BUAP

Análisis de vulnerabilidades a través de herramientas en AlmaLinux

Analysis of vulnerabilities through tools in AlmaLinux

Christian Amauri Amador Ortega[1], M.C. Yeiny Romero Hernández[2]
[1]Facultad 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, yeiny.romero@correo.buap.mx.

Abstract

In this article, we will introduce the reader to the RHEL and AlmaLinux operating systems. We will discuss basic cybersecurity concepts and theory, including its origins, followed by concepts related to cyberattacks through vulnerability exploitation. Next, we will list tools available in AlmaLinux (9.4) (or compatible with it) that can assist in the defense and management of the cybersecurity of the IT/computing systems we are responsible for. We will document the topics this entails, including the installation and usage of the tools (with the results of two usage examples) and their technical requirements. If necessary, we will also explore migrating tools and/or packages from other Linux distributions to this one. Finally, we will offer our interpretation of results, conclusions, and references in the corresponding final sections. (A complete version of this article is available, in which each topic is fully detailed and broken down, particularly the practical sections and full references).

Resumen

En este artículo vamos a presentar al lector en los sistemas operativos RHEL y AlmaLinux. Hablaremos sobre conceptos y teoría básica de ciberseguridad y cómo surge, luego sobre conceptos de ciberataques por explotación de vulnerabilidades. Luego enlistaremos herramientas que estén disponibles en AlmaLinux (9.4) (o que le sean compatibles), que nos pueden ayudar en la defensa y administración de la ciberseguridad de los sistemas informáticos/computacionales de los que somos responsables. Documentaremos los tópicos que esto conlleve, incluyendo la instalación y uso de las herramientas (con los resultados de dos ejemplos de uso), y sus requerimientos técnicos. Y, de ser necesario, migrar herramientas y/o paquetes de otras distribuciones de Linux a esta distribución. Y finalmente, ofreceremos nuestra interpretación de resultados, conclusiones y referencias en las secciones finales correspondientes. (Hay una versión completa de este artículo, en el que cada tema se detalla y se desglosa por completo, sobre todo las secciones prácticas y las referencias completas).

Palabras clave y frases, Introducción, Marco teórico y estado del arte, Seguridad de la información, seguridad informática.

***Keywords and phrases**: Vulnerabilidades, Vector de ataque, Amenazas, Exploit, Explotación, Ciberataque, Ataque, Hacker, Malware, Phishing, Payload, AlmaLinux, Herramientas, Comandos, Terminal, Ciberseguridad, Análisis, Protocolos y servicios de red, Sistemas operativos, Puertos.*

1 Introducción

AlmaLinux es un sistema operativo compatible a nivel binario con Red Hat Enterprise Linux (RHEL). Es gratuito y de código abierto, 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. Pero sus usuarios deben pagar una suscripción para acceder dichas actualizaciones. Por eso AlmaLinux es tan importante.

2 Marco Teórico y Estado del Arte

(2.1) Cualquier tipo de seguridad (laboral, vial, biológica, médica, tecnológica, informática, etc…) implica los conceptos de; ***(2.2) 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 [1].

2.3 El estado del arte en materia de administración de servidores y ciberseguridad incluye uso de VPNs (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).

2.4 El estado del arte del análisis de vulnerabilidades incluye escaneo automatizado, pruebas de penetración, simulación de ataques reales ("Red Teaming"), análisis dinámico y estático de vulnerabilidades (análisis del sistema cuando está desplegado en tiempo real y cuando no, respectivamente) priorización de vulnerabilidades, planificación de respuesta y herramientas emergentes que ayudan en tareas puntuales de cualquiera de los tópicos mencionados.

3 Seguridad de la información

Protege la CIA (Confidentiality, Integrity, Availability) en lo que a información respecta. No necesariamente implica medios o infraestructuras digitales, incluye también soportes físicos (como identificaciones, facturas, recibos, documentos y otros recursos físicos que puedan almacenar información), además del uso y divulgación de tal información a través de cualquier medio [2][5].

4 Seguridad informática

Protege toda la infraestructura de tecnologías de la información (computadoras, celulares, tablets, routers, módems, repetidores, antenas, cables, datos, software, etc.) de una entidad ante cualquier riesgo posible, como accesos no autorizados, ciberataques, filtraciones de datos e incluso incidentes físicos como apagones, terremotos, inundaciones, incendios etc… [2].

5 Ciberseguridad

La ciberseguridad se centra en proteger medios digitales que, por su naturaleza, son comprometidos de maneras más específicas, principalmente mediante ataques directos y debilidades de autenticación. Protege a los sistemas computacionales, redes, aplicaciones, datos, archivos y activos financieros, contra atacantes que usan virus, ransomware, spyware (malware) o cualquier medio para comprometer la "CIA" de dichos activos. Estos son los denominados 'ciberataques' [6].

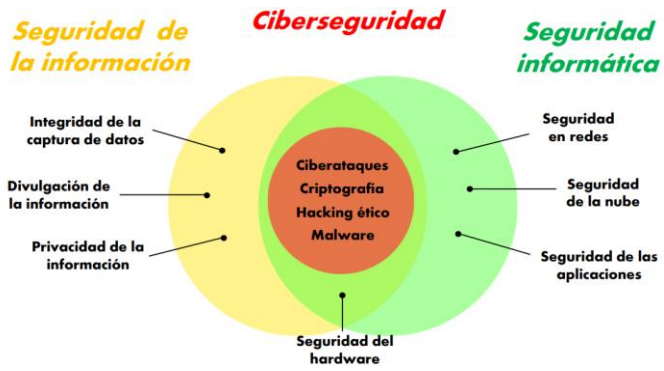


Diagrama orientativo.

6 Ramas de la Ciberseguridad

Entre las ramas de la ciberseguridad, podemos identificar tres enfoques principales: ***justicia*** (enfoque en la protección legal y ética dentro del ámbito digital: *peritaje judicial, informática forense, investigación y persecución del cibercrimen* [8]), ***gestión*** (enfoque en la administración de riesgos y recursos de seguridad en las organizaciones: *dirección, big data en entornos seguros, auditoría, consultoría* [7][8]) y ***práctico*** (enfoque en la implementación y operación de soluciones técnicas*: seguridad en redes o bases de datos, hacking ético* [6][7][8]). El hacking ético es una de las ramas más importantes de la ciberseguridad porque requiere 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.

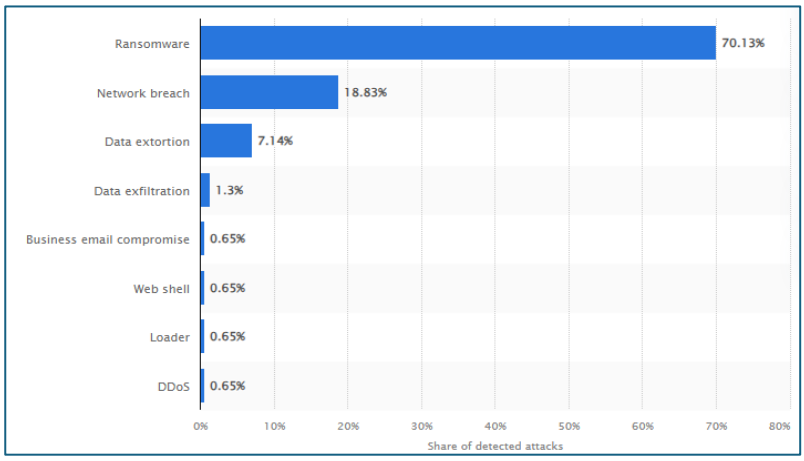
7 Ataques

7.1 Vulnerabilidades, Vectores de ataque y Exploits

Una *vulnerabilidad* es cualquier debilidad en el sistema víctima, que pueda ser usada por un atacante para comprometerlo. El *vector de ataque* es la técnica o método que el atacante usará para comprometer al sistema víctima, por ejemplo: *phishing, explotar de vulnerabilidades de software, ataques de fuerza bruta, usar ingeniería social, etc.* Un *exploit* es la técnica o herramienta específica que se usará para aprovecharse de la(s) vulnerabilidad(es) del sistema víctima y así atacarlo, son conceptos y elementos usados en la práctica en tiempo real de un ataque. Ejemplos de exploits incluyen: *desbordamiento de búfer, inyección SQL, inyección de comandos, Stuxnet, Mimikatz, etc* [10][11][12][17][31][32][33][34][37]. Acerca de los tipos de ataques que existen, los principales son: ***ataques basados en malware***, que incluyen: *ransomware, troyanos, spyware, gusanos, virus,*

rootkits, etc. ***Phishing***, que puede ramificarse en las categorías: *whale, smishing, spear, clone, pop-up, vishing, etc.* ***BEC***, ***denegación de servicio (DDOS)***, ***ataques de día cero*** y ***man in the middle (MITM)*** [9][13][18]. Según Techopedia [22], en general, los dos tipos de ataques más comunes en 2022 fueron el phishing y el ransomware. Además de ataques de ingeniería social. Statista reporta que en 2023, el ransomware superó a cualquier otro tipo de ciberataque *[26]*.

By Victim Count	
Crime Type	*Victims*
Phishing	300,497
Personal Data Breach	58,859
Non-Payment/Non-Delivery	51,679
Extortion	39,416
Tech Support	32,538
Investment	30,529
Identity Theft	27,922
Credit Card/Check Fraud	22,985
BEC	21,832
Spoofing	20,649
Confidence/Romance	19,021
Employment	14,946
Harassment/Stalking	11,779
Real Estate	11,727



Estadísticas de ciberataques. En 2022 según el FBI, y en 2023 según Statista.

8 Ataques por explotación de vulnerabilidades

Las cuatro fases de un análisis de vulnerabilidades son: *identificación de vulnerabilidades, evaluación, tratamiento e informe.* Y podemos clasificar a estos análisis en cuatro rubros: análisis de vulnerabilidades internas y externas, análisis autenticados y no autenticados. Y cuando se trata de explotación de vulnerabilidades, tenemos las siguientes fases: reconocimiento, escaneo, explotación y mantenimiento de acceso. Y tomando en cuenta los tipos de explotación de vulnerabilidades más comunes (inyección de comandos, ejecutables maliciosos, desbordamiento de búfer), tenemos que mencionar algunos de los servicios y protocolos que se pueden usar para realizar una explotación, para así entender cómo funciona un ataque en su forma más elemental. Estos elementos incluyen: ***servicios/protocolos web****: WordPress, Joomla y Drupal, HTTP/HTTPS, WebSocket, JSON-RPC, XML-RPC SSE*. ***De correo eletrónico****: SMTP, IMAP, POP3, SPF, DKIM*. ***De transferencia de archivos****: FTP, SFTP, WebDAV, Rsync*. ***De bases de datos****: MySQL, PostgreSQL, SQLite*. ***Servicios de red****: SSH, RDP, TCP, UDP, NAT, puertos de red. E incluso* ***APIs (REST, SOAP)***. Al identificar vulnerabilidades específicas en alguno de estos servicios, que son usados por alguna aplicación, proceso o sistema específico, se procede a explotarlas. Ahora, el payload es el módulo del exploit que contiene los códigos que se ejecutan después de que se ha logrado la explotación. Es el elemento que como tal, causa el daño buscado [35][36].

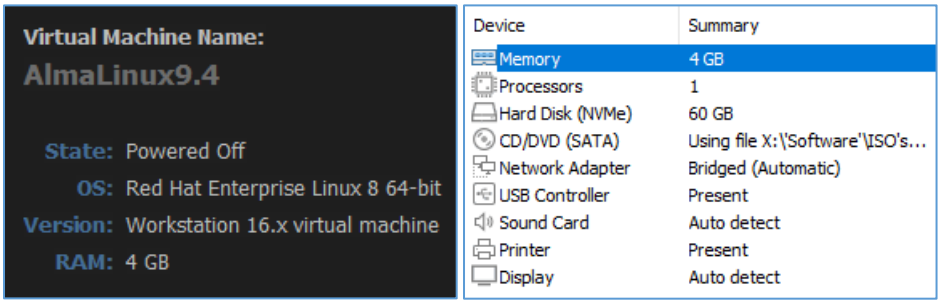
9 Herramientas de ciberseguridad de nuestro interés

Hemos seleccionado cinco herramientas de interés para probar y documentar su implementación en AlmaLinux: *Metasploit Framework, SQLmap, SearchSploit, Enum4Linux* y *SpamAssassin*.

9.1 Consideraciones generales para cada herramienta:

- ✓ La versión de AlmaLinux utilizada para esta documentación es la 9.4 (Seafoam Ocelot).
- ✓ Antes de cada instalación, es una buena práctica actualizar nuestro sistema, ejecutando el comando `sudo dnf update`.
- ✓ El comando: `rpm -q` nos ayudará a saber si tenemos una dependencia instalada o no. Además, de los parámetros `–version`, `–help` o `-h` para comprobar las versiones instaladas.

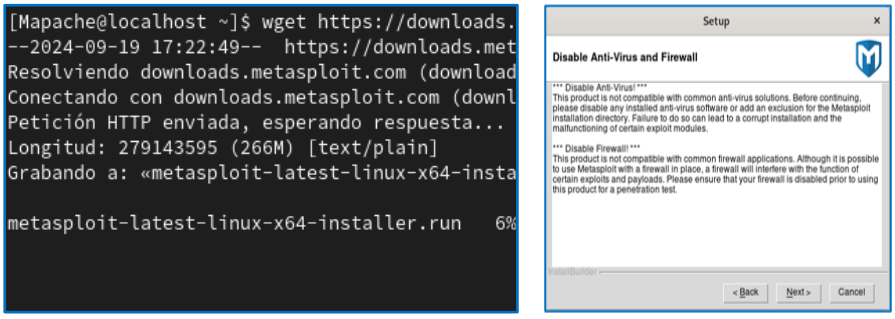
Recomendamos tener al menos 8 GB de RAM disponibles, ya sea en máquina física o virtual (recomendable física). Y otra máquina (física o virtual) para realizar sobre ella las pruebas de penetración y de escaneo correspondientes.



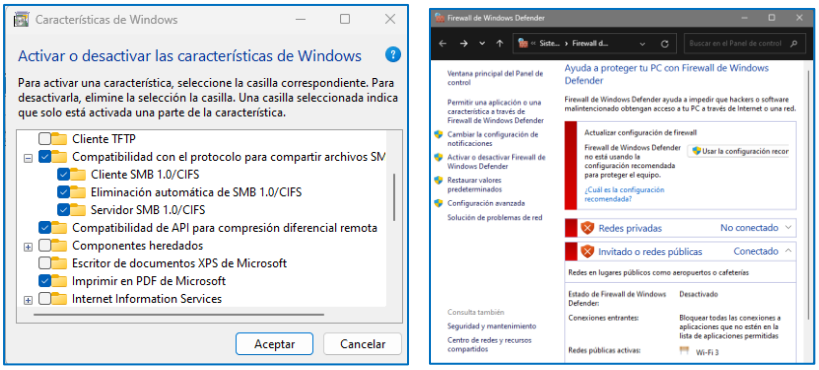
Especificaciones de la máquina virtual usada (VMware Workstation 16 Player: Non-commercial use)

10 Instalación de las herramientas, y preparación del escenario vulnerable

10.1 Los pasos para descargar e instalar Metasploit son, a grandes rasgos: descargar Metasploit usando wget, otorgar permiso de ejecución al instalador, ejecutar el instalador gráfico desde terminal, y configurar la instalación desde dicho instalador. El escenario vulnerable propuesto consiste en desactivar el firewall de Windows, y activar los servicios SMB para explotar la vulnerabilidad SMB con EternalBlue.



Descargar (desde terminal) e instalar (con el instalador gráfico) Metasploit en AlmaLinux.



Activar SMB, y desactivar el firewall en Windows 11.

10.2 La instalación de SQLmap consiste a grandes rasgos en descargar las dependencias correspondientes (Git y Python) y luego clonar el repositorio de Git de la herramienta. El escenario vulnerable que preparamos consiste en una base de datos PostgreSQL mal configurada, en Windows 11, con una tabla y una función (también mal diseñada).

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

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

```
[Mapache@localhost ~]$ git clone https://github.com/sqlmapproject/sqlmap.git
Clonando en 'sqlmap'...
remote: Enumerating objects: 83980, done.
```

Clonación con Git, del código fuente de SQLmap a nuestro sistema.

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
```

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

```
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)
```

```
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
```

Tabla de una base de datos PostgreSQL en windows 11. Mala configuración en los archivos: pg_hba.conf y postgresql.conf de la base de datos (configuraciones que permiten que la base de datos pueda escuchar a cualquier máquina). Y función SQL intencionalmente vulnerable.

10.3 La instalación de SearchSploit consiste a grandes rasgos, en añadir el repositorio EPEL a nuestro AlmaLinux, actualizar el sistema con upgrade, instalar snapd, y finalmente con snap, instalar SearchSploit (No necesitamos preparar escenario vulnerable).

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

```
[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.
```

```
[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
```

Pasos para la instalación de SearchSploit.

10.4 Instalar Enum4Linux, a grandes rasgos sólo requiere el comando: <sudo snap install enum4linux> (debemos añadir el repositorio EPEL a nuestro sistema si aún no lo hemos hecho). El escenario vulnerable que proponemos consiste en crear un usuario en Windows 11, que no tenga contraseña. En Windows 11: Configuración > Cuentas > Otros usuarios > Agregar cuenta > No tengo la información de inicio de sesión de esta persona > Agregar un usuario sin cuenta Microsoft ***Definir nombre de usuario** > Siguiente.

10.5 Para instalar SpamAssassin simplemente tenemos que usar el comando yum Install SpamAssassin, y luego asegurarnos de que después de instalarlo, esté activo.

```
[Mapache@localhost ~]$ sudo yum install spamassassin
20192782125 24Última comprobación de caducidad de meta
 hecha hace 18:06:50, el vie 20 sep 2024 18:31:06.
678Dependencias resueltas.
================================================================
 Paquete              Arq.    Versión        Repositorio
================================================================
Instalando:
 spamassassin         x86_64 3.4.6-5.el9    appstream
Instalando dependencias:
 perl-Algorithm-Diff noarch 1.2010-4.el9    appstream
```

```
[Mapache@localhost ~]$ sudo systemctl status spamassassin
● spamassassin.service - Spamassassin daemon
     Loaded: loaded (/usr/lib/systemd/system/spamassassin.service; enabled;
     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-
             ├─10846 "spamd child"
             └─10847 "spamd child"
```

Instalación de SpamAssassin desde terminal con yum, y verificación de su status con systemctl.

11 Resultados

11.1 Uso de Metasploit Framework

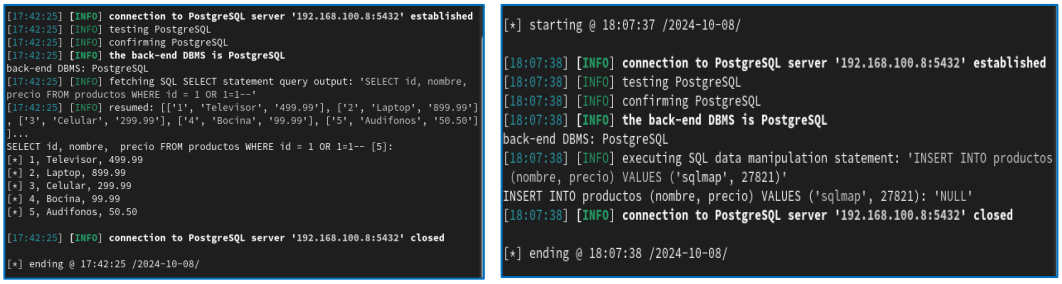
```
msf6 > use auxiliary/scanner/portscan/tcp
msf6 auxiliary(scanner/portscan/tcp) > set RHOSTS 192.168.100.8
RHOSTS => 192.168.100.8
msf6 auxiliary(scanner/portscan/tcp) > run

[+] 192.168.100.8:        - 192.168.100.8:135 - TCP OPEN
[+] 192.168.100.8:        - 192.168.100.8:139 - TCP OPEN
[+] 192.168.100.8:        - 192.168.100.8:445 - TCP OPEN
[+] 192.168.100.8:        - 192.168.100.8:902 - TCP OPEN
[+] 192.168.100.8:        - 192.168.100.8:912 - TCP OPEN
```

```
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) >
```

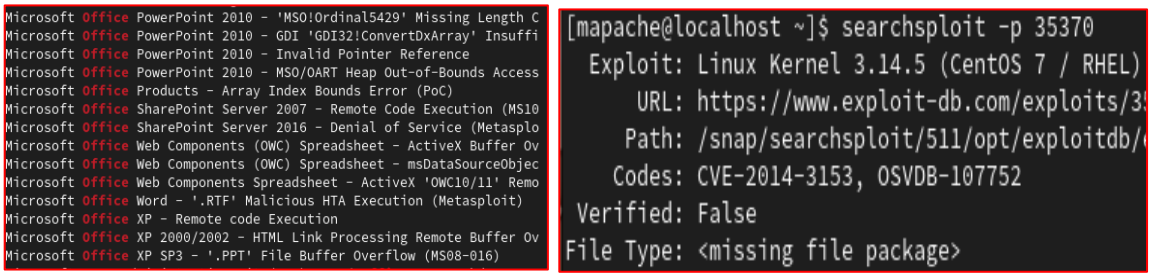
Ej. 1) Obtener los puertos abiertos de nuestra víctima: 192.168.100.8, y Ej. 2) Configurar un exploit, el host a atacar (misma víctima) y el payload (es decir, realizar un ataque).

11.2 Uso de SQLmap



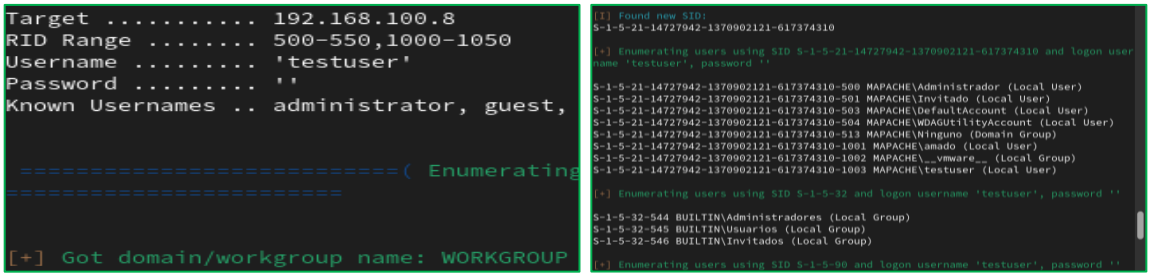
Ej. 1) Obtención de una tabla completa, y Ej. 2) Inserción de datos (ambos mediante inyección SQL).

11.3 Uso de SearchSploit



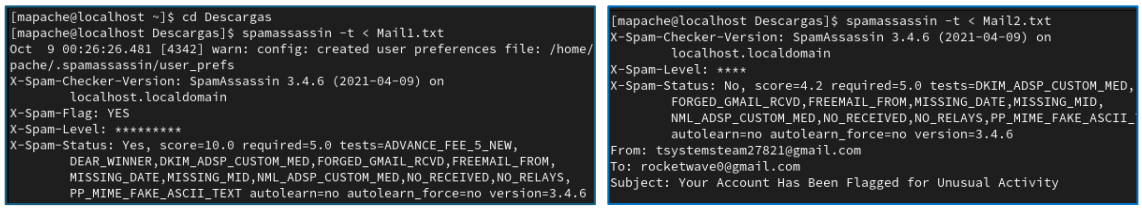
Ej. 1) Obtener vulnerabilidades y exploits para Microsoft Office, y Ej. 2) Obtener detalles sobre tales vulnerabilidades/exploits. por ejemplo, aquí sobre el exploit "CVE-2014-3153".

11.4 Uso de Enum4Linux



Ej. 1) Nombre del grupo de trabajo, y Ej. 2) usuarios. Obtenidos mediante los SID encontrados.

11.5 Uso de SpamAssassin



Ej. 1 y 2) Reportes de probabilidad de spam en correos examinados (ambos diagnósticos correctos).

12 Interpretación de resultados

Las instalaciones no siempre resultan como lo planeamos, en un campo de investigación como este (instalación de herramientas en un sistema operativo en el que han sido poco o nada documentadas), a veces se requieren pasos extra, descargas y modificaciones manuales que incluso con ellas, no se garantiza el funcionamiento de dichas herramientas. Además, los resultados obtenidos por cada herramienta pueden no ser de total utilidad, o pueden requerir complementarse con los resultados de otra, o de alguna fuente externa. Aún así, el funcionamiento en general de las herramientas en esta investigación fue satisfactorio.

12.1 Ventajas y desventajas de cada una

	Ventajas	Desventajas
MetaSploit (10/10)	Está muy integrada, muy completa, muy documentada, muy robusta.	Requiere más capacidad computacional que otras de las presentes herramientas.
SQLmap (9/10)	Muy bien construida, e implementada, muy especializada, muy robusta.	Tiene una curva de aprendizaje mayor que otras de las presentes herramientas.
SearchSploit (8/10)	Curva de aprendizaje muy baja, de fácil uso e interpretación.	La información que ofrece es referencial, no sacada de un escaneo a la víctima.
Enum4Linux (6/10)	Curva de aprendizaje muy baja, de fácil uso.	Es la menos robusta y actualizada de las presentes. Y solo puede escanear Windows.
SpamAssassin (9/10)	Curva de aprendizaje baja, resultados altamente efectivos. Reportes detallados.	Lo recomendable es automatizar su uso, pero eso puede resultar muy laborioso.

13 Conclusiones y trabajo a futuro

13.1 ¿Algunas de las herramientas se complementan entre sí?

Fueron diseñadas y desarrolladas por separado. Originalmente no están pensadas para complementarse directamente, pero las funcionalidades de cada una pueden aportar valor a las otras (y unas a otras más que otras a otras). (Metasploit y SearchSploit son las que más se complementan entre sí de forma directa, aunque SearchSploit prácticamente complementa a todas)

13.2 ¿Alguna se puede mejorar de alguna manera?

Sí, cada una tiene una o varias oportunidades de mejora y optimización tanto del lado del usuario, como del desarrollador encargado de su soporte y mantenimiento. A muy grandes rasgos: Metasploit necesita ser implementada en una máquina con muchos recursos computacionales, SQLmap no tiene un ejecutable para AlmaLinux, podríamos crearlo, SearchSploit siempre tiene espacio para agregar nuevos datos y además puede ser integrada a Metasploit, Enum4 Linux necesita mucha más documentación, actualización y mejora de sus actuales funcionalidades, SpamAssassin requiere automatizarse en un entorno grande para realmente aprovechar su máximo potencial.

13.3 ¿Estas herramientas actúan de forma independiente?

De entrada, sí. Cada una es autosuficiente para lo que fue diseñada, pero a pesar de eso, lo ideal siempre será complementar cada una con todas las herramientas y recursos posibles.

13.4 ¿Es mejor una que otra?

No podríamos comparar directamente unas con otras ya que todas tratan vulnerabilidades específicas diferentes. De entrada, ninguna es mejor que otra directamente. Sin embargo, sí podemos puntuarlas en base a las observaciones que hicimos de cada una (véase la tabla **12.1**).

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. El porcentaje asignado a cada herramienta en cada sector es una estimación empírica basada en la observación del comportamiento de las herramientas (el tipo de ataques que pueden manejar), contra el tipo de ataques que suele recibir cada sector.

	Educativo	*Empresarial*	*Guberna-mental*	*Automotriz*	*Farmacéutico (salud)*
Metasploit Framework	*%65*	*%95*	*%95*	*%95*	*%95*
Sqlmap	*%95*	*%95*	*%90*	*%90*	*%90*
SearchSploit	*%65*	*%95*	*%90*	*%95*	*%95*
Enum4Linux	*%60*	*%85*	*%80*	*%65*	*%75*
SpamAssassin	*%95*	*%100*	*%100*	*%65*	*%80*

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) (sin la teoría, la práctica es muy difícil o imposible).

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. E investigar más herramientas aún no documentadas (o no lo suficiente) para AlmaLinux (Por ejemplo, al inicio de esta investigación, se contemplaron dos herramientas cuya instalación no pudo tener éxito para esta distribución en esta oportunidad). Además de buscar realizar las implementaciones mencionadas en la respuesta de la pregunta **13.2**.

14 Agradecimientos

A mis amigos y familiares por acompañarme y apoyarme en estos cinco años de carrera, a todos mis docentes por los retos y las experiencias, a la BUAP y a la FCC como lugares y como entidades, a mi asesora de proyecto de investigación; Yeiny Romero Hernández, a todas las personas que de algún modo u otro me aportaron algo en estos cinco años, y a mis entidades arcanas personales como *"Marek"* o *"Love on The Rocks"*.

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*

[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*

[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/*

[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*

[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/*

[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/*