Open in app ↗ Sign up Sign in

Medium Search Write

Secedit and I know it!

BlueteamOps · Follow
6 min read · Nov 24, 2022

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

Sign up for free

Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

Try for 5 $/month

In today's Windows environments, Group Policy Objects (GPOs) are used to push configurations to hosts. Please click here to read more about how GPOs affect audit policy config on hosts.

In the event where an adversary modifies the audit configuration of a host (using auditpol.exe), next GPO refresh (default is every 90 minutes with a random time offset) will reinstate the configuration back to the state that is defined in the GPO.

However, it should be noted that the GPO audit policy configuration is

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

Ok let's talk about secedit.exe

Commonly found locations

C:\Windows\system32\SecEdit.exe
C:\Windows\SysWOW64\SecEdit.exe

secedit.exe is a native Windows command line tool which allows admins to carry out analysis and configuration of system security. References to secedit can be seen in early as Windows 95. During testing (with Windows

Medium

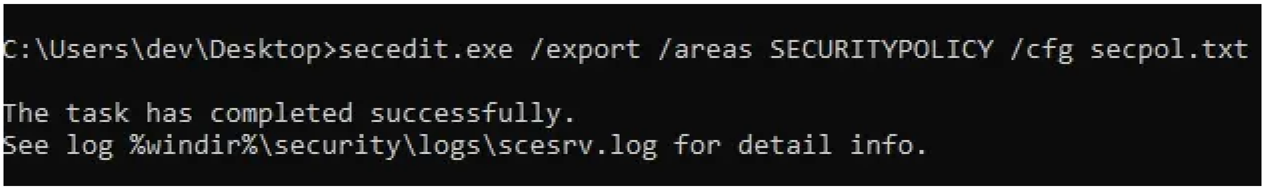
Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Membership

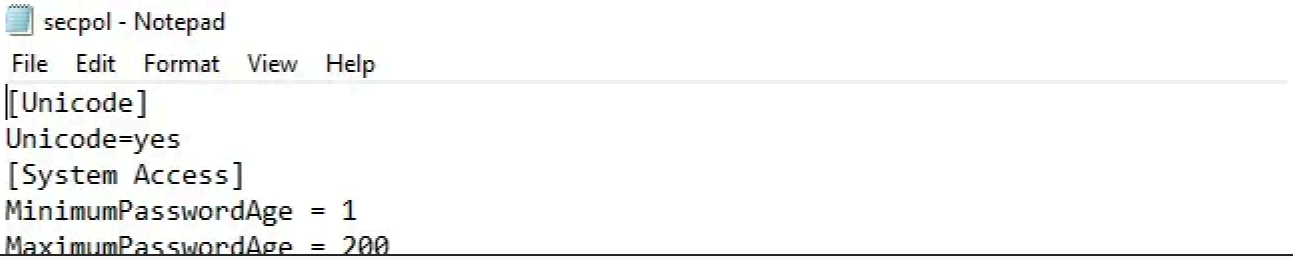
- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app



```
C:\Users\dev\Desktop>secedit.exe /export /areas SECURITYPOLICY /cfg secpol.txt

The task has completed successfully.
See log %windir%\security\logs\scesrv.log for detail info.
```

Figure 1 - secedit used for exporting the security policy of a host



```
[Unicode]
Unicode=yes
[System Access]
MinimumPasswordAge = 1
MaximumPasswordAge = 200
```

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- Distraction-free reading. No ads.
- Organize your knowledge with lists and highlights.
- Tell your story. Find your audience.

Membership

- Read member-only stories
- Support writers you read most
- Earn money for your writing
- Listen to audio narrations
- Read offline with the Medium app

Change the local security policy configuration of a host

Following steps can be taken to change the local security policy configuration of a host.

- Create a INI config template (See **Figure 3**) containing the config (file encoding should be UTF-16 LE BOM). Easiest way to obtain a sample INI file is to export the existing policy within the host (described earlier).

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

Create registry entries within a HKLM hive of a host

secedit can be used to carry out modifications to the HKLM registry hive. For e.g. An adversary can use secedit.exe to setup persistence via their own policy INI template.

Based on my research, when you run registry changes through secedit, you will not see any process interactions with reg.exe. The registry modification event via Sysmon generated EID 13 where the Image File name was services.exe.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

Detection

This includes detection ideas for secedit.exe as well as for detecting other potential audit config manipulations.

- In BAU operations, it should be rare to see secedit.exe being used to apply configurations and to retrieve configurations of hosts by named user accounts. An alert could be generated by baselining activity pertaining to secedit.exe and generate alert on any deviations.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

```
        - attack.credential_access
        - attack.privilege_escalation
        - attack.t1562.002
        - attack.t1547.001
        - attack.t1505.005
        - attack.t1556.002
        - attack.t1562
        - attack.t1574.007
        - attack.t1564.002
        - attack.t1546.008
        - attack.t1546.007
        - attack.t1547.014
        - attack.t1547.010
        - attack.t1547.002
        - attack.t1557
        - attack.t1082
```

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- Distraction-free reading. No ads.
- Organize your knowledge with lists and highlights.
- Tell your story. Find your audience.

Membership

- Read member-only stories
- Support writers you read most
- Earn money for your writing
- Listen to audio narrations
- Read offline with the Medium app

Addition/Removal of Success/Failure auditing of different audit sub-categories can be tracked via event ID 4719 in the Windows Security log. Activity carried out by machine accounts may be excluded to reduce false positives. You may create a detection which fires whenever success/failure audits for high impact sub-categories (i.e. Process Creation) gets removed by a named user account.

******Changes to the basic audit policy carried out using secedit did not result in generation of a 4719 event. However, this event was observed to be generated under the following scenarios — modifications using auditpol, modifications***

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

✦ Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

✦ Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

Written by BlueteamOps

Follow

81 Followers

Janantha Marasinghe’s Research

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app