



sense-of-security / ADRecon Public

Notifications Fork 281 Star 1.7k

<> Code Issues 17 Pull requests 2 Actions Projects Security Insights

ADRecon / ADRecon.ps1

...

🔄

12056 lines (10805 loc) · 612 KB

Code Blame Raw Copy Download

```
1 <#
2
3 .SYNOPSIS
4
5     ADRecon is a tool which gathers information about the Active Directory and generates a report w
6
7 .DESCRIPTION
8
9     ADRecon is a tool which extracts and combines various artefacts (as highlighted below) out of a
10    The tool is useful to various classes of security professionals like auditors, DFIR, students,
11    It can be run from any workstation that is connected to the environment, even hosts that are no
12    Fine Grained Password Policy, LAPS and BitLocker may require Privileged user accounts.
13    The tool will use Microsoft Remote Server Administration Tools (RSAT) if available, otherwise i
14    The following information is gathered by the tool:
15    - Forest;
16    - Domain;
17    - Trusts;
18    - Sites;
19    - Subnets;
20    - Default and Fine Grained Password Policy (if implemented);
21    - Domain Controllers, SMB versions, whether SMB Signing is supported and FSMO roles;
22    - Users and their attributes;
23    - Service Principal Names (SPNs);
24    - Groups and memberships;
25    - Organizational Units (OUs);
26    - Group Policy Object and gPLink details;
```

```
27     - DNS Zones and Records;
28     - Printers;
29     - Computers and their attributes;
30     - PasswordAttributes (Experimental);
31     - LAPS passwords (if implemented);
32     - BitLocker Recovery Keys (if implemented);
33     - ACLs (DACLs and SACLs) for the Domain, OUs, Root Containers, GPO, Users, Computers and Groups;
34     - GPOReport (requires RSAT);
35     - Kerberoast (not included in the default collection method); and
36     - Domain accounts used for service accounts (requires privileged account and not included in the default collection method);
```

```
38     Author       : Prashant Mahajan
39     Company      : https://www.senseofsecurity.com.au
```

#### 41 .NOTES

43 The following commands can be used to turn off ExecutionPolicy: (Requires Admin Privs)

```
45 PS > $ExecPolicy = Get-ExecutionPolicy
46 PS > Set-ExecutionPolicy bypass
47 PS > .\ADRecon.ps1
48 PS > Set-ExecutionPolicy $ExecPolicy
```

50 OR

52 Start the PowerShell as follows:

```
53 powershell.exe -ep bypass
```

55 OR

57 Already have a PowerShell open ?

```
58 PS > $Env:PSExecutionPolicyPreference = 'Bypass'
```

60 OR

```
62 powershell.exe -nologo -executionpolicy bypass -noprofile -file ADRecon.ps1
```

#### 64 .PARAMETER Protocol

65 Which protocol to use; ADWS (default) or LDAP

#### 67 .PARAMETER DomainController

68 Domain Controller IP Address or Domain FQDN.

#### 70 .PARAMETER Credential

71 Domain Credentials.

72

```
73 .PARAMETER GenExcel
74     Path for ADRecon output folder containing the CSV files to generate the ADRecon-Report.xlsx
75
76 .PARAMETER OutputDir
77     Path for ADRecon output folder to save the files and the ADRecon-Report.xlsx. (The folder s
78
79 .PARAMETER Collect
80     Which modules to run; Comma separated; e.g Forest,Domain (Default all except Kerberoast, Domain
81     Valid values include: Forest, Domain, Trusts, Sites, Subnets, PasswordPolicy, FineGrainedPasswo
82
83 .PARAMETER OutputType
84     Output Type; Comma seperated; e.g STDOUT,CSV,XML,JSON,HTML,Excel (Default STDOUT with -Collect
85     Valid values include: STDOUT, CSV, XML, JSON, HTML, Excel, All (excludes STDOUT).
86
87 .PARAMETER DormantTimeSpan
88     Timespan for Dormant accounts. (Default 90 days)
89
90 .PARAMETER PassMaxAge
91     Maximum machine account password age. (Default 30 days)
92
93 .PARAMETER PageSize
94     The PageSize to set for the LDAP searcher object.
95
96 .PARAMETER Threads
97     The number of threads to use during processing objects. (Default 10)
98
99 .PARAMETER Log
100     Create ADRecon Log using Start-Transcript
101
102 .EXAMPLE
103
104     .\ADRecon.ps1 -GenExcel C:\ADRecon-Report-<timestamp>
105     [*] ADRecon <version> by Prashant Mahajan (@prashant3535) from Sense of Security.
106     [*] Generating ADRecon-Report.xlsx
107     [+] Excelsheet Saved to: C:\ADRecon-Report-<timestamp>\<domain>-ADRecon-Report.xlsx
108
109 .EXAMPLE
110
111     .\ADRecon.ps1 -DomainController <IP or FQDN> -Credential <domain\username>
112     [*] ADRecon <version> by Prashant Mahajan (@prashant3535) from Sense of Security.
113     [*] Running on <domain>\<hostname> - Member Workstation
114     <snip>
115
116     Example output from Domain Member with Alternate Credentials.
117
118 EXAMPLE F
```

449 **EXAMPLE**





































































































































































































































































































































































































































































































































































































```
11983         Remove-Variable ADRObj
11984     }
11985     Remove-Variable ADRDomainAccountsusedforServiceLogon
11986 }
11987
11988 $TotalTime = "{0:N2}" -f ((Get-DateDiff -Date1 (Get-Date) -Date2 $date).TotalMinutes)
11989
11990 $AboutADRecon = Get-ADRAbout -Protocol $Protocol -date $date -ADReconVersion $ADReconVersion -C
11991
11992 If ( ($OutputType -Contains "CSV") -or ($OutputType -Contains "XML") -or ($OutputType -Contains
11993 {
11994     If ($AboutADRecon)
11995     {
11996         Export-ADR -ADRObj $AboutADRecon -ADROutputDir $ADROutputDir -OutputType $OutputType -A
11997     }
11998     Write-Output "[*] Total Execution Time (mins): $($TotalTime)"
11999     Write-Output "[*] Output Directory: $ADROutputDir"
12000     $ADRSTDOUT = $false
12001 }
12002
12003 Switch ($OutputType)
12004 {
12005     'STDOUT'
12006     {
12007         If ($ADRSTDOUT)
12008         {
12009             Write-Output "[*] Total Execution Time (mins): $($TotalTime)"
12010         }
12011     }
12012     'HTML'
12013     {
12014         Export-ADR -ADRObj $(New-Object PSObject) -ADROutputDir $ADROutputDir -OutputType $([ar
12015     }
12016     'EXCEL'
12017     {
12018         Export-ADRExcel $ADROutputDir
12019     }
12020 }
12021 Remove-Variable TotalTime
12022 Remove-Variable AboutADRecon
12023 Set-Location $returnndir
12024 Remove-Variable returnndir
12025
12026 If (($Protocol -eq 'ADWS') -and $UseAltCreds)
```

```
12026         If (($Protocol -eq 'LDAP' -and $objDomain))
12027         {
12028             Remove-PSDrive ADR
12029         }
12030
12031         If ($Protocol -eq 'LDAP')
12032         {
12033             $objDomain.Dispose()
12034             $objDomainRootDSE.Dispose()
12035         }
12036
12037         If ($ADROutputDir)
12038         {
12039             Remove-EmptyADROutputDir $ADROutputDir $OutputType
12040         }
12041
12042         Remove-Variable ADReconVersion
12043         Remove-Variable RanonComputer
12044     }
12045
12046     If ($Log)
12047     {
12048         Start-Transcript -Path "$(Get-Location)\ADRecon-Console-Log.txt"
12049     }
12050
12051     Invoke-ADRecon -GenExcel $GenExcel -Protocol $Protocol -Collect $Collect -DomainController $DomainC
12052
12053     If ($Log)
12054     {
12055         Stop-Transcript
12056     }
```