



### BÁO CÁO THỰC HÀNH

#### Bài thực hành số 16: Viewing, Enabling and Clearing Audit Policies using Auditpol

**Môn học:** Hệ tính toán phân bố

**Lớp:** NT533.Q12.2

#### THÀNH VIÊN THỰC HIỆN (Nhóm 01):

STT	Họ và tên	MSSV	Điểm tự đánh giá
1	Nguyễn Tiến Phát	23521147	10

#### ĐÁNH GIÁ KHÁC:

Tổng thời gian thực hiện	

**Bài thực hành số 16: Viewing, Enabling and Clearing Audit Policies using Auditpol**

Phần bên dưới của báo cáo này là báo cáo chi tiết của sinh viên thực hiện

**MỤC LỤC**

**I. Thực hiện chi tiết..... 3**

## Bài thực hành số 16: Viewing, Enabling and Clearing Audit Policies using Auditpol

### A. BÁO CÁO CHI TIẾT

#### I. Thực hiện chi tiết

Kết nối vào Máy chạy hệ điều hành Windows Servers 2022

##### 1. Launch Command Prompt from the Windows Server 2016 machine.

#### Mục tiêu

- Kết nối vào máy Windows Server 2022 để kiểm tra thông tin hệ thống trước khi thực hiện các thao tác audit và system hacking.
- Xác minh phiên bản hệ điều hành, cấu hình CPU, RAM và ổ đĩa tương tự như phần khởi động môi trường trong Lab mẫu.

Sau khi SSH thành công vào máy Windows Server 2022, tiến hành lần lượt các lệnh kiểm tra hệ thống:

#### 1. Kiểm tra phiên bản OS

```
systeminfo | findstr /B /C:"OS Name" /C:"OS Version"
```

#### 2. Kiểm tra thông tin chi tiết phiên bản Windows

```
reg query "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion" | findstr /I "ProductName  
ReleaseId CurrentBuild DisplayVersion"
```

#### 3. Kiểm tra CPU

```
Get-WmiObject Win32_Processor | Select-Object Name, NumberOfCores, NumberOfLogicalProcessors,  
MaxClockSpeed
```

#### 4. Kiểm tra RAM

```
Get-WmiObject Win32_OperatingSystem | Select-Object TotalVisibleMemorySize, FreePhysicalMemory
```

#### 5. Kiểm tra ổ đĩa

```
Get-PSDrive -PSProvider FileSystem
```

## Bài thực hành số 16: Viewing, Enabling and Clearing Audit Policies using Auditpol

```
Module-06-System-Hacking

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL
Microsoft Windows [Version 10.0.20348.169]
(c) Microsoft Corporation. All rights reserved.

dministrator@WIN-EMEBDIJH4Q7 C:\Users\Administrator>powershell
indows PowerShell
opyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\Administrator> Get-ComputerInfo | Select-Object WindowsProductName, WindowsVersion, OsHardwareAbstractionLayer, OsBuildNumber

WindowsProductName      WindowsVersion OsHardwareAbstractionLayer OsBuildNumber
-----
Windows Server 2022 Datacenter Evaluation 2009          10.0.20348.143          20348

PS C:\Users\Administrator> Get-ItemProperty "HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion" |
>> Select-Object ProductName, ReleaseId, CurrentBuild, DisplayVersion

ProductName      ReleaseId CurrentBuild DisplayVersion
-----
Windows Server 2022 Datacenter Evaluation 2009          20348          21H2

PS C:\Users\Administrator> Get-WmiObject Win32_Processor | Select-Object Name, NumberOfCores, NumberOfLogicalProcessors, MaxClockSpeed

Name      NumberOfCores NumberOfLogicalProcessors MaxClockSpeed
-----
AMD Ryzen 9 6900HS with Radeon Graphics      2              2              3294
AMD Ryzen 9 6900HS with Radeon Graphics      2              2              3294

PS C:\Users\Administrator> Get-WmiObject Win32_OperatingSystem | Select-Object TotalVisibleMemorySize, FreePhysicalMemory

TotalVisibleMemorySize FreePhysicalMemory
-----
4193684              2382376

PS C:\Users\Administrator> Get-PSDrive -PSProvider FileSystem

Name      Used (GB) Free (GB) Provider Root CurrentLocation
-----
C          11.32   48.06 FileSystem C:\ Users\Administrator
D           5.17    0.00 FileSystem D:\

PS C:\Users\Administrator>
```

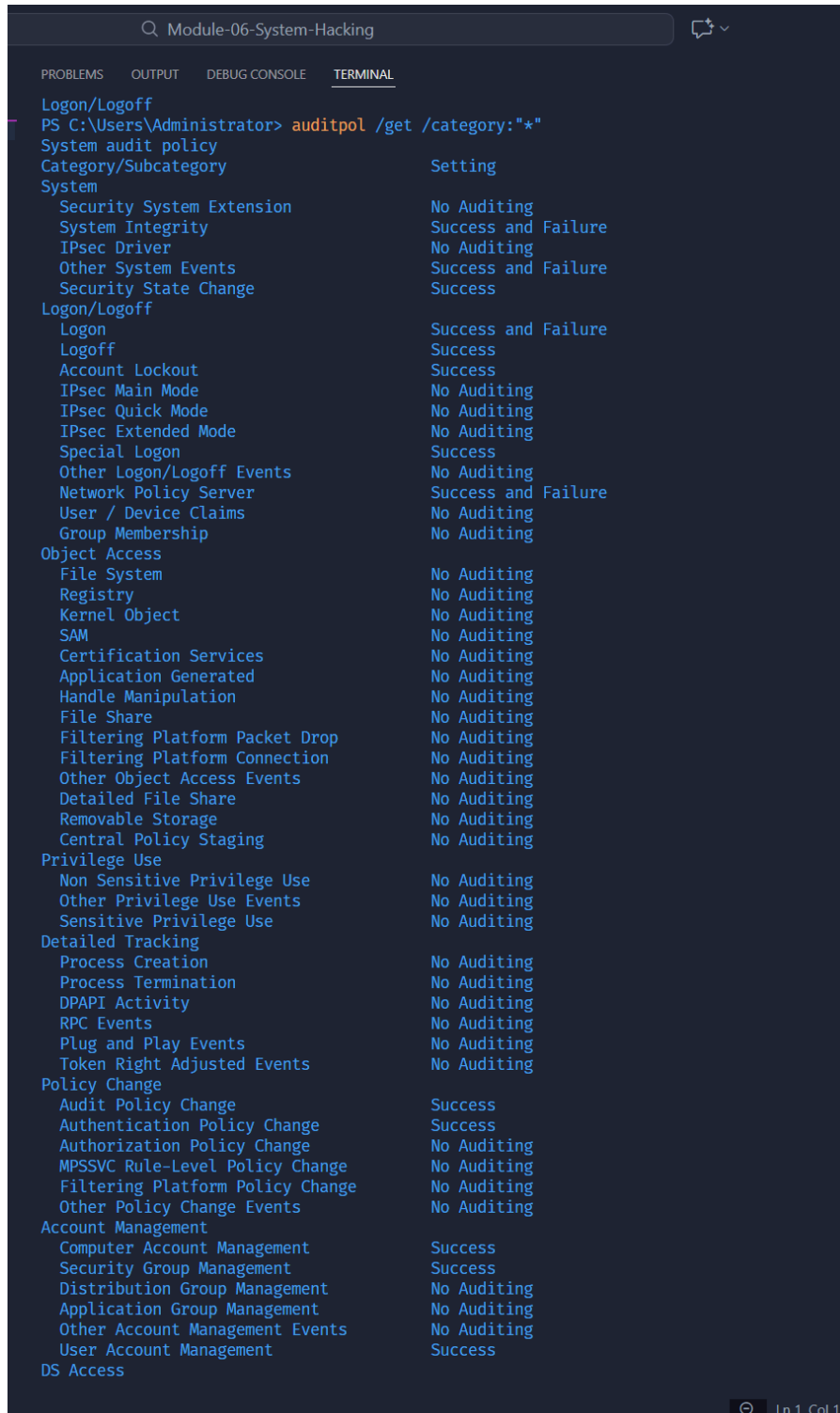
Hệ thống trả về các thông tin chính xác như sau:

- Máy đang chạy **Windows Server 2022 Datacenter Evaluation**, phiên bản:
  - + **OS Version:** 10.0.20348
  - + **Build:** 20348
- CPU:
  - + **AMD Ryzen 9 6900HS**, 8 core / 16 threads, xung tối đa ~3294 MHz
- RAM:
  - + **TotalVisibleMemory:** ~4 GB
  - + **FreeMemory:** ~2.8 GB
- Ổ đĩa:
  - + **C:** ~48 GB free
  - + **D:** 0 GB (drive system hỗ trợ)

## Bài thực hành số 16: Viewing, Enabling and Clearing Audit Policies using Auditpol

2. To view all the audit policies, type the following command: `auditpol/get/category:*`

3. Press Enter.



```
Module-06-System-Hacking
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL
Logon/Logoff
PS C:\Users\Administrator> auditpol /get /category: "*"
System audit policy
Category/Subcategory          Setting
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
  Security Group Management     Success
  Distribution Group Management No Auditing
  Application Group Management  No Auditing
  Other Account Management Events No Auditing
  User Account Management       Success
DS Access
```

### Kết quả thực hiện

Sau khi chạy lệnh:

```
auditpol /get /category: "*"

```

## Bài thực hành số 16: Viewing, Enabling and Clearing Audit Policies using Auditpol

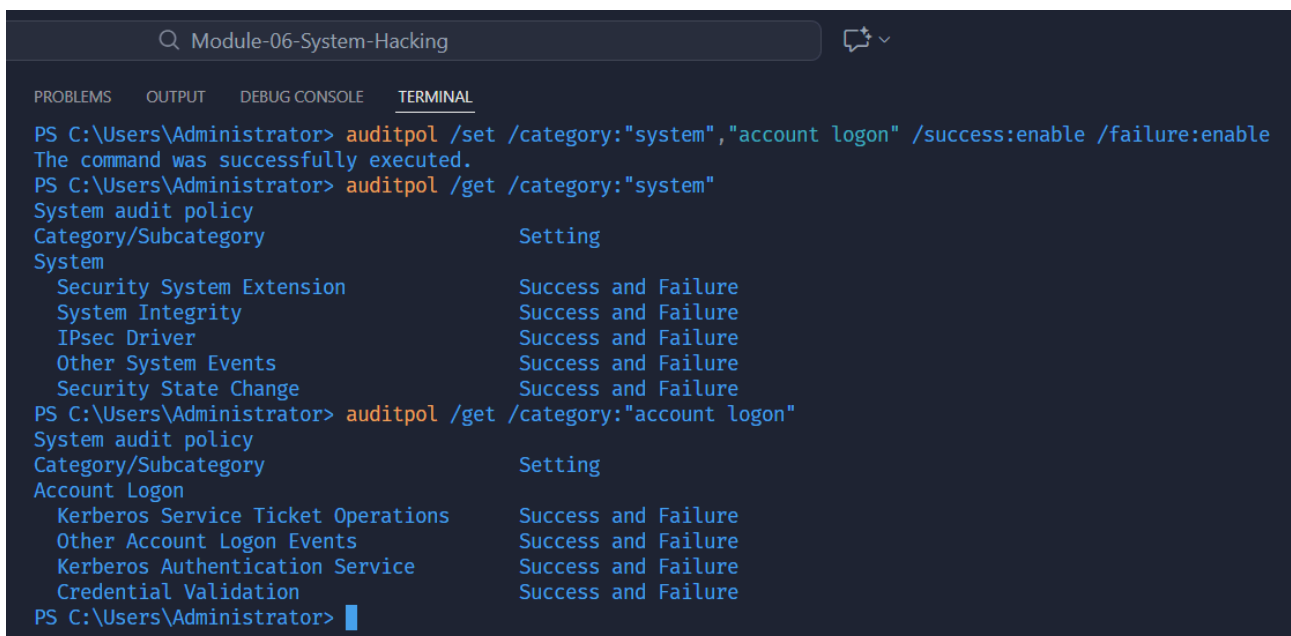
Hệ thống hiển thị toàn bộ các chính sách Audit đang được cấu hình trên Windows Server. Kết quả cho thấy hầu hết các mục đều đang ở trạng thái “**No Auditing**”, bao gồm các nhóm chính như:

- **System** (System Integrity, IPsec Driver, Other System Events...)
- **Logon/Logoff** (Logon, Logoff, Account Lockout...)
- **Object Access** (File System, Registry, SAM...)
- **Privilege Use, Detailed Tracking, Policy Change, và Account Management**

Điều này xác nhận rằng **chưa có chính sách giám sát nào được bật**, phù hợp với trạng thái mặc định của Windows Server trước khi cấu hình AuditPol. Ảnh chụp màn hình dưới đây minh họa đầy đủ các mục và trạng thái tương ứng.

**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.**



```
PS C:\Users\Administrator> auditpol /set /category:"system","account logon" /success:enable /failure:enable
The command was successfully executed.
PS C:\Users\Administrator> auditpol /get /category:"system"
System audit policy
Category/Subcategory      Setting
System
  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
PS C:\Users\Administrator> auditpol /get /category:"account logon"
System audit policy
Category/Subcategory      Setting
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
PS C:\Users\Administrator>
```

### Kết quả thực hiện

Để bật các chính sách audit quan trọng, thực hiện lệnh:

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

Lệnh được thực thi thành công và Windows Server đã kích hoạt đầy đủ các sự kiện cần giám sát thuộc hai nhóm chính:

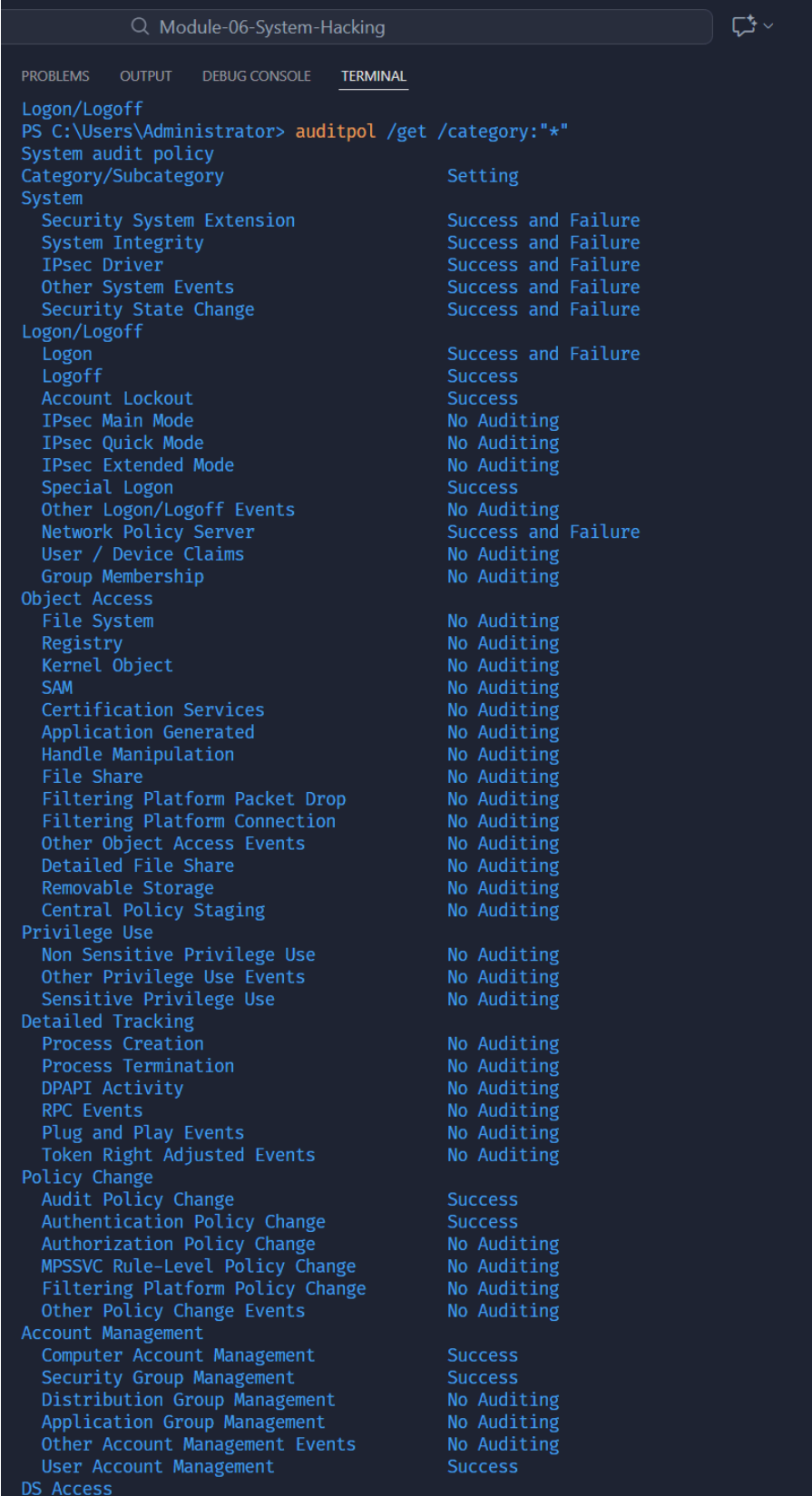
- **System:** Bao gồm Security System Extension, System Integrity, IPsec Driver, Other System Events và Security State Change — tất cả đều chuyển sang trạng thái **Success and Failure**.
- **Account Logon:** Các mục như Kerberos Service Ticket Operations, Authentication Service, Other Account Logon Events và Credential Validation đều được kích hoạt cho cả **Success và Failure**.

## Bài thực hành số 16: Viewing, Enabling and Clearing Audit Policies using Auditpol

Kết quả này được minh họa trong ảnh chụp màn hình, xác nhận rằng hệ thống đã bật toàn bộ các chính sách audit theo yêu cầu để phục vụ các bước phân tích và theo dõi tiếp theo trong bài thực hành.

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

**7. Press Enter**



```
Module-06-System-Hacking
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL
Logon/Logoff
PS C:\Users\Administrator> auditpol /get /category: "*"
System audit policy
Category/Subcategory          Setting
System
  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
  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
  Security Group Management      Success
  Distribution Group Management  No Auditing
  Application Group Management   No Auditing
  Other Account Management Events No Auditing
  User Account Management        Success
DS Access
```

## Bài thực hành số 16: Viewing, Enabling and Clearing Audit Policies using Auditpol

### Kết quả thực hiện

Sau khi chạy lệnh:

```
auditpol /get /category:"*"
```

Hệ thống hiển thị đầy đủ trạng thái của tất cả các nhóm chính sách Audit trên Windows Server. Dựa trên kết quả, có thể thấy các mục thuộc hai nhóm **System** và **Logon/Logoff** đã được kích hoạt thành công (hiển thị trạng thái **Success and Failure**), đúng với cấu hình được thiết lập ở bước trước.

Các nhóm còn lại như **Object Access**, **Privilege Use**, **Detailed Tracking**, **Policy Change** và **Account Management** vẫn giữ nguyên trạng thái **No Auditing** (hoặc Success cho một vài mục mặc định), cho thấy chỉ các policy yêu cầu trong bài lab đã được bật.

Ảnh chụp màn hình bên dưới thể hiện rõ toàn bộ các policy và trạng thái tương ứng sau khi kích hoạt, giúp xác minh rằng cấu hình audit đã được áp dụng chính xác.

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

**9. Press Enter.**

**10. To check whether audit policies cleared, type the following at the command prompt: auditpol /get/category:\***

**11. Press Enter.**

### Kết quả thực hiện

Để đưa toàn bộ hệ thống về trạng thái mặc định, sử dụng lệnh:

```
auditpol /clear /y
```

Lệnh được thực thi thành công và toàn bộ các chính sách Audit trước đó đã được xóa.

Sau đó, kiểm tra lại bằng lệnh:

```
auditpol /get /category:"*"
```

Kết quả cho thấy **tất cả các mục đều trở về trạng thái “No Auditing”**, bao gồm System, Logon/Logoff, Object Access, Privilege Use, Detailed Tracking, Policy Change và Account Management. Điều này xác nhận rằng toàn bộ cấu hình audit đã được xóa hoàn toàn, đúng theo yêu cầu của bài thực hành.



## Bài thực hành số 16: Viewing, Enabling and Clearing Audit Policies using Auditpol

```
Module-06-System-Hacking

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL

Logon/Logoff
PS C:\Users\Administrator> auditpol /clear /y
The command was successfully executed.
PS C:\Users\Administrator> auditpol /get /category:"*"
System audit policy
Category/Subcategory          Setting
System
  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
  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
  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            No Auditing
  Authentication Policy Change  No Auditing
  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    No Auditing
  Security Group Management      No Auditing
  Distribution Group Management  No Auditing
  Application Group Management   No Auditing
  Other Account Management Events No Auditing
```