

# Informe de Prueba de Penetración de DeathStar

M16 - Ciberseguridad y Hacking ético

**Por**

Biel Martín de Diego

Versión 1.0



**DJIBRIL**  
**BIEL**

---

**VulnHub**

M16 - Ciberseguridad y Hacking ético  
Copyright © Biel Martín de Diego

## Tabla de Contenidos

<b>RESUMEN DE LA EVALUACIÓN.....</b>	<b>3</b>
<b>COMPONENTES DE LA EVALUACIÓN .....</b>	<b>3</b>
<b>PRUEBA DE PENETRACIÓN INTERNA .....</b>	<b>3</b>
<b>PRUEBA DE PENETRACIÓN DE LA APLICACIÓN WEB.....</b>	<b>3</b>
<b>FACTORES DE RIESGO.....</b>	<b>5</b>
<b>PROBABILIDAD .....</b>	<b>5</b>
<b>IMPACTO .....</b>	<b>5</b>
<b>ÁMBITO.....</b>	<b>5</b>
<b>RESUMEN EJECUTIVO.....</b>	<b>6</b>
<b>RESUMEN DE PRUEBAS .....</b>	<b>6</b>
<b>HALLAZGOS TÉCNICOS .....</b>	<b>7</b>
<b>PRUEBA DE CONCEPTO DE EXPLOTACIÓN .....</b>	<b>9</b>
<b>ESCANEADO DE PUERTOS.....</b>	<b>9</b>
<b>ESCANEADO DE MOVIMIENTOS EN LA RED .....</b>	<b>9</b>
<b>USO DEL PUERTO 1440 .....</b>	<b>10</b>
<b>DESCIFRADO DEL TEXTO CODIFICADO .....</b>	<b>11</b>
<b>APERTURA DE PUERTO FILTRADO .....</b>	<b>12</b>
<b>ACCESO POR SSH.....</b>	<b>12</b>
<b>ESCALADA DE PRIVILEGIOS .....</b>	<b>13</b>

# Resumen de la Evaluación

Las fases de las actividades de prueba de penetración incluyen lo siguiente:

- Planificación – Se recopilan los objetivos del cliente y se obtienen las reglas de participación.
- Descubrimiento – Se realizan escaneos y enumeración para identificar posibles vulnerabilidades, áreas débiles y exploits.
- Ataque – Se confirman las posibles vulnerabilidades a través de la explotación y se realiza un descubrimiento adicional tras obtener un nuevo acceso.
- Informe: Se documentan todas las vulnerabilidades y exploits encontrados, intentos fallidos, y las fortalezas y debilidades de la máquina.

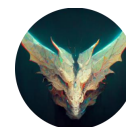
## Componentes de la Evaluación

### Prueba de Penetración Interna

Una prueba de penetración interna simula el papel de un atacante desde dentro de la red. Un ingeniero escaneará la red para identificar posibles vulnerabilidades en los hosts y llevará a cabo ataques comunes y avanzados en la red interna. El ingeniero buscará obtener acceso a los hosts mediante movimientos laterales, comprometer cuentas de usuario y administrador del dominio, y filtrar datos sensibles.

### Prueba de Penetración de la Aplicación Web

Una prueba de penetración de la aplicación web es una prueba de penetración detallada en las secciones no autenticadas y autenticadas del sitio web. El ingeniero probará todas las fallas de seguridad, así como diversas vulnerabilidades potenciales según las mejores prácticas de seguridad. Las actividades incluyen el mapeo del sitio web, enumeración de directorios, pruebas de inyección automatizadas y manuales, pruebas de traversing de directorios, carga de archivos maliciosos y ejecución remota de código, ataques de contraseñas y omisiones de autenticación, ataques de sesión, y otras pruebas según el contenido y los lenguajes específicos del sitio.



## Calificación de Severidad

La siguiente tabla define niveles de severidad y el rango correspondiente de puntuación CVSS que se utiliza en todo el documento para evaluar la vulnerabilidad.

Severidad	Rango de Puntuación CVSS V3	Definición
<b>Crítica</b>	9-10	La explotación es sencilla y generalmente el sistema resulta comprometido.
<b>Alta</b>	7-8	La explotación es más difícil, pero podría provocar privilegios elevados y potencialmente pérdida de datos o tiempo de inactividad.
<b>Moderada</b>	4-6	Existen vulnerabilidades, pero no son explotables o requieren pasos adicionales como la ingeniería social.
<b>Baja</b>	1-3	Las vulnerabilidades no son explotables, pero reducirían la superficie de ataque de la máquina.
<b>Informativa</b>	N/A	No existe ninguna vulnerabilidad. Se proporciona información adicional sobre elementos observados durante las pruebas, controles sólidos y documentación adicional.

## Factores de Riesgo

El riesgo se mide mediante dos factores: **Probabilidad** e **Impacto**:

### Probabilidad

La probabilidad mide el potencial de que una vulnerabilidad sea explotada. Las calificaciones se otorgan según la dificultad del ataque, las herramientas disponibles, el nivel de habilidad del atacante y el entorno de la máquina.

### Impacto

El impacto mide el efecto potencial de la vulnerabilidad en las operaciones, incluyendo la confidencialidad, integridad y disponibilidad de los sistemas y/o datos de la máquina, el daño a la reputación y la pérdida financiera de una hipotética empresa.

## Ámbito

Evaluación	Detalles
Prueba de Penetración Interna	10.40.2.0/24   10.40.2.28

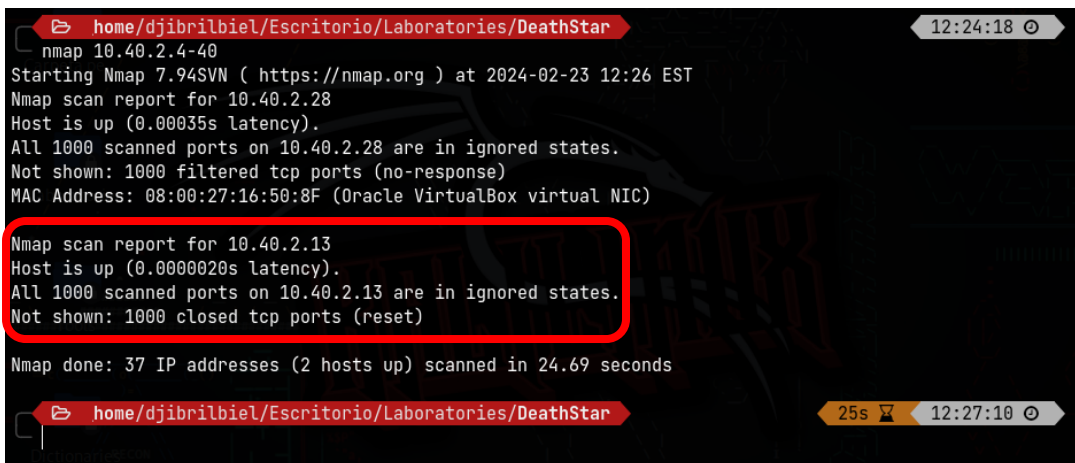
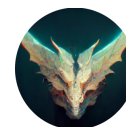


Figura 1: Evidencia de escaneo de red y puertos.

### VulnHub

M16 - Ciberseguridad y Hacking ético  
Copyright © Biel Martín de Diego



## Resumen Ejecutivo

Evalué la postura de seguridad del examen de. Al aprovechar una serie de ataques, encontré vulnerabilidades de nivel crítico que aproveché para acceder en la máquina.

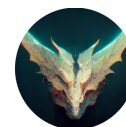
### Resumen de Pruebas

Se encontraron vulnerabilidades tanto en la “Prueba de Penetración de la Aplicación Web” como en la “Prueba de Penetración Interna”.

1	1	0	0	0
Crítica	Alta	Moderada	Baja	Informativa

Número de Vulnerabilidades Totales	2
------------------------------------	---

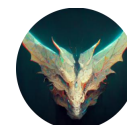
Hallazgo	Severidad
<u>Prueba de Penetración de la Aplicación Web</u>	
IPT-001: Desbordamiento de búfer en /bin/dartVader <b>(posiblemente)</b>	Crítica
IPT-002: Fallo en el filtrado de puertos TCP	Alta



## Hallazgos Técnicos

### **IPT:001 – Desbordamiento de búfer en /bin/dartVader (Crítica)**

<b>Descripción:</b>	El archivo ejecutable "/bin/dartVader" contiene una vulnerabilidad de desbordamiento de búfer en el segundo parámetro de ejecución, lo que podría permitir a un atacante ejecutar código arbitrario en el sistema.
<b>Sistemas:</b>	Archivo "/bin/dartVader" en la máquina DeathStar (IP: 10.40.2.28)
<b>Riesgo:</b>	<p>Probabilidad - Baja: La explotación de esta vulnerabilidad requeriría habilidades técnicas avanzadas por parte del atacante.</p> <p>Impacto - Crítico: Dado que esta vulnerabilidad permitiría a un atacante ejecutar código arbitrario con privilegios elevados, el impacto potencial de su explotación sería catastrófico. Podría conducir a la toma completa del control del sistema y la exposición de datos críticos.</p>

**IPT:002 – Fallo en el filtrado de puertos TCP (Alta)**

<b>Descripción:</b>	El puerto 10110/TCP está incorrectamente filtrado, lo que podría permitir a un atacante eludir restricciones de red y acceder a servicios no autorizados.
<b>Sistemas:</b>	Puerto 10110/TCP de la máquina DeathStar (IP: 10.40.2.28)
<b>Riesgo:</b>	<p>Probabilidad - Moderada: Existe una posibilidad significativa de que un atacante intente abrir los puertos TCP de la máquina para descubrir servicios ocultos, especialmente dada la información oculta de la imagen.</p> <p>Impacto -Alto: Si un atacante logra descubrir servicios sensibles, podría utilizarlos para comprometer la integridad del sistema o robar información confidencial, lo que tendría un impacto negativo en la seguridad de la red y la privacidad de los datos.</p>

```
home/djibrilbiel/Escritorio/Laboratories/DeathStar 15:54:23
steghide extract -sf image.jpg
Anotar salvoconducto:
anotar los datos extraídos e/"openTheExhaust.txt".

home/djibrilbiel/Escritorio/Laboratories/DeathStar 9s 15:54:35
cat openTheExhaust.txt
Each segment of the "unlock code" can only contain 3 characters sent in sequence to unlock port 10110.

home/djibrilbiel/Escritorio/Laboratories/DeathStar 15:54:41
```

Figura 2: Evidencia de la vulnerabilidad IPT:002



# Prueba de Concepto de Explotación

## Escaneo de Puertos

Se realizó un escaneo inicial de los primeros 1000 puertos utilizando la herramienta de escaneo de puertos sin éxito en los puertos TCP, lo que indicaba que todos los puertos estaban filtrados.

```
home/djibrilbiel/Escritorio/Laboratories/DeathStar 13:28:57
nmap -A 10.40.2.28
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-23 13:29 EST
Nmap scan report for 10.40.2.28
Host: 10.40.2.28 (10.40.2.28)
All 1000 scanned ports on 10.40.2.28 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:16:50:0F (Oracle VM VirtualBox virtual NIC)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT ADDRESS
1 0.54 ms 10.40.2.28

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.81 seconds
```

Se procedió a realizar un escaneo de puertos UDP, revelando que de los primeros 1000 puertos, 788 estaban cerrados y 212 estaban abiertos pero filtrados.

```
home/djibrilbiel/Escritorio/Laboratories/DeathStar 13:38:21
nmap -sU -T5 10.40.2.28
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-23 13:38 EST
Warning: 10.40.2.28 giving up on port because retransmission cap hit (2).
Nmap scan report for 10.40.2.28
Host: 10.40.2.28 (10.40.2.28)
All 1000 scanned ports on 10.40.2.28 are in ignored states.
Not shown: 788 closed udp ports (port-unreach), 212 open/filtered udp ports (no-response)
MAC Address: 08:00:27:16:50:0F (Oracle VM VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 858.82 seconds
```

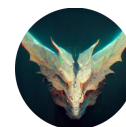
## Escaneo de Movimientos en la Red

Dado que todos los puertos parecían estar cerrados o filtrados, se llevó a cabo un análisis de la actividad de red utilizando Wireshark. Durante el análisis, se observaron dos paquetes enviados desde la máquina DeathStar.

No.	Time	Source	Destination	Protocol	Length	Info
181	69.490572846	10.40.2.28	10.40.2.13	ICMP	110	Destination unreachable (Port unreachable)
182	70.290944897	10.40.2.13	10.40.2.28	UDP	42	50110 → 772 Len=0
183	70.291260631	10.40.2.28	10.40.2.13	ICMP	70	Destination unreachable (Port unreachable)
184	71.104897418	10.40.2.13	10.40.2.28	UDP	42	50110 → 17146 Len=0
185	71.105779532	10.40.2.28	10.40.2.13	ICMP	70	Destination unreachable (Port unreachable)
186	71.954706006	10.40.2.13	10.40.2.28	UDP	82	50110 → 38412 Len=40
187	71.955040100	10.40.2.28	10.40.2.13	ICMP	110	Destination unreachable (Port unreachable)
188	72.757199231	10.40.2.13	10.40.2.28	UDP	82	50110 → 32818 Len=40
189	73.040543469	10.40.2.28	255.255.255.255	UDP	139	33647 → 357 Len=97
190	73.043221795	10.40.2.28	255.255.255.255	UDP	514	45120 → 160 Len=472
191	73.507190904	10.40.2.13	10.40.2.28	UDP	82	50110 → 32618 Len=40
192	73.507490148	10.40.2.28	10.40.2.13	ICMP	110	Destination unreachable (Port unreachable)
193	74.370979547	10.40.2.13	10.40.2.28	UDP	42	50110 → 17585 Len=0
194	74.371209569	10.40.2.28	10.40.2.13	ICMP	70	Destination unreachable (Port unreachable)
195	75.171807524	10.40.2.13	10.40.2.28	UDP	42	50110 → 17332 Len=0
196	75.172318703	10.40.2.28	10.40.2.13	ICMP	70	Destination unreachable (Port unreachable)
197	76.023804539	10.40.2.13	10.40.2.28	UDP	42	50110 → 838 Len=0
198	76.024132379	10.40.2.28	10.40.2.13	ICMP	70	Destination unreachable (Port unreachable)
199	76.833788709	10.40.2.13	10.40.2.28	UDP	82	50110 → 42508 Len=40

VulnHub

M16 - Ciberseguridad y Hacking ético  
Copyright © Biel Martín de Diego



El primer paquete contenía un código de acceso "DS-1@OBS", mientras que el segundo proporcionaba pistas adicionales, incluyendo intentos para utilizar el código de acceso cada 60 segundos y la mención de un número: 1440, cuyo propósito no estaba claro en ese momento.

```
0000 ff ff ff ff ff ff 08 00 27 16 50 8f 08 00 45 00 ..... ' P . E
0010 01 f4 69 35 40 00 40 11 c3 80 0a 28 02 1c ff ff ...15@_@_... (
0020 ff ff b0 40 00 a0 01 e0 78 eb 0a 54 68 61 6e 6b ...@_... x .Thank
0030 73 20 74 6f 20 74 68 65 20 73 75 63 63 65 73 73 s to the success
0040 66 75 6c 20 4f 70 65 72 61 74 69 6f 6e 20 53 6b ful Oper ation Sk
0050 79 68 6f 6f 6b 2c 20 74 68 65 20 52 65 62 65 6c yhook, t he Rebel
0060 20 41 6c 6c 69 61 6e 63 65 9a 6f 6f 74 20 73 6f Allianc e.got so
0070 6d 65 20 70 6c 61 6e 73 20 66 6f 72 20 74 68 65 me plans for the
0080 20 6e 65 77 20 77 65 61 70 6f 6e 20 6f 66 20 74 new wea pon of t
0090 68 65 20 47 61 6c 61 63 74 69 63 20 45 6d 70 69 he Galac tic Empl
00a0 72 65 2e 20 57 65 0a 6b 6e 6f 77 20 74 68 61 74 re. We-k now that
00b0 20 74 68 65 72 65 20 69 73 20 61 20 73 6d 61 6c there i s a smal
00c0 6c 20 6f 70 65 6e 69 6e 67 20 74 68 61 74 20 77 l openin g that w
00d0 65 20 63 61 6e 20 65 78 70 6c 6f 72 65 20 74 68 e can ex plore th
00e0 72 6f 75 67 68 20 61 6a 74 68 65 72 6d 61 6c 20 rough a thermal
00f0 65 78 68 61 75 73 74 20 74 68 61 74 20 69 73 20 exhaust that is
0100 64 69 72 65 63 74 6c 79 20 63 6f 6e 6e 65 63 74 directly connect
0110 65 64 20 74 6f 20 74 68 65 20 4d 61 69 6e 20 52 ed to th e Main R
0120 65 61 63 74 6f 72 20 6f 66 20 74 68 65 0a 44 65 eactor o f the De
0130 61 74 68 20 53 74 61 72 2e 20 54 68 65 20 73 75 ath Star . The su
0140 70 65 72 6c 61 73 65 72 20 74 61 6b 65 73 20 31 perlas er takes 1
0150 34 34 30 20 6d 69 6e 75 74 65 73 20 74 6f 20 72 440 minu tes to r
0160 55 6c 6f 61 64 2e 0a 49 74 20 69 73 20 76 65 72 eload. I t is ver
0170 79 20 69 6d 70 6f 72 74 61 6e 74 20 74 6f 20 6f y import ant to o
0180 62 73 65 72 76 65 20 27 74 68 69 73 20 77 69 6a bserve ' this win
0190 64 6f 77 27 20 69 6e 20 6f 72 64 65 72 20 74 6f dow' in order to
01a0 20 72 65 63 6f 76 65 72 20 74 68 65 20 62 6c 75 recover the blu
01b0 65 70 72 69 6e 74 2e 0a 54 68 69 73 20 69 73 20 eprint. This is
01c0 62 65 63 61 75 73 65 2c 20 69 74 20 69 73 20 6f because, it is o
01d0 6e 6c 79 20 70 6f 73 73 69 62 6c 65 20 74 6f 20 nly poss ible to
01e0 6d 61 6b 65 20 61 6e 20 61 74 74 65 6d 70 74 20 make an attempt
01f0 65 76 65 72 79 20 30 30 20 73 65 63 6f 6e 64 73 every 60 seconds
0200 2e 0a
```

## Uso del puerto 1440

Se identificó que el puerto 1440 estaba filtrado en TCP pero abierto en UDP.

```
home/djibrilbiel/Escritorio/Laboratories/DeathStar 13:57:11
nmap -p 1440 -A -sS -sU 10.40.2.28
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-23 13:57 EST
Nmap scan report for 10.40.2.28
Host is up (0.00061s latency).

PORT      STATE SERVICE VERSION
1440/tcp  filtered eicon-slp
1440/udp  open   eicon-slp?

MAC Address: 08:00:27:16:50:8f (Oracle VirtualBox virtual NIC)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT ADDRESS
1 0.61 ms 10.40.2.28

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.18 seconds

home/djibrilbiel/Escritorio/Laboratories/DeathStar 18s 13:58:03
```

Se decidió enviar el código de acceso recibido anteriormente ("DS-1@OBS") a través del puerto 1440, ya que estaba abierto, y se procedió a capturar y analizar la respuesta.

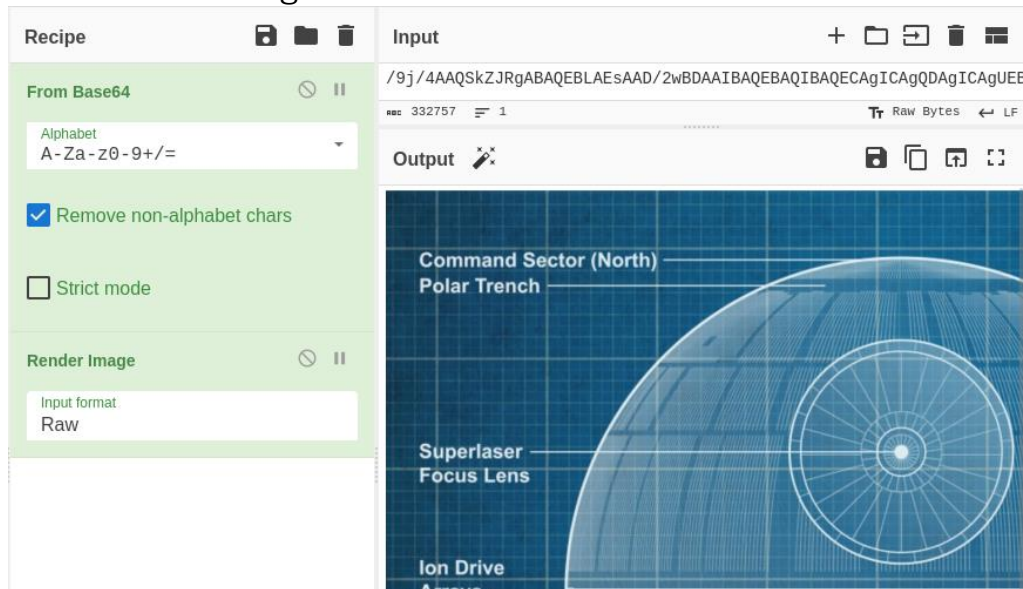
```
home/djibrilbiel/Escritorio/Laboratories/DeathStar 15:27:17
echo "DS-1@OBS" | nc -u 10.40.2.28 1440 > return
```

Se encontró un texto codificado en Base64 en la respuesta.

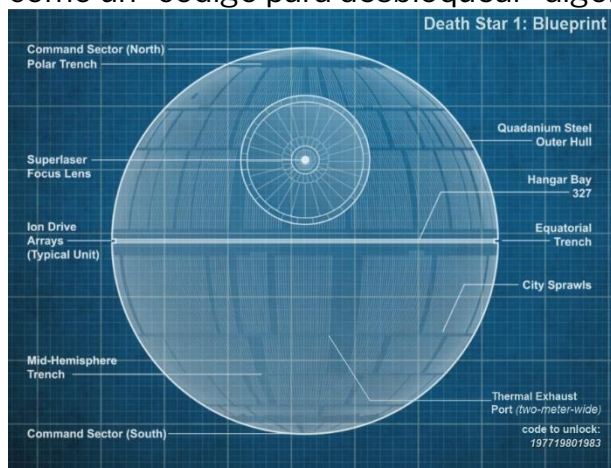
```
home/djibrilbie/Escritorio/Laboratorios/DeathStar 17:07:15
cat image.txt
/9j/4AAQSkZJRgABAQEBALEAAAD/2wBDAAIIBAQBGAQEBAQECAGICAgQDAGICAgUEBAMEBGUGBgYFBGkIBGcJBWYGCAICQoKCgoKBggLDASKDAKAChCkr
2wBDAQICAgICAgUDAwUKBwYHCGoKCgoKCgoKCgoKCgoKCgoKCgoKCgoKCgoKCgoKCgoKCgoKCgoKCgoKCgoKCgoKCgoKCgoKCgoKCgoKCgoKCgoKCgr/wAARCAKwAQDASIAAhEBAXeB/8QA
HwaAAAAUBAQEBAEAAAAAAAAEAACawFbgICQoL/8QATRAAAEDAwIEAwUFBAAQAAF9AQIDAAQRBRIhMUEGE1FhBgJxFDKBaEIIOkwRVSOFAkHM2Jyggk
```

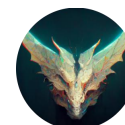
## Descifrado del Texto Codificado

El texto codificado en Base64 fue procesado utilizando la herramienta Cyberchef, revelando una imagen.



Al analizar la imagen, se descubrió un número en la esquina inferior derecha, identificado como un "código para desbloquear" algo.





## Apertura de Puerto Filtrado

Se utilizó la herramienta "stehide" para extraer información oculta de la imagen, revelando un mensaje que indicaba que un "código de desbloqueo" debía enviarse en secuencias de 3 caracteres para abrir el puerto 10110.

```
home/djibrilbiel/Escritorio/Laboratories/DeathStar 15:54:23
steghide extract -sf image.jpg
Anotar salvoconducto:
anotar los datos extraídos e/"openTheExhaust.txt".

home/djibrilbiel/Escritorio/Laboratories/DeathStar 9s 15:54:35
cat openTheExhaust.txt
Each segment of the "unlock code" can only contain 3 characters sent in sequence to unlock port 10110.

home/djibrilbiel/Escritorio/Laboratories/DeathStar 15:54:41
```

Se encontró el comando "knock" que permite realizar esta secuencia específica de conexiones de red, lo que resultó en la apertura exitosa del puerto 10110/tcp.

```
home/djibrilbiel/Escritorio/Laboratories/DeathStar 15:57:46
knock -v 10.40.2.28 197 719 801 983
hitting tcp 10.40.2.28:197
hitting tcp 10.40.2.28:719
hitting tcp 10.40.2.28:801
hitting tcp 10.40.2.28:983

home/djibrilbiel/Escritorio/Laboratories/DeathStar 16:01:37
nmap -p 10110 -A -sS -sU 10.40.2.28
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-23 16:02 EST
Nmap scan report for 10.40.2.28
Host is up (0.0011s latency).

PORT      STATE SERVICE VERSION
10110/tcp open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 2048 04:77:fb:4d:59:ef:ea:73:b7:f6:30:57:90:0c:78:81 (RSA)
|_ 256 82:dc:9d:9e:a8:a0:ba:36:a9:6f:e4:9d:5e:96:fa:ae (ECDSA)
10110/udp closed nmap-0183
MAC Address: 08:00:27:16:50:8F (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.10 - 4.11, Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT ADDRESS
1 1.09 ms 10.40.2.28

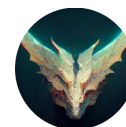
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.69 seconds

home/djibrilbiel/Escritorio/Laboratories/DeathStar 16:02:09
```

## Acceso por SSH

Con el puerto 10110/tcp abierto, se intentó el acceso por SSH. Dado que no se disponía de un usuario, se intentó acceder como "root". Se encontró información adicional, incluyendo un usuario "erso" y una contraseña encriptada que se basaba en el nombre y año de fallecimiento de la esposa de Galen Walton Erso.





```
home/djibrilbiel/Escritorio/Laboratories/DeathStar 16:36:51
ssh -p 10110 root@10.40.2.28

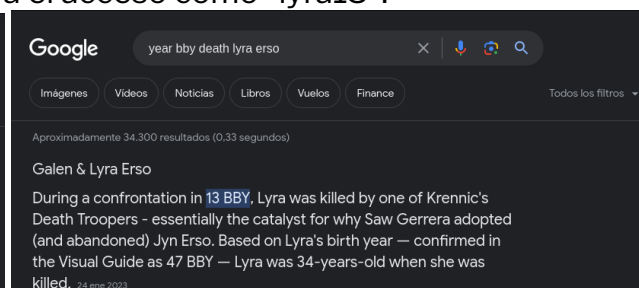
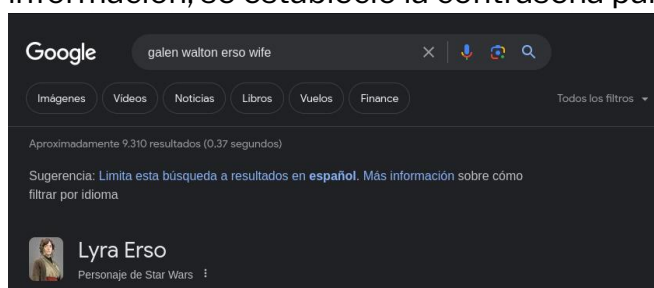
DEATHSTAR

Devoloped by Galen Walton Erso
System's user: erso
Pass Hint: My wife's first name plus the year (BBY) she died.

Glory to the Empire - Project DS-1: Orbital Battle Station

root@10.40.2.28's password: |
```

Utilizando las pistas proporcionadas anteriormente, se llevó a cabo una búsqueda en línea y se confirmó que la esposa se llamaba Lyra y que falleció en el año 13 (ABY). Con esta información, se estableció la contraseña para el acceso como "lyra13".



```
home/djibrilbiel/Escritorio/Laboratories/DeathStar 16:46:57
ssh -p 10110 erso@10.40.2.28

DEATHSTAR

Devoloped by Galen Walton Erso
System's user: erso
Pass Hint: My wife's first name plus the year (BBY) she died.

Glory to the Empire - Project DS-1: Orbital Battle Station

erso@10.40.2.28's password:
Welcome to Ubuntu 14.04.1 LTS (GNU/Linux 4.4.0-146-generic i686)

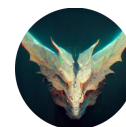
* Documentation:  https://help.ubuntu.com/

System information disabled due to load higher than 2.0

Last login: Thu Feb 22 10:47:40 2024 from 10.40.2.13
erso@deathStar1:~$ |
```

## Escalada de Privilegios

Al explorar el sistema, se encontró un archivo llamado "warning.txt" que no proporcionaba mucha información.



```
erso@deathStar1:~$ cat warning.txt

Message from GALEN ERSO:

This is your chance. Destroy the plans of the Galactic Empire. I know that Lord Vader will not like this at all. But, this will be my chance for redemption. I hope you have enough knowledge to help destroy this new weapon.

Explore the system and get 'root access' to read the secret message located at '/root/message.txt'.

Hack or fail!!

erso@deathStar1:~$
```

Además, se identificó un archivo ejecutable llamado `"/bin/dartVader"` que indicaba en portugués: `"dartVader: Tienes un futuro así. No seas un Lammer, busca y aprende de verdad..."`.

```
erso@deathStar1:/bin$ ls -l | grep dartVader
-rwsr-xr-x 1 root root 7338 Nov 7 2019 dartVader
erso@deathStar1:/bin$ ./dartVader
dartVader: Voce tem um futuro aqui. Nao seja um Lammer, busque e aprenda realmente...

erso@deathStar1:/bin$
```

Dada la sospecha de una posible vulnerabilidad, se tomó la precaución de trasladar este archivo al entorno de prueba en Kali Linux para realizar un análisis exhaustivo.

```
home/djibrilbiel/Escritorio/Laboratories/DeathStar 16:59:53
scp -P 10110 -q erso@10.40.2.28:/bin/dartVader ./
erso@10.40.2.28's password:

home/djibrilbiel/Escritorio/Laboratories/DeathStar 8s 17:00:04
ls -l | grep dartVader
-rwxr-xr-x 1 root root 7338 feb 23 17:00 dartVader

home/djibrilbiel/Escritorio/Laboratories/DeathStar 17:00:08
```

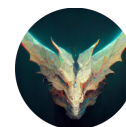
Tras una minuciosa investigación en Kali Linux, se detectó una vulnerabilidad potencial en el archivo `"/bin/dartVader"`. Concretamente, sospecho que dicho archivo podría estar expuesto a un desbordamiento de búfer en el segundo parámetro de ejecución.

```
home/djibrilbiel/Escritorio/Laboratories/DeathStar 17:01:17
objdump -d dartVader > dartVader.asm
```

El siguiente paso es analizar el código ensamblador proporcionado para comprender qué hace el ejecutable. Al observar el desensamblado de la sección ``.text``, parece que el programa primero verifica si se le ha pasado un argumento en la línea de comandos. Si no se proporciona un argumento, el programa imprime un mensaje de error y sale.

Luego, el programa parece realizar una operación de copia (posiblemente insegura) con la función ``strcpy``. Este es un punto potencialmente débil en el programa, ya que ``strcpy`` puede ser vulnerable a ataques de desbordamiento de búfer si no se usa correctamente.

Sin embargo, es importante destacar, que, hasta la fecha actual, 23 de febrero, esta vulnerabilidad no la he podido explotar ni confirmar con éxito alguno.



---

### **VulnHub**

M16 - Ciberseguridad y Hacking ético  
Copyright © Biel Martín de Diego