Lab

16

Viewing, Enabling and Clearing Audit Policies using Auditpol

Auditpol is a command in Windows Server 2016, Windows Server 2012, and Windows Server 2008, and is required for querying or configuring audit policy at the subcategory level.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

In the previous labs you have seen different steps that attackers take during the system hacking lifecycle. They start with gaining access to the system, escalating privileges, executing malicious applications, and hiding files. However, to maintain their access to the target system longer and avoid detection, they need to clear any traces of their intrusion. It is also essential to avoid a trace back and a possible prosecution for hacking.

One of the primary techniques to achieve this goal is to manipulate, disable, or erase the system logs. Once they have access to the target system, attackers can use inbuilt system utilities to disable or tamper logging and auditing mechanisms in the system.

Lab Objectives

The objective of this lab is to help students learn:

- How to set the Audit Policies?

Lab Environment

Tools demonstrated in this lab are available in Z:\CEH-Tools\CEHv10 Module 06 System Hacking

To carry out this lab, you need:

- Auditpol which is an built-in command in Windows Server 2016
- You can see more audit commands at **http://technet.microsoft.com/en-us/library/cc731451%28v=ws.10%29.aspx** for Windows Server 2016
- Run this on Windows Server 2016

Lab Duration

Time: 10 Minutes

Overview of Auditpol

Auditpol displays the information on the performance and functions to manipulate audit policies.

Lab Task

1. Launch Command Prompt from the **Windows Server 2016** machine.
2. To **view** all the audit policies, type the following command:

   auditpol /get /category:*

/set
Sets the audit policy.

3. Press **Enter**.

/backup
Saves the audit policy to a file.

/list
Displays selectable policy elements.

/restore
Restores the audit policy from a file that was previously created by using auditpol /backup.

/remove
Removes all per-user audit policy settings and disables all system audit policy settings.

/get
Displays the current audit policy.

/clear
Clears the audit policy.

FIGURE 16.1: Auditpol viewing the policies

/resourceSACL
Configures global resource system access control lists (SACLs).

4. To **enable** the audit policies, type the following at the command prompt:

   auditpol /set /category:"system","account logon" /success:enable /failure:enable

5. Press **Enter**.

Auditpol /get
[/user[:<username>|<{sid}>]]
[/category:*|<name>|<{guid}>[,:<name|<{guid}>…]]
[/subcategory:*|<name>|<{guid}>[,:<name|<{guid}>…]]
[/option:<option name>]
[/sd]
[/r]

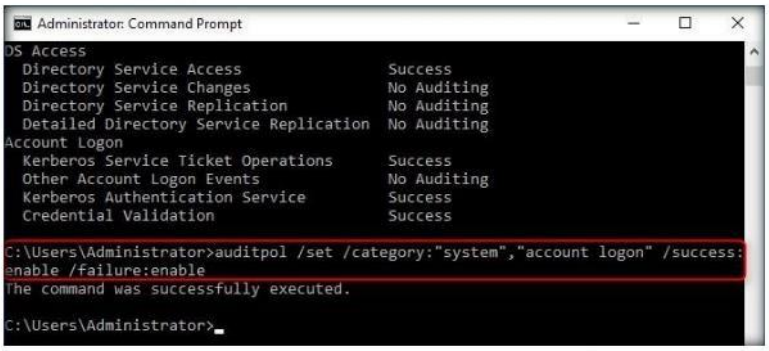

FIGURE 16.2: Auditpol Local Security Policies in Windows Server 2016

6. To check whether audit policies are enabled, type the following at the command prompt: **auditpol /get /category:***

7. Press **Enter**

Auditpol /set
[/user[:<username>|<{sid}>][/include][/exclude]]
[/category:<name>|<{guid}>[,:<name|<{guid}>…]]
[/success:<enable>|<disable>][/failure:<enable>|<disable>]
[/subcategory:<name>|<{guid}>[,:<name|<{guid}>…]]
[/success:<enable>|<disable>][/failure:<enable>|<disable>]
[/option:<option name>
/value:
<enable>|<disable>]

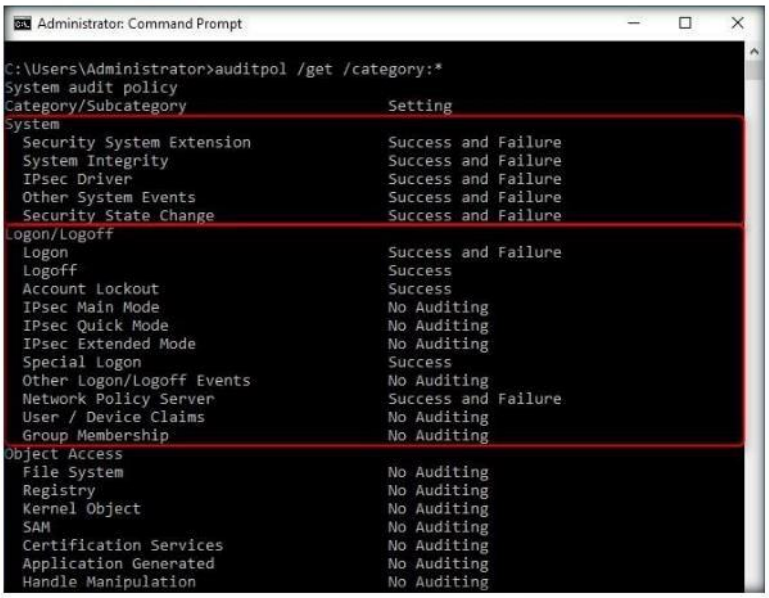

FIGURE 16.3:Auditpol enabling system and account logon policies

8. To **clear** the audit policies, type the following at the command prompt:

   auditpol /clear /y

9. Press **Enter**.

auditpol /list
[/user|/category|subcategory[:<categoryname>|<{guid}>|*]]
[/v] [/r]

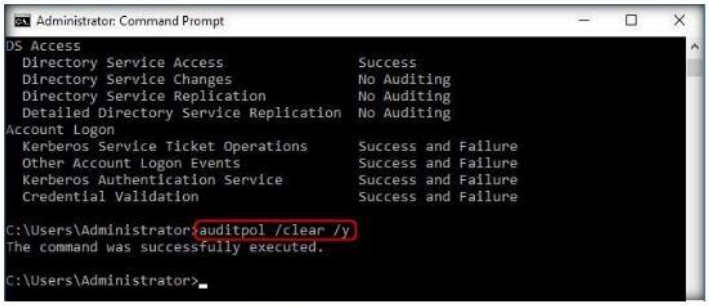

FIGURE 16.4: Auditpol clearing the policies

10. To check whether audit policies cleared, type the following at the command prompt:

    auditpol /get /category:*

11. Press **Enter**.

Auditpol /set
[/user[:<username>|<{sid}>][/include|/exclude]]
[/category:<name>|<{guid}>[,<name|<{guid}>...]]
[/success:<enable>|<disable>|/failure:<enable>|<disable>]
[/subcategory:<name>|<{guid}>[,:<name|<{guid}>...]]
[/success:<enable>|<disable>|/failure:<enable>|<disable>]
[/option:<option name> /value:<enable>|<disable>]

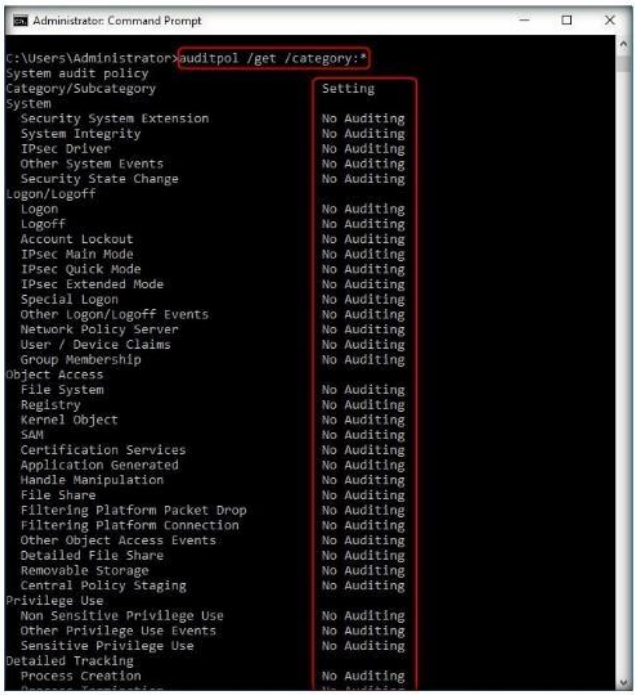

FIGURE 16.5: Auditpol policies cleared

Lab Analysis

Analyze and document the results related to the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs