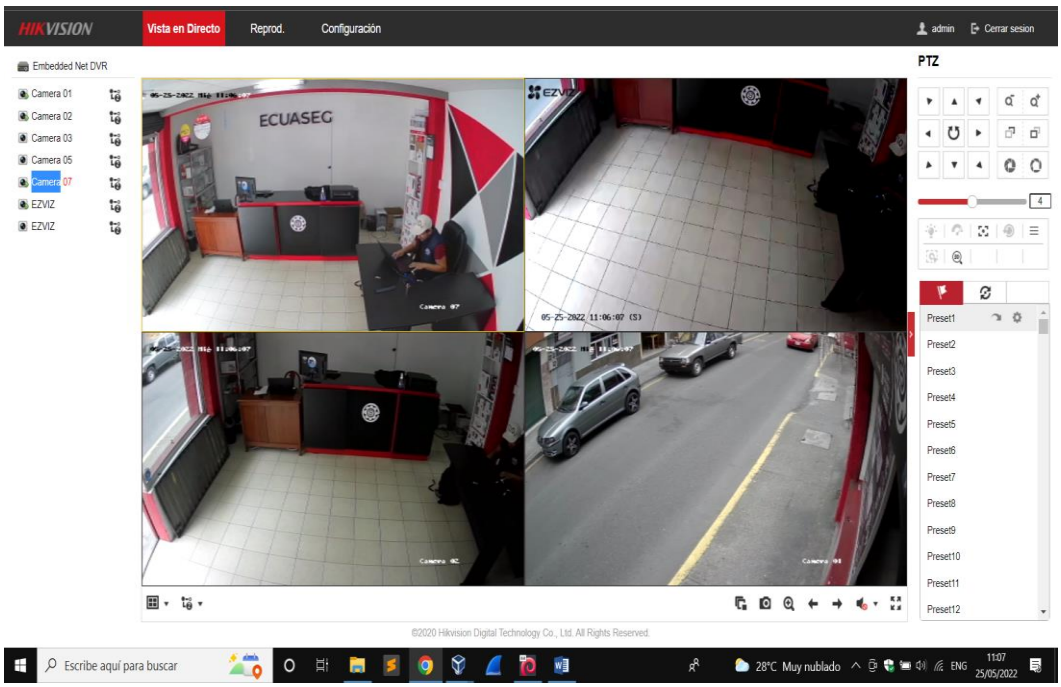


Figura 66. Visualización de las cámaras conectadas al DVR

Elaborado por el investigador

En la figura 66, se observan las cámaras conectadas al DVR y se tiene completo control de la interfaz y de los equipos.

Análisis de la configuración del DVR

Se analizó la configuración del DVR para identificar posibles vulnerabilidades, en donde se observó que el firmware no está actualizado

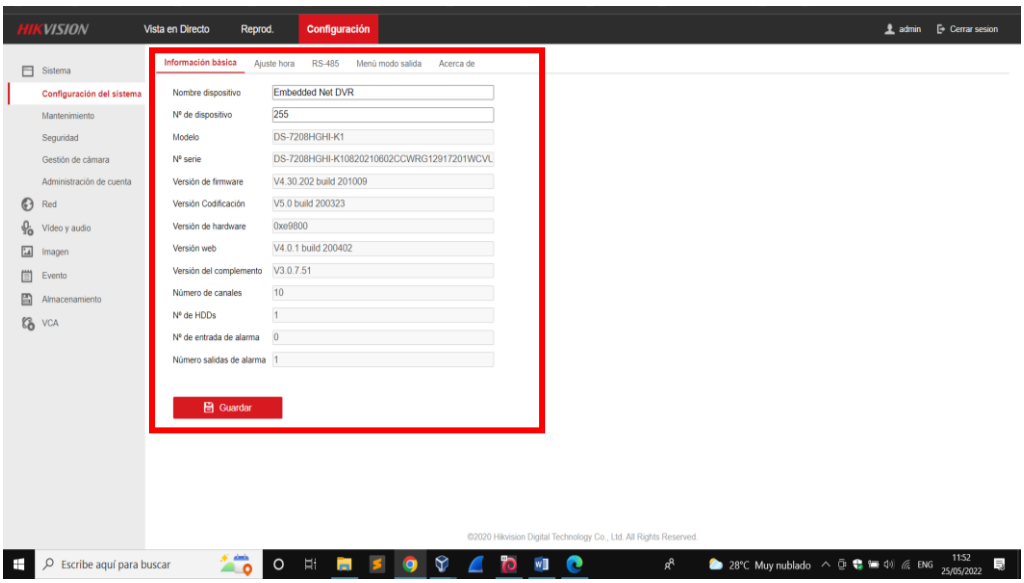


Figura 67. Configuración del DVR

Elaborado por el investigador

Para el segundo análisis, se identifica la seguridad configurada en el sistema.

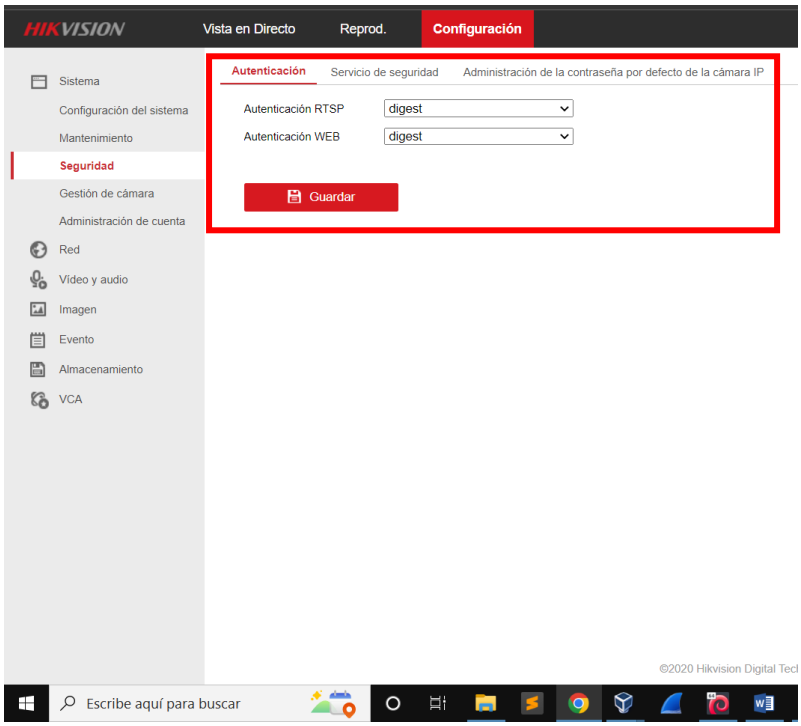


Figura 68. Configuración de la seguridad del DVR

Elaborado por el investigador

Para el tercer análisis, se identifica la configuración de la red del DVR.

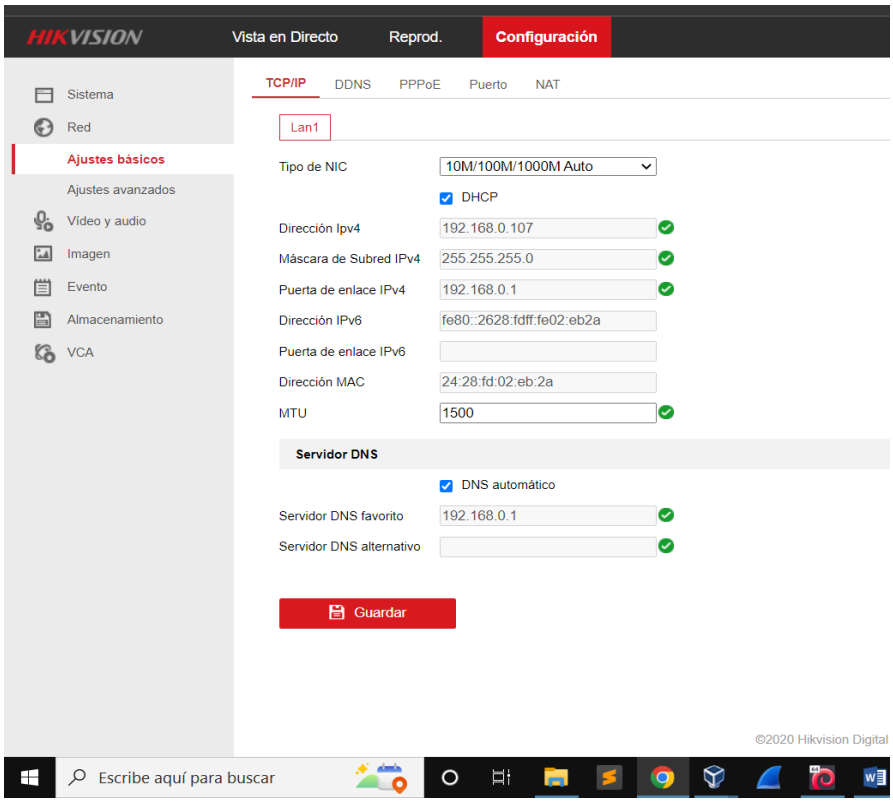


Figura 69. Configuración de la Red

Elaborado por el investigador

Mantenerse Oculto

En la siguiente fase del pentesting, se utilizó la herramienta Metasploit y la base de datos EXPLOIT DATABASE.

Metasploit

Descripción general del módulo CVE-2014-4880

Este módulo explota un desbordamiento de búfer en el código de análisis de solicitud RTSP de los dispositivos Hikvision DVR. Los dispositivos Hikvision DVR graban transmisiones de video de cámaras de vigilancia y ofrecen administración remota y reproducción de imágenes grabadas. La vulnerabilidad está presente en varios modelos/versiones de firmware, pero debido al dispositivo de prueba disponible, este módulo solo es compatible con el modelo DS-7204. [14]

Tabla 5. Exploit CVE-2014-4880

Información	**Detalles**
Nombre:	Hikvision DVR RTSP Solicitar ejecución remota de código
Módulo de inyección de comandos sin autenticar:	exploit/linux/misc/Hikvision_rtsp_bof
Código fuente:	módulos/exploits/linux/misc/Hikvision_rtsp_bof.rb
Fecha de divulgación:	2014-11-19
última modificación:	2022-01-23 15 :28:32 +0000
Arquitectura(s) admitida(s):	armle
Plataforma(s) admitida(s):	Unix
Servicio/protocolo de destino:	-
Puerto(s) de red de destino:	554

Elaborado por el investigador

Se ejecutó la herramienta exploit que se encuentra en la librería Metasploit, pero no se logró crear la sesión por lo que no es efectivo para ingresar a este DVR como se observa en la figura 70 y 71.

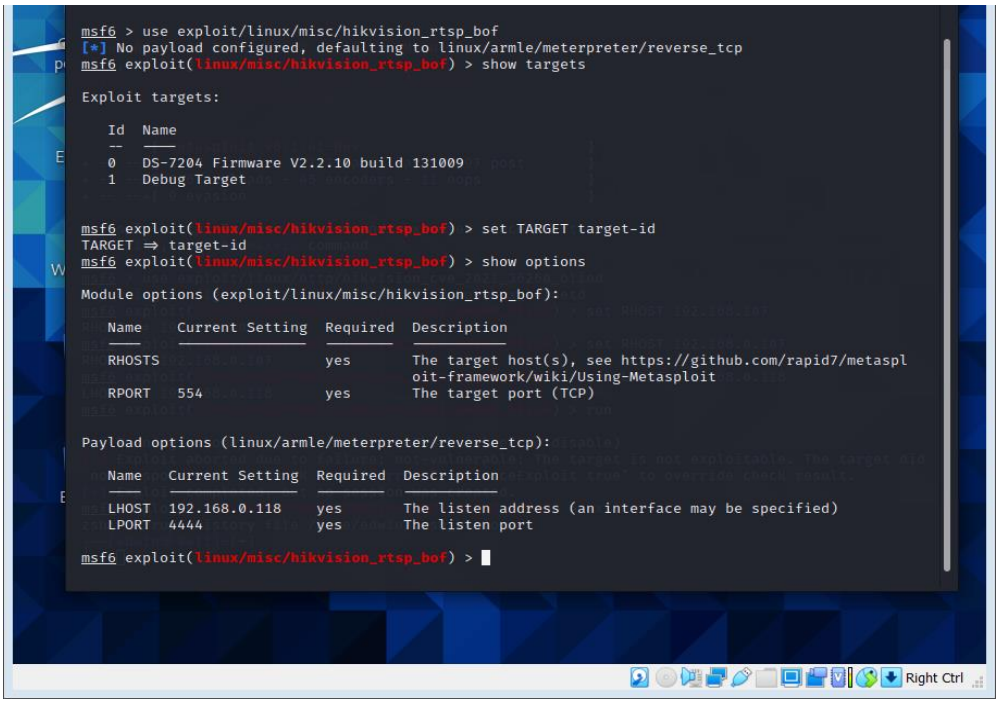


Figura 70. Configuración del Exploit

Elaborado por el investigador

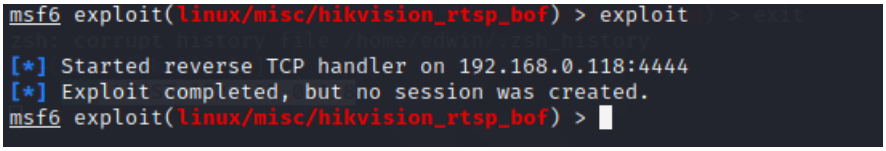


Figura 71. Ejecución del Exploit

Elaborado por el investigador

Descripción general del módulo CVE-2021-36260

El módulo ingresa un comando en una carga útil XML utilizada con una solicitud HTTP PUT enviada al /SDK/webLanguage, lo que da como resultado la ejecución del comando como root. Este módulo intenta explotar específicamente la variante ciega del ataque. El módulo se probó con éxito con un HWI-B120-D/W con el firmware V5.5.101 compilación 200408. Se probó con un DS-2CD2142FWD-I no afectado con el firmware V5.5.0 compilación 170725. [15]

Tabla 6. Exploit CVE-2021-36260

Información	**Detalles**
Nombre:	Cámara IP de Hikvision
Módulo de inyección de comandos sin autenticar:	exploit/linux/http/Hikvision_cve_2021_36260_blind
Código fuente:	módulos/exploits/linux/http/Hikvision_cve_2021_36260_blind.rb
Fecha de divulgación:	2021-09-18
última modificación:	2022-02-25 08: 32:06 +0000
Arquitectura(s) admitida(s):	cmd, armle
Plataforma(s) admitida(s):	Linux, Unix
Servicio/protocolo de destino:	http, https
Puerto(s) de red de destino:	80, 443, 3000, 8000, 8008, 8080, 8443, 8880, 8888

Elaborado por el investigador

Este módulo explota una inyección de comando no autenticada en una variedad de cámaras IP de Hikvision (CVE-2021-36260).

Verificación del exploit

Configuración del exploit con la herramienta Metasploit, mediante el siguiente código de línea:

```
-use exploit/linux/http/Hikvision_cve_2021_36260_blind
```

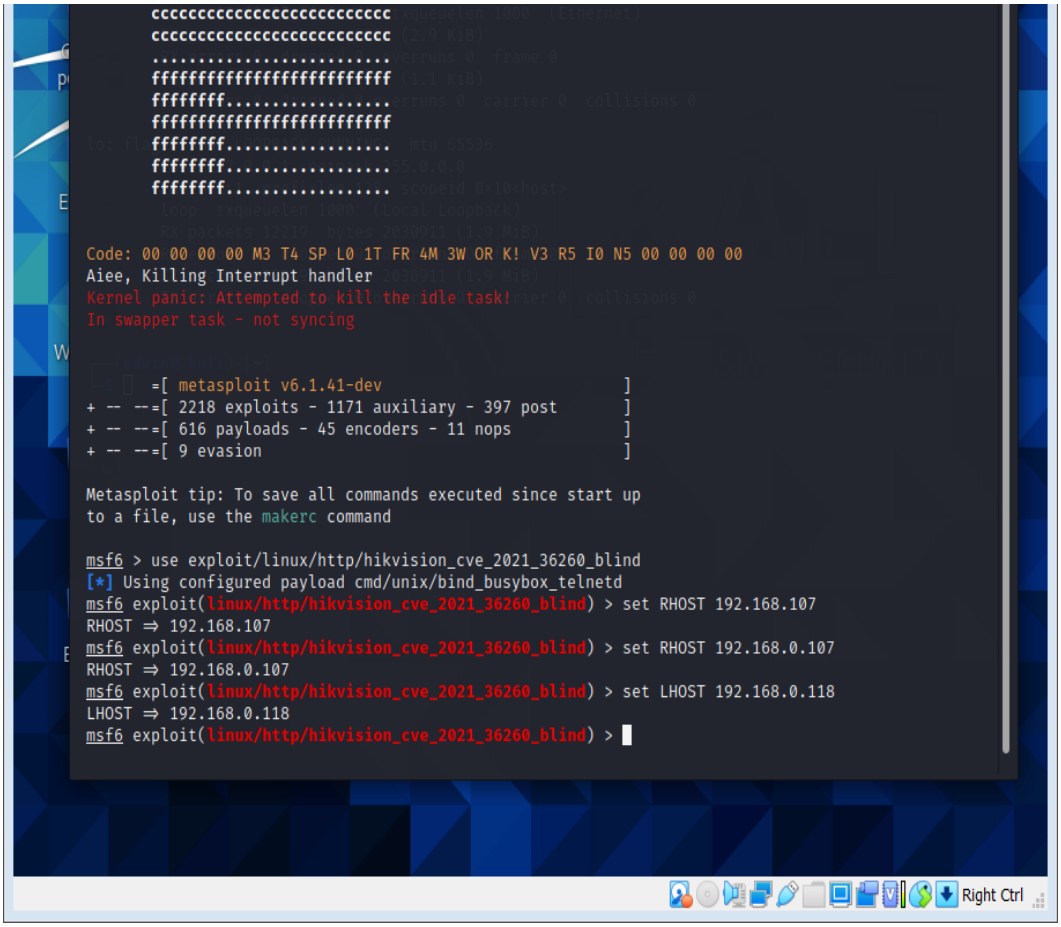


Figura 72. Exploit CVE-2021-36260

Elaborado por Autor

Como se puede observar en la figura 73, el exploit no tuvo efecto en el DVR lo que indica que tener control remoto no es posible con los exploit encontrados.

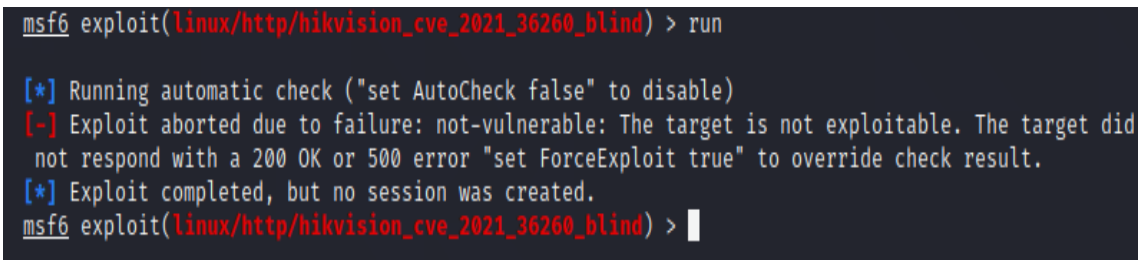


Figura 73. Resultado del Exploit

Elaborado por el investigador

Reportar o Informes

Informe Ejecutivo

El informe ejecutivo, no es para el experto en seguridad, es para el ejecutivo o director de la empresa que no tiene conocimientos o interés en los detalles técnicos del estado de seguridad de su organización, a esta persona le interesa conocer el estado general de la situación, y el cómo y en cuanto tiempo se solucionaran los problemas. [17]

Tabla 7.Informe Ejecutivo

<table>
<tr><th colspan="3">Informe Ejecutivo</th></tr>
<tr><th colspan="3">Contexto</th></tr>
<tr><th>Objetivo</th><th>Activos</th><th>Tiempo</th></tr>
<tr><td rowspan="2">Evaluar la seguridad del sistema de video vigilancia de la empresa ECUASEG.</td><td>Access Point</td><td>3 semanas</td></tr>
<tr><td>DVR</td><td>3 semanas</td></tr>
<tr><th colspan="3">Resultados</th></tr>
<tr><td colspan="3">En los ataques a Access Point, se comprometió el sistema por medio de varios ataques sistemáticos que ayudaron en conseguir acceso de la contraseña.
En los ataques realizados al DVR, se obtuvo acceso al dispositivo por medio de analizar la vulnerabilidad del dispositivo, conjuntamente con ataque de fuerza bruta y ataques con diccionarios.
Los exploit para el DVR y Cámaras IP no son efectivos por lo cual no se puedo dejar una puerta trasera abierta.</td></tr>
<tr><th colspan="3">Ranking de Riesgo</th></tr>
<tr><td>Access Point</td><td colspan="2">El nivel de riego fue muy bajo según las herramientas de análisis donde la mayoría eran informativas, pero se logró vulnerar la seguridad del dispositivo por medio de varias técnicas.</td></tr>
<tr><td>DVR</td><td colspan="2">En el caso del DVR el nivel de riesgo es muy bajo y casi todas las vulnerabilidades eran informativas, pero se</td></tr>
</table>

	logró acceder y tener control del mismo por medio de varias técnicas y análisis del dispositivo y direcciones Ip
Encuentros Generales	
Resumen de Recomendaciones	
Recomendaciones que permiten incrementar la seguridad de la red de la Empresa de ECUASEG: • En la mayoría de empresas en ecuador y Ambato no se han establecido políticas de seguridad informática con el objetivo de tener derechos, obligaciones y sanciones a los trabajadores y gerentes de la empresa deben manejar. • Se recomienda que la red del sistema de video vigilancia debe estar separado con la red que utilizan los empleados y clientes de la empresa. • Se analiza el uso de contraseñas de mayor longitud con una combinación de letras, números y símbolos especiales.	
Plan de Acción	
1. Primero se debe actualizar las versiones de firmware periódicamente para evitar dejar puertas traseras abierta a cualquier ataque	
2. Segundo se debe cambiar periódicamente la clave de la red mínimo cada 3 meses	
3. Implementación de una base datos para el control y mantenimiento de las claves DVR de la empresa y los clientes para evitar la utilización del mismo en cada dispositivo	
4. Supervisión del sistema en busca de picos de trafico	
5. Asegúrese de que las grabadoras de video y los servidores se mantengan en un área con tecnología de control de acceso estricto e incluso cámaras de vigilancia como medida adicional de protección.	
6. Realizar pruebas periódicas de vulnerabilidad para todas las cámaras de video IP y DVR.	

Elaborado por el investigador [17]

Informe Técnico

Esta sección no va dirigida a los ejecutivos, si no a los programadores, o ingenieros de sistemas, aquí es donde deberás ser tan detallado y técnico como sea posible, capturas de pantalla y detalles de las herramientas y comandos utilizados. Ver Anexo C.

Guía General

La ciberseguridad es especialmente importante para los sistemas de video seguridad, por su naturaleza, generalmente incluye datos confidenciales o privados. Muchas organizaciones utilizan cámaras de seguridad exclusivamente con fines de seguridad y protección. Las personas que se graban esperan que las imágenes de ellos se utilicen en un contexto de seguridad y se mantengan en privado. Esto es especialmente importante para los sistemas de seguridad que incluyen datos biométricos como el reconocimiento facial.

MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD

1. SEGURIDAD DE CONTRASEÑA

Los nombres de usuario y las contraseñas son uno de los puntos de entrada más vulnerables para cualquier sistema en línea. Garantizar que los inicios de sesión sean complejos y difíciles de descifrar es un cambio simple que instantáneamente hace que su red sea más segura. Los piratas informáticos irrumpirán en los sistemas ejecutando variaciones de las combinaciones de nombre de usuario/ contraseñas más utilizadas a través de aplicaciones de descifrado de contraseñas hasta que obtengan acceso, lo que le da una puerta trasera al resto del sistema.

5 cambios para mejorar la seguridad de su contraseña:

- Use una combinación de letras (mayúsculas y minúsculas), números y símbolos.
- Solo use contraseñas una vez; no utilice las mismas contraseñas para múltiples inicios de sesión.
- No comparta inicios de sesión; cada miembro del personal debe tener sus
- propios nombres de usuario y contraseñas para cada una de las aplicaciones que usa en el trabajo.
- Cambie sus contraseñas más importantes cada 90 días; la mayoría de los dispositivos y el software le recuerdan automáticamente que haga esto hoy en día.

- Configure un sistema de bloqueo de contraseña, que bloquea a alguien después de una cierta cantidad de intentos fallidos de inicio de sesión.

2. ACTUALIZACIONES DE FIRMWARE Y SOFTWARE

Una de las formas más fáciles para que los virus y el malware ingresen a su sistema es a través de las debilidades causadas por el firmware y el software desactualizados.

Algunos de los vectores de ataque más débiles para un sistema de video vigilancia son los sistemas operativos Windows y Linux. Como era de esperar, tienden a instalarse en los tipos de dispositivos que también son fáciles de piratear, como cámaras de seguridad, NVR y DVR.

Los sistemas operativos Windows tienen vulnerabilidades y, en los últimos años, Linux también ha mostrado importantes debilidades del sistema, como el error Shell Shock. Por esta razón, se realizan un seguimiento de cualquier error o vulnerabilidad y lanzan actualizaciones de parches para mejorar la seguridad del sistema. Para garantizar que su sistema sea lo más seguro posible, debe instalar regularmente las últimas actualizaciones de parches y correcciones de errores en las computadoras de sus empleados, el equipo de su sala de control y su equipo de monitoreo.

Asegúrese de que cualquier firmware que utilice esté encriptado por el fabricante, para reducir la posibilidad de que se descargue y realice ingeniería inversa; cuanto menos sepan los piratas informáticos acerca de sus sistemas, más difícil será comprometerlos. Cuando descargue y actualice el firmware, hágalo siempre desde el sitio web del fabricante.

Al igual que con el firmware, cualquier software que utilice como parte de sus procesos de seguridad debe actualizarse periódicamente. Esto es particularmente importante para el software que está instalado en su dispositivo, ya que puede ser igualmente susceptible a las vulnerabilidades. El software de administración de video que recibe datos de todos sus dispositivos remotos es un vector particularmente expuesto que debe protegerse y actualizarse con la mayor frecuencia posible.

3. SEGURIDAD DE CONEXIÓN

Las conexiones son algunos de los puntos más expuestos de su red donde pueden tener lugar la intromisión y la entrada al sistema. Idealmente, sus dispositivos de

seguridad no deben estar conectados directamente a su red principal, sino que deben configurarse en una red separada.

Hay tres elementos clave para que la seguridad de la conexión sea lo más estricta posible: cortafuegos, cifrado y puertos.

A) Instale cortafuegos fuertes

Un firewall instalado entre sus dispositivos conectados e Internet es una primera línea de defensa. La tecnología como un traductor de direcciones de red (NAT) puede reducir la cantidad de información del dispositivo que comparte públicamente. Cada dispositivo conectado tiene una dirección IP que lo hace identificable individualmente; un NAT consolidará las múltiples direcciones privadas locales en su sistema en una dirección IP para toda su organización.

Se debe configurar cortafuegos entre sus cámaras y su NVR/DVR, así como entre su NVR/DVR y su software VMS; dado que la información de video vigilancia se envía a lo largo de esta cadena de mando, es fundamental que estos datos no sean interceptados.

B) Cifrar conexiones e inicio de sesión remoto

Ciertos tipos de inicios de sesión están especialmente desactualizados y son fáciles de comprometer. Telnet y el Protocolo de transferencia de archivos (FTP) son algunos de los protocolos de conexión más antiguos que existen; a diferencia de los protocolos de conexión más modernos, no tienen medidas de seguridad incorporadas, así que evite iniciar sesión de forma remota utilizando estos métodos. También evite usar servicios de transferencia de archivos para enviar archivos confidenciales, ya que ninguno de los datos que se comparten está encriptado, lo que facilita su interceptación y visualización.

Cifrar sus conexiones con protocolos SSL/TLS a través de una conexión HTTPS hace que los datos que comparte sean difíciles de ver y decodificar. HTTPS y las redes privadas virtuales (VPN) cifran la ruta de comunicación de inicios de sesión, transferencias de archivos o conexiones de dispositivos. Al encriptar las conexiones entre dispositivos, su red tiene menos puntos débiles para aprovechar.

C) Evite los puertos predeterminados

Los puertos permiten que los dispositivos se comuniquen entre sí, creando el Internet de las cosas que necesitamos para nuestras redes de seguridad inteligentes. Hay 65.535 puertos disponibles, pero los puertos 0-1.023 son los más utilizados. Cuando se fabrican las cámaras, a menudo se programan para enviar información a través de uno de los 1024 puertos de comunicación predeterminados.

El uso de los fabricantes está disponible en Internet. Al observar los puertos predeterminados que usan los dispositivos, los piratas informáticos pueden obtener una cantidad sorprendente de información: el fabricante, el tipo de dispositivo y sus vías de comunicación. En conjunto, esta información puede proporcionar un rastro de pistas para que alguien encuentre un punto de entrada en un sistema.

Siempre que sea posible, elija dispositivos que puedan reprogramarse para usar puertos alternativos menos obvios. Dependiendo del fabricante, esta no siempre es una opción, pero si la información que se transmite desde estos dispositivos es confidencial, definitivamente vale la pena investigarla. Otra opción es impedir el acceso a todos los puertos, excepto a los que utilizan sus dispositivos. Esto les da a los piratas informáticos un obstáculo adicional que superar, lo que dificulta el ingreso a un sistema con menos puertos disponibles.

4. VIDEO SEGURO

Una combinación de todas las medidas anteriores mantendrá seguras las secuencias de video enviadas y almacenadas en su sistema de video vigilancia. Sin embargo, hay medidas adicionales que puede tomar para proteger los datos en sí, en caso de que suceda lo peor.

Los certificados digitales son una gran característica a tener en cuenta al comprar equipos como cámaras IP y DVR. Estos certificados emparejan la clave pública de un fabricante con una clave privada que almacena la información del propietario. El emparejamiento de estas dos claves crea un certificado único para ese dispositivo específico, y todos los datos transferidos o almacenados en el dispositivo se cifran con él.

Si sus dispositivos aún no tienen certificados digitales, vale la pena invertir en una solución que cifre todo el almacenamiento de video transmitido o almacenado. Esto

significa que incluso si los dispositivos o las tarjetas de almacenamiento son robados, la información que contienen es inaccesible para el público. Además de las conexiones seguras que cubrimos en la sección anterior, también debe asegurarse de que cualquier comando o configuración a sus cámaras se transmita de forma segura, utilizando los mismos canales encriptados.

También debe asegurarse de que estos dispositivos sean físicamente difíciles de acceder. Mantenga todos los dispositivos de almacenamiento de video en lugares seguros a los que solo puedan acceder los miembros aprobados del personal, para evitar la manipulación física del equipo o el robo. También grabe video en dispositivos de respaldo, o guarde el metraje en la nube, para evitar perder el metraje como resultado de un robo.

5. ACCESO DE EMPLEADOS AUTORIZADOS

Limitar el acceso de los usuarios

Solo permita que los empleados accedan a los dispositivos, plataformas y software que necesitan para realizar su trabajo. Esto significa proporcionar a cada miembro del personal detalles de inicio de sesión individuales (consulte el capítulo anterior sobre Seguridad de contraseña para obtener más detalles) y asegurarse de que tengan el nivel de acceso adecuado.

Rastree el dispositivo y el acceso a la plataforma

Asegúrese de que cada dispositivo y/o plataforma requiera pasos de autorización y autenticación; esto le da un seguimiento de cada empleado que ha accedido a su red. En el caso de una infracción, esto permite a los profesionales forenses de TI identificar si alguien tuvo acceso no autorizado a su red, ya sea al comprometer las credenciales de inicio de sesión de un empleado o el propio dispositivo.

4. Presupuesto

Tabla 8. Costos del proyecto

ANEXO 1: ESTRUCTURAS OCUPACIONALES - SALARIOS MÍNIMOS SECTORIALES Y TARIFAS
COMISIÓN SECTORIAL No. 12 "TECNOLOGÍA: HARDWARE Y SOFTWARE (INCLUYE TIC'S)"

RAMAS DE ACTIVIDAD ECONÓMICA:
1.- INFORMÁTICA Y ACTIVIDADES CONEXAS
2.- TÉCNICOS EN TELECOMUNICACIONES Y COMPUTACIÓN (TÉCNICOS EN PROGRAMACIÓN Y SOFTWARE-TÉCNICOS EN HARDWARE)
3.- OTROS SERVICIOS RELACIONADOS CON TECNOLOGÍA: HARDWARE Y SOFTWARE (INCLUYE TIC´S)

CARGO / ACTIVIDAD	ESTRUCTURA OCUPACIONAL	COMENTARIOS / DETALLES DEL CARGO O ACTIVIDAD	CÓDIGO IESS	SALARIO MÍNIMO SECTORIAL 2022
DIRECTOR DE TELECOMUNICACIONES / JEFE DE ÁREA	A1		1209642000004	458,79
SUPERVISOR GENERAL DE TELECOMUNICACIONES	B1		1209642000005	458,15
SUPERVISOR DE SISTEMAS, DESARROLLO, TECNOLOGÍA Y PROYECTOS	B1		1209642000006	458,15
ARQUITECTO Y USABILIDAD DE SOFTWARE	B1		1209642000007	458,15
SUPERVISOR DE DISEÑO DE SOFTWARE	B2		1209642000008	457,52
ADMINISTRADOR DE BASE DE DATOS	B2		1209642000009	457,52
INGENIERO ELECTRÓNICO ESPECIALISTA EN MANTENIMIENTO	B2		1220030000001	457,52
ANALISTA DE INVESTIGACIÓN Y DESARROLLO DE HARDWARE Y SOFTWARE	B2		1220000000001	457,52
ANALISTA/CONTROLLER DE CALIDAD DE SOFTWARE	B2		1220000000002	457,52
ESPECIALISTA DE TELECOMUNICACIONES	B3		1209642000010	456,88
SUPERVISOR DE PLATAFORMAS / EQUIPO DE VOZ Y DATOS	B3		1209642000011	456,88
TÉCNICO OPERADOR DE RADAR	B3		1209642000014	456,88
SUPERVISOR DE PLANTA EXTERNA / SEGURIDAD ELECTRÓNICA / CABLEADO ESTRUCTURADO	B3		1230000000003	456,88
PROGRAMADOR EN TELECOMUNICACIONES	C1		1209642000016	456,25
ANALISTA DE SOFTWARE	C1		1209642000017	456,25
TESTER DE SOFTWARE	C1		1209642000018	456,25
PROGRAMADOR Y DISEÑADOR MULTIMEDIA/WEB	C1		1209642000019	456,25
TÉCNICO EN MANTENIMIENTO DE SERVIDORES	C1		1209642000020	456,25
TÉCNICO INSTALADOR DE SERVICIOS AGREGADOS	C1		1209642000022	456,25
TÉCNICO DE FIBRA ÓPTICA/ COBRE / EMPALMADOR	C1		1209642000024	456,25
ANALISTA DE REDES	C1		1210000000004	456,25
ANALISTA DE SISTEMAS / TELECOMUNICACIONES	C1		1210000000005	456,25
ESPECIALISTA FUNCIONAL	C1	INCLUYE: IMPLEMENTADOR DE SOLUCIONES (SOFTWARE ESPECIALIZADO)	1210000000006	456,25
PROGRAMADOR SEMI SENIOR DE SOFTWARE	C1		1210000000007	456,25
TÉCNICO DE REDES DE DATOS	C2		1209642000015	454,54

Figura 74. Salario Mínimo Sectorial del 2022 [17]

$$\text{Tarifa por hora}=\frac{Ingreso}{Horas}=\frac{452.52}{40}=14{,}14\ por\ hora$$

Tabla 9. Presupuesto

Descripción	Cantidad	Precio Unitario ($)	Precio Total ($)
Internet	4 meses	30,00	120,00
Computadora con Software de análisis y monitoreo	1	900,00	900,00

Materiales de oficina	1	30,00	30,00
Impresiones	1	50,00	50,00
Transporte	1	30,00	30,00
Tarifa por hora	4 meses	452,52	1810,08
Subtotal			2940,08
Imprevistos (15%)			174,00
Total			1334,00

CAPÍTULO IV

CONCLUSIONES Y RECOMENDACIONES

4.1. Conclusiones

- En esta investigación, se probó un DVR de la marca Hikvision y se identificaron muchos puntos de vulnerabilidad, por ejemplo, se podía acceder abiertamente al punto de entrada del sistema de cámaras a través del Explorador; la contraseña del sistema se descifró fácilmente con las herramientas Hydra y Crunch. Para proteger el ingreso al DVR y evitar el control de las cámaras IP, es importante tener una estrategia de ciberseguridad que cubra todos los componentes del sistema y que incluya la planificación, diseño, implementación y pentesting, porque un sistema es vulnerable a los ataques, especialmente cuando está conectado a Internet.
- La herramienta airmon-ng, permitió realizar un ataque remoto a la infraestructura de la empresa para hacer un análisis de la red WiFi y de los dispositivos conectados identificando su dirección MAC, se realizó un ataque de denegación de servicio específico a los dispositivos conectados, con el fin de obtener el mensaje de 4 vías que contiene la clave encriptada, consiguiéndose al cuarto intento por medio de la dirección MAC de la computadora de la oficina conectada a WiFi, posteriormente fue descifrada por medio de un ataque de fuerza bruta a través de Nessus, que conjuntamente con un ataque de diccionario se logró el acceso a la red, después de 6 intentos con diccionarios diferentes, elaborados con la herramienta crunch y con un tamaño final de muestras de 333000 líneas, con un tiempo de ejecución del ataque, de una hora.
- Con la herramienta Hydra y después de un análisis de los puertos abiertos con la herramienta Nmap, se pudo realizar un ataque interno a la interfaz del DVR por el puerto 80, demostrando la vulnerabilidad del dispositivo a ataques de fuerza bruta utilizando el diccionario yourock que permitió obtener la clave después de 6 intentos.

- Metasploit fue elegido para desarrollar y ejecutar código de explotación contra el DVR. Los resultados mostraron que la computadora atacante no pudo establecer conexión con la dirección IP 192.168.0.107 en el puerto 4444. También se probó en los puertos 80, 443, 3000, 8000, 8008, 8080, 8443, 8880, 8888, obteniendo los mismos resultados.

4.2. Recomendaciones

- Se recomienda mantener el SSID de la red oculta y habilitar el cifrado de imagen en los dispositivos tanto de DVR, NVR y cámaras IP, para evitar robos de información, suplantación de identidad por medio de Ataques Man in The Middle.
- Se recomienda las herramientas Wireshark y Nessus para monitorear y analizar la infraestructura de la empresa para determinar en tiempo real posibles actividades maliciosas. Además de ello, estas herramientas pueden utilizarse en diferentes sistemas operativos debido a su fácil instalación y ejecución de análisis.
- Se recomienda revisar cuidadosamente las configuraciones de las cámaras, enrutadores, terminales y DVR. Por ejemplo, las contraseñas débiles o predeterminadas deben cambiarse periódicamente, reemplazar los puertos de acceso comunes como el 80 y 8000 a puertos poco utilizados, deshabilitar servicios en la nube, y, si es posible, deben usarse contraseñas diferentes entre dispositivos. Además, las API y otras características similares deben desactivarse si no son necesarias.
- Se recomienda al propietario de la infraestructura tecnológica, asegurarse de que el firmware de cada dispositivo, esté actualizado a su última versión para evitar la explotación de los mismos por ataque remotos.
- Se recomienda restringir el acceso físico a los activos del sistema. Si es posible, el cableado no debe pasar por áreas públicas, todo el equipo de red debe protegerse con candado y llave, y el acceso al sistema debe administrarse, registrarse y monitorearse

5. Bibliografía

[1] B. C. Z. Tian, Evaluating IP surveillance camera vulnerabilities, Western Australia: Auckland University of Technology, 2017.

[2] T. A. Reem Alshalawi, Forensic Tool for Wireless Surveillance Camera, Reino de Arabia Saudita: Universidad Umm Al-Qura, 2017.

[3] N. K. Y. M. A. S. y. Y. Elovici, The Security of IP-Based Video Surveillance Systems, Atlanta: College of Computing, Georgia Institute of Technology , 2020.

[4] B. C. I. ESTEFANÍA, APLICACIÓN DE HACKING ÉTICO PARA LA DETERMINACIÓN DE AMENAZAS, RIESGOS Y VULNERABILIDADES EN LA RED DE LA UNIVERSIDAD ESTATAL DEL SUR DE MANABÍ, JIPIJAPA – MANABÍ – ECUADOR: UNIVERSIDAD ESTATAL DEL SUR DE MANABÍ, 2020.

[5] B. C. Z. Tian, Evaluating IP surveillance camera vulnerabilities, Western : Edith Cowan University, 2017.

[6] Y. Mirsky, The Security of IP-Based Video Surveillance Systems, Atlanta: Sensors, 2020.

[7] J. A. Sava, «Statista,» Statista, 25 01 2022. [En línea]. Available: https://www.statista.com/topics/7126/cybersecurity-in-latin-america/#topicHeader__wrapper.

[8] F. Velásquez, «thesecuritydistillery,» https://thesecuritydistillery.org/, 9 08 2019. [En línea]. Available: https://thesecuritydistillery.org/all-articles/cybercrime-in-ecuador-an-asymmetrical-threat.

[9] Ethical Hacking - Learn Penetration Testing, Cybersecurity with Advanced Ethical Hacking Techniques and Methods, Joe Grant, 2020.

[10] G. D. Singh, Learn Kali Linux 2019, Birmingham: Packt, 2019.

[11] N. I. o. S. a. T. (NIST), «vd.nist.gov,» 16 05 2019. [En línea]. Available: https://nvd.nist.gov/vuln/detail/CVE-2019-0708. [Último acceso: 2022 06 28].

[12] N. V. DATABASE, 12 03 2020. [En línea]. Available: https://nvd.nist.gov/vuln/detail/CVE-2020-0796. [Último acceso: 2022 06 28].

[13] Microsoft, «docs.microsoft.com,» 12 02 2019. [En línea]. Available: https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2015/ms15-034. [Último acceso: 28 06 2022].

[14] K. Astudillo, HACKING ÉTICO 101, Karina Astudillo B, 2013.

[15] Vigilante_IP, «https://www.infosecmatter.com/,» infosecmatter, 25 02 2021. [En línea]. Available: https://www.infosecmatter.com/metasploit-module-library/?mm=exploit/linux/http/Hikvision_cve_2021_36260_blind. [Último acceso: 10 06 2022].

[16] F. J. A. Feijóo, LOS ATAQUES INFORMÁTICOS Y SU INCIDENCIA EN LA SEGURIDAD DE SERVIDORES CON SISTEMA OPERATIVO LINUX DE ENTIDADES DE GOBIERNO LOCAL, Ambato: Universidad Tecnica de Ambato, 2019.

[17] A. I. R. Buenaño, HACKING ÉTICO PARA ANALIZAR Y EVALUAR LA SEGURIDAD INFORMÁTICA EN LA INFRAESTRUCTURA DE LA EMPRESA PLASTICAUCHO

INDUSTRIAL S.A, Ambato: Universidad Tecnica de Ambato, 2018.

[18] L. V. V. Constante, HACKING ÉTICO EN DISPOSITIVOS PLC DE CONTROL INDUSTRIAL CONECTADOS A RED, Ambato: Universidad Tecnica de Ambato, 2017.

[19] P. G. Salazar, Hacker's WhiteBook, 2019.

[20] C. P. Q. García, PROCEDIMIENTO DE GESTIÓN PARA CIBERSEGURIDAD EN LA INFRAESTRUCTURA TECNOLÓGICA DEL SECTOR FINANCIERO SEGMENTO 1 REGULADO POR LA SUPERINTENDENCIA DE ECONOMÍA POPULAR Y SOLIDARIA (SEPS) EN EL CANTÓN AMBATO–ECUADOR, Ambato: Universidad Tecnica de Ambato, 2021.

[21] J. F. E. Miranda, POLÍTICAS DE SEGURIDAD INFORMÁTICA Y LA VULNERABILIDAD DE LOS ENTORNOS WEB DE LA EMPRESA TURBOTECH DURANTE EL AÑO 2010, Ambato : Universidad Tecnica de Ambato, 2011.

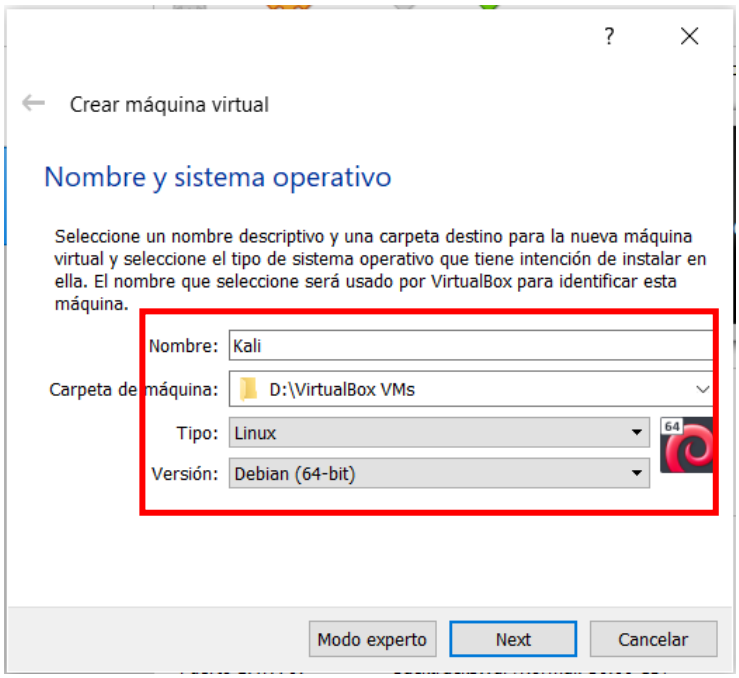
[22] A. A. P. Caluña, APLICACIÓN DE HACKING ETICO PARA LA DETERMINACIÓN DE VULNERABILIDADES DE ACCESO A REDES INALÁMBRICAS WIFI, Riobamba: ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO, 2011.

Anexos

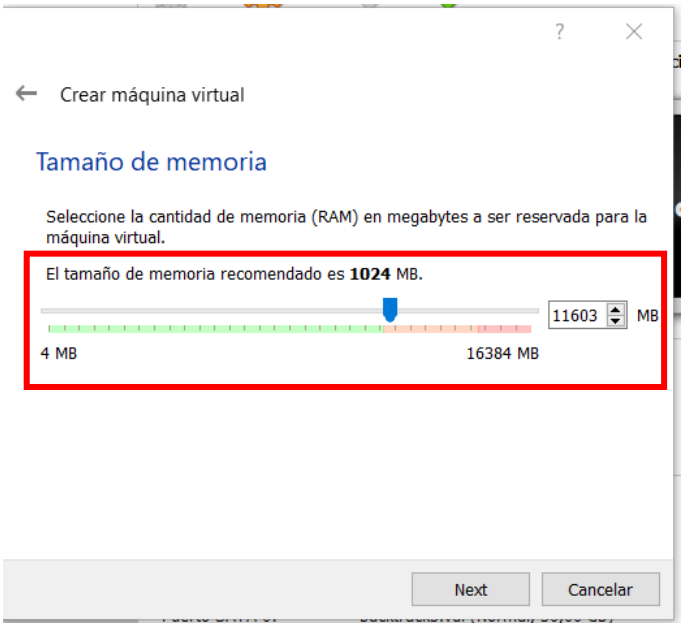
Anexo A: Configuración de Virtual box

Ir awww.virtualbox.org, luego navegue hasta el Descargas del sitio web y elija su tipo de plataforma según su sistema operativo actual:

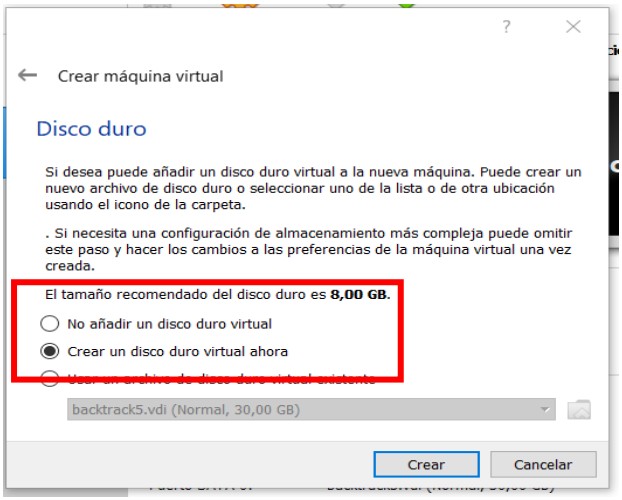
Anexo B instalación de Kali Linux



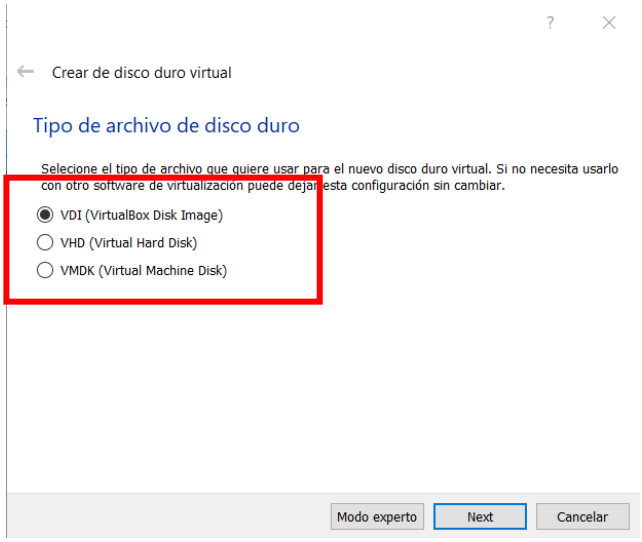
Configuración del tamaño de memoria de la máquina virtual



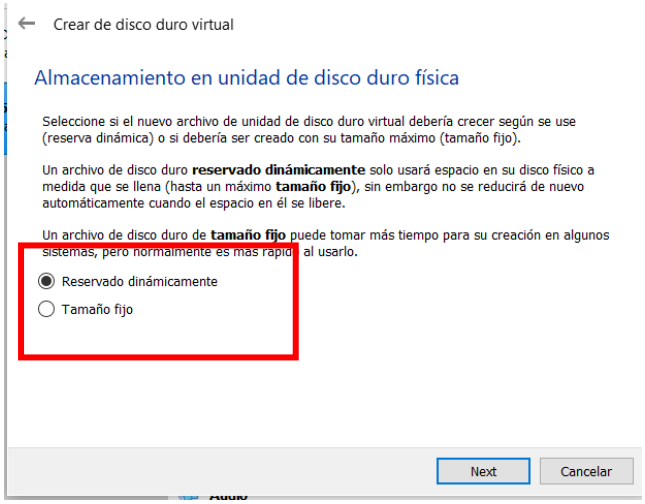
Creación del disco duro virtual



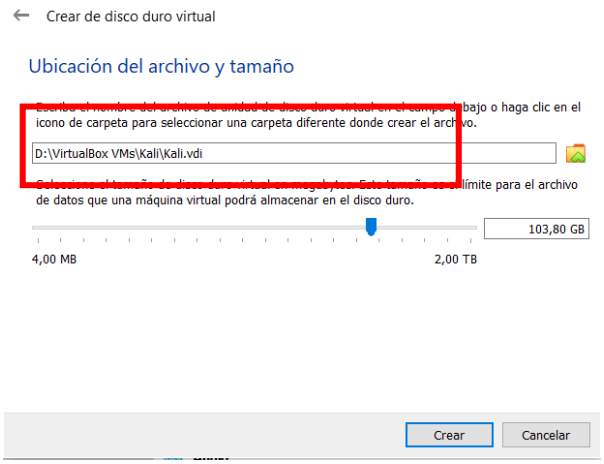
Elección del tipo de disco duro virtual



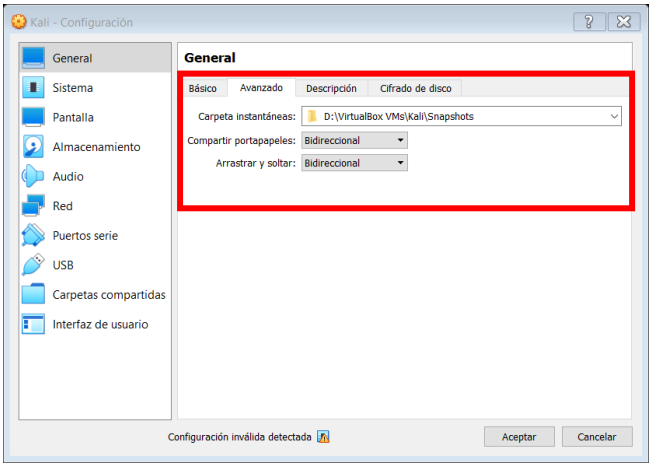
Elección del tipo de almacenamiento de la unidad de disco duro físico



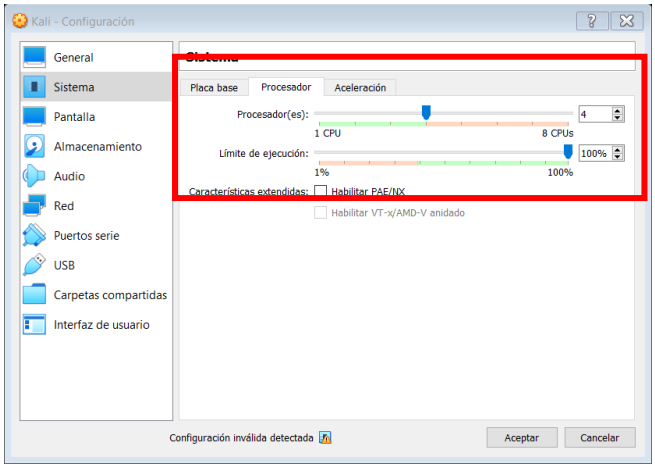
Elección de la ubicación y el tamaño del disco duro



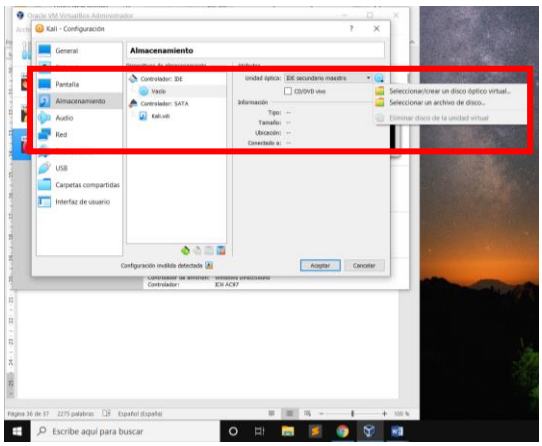
Identificación de la carpeta donde ubica la máquina virtual



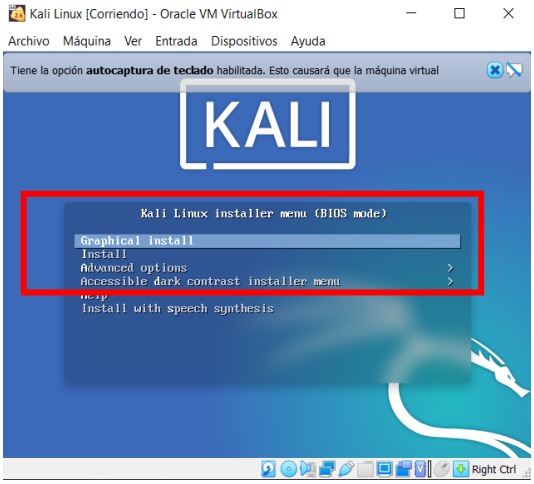
Elección del número de procesadores y el límite de ejecución



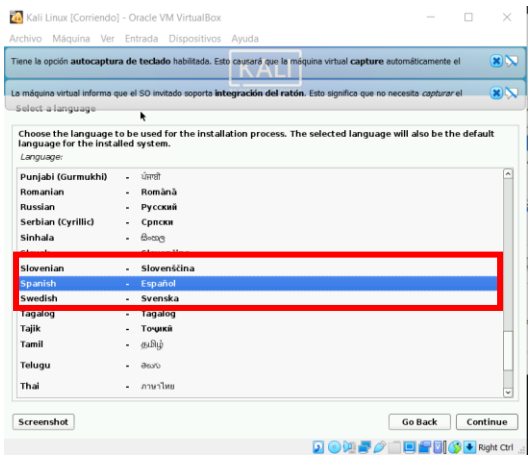
Selección de la imagen para creación de la máquina virtual



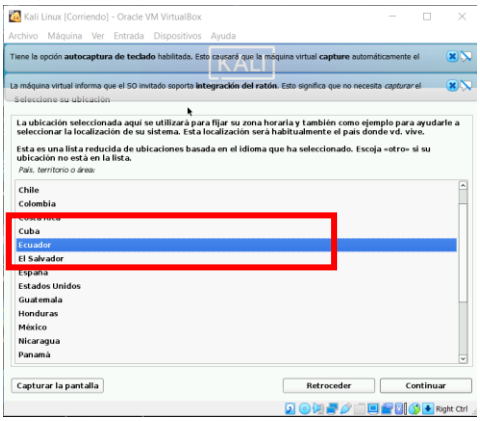
Instalar y configurar Kali Linux en modo grafico



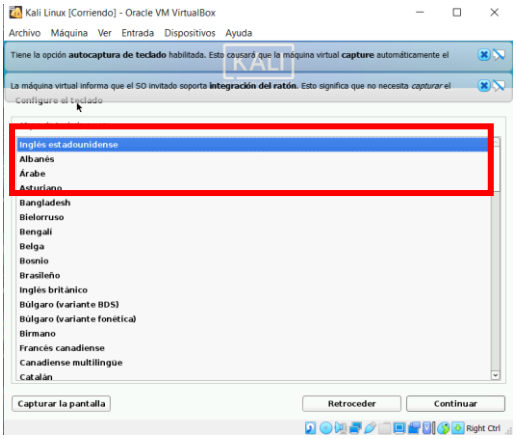
Seleccione un idioma español



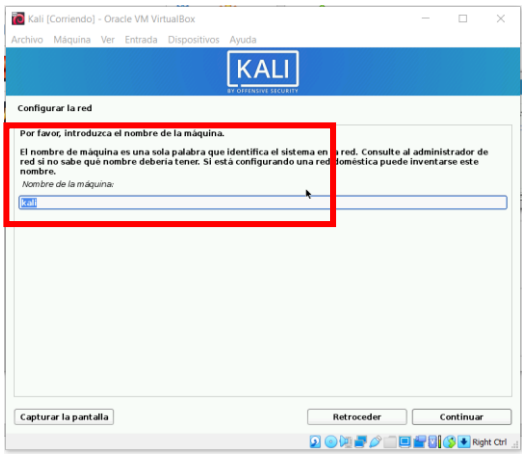
Seleccione su ubicación



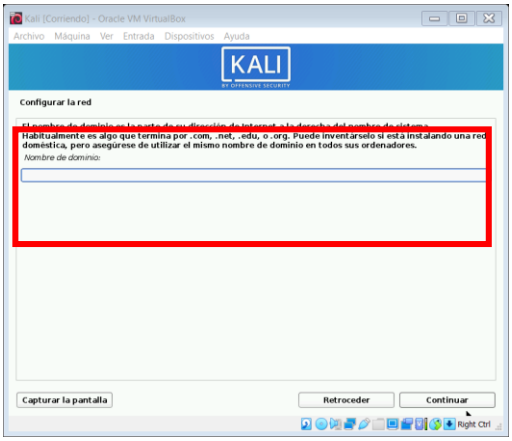
Configure el teclado.



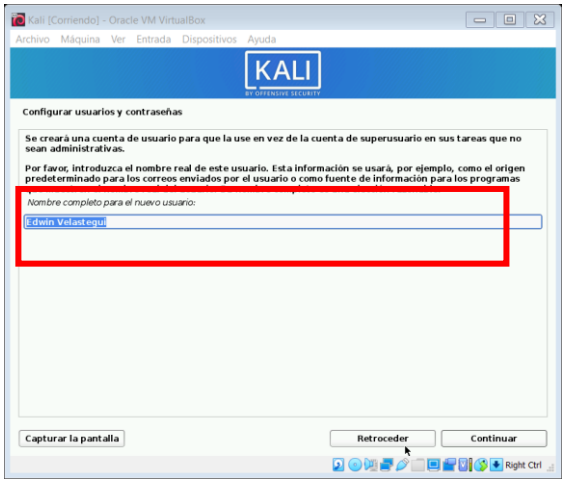
Configure la red**.**



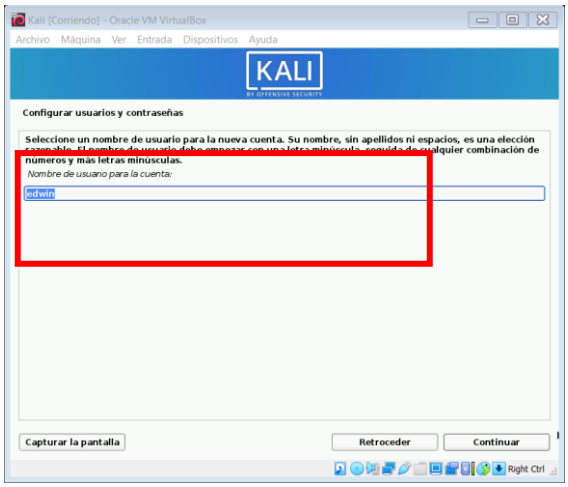
Configuración de la red



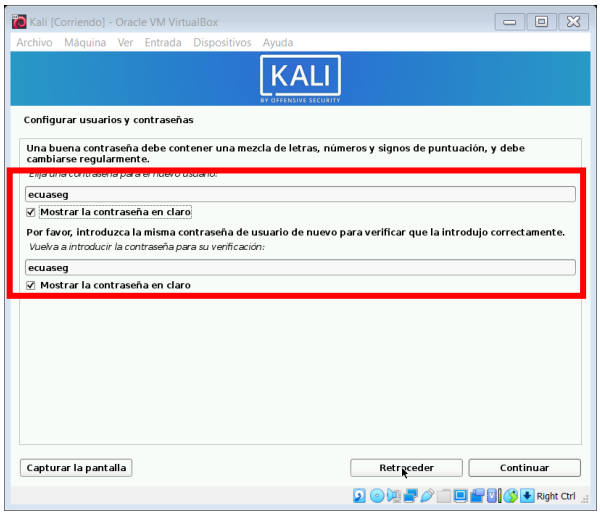
Creación del usuario de la maquina virtual



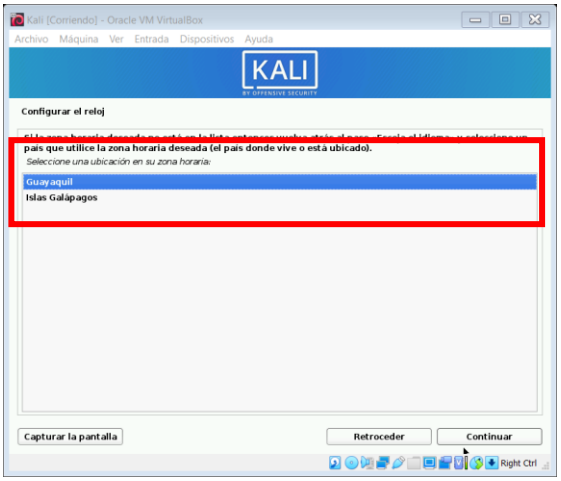
Configuración del usuario de la cuenta



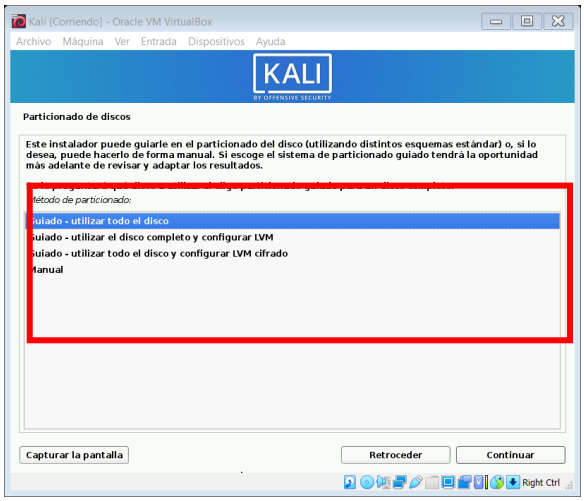
Creación de la contraseña



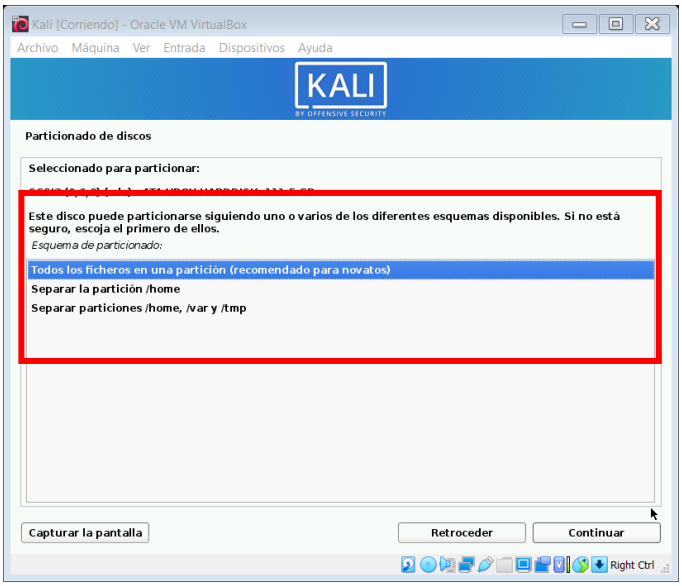
Selección de la hora en ecuador



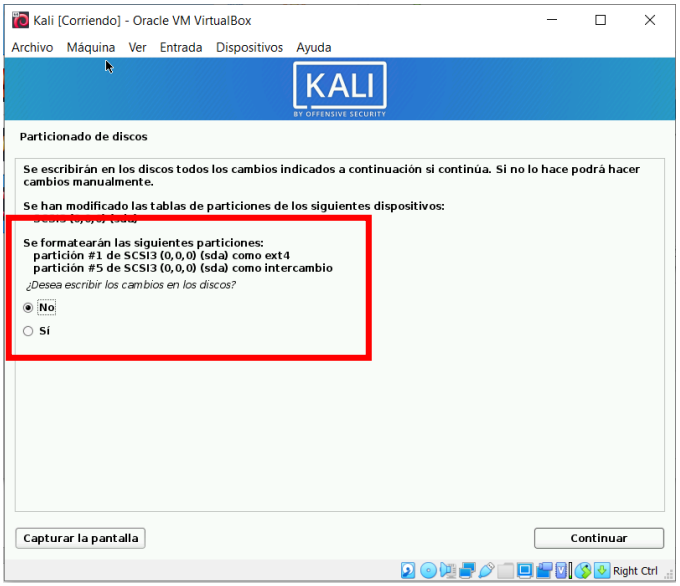
Elección de la partición del disco



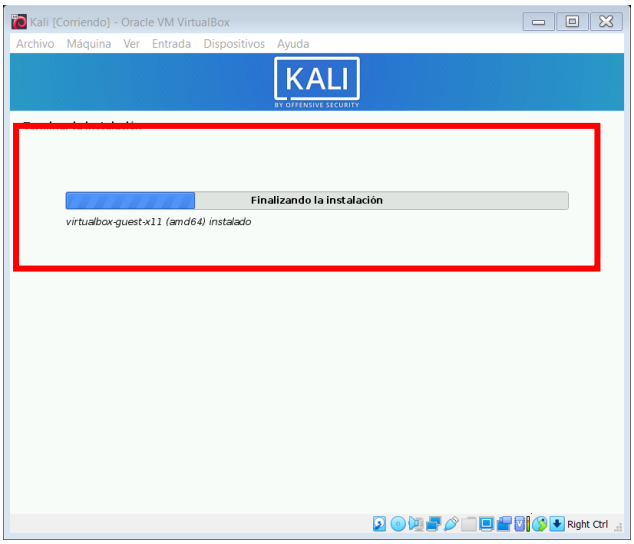
Selección de los ficheros para partición



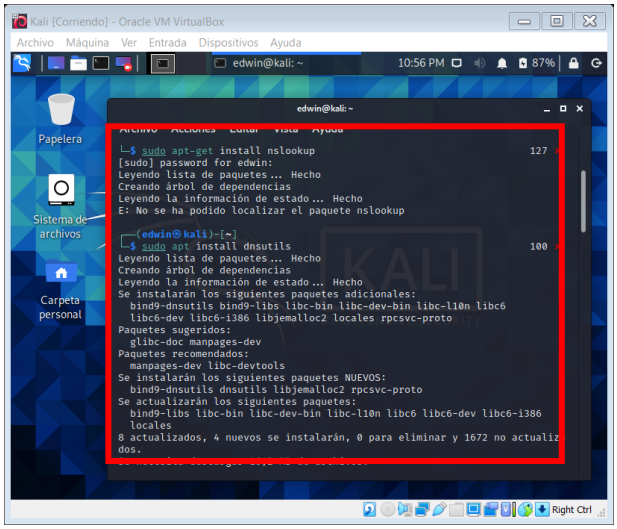
Eleccion de escribir los cambios en los discos



Finalización de la instalación



Inatlacion de dependencias y actualizacion



Anexo C informe Técnico

Informe Técnico	
1. Introducción	El presente proyecto tienen como objetivo evaluar la seguridad del sistema de video vigilancia en la empresa ECUASEG con previo consentimiento de la dicha empresa, A continuación se realizó un resumen del proceso efectuado y el detalle de la vulnerabilidades identificados así como las recomendaciones que se deben tomar en cuenta por medio de sistema operativo Kali Linux que permite realizar un hacking ético.
2. Reconocimiento	En la fase de reconocimiento se utilizó google dorks [16] y Maltego para recabar información de la empresa y de los trabajadores de la misma Hallazgos • Información de equipos que instalan y venden • Obtención de número de teléfono de la empresa y email del mismo
3. Análisis de vulnerabilidades	En la fase de vulnerabilidades se utilizó la herramienta shodan que permite analizar dispositivos conectados a la red en este caso de los equipos Hikvision a nivel mundial, ecuador, y Ambato para entender la complejidad que los sistemas conectados a internet son propensos ataques.

4. Explotación	En la fase de explotación se vulnero primero el punto de acceso a internet, primero se realizó un ataque de desauntentificacion de dispositivos para obtener la clave de la red ECUASEG encriptada y por medio de ataque de fuerza bruta y diccionario se logró tener acceso a la red Hallazgos • Ingreso a conexión física del Access Point • Obtención de la clave y dirección Ip del dispositivo. En la segunda etapa del ataque se analizó la dirección Ip del DVR por medio de la herramienta Nmap y la verificación de los puertos abierto, después se realizó un ataque de fuerza bruta con la herramienta Hydra en conjunto con el puerto 80. Hallazgos • Tipos de seguridad configurado en DVR • Versión de firmware del DVR
Recomendaciones • Para evitar el ataque de diccionario afecte al DVR asegurarse de que la contraseña de administrador esté configurada para ser compleja y que solo la conozcan los usuarios en los que confía. No olvide guardar la contraseña en un lugar seguro, ya que restablecer la contraseña puede ser engorroso e incluso costoso en algunas grabadoras que requieren un restablecimiento de fábrica.	

• Crear cuentas de usuario secundarias que no sean el usuario administrador principal para su uso diario. Si tiene otros usuarios a los que le gustaría permitir el acceso, cree cuentas únicas y separadas para esos usuarios. • Esté atento a un uso elevado o picos de datos, y verifique la lista de dispositivos de inicio de sesión para asegurarse de que no haya dispositivos o usuarios desconocidos en la red de la Empresa • Configure la autenticación de dos factores si su cámara de seguridad o DVR lo ofrece, lo que proporcionará una capa adicional de seguridad. Si inicia sesión en la cámara, recibirá un mensaje o un correo electrónico de la empresa para autenticar su cuenta.	
5. Post-Explotación	En el post-explotacion se utilizó la herramienta Metasploit para poder dejar una puerta abierta para tener acceso del NVR
6. Riesgo	En nivel de riesgo en el análisis realizado por la herramienta Nessus no mostro vulnerabilidades de alto riego.

Anexo D informe ECUASEG

Análisis de Vulnerabilidades y Auditoria de Seguridad realizado desde la red interna y sistema de video vigilancia de la empresa ECUASEG

Informe de resultados Confidencial

Estatuto de Confidencialidad

Este documento incluyendo la totalidad de su contenido, es propiedad de ECUASEG. La información no podrá ser presentada o distribuida a personas ajenas a este proceso o utilizada para cualquier otro propósito ajeno a la evaluación de seguridad.

Propósito del Documento

Este documento forma parte del reporte de la evaluación del cumplimiento al plan de trabajo de auditoria interna en lo que refiere a Seguridad informática, escaneo y análisis de vulnerabilidades del sistema de video vigilancia. Descarga de Responsabilidades las observaciones y recomendaciones expresadas en este documento representan el resultado de la revisión y son una opinión con base en estándares internacionales y en mejores prácticas. Es responsabilidad de ECUASEG, tomar las decisiones y ejecutar los cambios en su organización, procesos y normatividad que considere pertinentes. Auditoria Interna, no es, ni será responsable

sobre la toma de decisiones con base en los mismos. ECUASEG, reconoce y acepta que lo hace bajo su propia responsabilidad y que excluye a Auditoria Interna de cualquier responsabilidad por los daños y perjuicios de toda naturaleza que puedan deberse al contenido del documento y/o de los servicios prestados.

Análisis de vulnerabilidades

1. Resumen ejecutivo

1.1. Equipos examinados

Nombre	IP
Access Point	xxx.xxx.xxx.xx x
DVR(DS-7208HGHI-KI)	xxx.xxx.xxx.xx x
CAMARA(HANGZHOU HIKVISION DIGITAL TECHNOLOGY)	xxx.xxx.xxx.xx x
CAMARA(HANGZHOU HIKVISION DIGITAL TECHNOLOGY)	xxx.xxx.xxx.xx x

1.2. Metodología

El análisis y escaneo de vulnerabilidades proporciona valiosa información en cuanto al grado de exposición de una organización a los ataques y el uso indebido de recursos. Sin esta información, los servicios permanecen expuestos a cientos de debilidades, las cuales pueden ser aprovechadas por atacantes internos o externos. La metodología utilizada se basa en 6 etapas, donde se recolecta información, la cual es aprovechada después para realizar los ataques, terminando con la generación de recomendaciones más efectivas a fin de corregir las brechas encontradas.

Análisis de vulnerabilidades

Fases del hacking ético Como todas las disciplinas que existen en el mundo, la piratería ética se divide en distintas fases.

La piratería ética tiene 6 fases distintas. Estas fases no son reglas estrictas, sino más bien una pauta a seguir.

Reconocimiento: Es el proceso de recopilación de información. En esta fase, el pirata informático recopila información relevante sobre el sistema de destino.

Escaneo: En la fase de exploración, el hacker comienza a sondear activamente la máquina o la red de destino en busca de vulnerabilidades que puedan explotarse. Obteniendo acceso: En esta fase, la vulnerabilidad localizada durante el escaneo se explota utilizando varios métodos y el hacker intenta ingresar al sistema objetivo sin generar ninguna alarma.

Mantener el acceso: Esta es una de las fases más integrales. En esta fase, el hacker instala varias puertas traseras y cargas útiles en el sistema de destino.

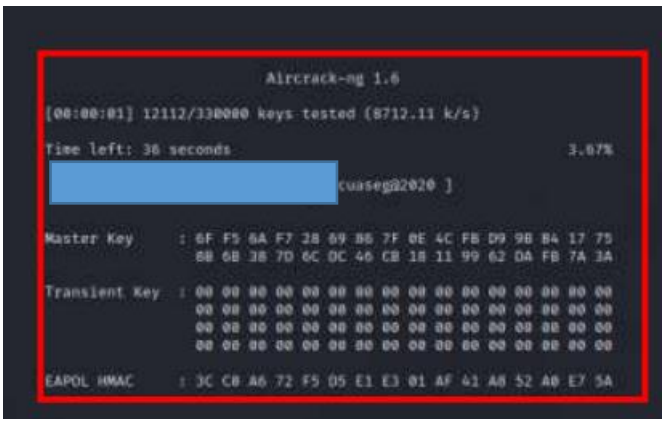
Mantenerse oculto: Este proceso tiene que ver con la eliminación de logs de todas las actividades que tienen lugar durante el proceso de hacking.

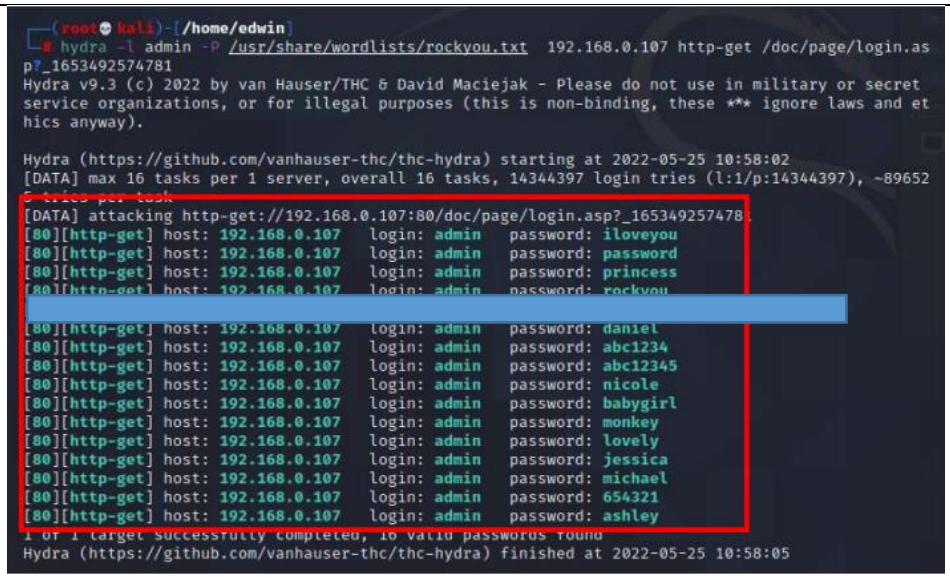
Reportar: es el último paso para finalizar el proceso de piratería ética. Aquí se compila un informe con sus hallazgos y el trabajo que se realizó, como las herramientas utilizadas, la tasa de éxito, las vulnerabilidades encontradas y los procesos de explotación.

1.3. Herramientas utilizadas

Actividad	**Herramienta**
Búsqueda de información de la Empresa	Google Dorks
Búsqueda de información del personal	Maltego
Búsqueda de vulnerabilidades de cámaras de la empresa	Shodan
Obtención de acceso del sistema	Airmon-ng
Creación de diccionario	Crunch
Búsqueda de vulnerabilidades de los dispositivos	Nessus
Análisis de puertos	Nmap
Ataque en fuerza bruta	Hydra

2. Resultados obtenidos del escaneo y análisis de vulnerabilidad

Equipo	**Vulnerabilidad**
Datos Personales	**Gerente:** [redacted] **Direccion:** [redacted] **Correo:** [redacted] **Celular:** [redacted]
Access Point	Tiene una vulnerabilidad que consiste en que la contraseña en forma cifrada se comparte por medio de un protocolo de enlace de 4 vías. Cuando un usuario se autentica a través del punto de acceso, el usuario y el punto de acceso deben pasar por un protocolo de enlace de 4 vías para completar el proceso de autenticación. En el sistema de video vigilancia conectada a la red ECUASEG se capturo el paquete de protocolo de enlace de 4 vías y se buscó la clave cifrada en esos paquetes. Después de obtener la clave cifrada, probamos una lista de palabras específica para descifrar la contraseña cifrada. 
DVR(DS-7208HGHI-KI)	Para ataques de fuerza bruta y los ataques de diccionario, se utilizó un software para enviar una secuencia rápida de contraseñas al DVR hasta encontrar la actual, es como un enfoque de prueba y error. Un software desarrollado para este propósito puede probar miles de combinaciones en cuestión de minutos hasta encontrar la contraseña correcta del sistema.

	 Por lo que se obtuvo acceso al DVR y a sus datos y configuraciones 
CAMARA(HANGZHOU HIKVISION DIGITAL TECHNOLOGY)	No son propensas a taques de exploit por lo cual no se pudo dejar una puerta trasera por estar configurado con direcciones IP aleatorias.

3. Conclusión y recomendación general

En base a la revisión efectuada y resultados obtenidos, se concluye que:

El sistema de video vigilancia se encuentra desactualizado y posee vulnerabilidades conocidas, las cuales, es importante mitigar, a fin de que el riesgo inherente asociado no sea aprovechado por un atacante mediante el uso de “exploits” y ejecutar un ataque “dirigido” hacia el DVR y cámaras IP, y se comprometa la información “sensitiva” de la empresa ECUASEG

Recomendaciones Generales:

- Se debe endurecer la seguridad del AP, mediante la elaboración e implementación de estándares de seguridad para AP en ambiente de trabajo, a fin de asegurar que los aspectos de seguridad mínima y de endurecimiento a

nivel de Sistemas operativos, claves, nombre de usuarios tanto para el AP, DVR, Aplicaciones de visualización de Camaras IP y Correo Electronico.

- El sistema de video vigilancia, debe considerar la elaboración de procedimientos y estándares para la administración y gestión de vulnerabilidades, documentos que se sugieren contengan como mínimo los temas que se describen a continuación:

Plan de Acción
1. Primero se debe actualizar las versiones de firmware periódicamente para evitar dejar puertas traseras abierta a cualquier ataque
2. Segundo se debe cambiar periódicamente la clave de la red mínimo cada 3 meses
3. Implementación de una base datos para el control y mantenimiento de las claves DVR de la empresa y los clientes para evitar la utilización del mismo en cada dispositivo
4. Supervisión del sistema en busca de picos de trafico
5. Asegúrese de que las grabadoras de video y los servidores se mantengan en un área con tecnología de control de acceso estricto e incluso cámaras de vigilancia como medida adicional de protección.
6. Realizar pruebas periódicas de vulnerabilidad para todas las cámaras de video IP y DVR.