

Product ▼

Solutions ▼

Resources ▼

Open Source ▼


Enterprise ▼

Pricing


Search


Sign in


Sign up


 adrecon / AzureADRecon

Public


 Sponsor


 Notifications


 Fork 35


 Star 185


<> Code


 Issues 2


 Pull requests


 Actions


 Projects

 Security

 Insights


 master ▼







Go to file






<> Code ▼


 semgrep-bot


Add Semgrep CI 


88d8bad · 3 weeks ago

 24 Commits


 .github	Add Semgrep CI	3 weeks ago
 AzureADRecon.ps1	Update AzureADRecon.ps1	10 months ago
 LICENSE	Initial commit	5 years ago
 MSGraph-Credentials.csv	Added MSGraph method for Users & T...	2 years ago
 README.md	Added MSGraph method for Users & T...	2 years ago

 README

 AGPL-3.0 license



AzureADRecon: Azure Active Directory Recon

 Follow @ad_recon

AzureADRecon is a tool which extracts and combines various artefacts (as highlighted below) out of an Azure AD environment with a valid credential. The information can be presented in a specially formatted Microsoft Excel report that includes summary views with metrics to facilitate analysis and provide a holistic picture of the current state of the target environment.

The tool is useful to various classes of security professionals like auditors, DFIR, students, administrators, etc. It can also be an invaluable post-exploitation tool for a penetration tester.

The tool requires AzureAD PowerShell Module to be installed.

The following information is gathered by the tool:

- Tenant
- Domain
- Licenses
- Users
- ServicePrincipals
- DirectoryRoles
- DirectoryRoleMembers
- Groups
- GroupMembers
- Devices

Getting Started


These instructions will get you a copy of the tool up and running on your local machine.


Prerequisites


- .NET Framework 3.0 or later (Windows 7 includes 3.0)


About


AzureADRecon is a tool which gathers information about the Azure Active Directory and generates a report which can provide a holistic picture of the current state of the target environment.


 Readme


 AGPL-3.0 license

 Activity

 Custom properties

 185 stars

 8 watching


 35 forks

Report repository


Releases

No releases published

Sponsor this project

 prashant3535

Prashant Mahajan


 Sponsor

[Learn more about GitHub Sponsors](#)


Packages

No packages published


Contributors 4


 prashant3535

Prashant Mahajan

 adrecon

ADRecon

 0xshyam shyam

 semgrep-bot

Languages

PowerShell 100.0%

- PowerShell
 - PowerShell 2.0 or later (Windows 7 includes 2.0)
 - AzureAD PowerShell Module
(<https://www.powershellgallery.com/packages/AzureAD/>) Requires PowerShell 3.0 or later
 - `Install-Module -Name AzureAD`
 - Limited PowerShell Core support (Tested on PowerShell v7.3.1; Excel generation requires Windows)
 - Microsoft Graph Module
(<https://www.powershellgallery.com/packages/microsoft.graph>)
 - `Install-Module -Name Microsoft.Graph`
 - Scopes required: AuditLog.Read.All, User.Read.All, UserAuthenticationMethod.Read.All

Optional

- Microsoft Excel (to generate the report)

Installing

If you have git installed, you can start by cloning the [repository](#):

```
git clone https://github.com/adrecon/AzureADRecon.git
```

Otherwise, you can [download a zip archive of the latest release](#). The intent is to always keep the master branch in a working state.

Usage

Examples

To run AzureADRecon (will prompt for credentials).

```
PS C:\> .\AzureADRecon.ps1

or

PS C:\> $username = "username@fqdn"
PS C:\> $passwd = ConvertTo-SecureString "PlainTextPassword" -AsPlainText
PS C:\> $creds = New-Object System.Management.Automation.PSCredential($username,$passwd)
PS C:\> .\AzureADRecon.ps1 -Credential $creds
```

To generate the AzureADRecon-Report.xlsx based on AzureADRecon output (CSV Files).

```
PS C:\> .\AzureADRecon.ps1 -GenExcel C:\AzureADRecon-Report-<timestamp>
```

Fill in the relevant details in the `MSGraph-Credentials.csv` and use the following command

```
PS C:\> .\AzureADRecon.ps1 -Method MSGraph
```

When you run AzureADRecon, a `AzureADRecon-Report-<timestamp>` folder will be created which will contain AzureADRecon-Report.xlsx and CSV-Folder with the raw files.

Parameters

```
-Method <String>
    Which method to use; AzureAD (default), MSGraph (default for non-

-Credential <PSCredential>
    Domain Credentials.
```

```
-GenExcel <String>
    Path for AzureADRecon output folder containing the CSV files to save

-TenantID <String>
    The Azure TenantID to connect to when you have multiple tenants.

-OutputDir <String>
    Path for AzureADRecon output folder to save the CSV/XML/JSON/HTML

-Collect <String>
    Which modules to run (Comma separated; e.g Tenant,Domain. Default: Tenant,Domain)
    Valid values include: Tenant, Domain, Licenses, Users, ServicePrincipals

-OutputType <String>
    Output Type; Comma seperated; e.g CSV,STDOUT,Excel (Default STDOUT)
    Valid values include: STDOUT, CSV, XML, JSON, HTML, Excel, All (Default All)

-DormantTimeSpan <Int>
    Timespan for Dormant accounts. (Default 30 days)

-PassMaxAge <Int>
    Maximum machine account password age. (Default 90 days)

-PageSize <Int>
    The PageSize to set for the LDAP searcher object. (Default 200)

-Threads <Int>
    The number of threads to use during processing objects (Default 10)

-Log <Switch>
    Create ADRecon Log using Start-Transcript
```

Bugs, Issues and Feature Requests

Please report all bugs, issues and feature requests in the [issue tracker](#). Or let me (@prashant3535) know directly.

Contributing

Pull request are always welcome.

Mad props

Thanks for the awesome work by @_wald0, @CptJesus, @harmj0y, @mattifestation, @PyroTek3, @darkoperator, @ITsecurityAU Team, @CTXIS Team and others.

License

AzureADRecon is a tool which gathers information about the Azure Active Directory and generates a report which can provide a holistic picture of the current state of the target environment.

This program is free software: you can redistribute it and/or modify it under the terms of the GNU Affero General Public License as published by the Free Software Foundation, either version 3 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Affero General Public License for more details.

You should have received a copy of the GNU Affero General Public License along with this program. If not, see <http://www.gnu.org/licenses/>.

This program borrows and uses code from many sources. All attempts are made to credit the original author. If you find that your code is used without proper credit, please shoot an insult to @prashant3535, Thanks.

