



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:*

3. Press **Enter**.

Administrator Command Prompt	
Microsoft Windows [Version 10.0.14393]	
(c) 2016 Microsoft Corporation. All rights reserved.	
C:\Users\Administrator>auditpol /get /category:*	
System audit policy	Setting
Category/Subcategory	
System	
Security System Extension	No Auditing
System Integrity	Success and Failure
IPSec Driver	No Auditing
Other System Events	Success and Failure
Security State Change	Success
Logon/Logoff	
Logon	Success and Failure
Logoff	Success
Account Lockout	Success
IPSec Main Mode	No Auditing
IPSec Quick Mode	No Auditing
IPSec Extended Mode	No Auditing
Special Logon	Success
Other Logon/Logoff Events	No Auditing
Network Policy Server	Success and Failure
User / Device Claims	No Auditing
Group Membership	No Auditing
Object Access	
File System	No Auditing
Registry	No Auditing
Kernel Object	No Auditing
SAM	No Auditing
Certification Services	No Auditing
Application Generated	No Auditing
Handle Manipulation	No Auditing
File Share	No Auditing
Filtering Platform Packet Drop	No Auditing
Filtering Platform Connection	No Auditing
Other Object Access Events	No Auditing
Detailed File Share	No Auditing
Removable Storage	No Auditing
Central Policy Staging	No Auditing
Privilege Use	
Non Sensitive Privilege Use	No Auditing
Other Privilege Use Events	No Auditing
Sensitive Privilege Use	No Auditing
Detailed Tracking	
Process Creation	No Auditing
Process Termination	No Auditing
DPAPI Activity	No Auditing
RPC Events	No Auditing
Plug and Play Events	No Auditing
Token Right Adjusted Events	No Auditing
Policy Change	
Audit Policy Change	Success
Authentication Policy Change	Success
Authorization Policy Change	No Auditing
MPSSVC Rule-Level Policy Change	No Auditing
Filtering Platform Policy Change	No Auditing
Other Policy Change Events	No Auditing
Account Management	
Computer Account Management	Success
Enterprise Group Management	Success

FIGURE 16.1: Auditpol viewing the policies

Module 06 - System Hacking

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>|<{g  
uid}>|,<name|<{guid}>  
...]]  
[/subcategory:*|<name>  
<{guid}>|,<name|<{guid  
}>>...]]  
[/option:<option name>  
/sd]  
/t]
```

Category/Subcategory	Setting
DS Access	Success
Directory Service Access	No Auditing
Directory Service Changes	No Auditing
Directory Service Replication	No Auditing
Detailed Directory Service Replication	No Auditing
Account Logon	Success
Kerberos Service Ticket Operations	No Auditing
Other Account Logon Events	Success
Kerberos Authentication Service	Success
Credential Validation	Success

```
C:\Users\Administrator>auditpol /set /category:"system","account logon" /success:  
enable /failure:enable  
The command was successfully executed.
```

```
C:\Users\Administrator>
```

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**

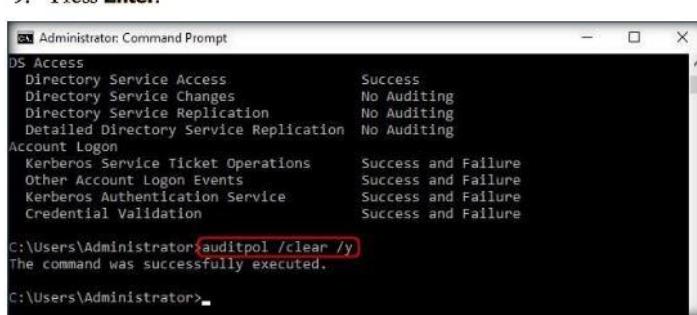
```
C:\Users\Administrator>auditpol /get /category:*
```

Category/Subcategory	Setting
System	Success and Failure
Security System Extension	Success and Failure
System Integrity	Success and Failure
IPSec Driver	Success and Failure
Other System Events	Success and Failure
Security State Change	Success and Failure
Logon/Logoff	Success and Failure
Logon	Success
Logoff	Success
Account Lockout	Success
IPSec Main Mode	No Auditing
IPSec Quick Mode	No Auditing
IPsec Extended Mode	No Auditing
Special Logon	Success
Other Logon/Logoff Events	No Auditing
Network Policy Server	Success and Failure
User / Device Claims	No Auditing
Group Membership	No Auditing
Object Access	No Auditing
File System	No Auditing
Registry	No Auditing
Kernel Object	No Auditing
SAM	No Auditing
Certification Services	No Auditing
Application Generated	No Auditing
Handle Manipulation	No Auditing

FIGURE 16.3: Auditpol enabling system and account logon policies

Module 06 - System Hacking

8. To **clear** the audit policies, type the following at the command prompt:
auditpol /clear /y
9. Press **Enter**.



The screenshot shows an Administrator Command Prompt window. The command entered is `auditpol /clear /y`. The output shows the command was successfully executed.

```
Administrator: Command Prompt
DS Access
Directory Service Access Success
Directory Service Changes No Auditing
Directory Service Replication No Auditing
Detailed Directory Service Replication No Auditing
Account Logon
Kerberos Service Ticket Operations Success and Failure
Other Account Logon Events Success and Failure
Kerberos Authentication Service Success and Failure
Credential Validation Success and Failure
C:\Users\Administrator>auditpol /clear /y
The command was successfully executed.
C:\Users\Administrator>
```

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**.



The screenshot shows an Administrator Command Prompt window. The command entered is `auditpol /get /category:*`. The output shows a table of audit policies with their settings cleared to "No Auditing".

Category/Subcategory	Setting
System	No Auditing
Security System Extension	No Auditing
System Integrity	No Auditing
IPsec Driver	No Auditing
Other System Events	No Auditing
Security State Change	No Auditing
Logon/Logoff	No Auditing
Logon	No Auditing
Logoff	No Auditing
Account Lockout	No Auditing
IPsec Main Mode	No Auditing
IPsec Quick Mode	No Auditing
IPsec Extended Mode	No Auditing
Special Logon	No Auditing
Other Logon/Logoff Events	No Auditing
Network Policy Server	No Auditing
User / Device Claims	No Auditing
Group Membership	No Auditing
Object Access	No Auditing
File System	No Auditing
Registry	No Auditing
Kernel Object	No Auditing
SAM	No Auditing
Certification Services	No Auditing
Application Generated	No Auditing
Handle Manipulation	No Auditing
File Share	No Auditing
Filtering Platform Packet Drop	No Auditing
Filtering Platform Connection	No Auditing
Other Object Access Events	No Auditing
Detailed File Share	No Auditing
Removable Storage	No Auditing
Central Policy Staging	No Auditing
Privilege Use	No Auditing
Non Sensitive Privilege Use	No Auditing
Other Privilege Use Events	No Auditing
Sensitive Privilege Use	No Auditing
Detailed Tracking	No Auditing
Process Creation	No Auditing
Resource Protection	No Auditing

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	
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> iLabs