AD_Recon/SecurityAssessment.ps1 at dde2daba9b3393a9388cbebda87068972cc0bd3b · projectHULK/AD_Recon · GitHub · 02/11/2024 16:19

https://github.com/projectHULK/AD_Recon/blob/dde2daba9b3393a9388cbebda87068972cc0bd3b/SecurityAssessment.ps1#L2699

Product ⌄   Solutions ⌄   Resources ⌄   Open Source ⌄   Enterprise ⌄   Pricing

🔍   Sign in   Sign up

☐ **projectHULK** / **AD_Recon**   Public

🔔 Notifications   ⑂ Fork 0   ☆ Star 13

<> Code   ⊙ Issues   ⑂ Pull requests   ▶ Actions   ▣ Projects   🛡 Security   📈 Insights

⟤ Files

AD_Recon / SecurityAssessment.ps1 ⧉

⌥ History

🎋 dde2dab ⌄   🔍

🔍 Go to file

> 📁 ACLight
> 📁 ADAPE-Script
> 📁 ADFind
> 📁 ADModule
> 📁 ADReaper
> 📁 ADRecon
> 📁 ASREPRoast
> 📁 BrowersData
> 📁 Certify
> 📁 DomainPasswordSpray
> 📁 DonPAPI
> 📁 ForgeCert
> 📁 Get-LAPSPasswords
> 📁 Get-SPN
> 📁 Group3r
> 📁 Inveigh
> 📁 Koh
> 📁 LAPSToolkit
> 📁 LaZagne
> 📁 Lockless
> 📁 NetCease
> 📁 PPLKiller
> 📁 PPLdump
> 📁 PoisonHandler
> 📁 PoshC2
> 📁 PowerSCCM
> 📁 PowerUpSQL
> 📁 Powermad
> 📁 PrivilegeEscalationTools
> 📁 RdpThief
> 📁 Responder-Windows
> 📁 RestrictedAdmin
> 📁 Rubeus
> 📁 SCShell
> 📁 SQLcmd
> 📁 SafetyKatz

Code   Blame   3093 lines (2742 loc) · 143 KB   Raw ⧉ ⬇ <>

```
 1
 2    <#
 3        Author: Cube0x0
 4        License: BSD 3-Clause
 5    #>
 6    Function Get-SpoolStatus {
 7        <#
 8        https://github.com/vletoux/SpoolerScanner
 9
10        .OUTPUT
11        PS > Get-SpoolStatus -ComputerName localhost
12        ComputerName Status
13        ------------ ------
14        localhost    False
15        dc           True
16        #>
17        Param(
18        [parameter(Mandatory=$true,ValueFromPipeline=$true,ValueFromPipelineByPropertyN
19        [string[]]$ComputerName
20        )
21        $sourceSpooler = @"
22    using System;
23    using System.Collections.Generic;
24    using System.Diagnostics;
25    using System.Runtime.InteropServices;
26    using System.Security.Permissions;
27    using System.Text;
28
29    namespace PingCastle.ExtractedCode
30    {
31        public class rprn
32        {
33            [DllImport("Rpcrt4.dll", EntryPoint = "RpcBindingFromStringBindingW",
34            CallingConvention = CallingConvention.StdCall,
35            CharSet = CharSet.Unicode, SetLastError = false)]
36            private static extern Int32 RpcBindingFromStringBinding(String bindingStrin
37
38            [DllImport("Rpcrt4.dll", EntryPoint = "NdrClientCall2", CallingConvention =
39                CharSet = CharSet.Unicode, SetLastError = false)]
40            private static extern IntPtr NdrClientCall2x86(IntPtr pMIDL_STUB_DESC, IntP
41
42            [DllImport("Rpcrt4.dll", EntryPoint = "RpcBindingFree", CallingConvention =
43                CharSet = CharSet.Unicode, SetLastError = false)]
44            private static extern Int32 RpcBindingFree(ref IntPtr lpString);
45
46            [DllImport("Rpcrt4.dll", EntryPoint = "RpcStringBindingComposeW", CallingCo
47                CharSet = CharSet.Unicode, SetLastError = false)]
48            private static extern Int32 RpcStringBindingCompose(
49                String ObjUuid, String ProtSeq, String NetworkAddr, String Endpoint, St
50                out IntPtr lpBindingString
51                );
52
53            [DllImport("Rpcrt4.dll", EntryPoint = "RpcBindingSetOption", CallingConvent
54            private static extern Int32 RpcBindingSetOption(IntPtr Binding, UInt32 Opti
55
56            [DllImport("Rpcrt4.dll", EntryPoint = "NdrClientCall2", CallingConventi
57            ChanSet = ChanSet Unicode SetLactEnnon = false)]
```

```
57                            CharSet = CharSet.Unicode, SetLastError = false)]
58              internal static extern IntPtr NdrClientCall2x64(IntPtr pMIDL_STUB_DESC,
59
60         [DllImport("Rpcrt4.dll", EntryPoint = "NdrClientCall2", CallingConvention = Cal
61                    CharSet = CharSet.Unicode, SetLastError = false)]
62              private static extern IntPtr NdrClientCall2x64(IntPtr intPtr1, IntPtr i
63
64         [DllImport("Rpcrt4.dll", EntryPoint = "NdrClientCall2", CallingConventi
65                    CharSet = CharSet.Unicode, SetLastError = false)]
66              private static extern IntPtr NdrClientCall2x64(IntPtr intPtr1, IntPtr i
67
68              private static byte[] MIDL_ProcFormatStringx86 = new byte[] {
69                         0x00,0x48,0x00,0x00,0x00,0x00,0x00,0x00,0x08,0x00,0x32,
70                         0x00,0x04,0x00,0x08,0x00,0x00,0x48,0x00,0x00,0x00,0x00,
71                         0x00,0x00,0x01,0x00,0x00,0x00,0x0b,0x00,0x00,0x00,0x02,
72                         0x00,0x48,0x00,0x10,0x00,0x08,0x00,0x70,0x00,0x14,0x00,
73                         0x08,0x00,0x44,0x01,0x08,0x01,0x00,0x00,0x00,0x00,0x00,
74                         0x00,0x00,0x00,0x00,0x00,0x08,0x00,0x44,0x01,0x08,0x01,
75                         0x04,0x00,0x08,0x00,0x32,0x00,0x00,0x00,0x00,0x08,
76                         0x48,0x00,0x00,0x00,0x00,0x05,0x00,0x08,0x00,0x32,0x00,
77                         0x04,0x00,0x08,0x00,0x00,0x48,0x00,0x00,0x00,0x00,0x06,
78                         0x00,0x00,0x00,0x70,0x00,0x04,0x00,0x08,0x00,0x00,0x48,
79                         0x08,0x01,0x00,0x00,0x00,0x00,0x00,0x70,0x00,0x04,
80                         0x00,0x08,0x00,0x44,0x01,0x08,0x01,0x00,0x00,0x00,
81                         0x32,0x00,0x00,0x00,0x00,0x08,0x00,0x44,0x01,0x08,
82                         0x00,0x0a,0x00,0x08,0x00,0x32,0x00,0x00,0x00,0x00,0x00,
83                         0x00,0x48,0x00,0x00,0x00,0x00,0x0b,0x00,0x08,0x00,0x32,
84                         0x00,0x04,0x00,0x08,0x00,0x00,0x48,0x00,0x00,0x00,0x00,
85                         0x00,0x00,0x00,0x00,0x70,0x00,0x04,0x00,0x08,0x00,0x00,
86                         0x01,0x08,0x01,0x00,0x00,0x00,0x00,0x00,0x00,0x70,0x00,
87                         0x00,0x00,0x08,0x00,0x44,0x01,0x08,0x01,0x00,0x00,0x00,
88                         0x00,0x32,0x00,0x00,0x00,0x00,0x00,0x08,0x00,0x44,0x01,
89                         0x00,0x00,0x10,0x00,0x08,0x00,0x32,0x00,0x00,0x00,0x00,
90                         0x00,0x00,0x48,0x00,0x00,0x00,0x00,0x11,0x00,0x08,0x00,
91                         0x70,0x00,0x04,0x00,0x08,0x00,0x00,0x48,0x00,0x00,0x00,
92                         0x00,0x00,0x00,0x00,0x00,0x70,0x00,0x04,0x00,0x08,0x00,
93                         0x44,0x01,0x08,0x01,0x00,0x00,0x00,0x00,0x00,0x00,0x70,
94                         0x00,0x00,0x00,0x08,0x00,0x44,0x01,0x08,0x01,0x00,0x00,
95                         0x08,0x00,0x32,0x00,0x00,0x00,0x00,0x00,0x08,0x00,0x44,
96                         0x00,0x00,0x00,0x16,0x00,0x08,0x00,0x32,0x00,0x00,0x00,
97                         0x08,0x00,0x00,0x48,0x00,0x00,0x00,0x00,0x17,0x00,0x08,
98                         0x00,0x70,0x00,0x04,0x00,0x08,0x00,0x00,0x48,0x00,0x00,
99                         0x00,0x00,0x00,0x00,0x00,0x00,0x70,0x00,0x04,0x00,0x08,
100                        0x00,0x44,0x01,0x08,0x01,0x00,0x00,0x00,0x00,0x00,0x00,
101                        0x00,0x00,0x00,0x00,0x08,0x00,0x44,0x01,0x08,0x01,0x00,
102                        0x00,0x08,0x00,0x32,0x00,0x00,0x00,0x00,0x00,0x08,0x00,
103                        0x00,0x00,0x00,0x00,0x1c,0x00,0x08,0x00,0x32,0x00,0x00,
104                        0x00,0x08,0x00,0x00,0x48,0x00,0x00,0x00,0x00,0x1d,0x00,
105                        0x00,0x00,0x00,0x00,0x18,0x01,0x00,0x00,0x36,0x00,0x70,
106                        0x00,0x00,0x00,0x08,0x00,0x44,0x01,0x08,0x01,0x00,0x00,
107                        0x08,0x00,0x32,0x00,0x00,0x00,0x00,0x00,0x08,0x00,0x44,
108                        0x00,0x00,0x00,0x20,0x00,0x08,0x00,0x32,0x00,0x00,0x00,
109                        0x08,0x00,0x00,0x48,0x00,0x00,0x00,0x00,0x21,0x00,0x08,
110                        0x00,0x70,0x00,0x04,0x00,0x08,0x00,0x00,0x48,0x00,0x00,
111                        0x00,0x00,0x00,0x00,0x00,0x00,0x70,0x00,0x04,0x00,0x08,
112                        0x00,0x44,0x01,0x08,0x01,0x00,0x00,0x00,0x00,0x00,0x00,
113                        0x00,0x00,0x00,0x00,0x08,0x00,0x44,0x01,0x08,0x01,0x00,
114                        0x00,0x04,0x00,0x32,0x00,0x00,0x00,0x00,0x00,0x00,0x00,
115                        0x04,0x00,0x32,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x40,
116                        0x00,0x32,0x00,0x00,0x00,0x00,0x00,0x08,0x00,0x44,0x01,
117                        0x00,0x00,0x28,0x00,0x08,0x00,0x32,0x00,0x00,0x00,0x00,
118                        0x00,0x00,0x48,0x00,0x00,0x00,0x00,0x29,0x00,0x08,0x00,
```

Page 8 of 42

```
3020        "@
3021                                        Invoke-Neo4jQuery -Query $query |  Format-List -Property
3022                            }
3023                        return
3024                    }
3025                return
3026            }
3027        }
3028    }
3029    }
3030    }
3031    Write-Output "Found $count weak passwords"
3032 }
3033 function ConvertFrom-CisHtml{
3034    <#
3035    .EXAMPLE
3036    PS > gci *html | foreach {ConvertFrom-CisHtml -html $_.fullname -output "C:\$($_.na
3037    Found 0 improvements
3038    saved to C:\LAPTOP-CIS_Microsoft_Office_2016_Benchmark-XCCDF-.html
3039    Found 6 improvements
3040    saved to C:\LAPTOP-CIS_Microsoft_Office_Access_2016_Benchmark-XCCDF-.html
3041    Found 26 improvements
```

```
3041        Found 26 improvements
3042        saved to C:\LAPTOP-CIS_Microsoft_Office_Excel_2016_Benchmark-XCCDF-.html
3043        Found 39 improvements
3044        saved to C:\LAPTOP-CIS_Microsoft_Office_Outlook_2016_Benchmark-XCCDF-.html
3045        Found 12 improvements
3046        saved to C:\LAPTOP-CIS_Microsoft_Office_PowerPoint_2016_Benchmark-XCCDF-.html
3047        Found 19 improvements
3048        saved to C:\LAPTOP-CIS_Microsoft_Office_Word_2016_Benchmark-XCCDF-.html
3049        Found 195 improvements
3050        saved to C:\LAPTOP-CIS_Microsoft_Windows_10_Enterprise_Release_1803_Benchmark-XCCDF
3051        Found 196 improvements
3052        saved to C:\LAPTOP-CIS_Microsoft_Windows_10_Enterprise_Release_1809_Benchmark-XCCDF
3053        #>
3054        param(
3055            [CmdletBinding()]
3056            [Parameter(Mandatory=$true, Position=0, ValueFromPipeline=$true)]
3057            [ValidateScript({Test-Path -Path $_ })]
3058            $html,
3059
3060            [Parameter(Mandatory=$true, Position=1)]
3061            $output
3062        )
3063        if(get-module PSWriteWord -ListAvailable){
3064            import-module PSWriteWord
3065        }else{
3066            Write-Output "install-module PSWriteWord"
3067            throw
3068        }
3069        $html_ = Get-Content $html -Raw
3070        $rep = New-Object -com "HTMLFILE"
3071        $rep.IHTMLDocument2_write($html_)
3072        $WordDocument = New-WordDocument $output
3073        $count = 0
3074        foreach($i in ($rep.body.getElementsByClassName('Rule'))){
3075            $doc = New-Object -com "HTMLFILE"
3076            $doc.IHTMLDocument2_write(($i | select -ExpandProperty innerhtml))
3077            $res = ($doc.body.getElementsByClassName('outcome') | select -ExpandProperty ou
3078            if(($res) -and ($res -notmatch 'pass')){
3079                $count +=1
3080                Add-WordText -WordDocument $WordDocument -FontSize 12 -SpacingBefore 15 -Bo
3081                Add-WordText -WordDocument $WordDocument -FontSize 12 -SpacingBefore 15 -Su
3082                Add-WordText -WordDocument $WordDocument -FontSize 12 -SpacingBefore 15 -Bo
3083                Add-WordText -WordDocument $WordDocument -FontSize 12 -SpacingBefore 15 -Su
3084                Add-WordText -WordDocument $WordDocument -FontSize 12 -SpacingBefore 15 -Bo
3085                Add-WordText -WordDocument $WordDocument -FontSize 12 -SpacingBefore 15 -Su
3086                Add-WordText -WordDocument $WordDocument -FontSize 12 -SpacingBefore 15 -Bo
3087                Add-WordText -WordDocument $WordDocument -FontSize 12 -SpacingBefore 15 -Su
3088            }
3089        }
3090        $out = Save-WordDocument $WordDocument -Language 'en-US'
3091        Write-Output "Found $count improvements"
3092        Write-Output "saved to $out"
3093    }
```