TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN
**KHOA MẠNG MÁY TÍNH VÀ TRUYỀN THÔNG**

# 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**

# 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
```

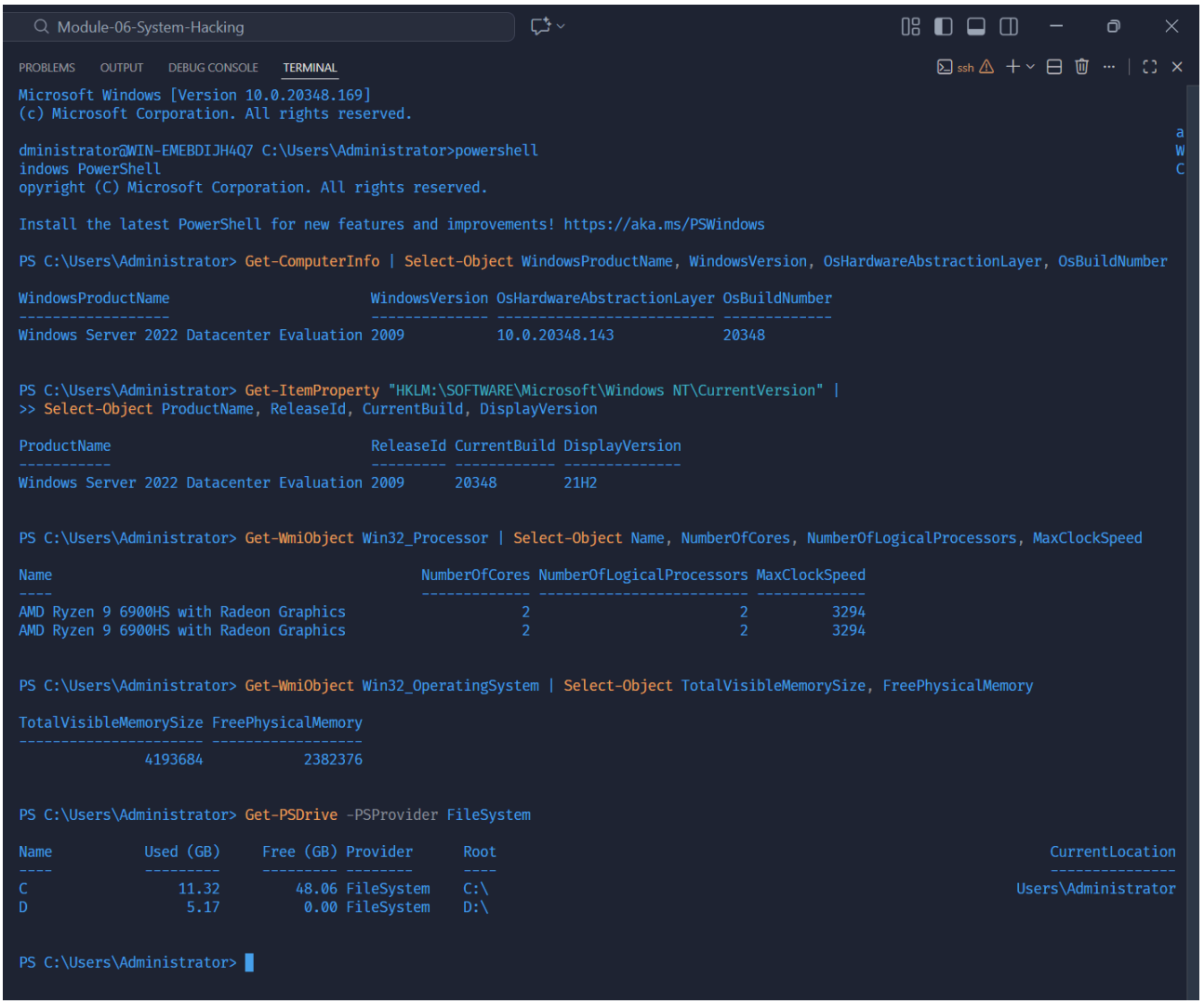
**4. Kiểm tra RAM**

```
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



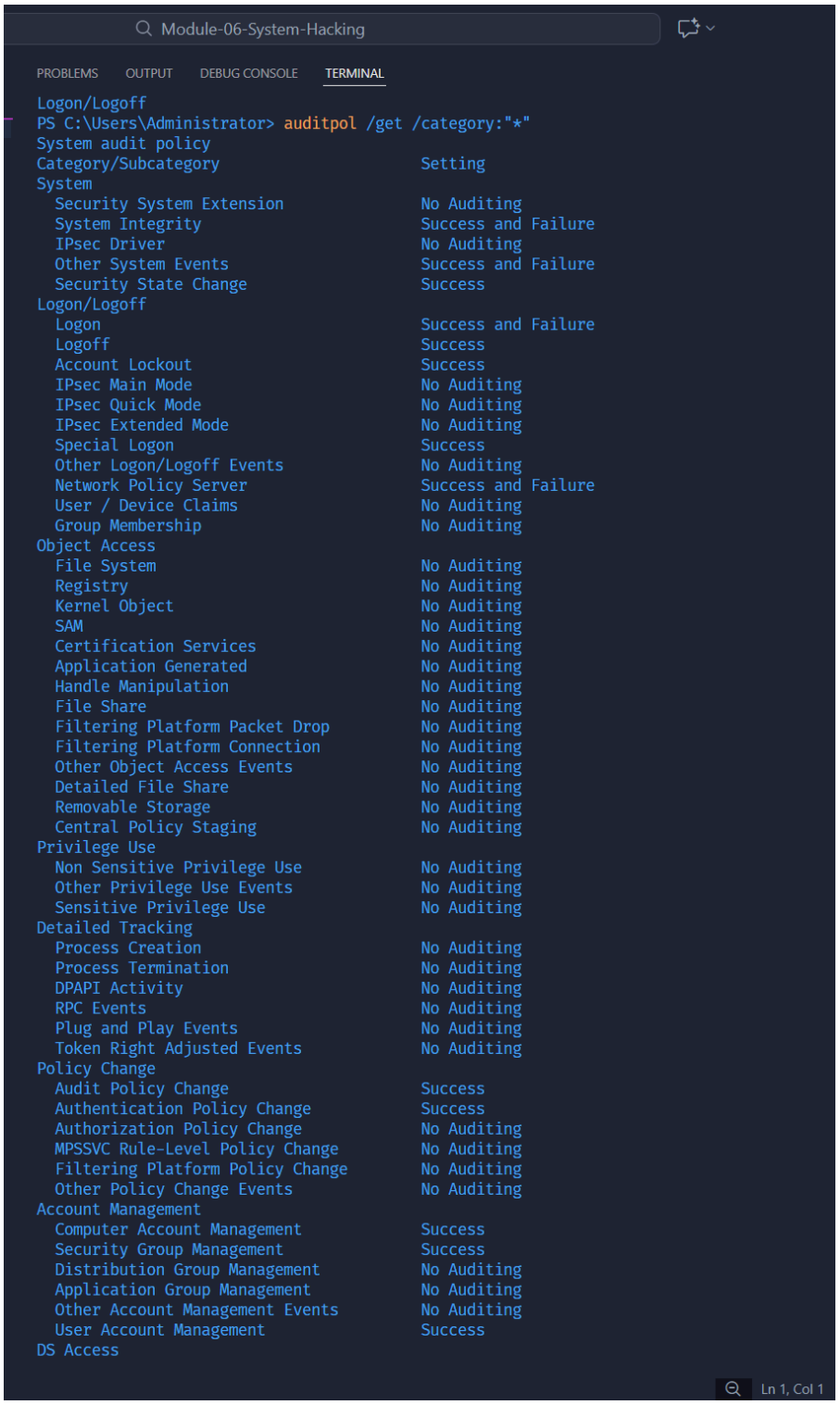

**Hệ thống trả về các thông tin chính xác như sau:**

- 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.**




## Kết quả thực hiện

Sau khi chạy lệnh:

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

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

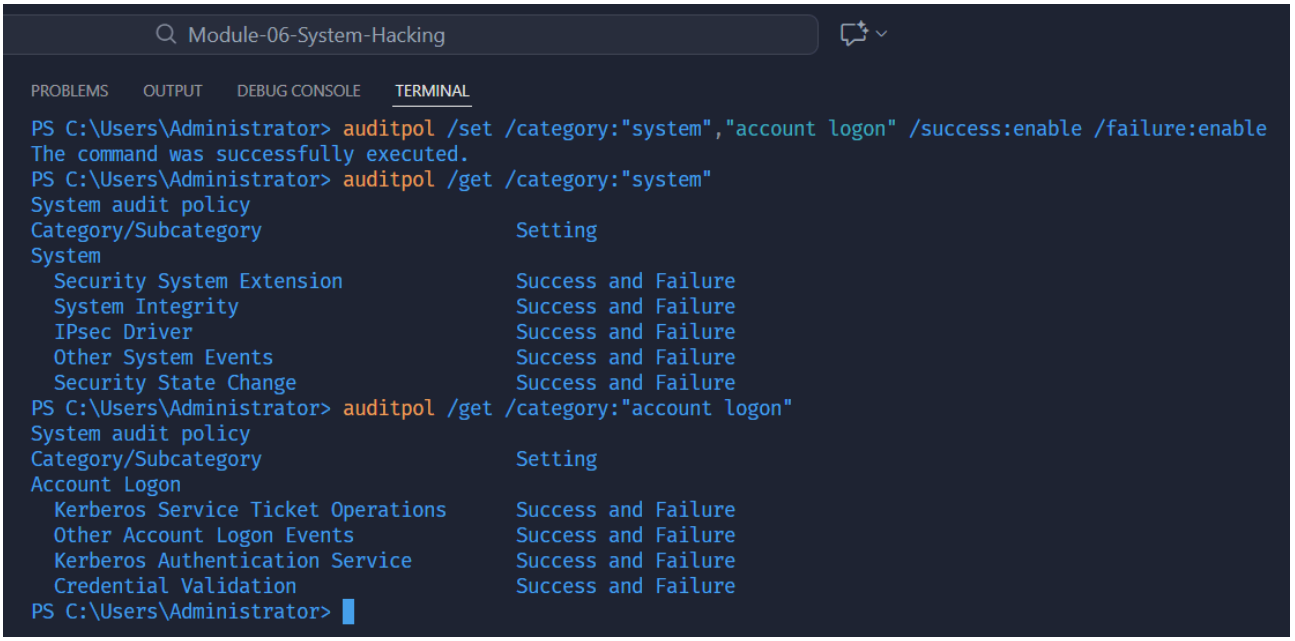
Hệ thống hiển thị toàn bộ các chính sách Audit đang được cấu hình trên Windows Server. Kết quả cho thấy hầu hết các mục đều đang ở trạng thái **"No Auditing"**, bao gồm các nhóm chính như:

- **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.**




### 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**

# 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