Análisis de vulnerabilidades a través de herramientas en AlmaLinux

Christian Amauri Amador Ortega

M.C. Yeiny Romero Hernández

- *Introducción*
- *Metodología*
- *Desarrollo*
- *Resultados*
- *Conclusión*
- *Referencias*

INTRODUCCIÓN

AlmaLinux es, al igual que su descontinuado precursor CentOS, un sistema operativo creado para ofrecer una versión gratuita y de código abierto, compatible a nivel binario con Red Hat Enterprise Linux (RHEL).

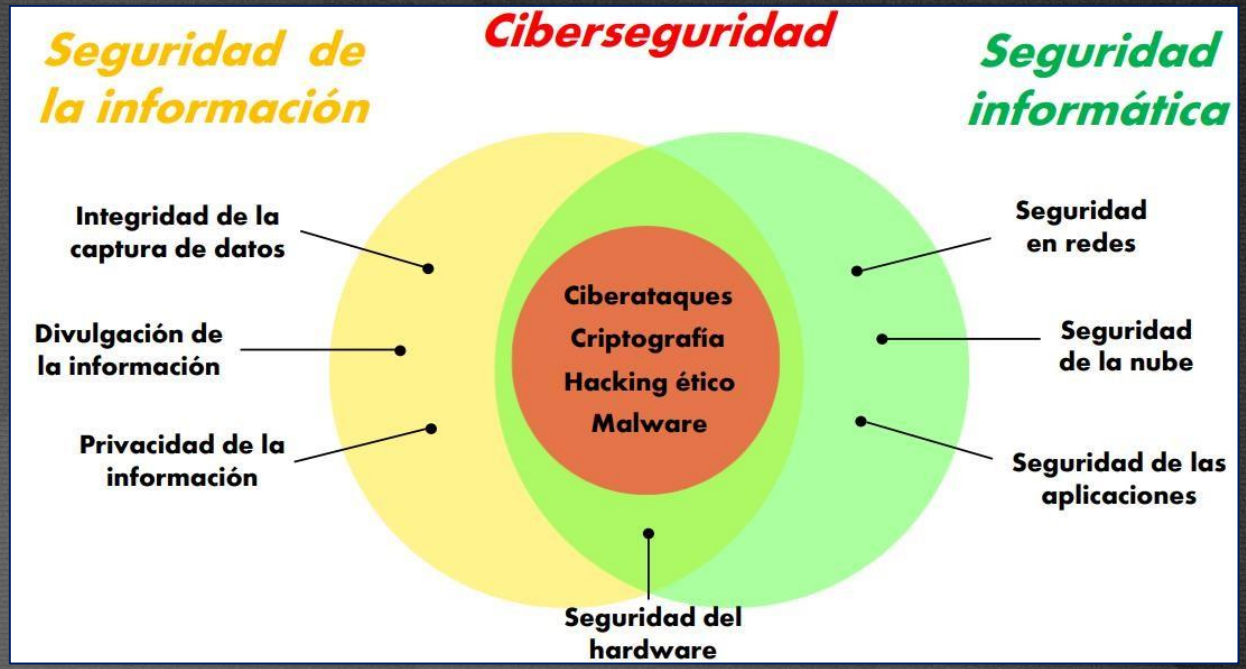
RHEL es otro sistema operativo estable, que ofrece muchas funcionalidades de administración y ciberseguridad en servidores a nivel empresarial. Además, recibe actualizaciones y parches constantemente, de ahí su gran atractivo. Sin embargo, este es de paga.

Los Dominios de la Seguridad que nos interesan son:

Seguridad de la información: Protege todo tipo de información física o digital, y su uso.

Seguridad informática: Protege software y hardware de todo tipo de riesgos y amenazas.

Ciberseguridad: Se especializa en combatir y prevenir ciberataques (amenazas contra infraestructuras puramente digitales y virtuales) (En esta se basa todo el presente trabajo).



(Diagrama orientativo)

La ciberseguridad tiene múltiples áreas (por ejemplo: peritaje judicial, informática forense, seguridad en redes, seguridad de bases de datos, etc…). Y un sinfín de conceptos técnicos para aprender (por ejemplo: payload, vector de ataque, DoS, XSS, MITM, inyección SQL o de comandos, desbordamiento de búfer, rootkit, etc…). El área que nos interesa es el **hacking ético.**

Dentro de esta, las prácticas de interés son las **pruebas de penetración** (simulación de un ciberataque, para identificar y posteriormente corregir vulnerabilidades) y la **explotación de vulnerabilidades** (aprovechamiento de debilidades en sistemas para comprometer su seguridad). Y para entender y llevar a cabo esas actividades, hay que entender primero los siguientes conceptos por separado…

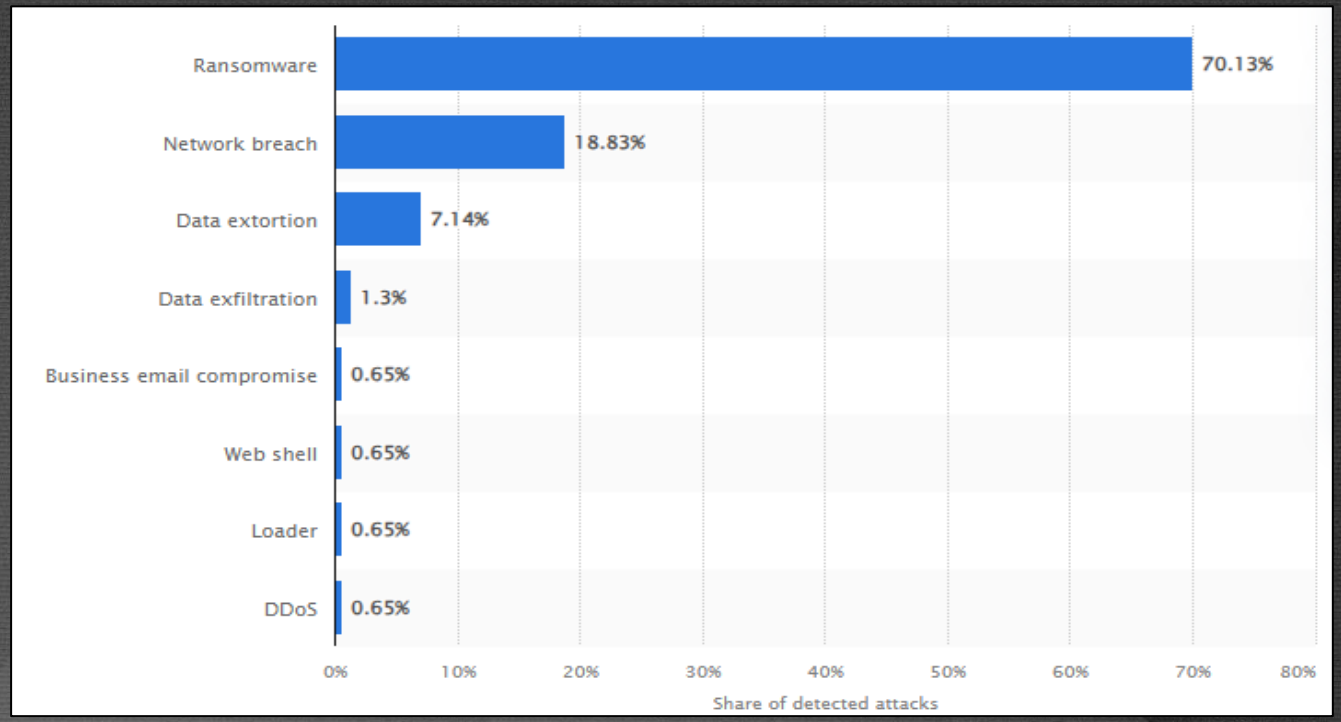
- ✓ **Vulnerabilidad:** debilidad o fallo en un sistema, aplicación o red que puede ser aprovechada por atacantes para causar daños de diversa naturaleza.

- ✓ **Explotación:** acción de aprovechar una vulnerabilidad de un sistema para comprometerlo. Esto implica una serie de fases (como reconocimiento, escaneo, mantenimiento de acceso, etc), herramientas (como las que veremos más adelante) y profundos conocimientos técnicos en diversos campos como redes, sistemas operativos, protocolos, servicios, programación, uso de memoria/almacenamiento, privilegios de administrador, etc.

- ✓ **Exploit:** conjunto de instrucciones, software o programa diseñado para aprovechar (explotar) una vulnerabilidad específica (o varias) en un sistema.

By Victim Count

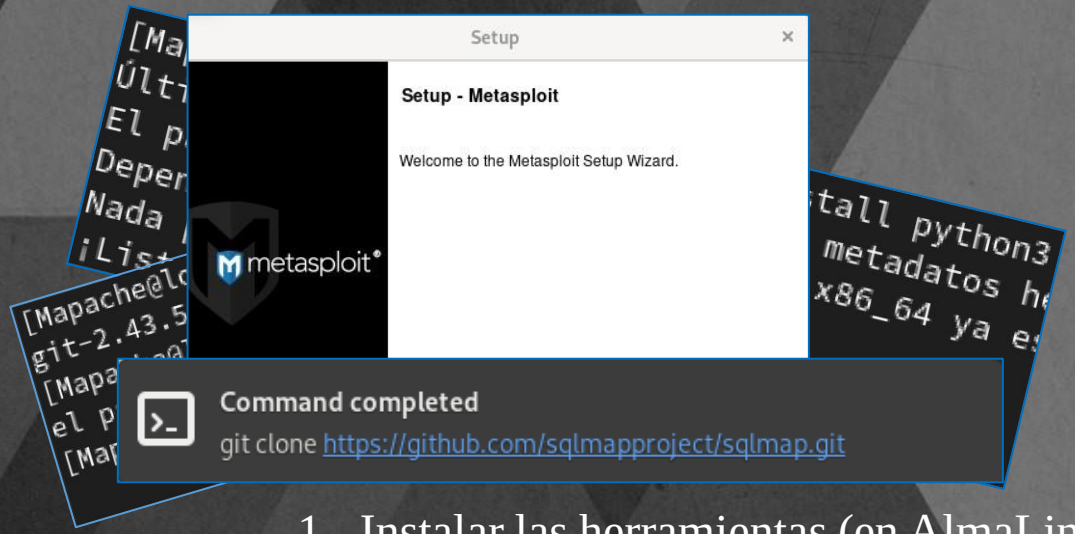
Crime Type	Victims	Crime Type	Victims
Phishing	300,497	Government Impersonation	11,554
Personal Data Breach	58,859	Advanced Fee	11,264
Non-Payment/Non-Delivery	51,679	Other	9,966
Extortion	39,416	Overpayment	6,183
Tech Support	32,538	Lottery/Sweepstakes/Inheritance	5,650
Investment	30,529	Data Breach	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		



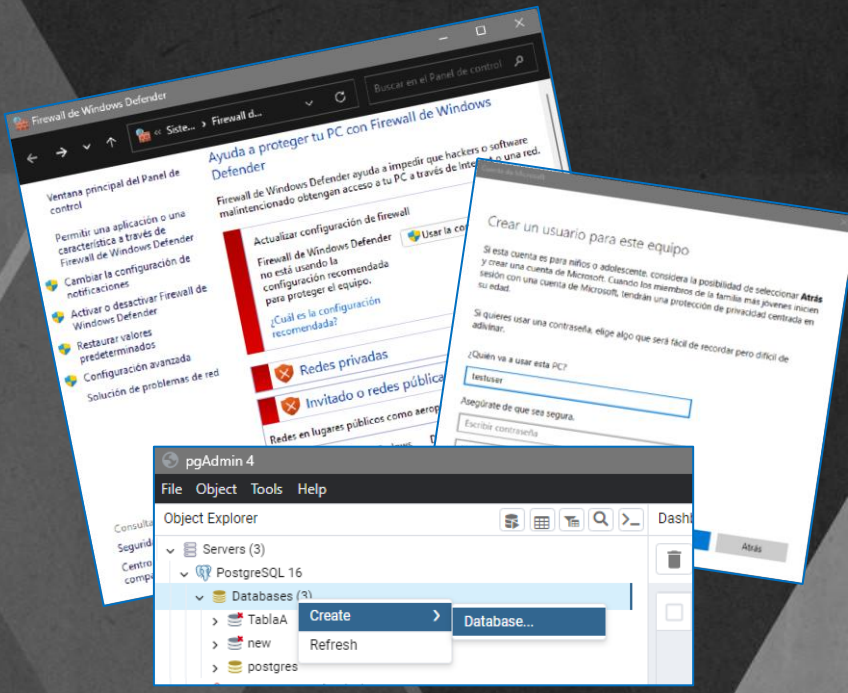
Cualquier ciberataque implica explotación de vulnerabilidades, ya sea en mayor o menor medida. Numerosas fuentes indican que desde siempre y hasta los más recientes años, los dos tipos de ciberataque más comunes son el phishing (junto a fugas de información, comúnmente relacionadas también con phishing), y el ransomware. Y casi siempre, estos dos ataques están muy relacionados con explotación de vulnerabilidades de software.

METODOLOGÍA

Después de instalar y comprobar el estado de cada herramienta, hay que preparar un escenario de ataque en nuestra máquina vulnerable (en este caso, Windows 11). Ya sea desactivando el firewall, creando usuarios sin contraseña, crear bases de datos mal configuradas, o lo que la prueba requiera, luego realizar el ataque, y documentar cada etapa.



1.- Instalar las herramientas (en AlmaLinux).



2.- Preparar escenarios vulnerables (en este caso: en Windows 11).

DESARROLLO

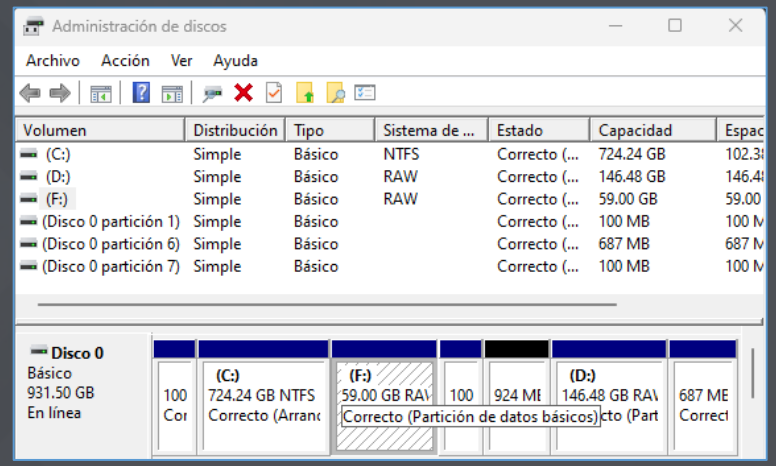
Para **esta investigación**, se usaron las siguientes especificaciones de software y hardware:

- ✓ Sistema operativo AlmaLinux 9.4 (Seafoam Ocelot) (una máquia física, y una máquina virtual) Para instalar las herramientas.

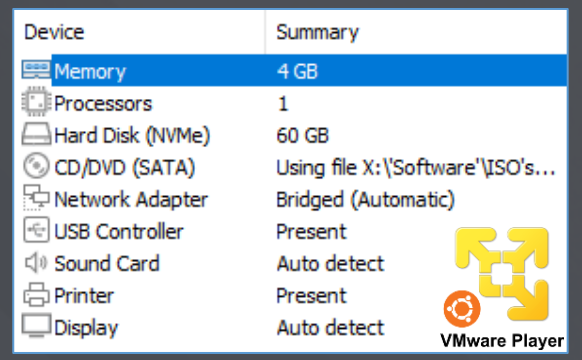
- ✓ Otro sistema operativo en máquina física o virtual para ocuparlo como sistema víctima (en este caso, Windows 11 física con diversos servicios y aplicaciones activas para atacar) (para Enum4Linux, usar Windows es obligatorio).

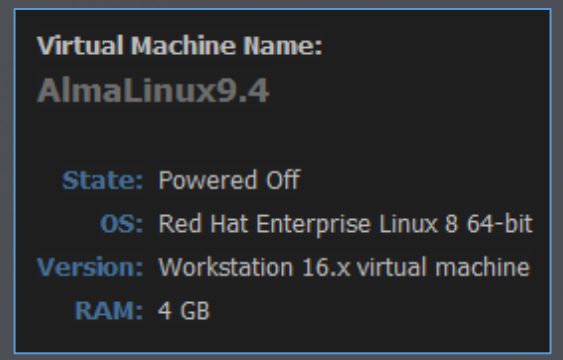
Para las dos instalaciones de AlmaLinux:

- ✓ Partición de 60GB en una unidad de almacenamiento M.2 (para aprovechar lo máximo posible el hardware disponible) (en este caso: 8GB de RAM, 1TB de almacenamiento en una unidad M.2, y un procesador Intel Core i3-8145U 2.10GHz).



- ✓ Máquina virtual VMware Workstation 16 player – Non commercial use (para pruebas y ensayos) **(opcional)**.





Instalamos cinco herramientas de ciberseguridad relacionadas con el análisis de vulnerabilidades en Alma Linux, y documentamos tanto instalación como uso. (Algunas requieren configuraciones adicionales para su instalación en esta distribución):

- ✓ **1:** Metasploit Framework
- ✓ **2:** SQLmap
- ✓ **3:** SearchSploit
- ✓ **4:** Enum4Linux
- ✓ **5:** SpamAssassin

# 1	Metasploit Framework
Categorías: ▪ Explotación de vulnerabilidades ▪ Pruebas de penetración	***Principales funcionalidades:*** ▪ Escaneo de vulnerabilidades ▪ Ejecución de payloads ▪ Automatización de pruebas
Descripción: Plataforma de pruebas de penetración que permite identificar, explotar y gestionar vulnerabilidades en sistemas mediante una gran colección de exploits, payloads y herramientas auxiliares.	

2 SQLmap

Descripción:

Herramienta diseñada para automatizar la detección y explotación de vulnerabilidades de inyección SQL. 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.

3 SearchSploit

Descripción:

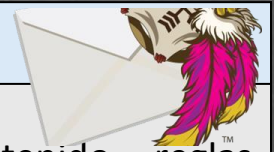
herramienta de línea de comandos que facilita la búsqueda de exploits y vulnerabilidades en la base de datos de Exploit Database. Ofrece resultados detallados, incluyendo títulos de exploits, rutas locales y enlaces a la base de datos en línea, todo a través de un repositorio local que se puede actualizar en cualquier momento.

4 Enum4Linux

Descripción:

Herramienta de escaneo que recopila y reporta información sobre sistemas Windows, como nombres de dominios, usuarios, grupos, políticas de seguridad. cuentas activas, y permisos.

5 SpamAssassin



Descripción:

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. (no está relacionado con escaneo de vulnerabilidades, pero puede servir para detectar/combatir phishing).

RESULTADOS

Tras la instalación, configuración y uso de las herramientas presentadas, logramos demostrar los casos de uso básicos de cada herramienta, a través de los escenarios propuestos.

```
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
```

1.- Escanear y mostrar los puertos abiertos de la víctima con Metasploit.

```
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] 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    |
+----+------------+----------+
```

2.- Recuperación y exportación en .csv de una tabla en una Base de datos PostgreSQL con SQLmap.

```
Microsoft Office 97 - HTMLMARQ.OCX Library Denial of Service                |
Microsoft Office Groove - 'Workspace Shortcut' Arbitrary Code Executi       |
Microsoft Office Groove 2007 - 'mso.dll' DLL Hijacking                      |
Microsoft Office OneNote 2010 - Crash (PoC)                                 |
Microsoft Office Outlook Recipient Control - 'ole32.dll' Denial of Se       |
Microsoft Office Picture Manager 2010 - Crash (PoC)                         |
Microsoft Office PowerPoint 2010 - 'MSO!Ordinal5429' Missing Length C       |
Microsoft Office PowerPoint 2010 - GDI 'GDI32!ConvertDxArray' Insuffi       |
Microsoft Office PowerPoint 2010 - Invalid Pointer Reference                |
Microsoft Office PowerPoint 2010 - MSO/OART Heap Out-of-Bounds Access       |
Microsoft Office Products - Array Index Bounds Error (PoC)                  |
Microsoft Office SharePoint Server 2007 - Remote Code Execution (MS10       |
Microsoft Office SharePoint Server 2016 - Denial of Service (Metasplo       |
Microsoft Office Web Components (OWC) Spreadsheet - ActiveX Buffer Ov       |
Microsoft Office Web Components (OWC) Spreadsheet - msDataSourceObjec       |
Microsoft Office Web Components Spreadsheet - ActiveX 'OWC10/11' Remo       |
Microsoft Office Word - '.RTF' Malicious HTA Execution (Metasploit)         |
Microsoft Office XP - Remote code Execution                                 |
Microsoft Office XP 2000/2002 - HTML Link Processing Remote Buffer Ov       |
Microsoft Office XP SP3 - '.PPT' File Buffer Overflow (MS08-016)            |
```

3.- Vulnerabilidades y exploits para Microsoft Office encontrados con SearchSploit.

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

[I] 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 ''
```

4.- Enumeración de usuarios en un sistema Windows, usando los SID (Security Identifier) encontrados por Enum4Linux.

```
[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
```

5.- Reporte completo del análisis de probabilidad de spam en un correo, según SpamAssassin (diagnóstico positivo) (correcto).

CONCLUSIONES

I) ¿Algunas de las herramientas se complementan entre sí?

Fueron desarrolladas por separado, y originalmente no están pensadas para complementarse directamente, pero las funcionalidades de cada una, pueden aportar valor a las otras.

II) ¿Se pueden mejorar de alguna manera?

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.

III) ¿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.

IV) ¿Es mejor una que otra?

Al tratar cada una un área diferente, no podemos compararlas directamente. pero dentro de sus áreas, sí podemos asignarles calificaciones generales y observaciones específicas.

	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 ligeramente 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 histórica/referencial, no es 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 cinco presentes. Y se limita a escanear sólo Windows.
SpamAssassin (9/10)	Curva de aprendizaje baja, y resultados altamente efectivos. Reportes detallados.	Lo recomendable es automatizar su uso, pero eso puede resultar muy laborioso.

V) Entre los Sectores: Educativo, empresarial, gubernamental, automotriz y farmacéutico (salud). ¿cuál herramienta es la más apropiada para proteger qué sector?

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	*%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*

CONCLUSIONES FINALES

- ✓ La mejor forma de utilizar estas herramientas es conociendo lo más a fondo que podamos, la teoría de lo que estamos haciendo. (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).
- ✓ Ya que en esta investigación se trató con herramientas que no han sido muy documentadas para Alma Linux, debemos tener en cuenta que en escenarios como este, muchas cosas pueden salir mal, las herramientas pueden requerir muchas configuraciones manuales adicionales y profundas. Y aún así no siempre se puede garantizar el funcionamiento de las herramientas.

- ✓ El trabajo a futuro de esta investigación consiste en Buscar escenarios y resultados más robustos para cada una de las herramientas presentadas. Implementar las mejoras sugeridas en la pregunta (II) (13.2 en la ***documentación completa***) y por último, agregar más documentación de las mismas herramientas, de otras (ya probadas o no en AlmaLinux) e incluso las que intentamos documentar aquí pero no lo conseguimos (Veil Framework y OpenVas)

REFERENCIAS

1 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

2 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

3Techopedia. (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

4 Zubieta Moreno, J. (201S). Ciberdiccionario: Conceptos de ciberseguridad en lenguaje #Entendible.

[5] García-Moran, J. P. (2011). Hacking y Seguridad en Internet. Grupo Editorial RA-MA.

[C] Offsec. (2024). Kali Linux Tools. Recuperado el 5 de Septiembre de 2024, de https://www.kali.org/tools/