



Secedit and I know it!

 BlueteamOps · Follow
6 min read · Nov 24, 2022

 -- 

First, let's talk a bit about auditpol.exe, previous occasions of it being misused and how security policies gets applied to Windows hosts.

Windows Event logs plays a crucial role during threat detection and response operations. Microsoft's reporting of the [Solarwinds incident](#) provided an example of a novel technique where an adversary has used [auditpol.exe](#) (a native Microsoft command-line tool) to retrieve the current audit policy configuration and used the same tool to disable logging of a specific Windows audit category (in this instance it was Detailed Tracking). This approach can be considered to be more stealthier than clearing the event log or manipulating it via other means (Check out [svch0st's part 1](#) and [part 2](#)).

But then there are GPOs....

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 written to a file called audit.csv and resides within the SYSVOL directory of DCs. An adversary having access to a DC can edit the audit.csv file to update the config (i.e. Turn off auditing of Process Creation events) and save it. During the next GPO refresh cycle this updated configuration gets pushed to all the member servers.

Microsoft provides a means of changing the GPO update interval on a system. This is carried out using the following registry setting. As a defender, detecting modification/setting of the following registry key should be of

interest. Refresh time can have a maximum value of 44640 minutes (31 days). As defenders we should watch out for changes to this registry key as it may be abused by an adversary to delay GPOs getting pushed to a host.

HKLM\Software\Policies\Microsoft\Windows\System\GroupPolicyRefreshTime

. . .

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 Server 2019) it was noted that secedit can only modify the local security policy of a host (aka the basic audit policy). While, auditpol can modify/clear audit policy, secedit has a capability to carryout modification of system access policies, HKLM hive, file security and privilege rights of a host.

secedit.exe operations are carried out using an ESE database. To create a database you need to first create an INI config template file (see **Figure 2**) with the required configuration. Once the database is created, secedit is used to read the config out of the database and apply to the host.

Whenever, secedit is executed, high-level information regarding the job is written to %windir%\security\logs\scesrv.log. Unfortunately, the file gets overwritten with every execution.

Retrieving the local security policy and more

Following command can be used to export the current security policy applied to the host.

secedit.exe /export /areas SECURITYPOLICY /cfg output_mysecpol.txt

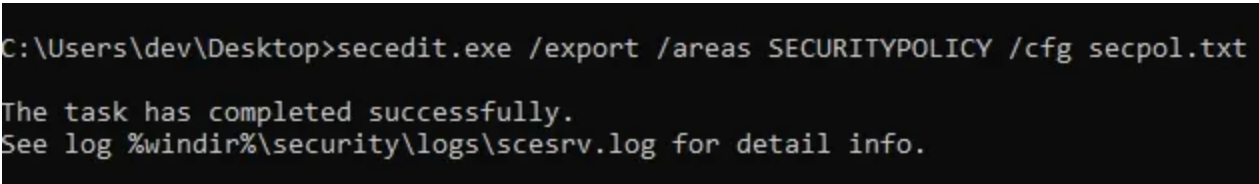


Figure 1 - secedit used for exporting the security policy of a host



```
secpol - Notepad
File Edit Format View Help
[[Unicode]
Unicode=yes
[System Access]
MinimumPasswordAge = 1
MaximumPasswordAge = 200
MinimumPasswordLength = 14
PasswordComplexity = 1
PasswordHistorySize = 24
LockoutBadCount = 5
ResetLockoutCount = 15
LockoutDuration = 15
AllowAdministratorLockout = 0
RequireLogonToChangePassword = 0
ForceLogoffWhenHourExpire = 0
NewAdministratorName = "Administrator"
NewGuestName = "Unwanted"
ClearTextPassword = 0
LSAAnonymousNameLookup = 0
EnableAdminAccount = 0
EnableGuestAccount = 0
[Event Audit]
AuditSystemEvents = 0
AuditLogonEvents = 0
AuditObjectAccess = 0
AuditPrivilegeUse = 0
AuditPolicyChange = 0
AuditAccountManage = 0
AuditProcessTracking = 0
AuditDSAccess = 0
AuditAccountLogon = 0
[Version]
signature="$CHICAGO$"
Revision=1
[Registry Values]
```

Figure 2 - Contents of the exported security policy via secdit

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).

Figure 3 -Custom INI template

- Use secdit to create a db file using the template ini file and apply the configuration to the host.

Figure 4 -Import the ini template and configure the system using secedit

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.

Manipulate Privilege Rights

secedit can be used to carry out changes to privileges rights. For e.g. A template can define which SIDs can have the SeDebugPrivilege on a host.

Manipulate System Access Configuration

Modification of system access configuration such as (but not limited to) enabling guest account, account lock out duration, storing passwords in reversible encryption etc.

Manipulate File ACLs

File access control lists may be modified using security descriptors.

Manipulate Windows Service

Manipulate Windows Service settings which can result in change of status of a Windows service or change to its security descriptor.

. . .

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.
- Registry modifications carried out using secedit may be captured via Sysmon EID 13 where Image File Name ends with services.exe. However, this may need further validation using historical data.

- Monitor process creation events — Look for secedit.exe being spawned by non machine accounts. Following Sigma rule may be used to a develop detection for this.
https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/proc_creation_win_susp_secedit.yml

```
title: Potential Suspicious Activity Using SeCEdit
id: c2c76b77-32be-4d1f-82c9-7e544bdfe0eb
status: experimental
description: Detects potential suspicious behaviour using secedit.exe. Such as export
references:
  - https://blueteamops.medium.com/secedit-and-i-know-it-595056dee53d
  - https://learn.microsoft.com/en-us/windows-server/administration/windows-command-shell
author: Janantha Marasinghe
date: 2022/11/18
tags:
  - attack.discovery
  - attack.persistence
  - attack.defense_evasion
  - 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
logsource:
  category: process_creation
  product: windows
detection:
  selection_img:
    - Image|endswith: '\secedit.exe'
    - OriginalFileName: 'SeCEdit'
  selection_flags_discovery:
    CommandLine|contains|all:
      - '/export'
      - '/cfg'
  selection_flags_configure:
    CommandLine|contains|all:
      - '/configure'
      - '/db'
  filter:
    SubjectUserName|endswith: '$'
  condition: selection_img and (1 of selection_flags_*) and not filter
falsepositives:
  - Legitimate administrative use
level: medium
```

- Monitor file modification to audit.csv files in SYSVOL on DCs.
- Windows Security Event Log

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.

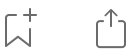
**Changes to the basic audit policy carried out using secedit did not result in generation of a 4719 event. However, this event was observed to be generated under the following scenarios — modifications using auditpol , modifications via the MMC or via GPO.*

Within XML data of the raw event you will see the following values under the “Changes” field. [Refer here](#) for the GUID to sub-category mapping.

%%8448 Success removed — means the audit success tick box has been unticked for the specified audit sub-category
%%8450 Failure removed — means the audit failure tick box has been unticked for the specified audit sub-category

- Dfir
- Forensics
- Secedit
- Lolbin

Some rights reserved ⓘ ©





Written by BlueteamOps

81 Followers

Janantha Marasinghe’s Research

Follow

