Sign in

bats3c / **ADCSPwn** Public

Notifications | Fork 122 | Star 816

Code | Issues 1 | Pull requests 1 | Actions | Projects | Security | Insights

master | Go to file | Code

ADCSPwn

README.md

README

ADCSPwn

A tool to escalate privileges in an active directory network by coercing authenticate from machine accounts (Petitpotam) and relaying to the certificate service.

Usage

Run `ADCSPwn` on your target network.

```
Author: @_batsec_ - MDSec ActiveBreach
Contributor: @Flangvik -  TrustedSec
Contributor: @424f424f -  Black Hills Informati

adcspwn.exe --adcs <cs server> --port [local po

Required arguments:
adcs            -       This is the address of 
```

About

A tool to escalate privileges in an active directory network by coercing authenticate from machine accounts and relaying to the certificate service.

Readme

Activity

816 stars

16 watching

122 forks

Report repository

Releases 2

ADCSPwn v1.1 Latest
on Aug 2, 2021

+ 1 release

Packages

No packages published

Contributors 4

bats3c batsec

```
Optional arguments:
secure          -       Use HTTPS with the cert
port            -       The port ADCSPwn will l
remote          -       Remote machine to trigg
username        -       Username for non-domain
password        -       Password for non-domain
dc              -       Domain controller to qu
unc             -       Set custom UNC callback
output          -       Output path to store ba

Example usage:
adcspwn.exe --adcs cs.pwnlab.local
adcspwn.exe --adcs cs.pwnlab.local --secure
adcspwn.exe --adcs cs.pwnlab.local --port 9001
adcspwn.exe --adcs cs.pwnlab.local --remote dc.
adcspwn.exe --adcs cs.pwnlab.local --remote dc.
adcspwn.exe --adcs cs.pwnlab.local --remote dc.
adcspwn.exe --adcs cs.pwnlab.local --remote dc.
adcspwn.exe --adcs cs.pwnlab.local --remote dc.
```

Credits

- @harmj0y & @tifkin_ for their whitepaper detailing this issue.
- @topotam77 for showing how `EfsRpcOpenFileRaw` can be abused.

FlangvikOld

rvrsh3ll Steve Borosh

inspiringz 3ND

Languages

● C# 100.0%

Terms Privacy Security Status Docs Contact Manage cookies Do not share my personal information