adrecon / ADRecon Public

Sponsor Notifications Fork 101 Star 694

Code Issues 13 Pull requests Actions Projects Security Insights

master Go to file Code

prashant3535 Merge pull request #29 from kvn1338... d2ba12c · 3 weeks ago 118 Commits

| | | |
|---|---|---|
| .github | Add Semgrep CI | 3 weeks ago |
| ADRecon.ps1 | Merge pull request #29 from kvn1338/... | 3 weeks ago |
| LICENSE.md | Initial Commit | 7 years ago |
| README.md | Added PowerShell Core on Windows S... | 2 years ago |

README AGPL-3.0 license

# ADRecon: Active Directory Recon

Follow @ad_recon

This repo contains updates to the original concept and code by Prashant Mahajan (@prashant3535) while working at Sense of Security.

ADRecon is a tool which extracts and combines various artefacts (as highlighted below) out of an AD environment. 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 AD 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.

It can be run from any workstation that is connected to the environment, even hosts that are not domain members. Furthermore, the tool can be executed in the context of a non-privileged (i.e. standard domain user) account. Fine Grained Password Policy, LAPS and BitLocker may require Privileged user accounts. The tool will use Microsoft Remote Server Administration Tools (RSAT) if available, otherwise it will communicate with the Domain Controller using LDAP.

The following information is gathered by the tool:

- Forest;
- Domain;
- Trusts;
- Sites;
- Subnets;
- Schema History;
- Default and Fine Grained Password Policy (if implemented);
- Domain Controllers, SMB versions, whether SMB Signing is supported and FSMO roles;
- Users and their attributes;
- Service Principal Names (SPNs);
- Groups, memberships and changes;

## About

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

Readme
AGPL-3.0 license
Activity
Custom properties
694 stars
16 watching
101 forks
Report repository

## Releases

No releases published

## Sponsor this project

prashant3535 Prashant Mahajan

Sponsor

Learn more about GitHub Sponsors

## Packages

No packages published

## Contributors 6

## Languages

PowerShell 100.0%

- Organizational Units (OUs);
- GroupPolicy objects and gPLink details;
- DNS Zones and Records;
- Printers;
- Computers and their attributes;
- PasswordAttributes (Experimental);
- LAPS passwords (if implemented);
- BitLocker Recovery Keys (if implemented);
- ACLs (DACLs and SACLs) for the Domain, OUs, Root Containers, GPO, Users, Computers and Groups objects (not included in the default collection method);
- GPOReport (requires RSAT);
- Kerberoast (not included in the default collection method); and
- Domain accounts used for service accounts (requires privileged account and not included in the default collection method).

ADRecon was presented at: Black Hat Arsenal Asia 2018 - Slidedeck

Black Hat Arsenal USA 2018 | DEFCON 26 Demo Labs - Slidedeck

Bay Area OWASP - Slidedeck

CHCON - Slidedeck

## 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)
- PowerShell 2.0 or later (Windows 7 includes 2.0)
  - Powershell Core on Windows is supported (Tested on PowerShell v7.2.2 running on Windows 10)
- A Windows host (Powershell for Linux/macOS is not supported)

### Optional

- Microsoft Excel (to generate the report)
- Remote Server Administration Tools (RSAT):
  - Windows 10 (October 2018 Update or 1809 and later), RSAT is included as a set of `Features on Demand`.
    - Click on Start --> Settings --> Apps --> Apps & features --> Manage optional features --> Add a feature --> Select the following:
      - RSAT: Active Directory Domain Services and Lightweight Directory Services Tools
      - RSAT: Group Policy Management Tools
  - Windows 10 (https://www.microsoft.com/en-au/download/details.aspx?id=45520)
  - Windows 7 (https://www.microsoft.com/en-au/download/details.aspx?id=7887)

### Installing

If you have git installed, you can start by cloning the repository:

```
git clone https://github.com/adrecon/ADRecon.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 ADRecon on a domain member host.

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

To run ADRecon on a domain member host as a different user.

```
PS C:\>.\ADRecon.ps1 -DomainController <IP or FQDN> -Credential <dom
```

To run ADRecon on a non-member host using LDAP.

```
PS C:\>.\ADRecon.ps1 -Method LDAP -DomainController <IP or FQDN> -Cr
```

To run ADRecon with specific modules on a non-member host with RSAT. (Default OutputType is STDOUT with -Collect parameter)

```
PS C:\>.\ADRecon.ps1 -Method ADWS -DomainController <IP or FQDN> -Cr
```

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

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

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

## Parameters

```
-Method <String>
    Which method to use; ADWS (default), LDAP

-DomainController <String>
    Domain Controller IP Address or Domain FQDN.

-Credential <PSCredential>
    Domain Credentials.

-GenExcel <String>
    Path for ADRecon output folder containing the CSV files to gener

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

-Collect <String>
    Which modules to run (Comma separated; e.g Forest,Domain. Defaul
    Valid values include: Forest, Domain, Trusts, Sites, Subnets, Sc

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

-DormantTimeSpan <Int>
    Timespan for Dormant accounts. (Default 90 days)

-PassMaxAge <Int>
    Maximum machine account password age. (Default 30 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
```

```
-OnlyEnabled <Bool>
    Only collect details for enabled objects.

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

-Logo <String>
    Which Logo to use in the excel file? (Default ADRecon)
    Values include: ADRecon, CyberCX, Payatu.
```

## Future Plans

- Replace System.DirectoryServices.DirectorySearch with System.DirectoryServices.Protocols and add support for LDAP STARTTLS and LDAPS (TCP port 636).
- ~~Add Domain Trust Enumeration.~~
- Add option to filter default ACLs.
- ~~Gather ACLs for other objects such as Users, Group, etc.~~
- Additional export and storage option: export to ~~STDOUT~~, SQLite, ~~xml~~, ~~json~~, ~~html~~, pdf.
- Use the EPPlus library for Excel Report generation and remove the dependency on MS Excel.
- List issues identified and provide recommended remediation advice based on analysis of the data.
- Add PowerShell Core support.

## 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, @CxCyber Team, @payatulabs Team and others.

## License

ADRecon is a tool which gathers information about the Active Directory and generates a report which can provide a holistic picture of the current state of the target AD 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