

# **EVENT VIEWER AUDIT REPORT**

**ANALYSED BY**

**GLADYS GORDON**

**INSTRUCTOR: MR OLA OLAITAN**

**DATE: September 2024**

## INTRODUCTION

This report analyses five (5) different event IDs using Event Viewer to audit and access the security posture of the host device. Event viewer is a built-in tool in windows operating system that enables you view and manage system logs. It is very useful for performing security auditing. From this analysis, we can identify any potential threats or troubleshoot any issues with the host device.

## ANALYSIS OF THE EVENT IDS

### 1. Event ID: 5379

Task Category: User Account Management

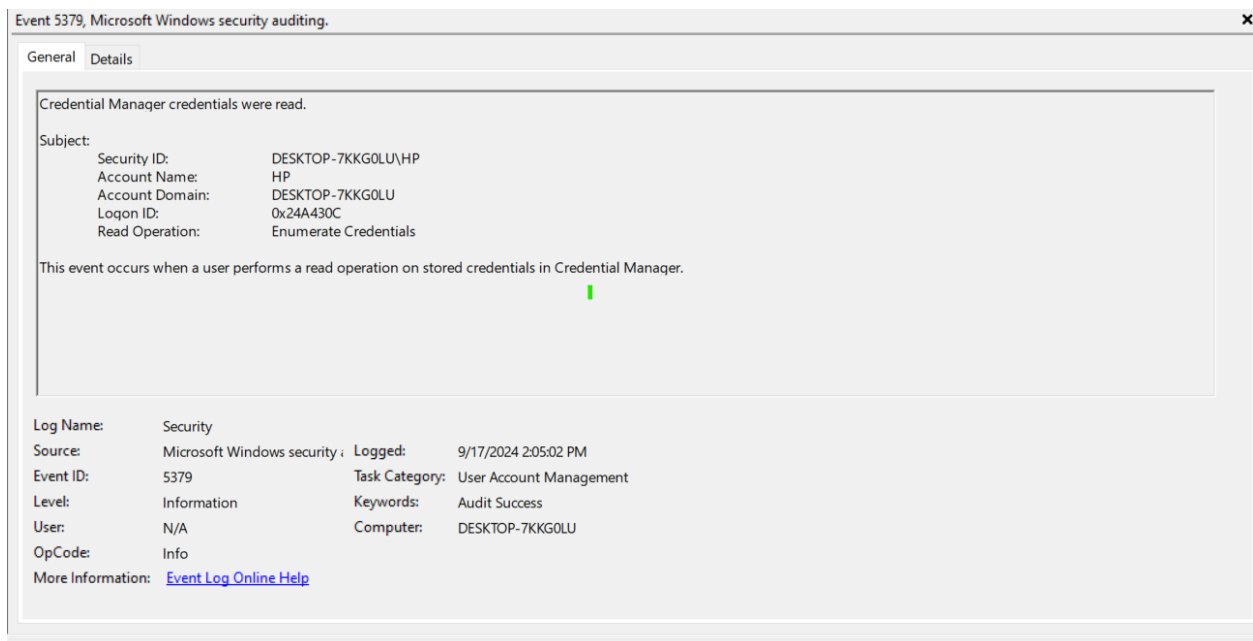
Security ID: DESKTOP-7KKG0LU

Account name: HP

Date: 9/17/2024 2:05:02 PM

Keywords: Audit Success

Credential Manager credentials were read and returned successful



2. Event ID: 4672

Security

Number of events: 33,519 (1) New events available

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	9/17/2024 2:05:02 PM	Microsoft Windows security au...	5379	User Account Management
Audit Success	9/17/2024 2:05:02 PM	Microsoft Windows security au...	5379	User Account Management
Audit Success	9/17/2024 2:05:02 PM	Microsoft Windows security au...	5379	User Account Management
Audit Success	9/17/2024 2:05:00 PM	Microsoft Windows security au...	4672	Special Logon
Audit Success	9/17/2024 2:05:00 PM	Microsoft Windows security au...	4624	Logon
Audit Success	9/17/2024 2:04:58 PM	Microsoft Windows security au...	5379	User Account Management
Audit Success	9/17/2024 2:04:58 PM	Microsoft Windows security au...	5379	User Account Management
Audit Success	9/17/2024 2:04:58 PM	Microsoft Windows security au...	5379	User Account Management

Event 4672, Microsoft Windows security auditing.

General

Details

Special privileges assigned to new logon.

Subject:

Security ID: SYSTEM  
Account Name: SYSTEM  
Account Domain: NT AUTHORITY  
Logon ID: 0x3E7

Privileges:

SeAssignPrimaryTokenPrivilege  
SeTcbPrivilege  
SeSecurityPrivilege  
SeTakeOwnershipPrivilege  
SeLoadDriverPrivilege  
SeBackupPrivilege  
SeRestorePrivilege  
SeDebugPrivilege  
SeAuditPrivilege

Log Name:

Security

Source:

Microsoft Windows security : Logged:

9/17/2024 2:05:00 PM

Event ID:

4672

Task Category:

Special Logon

Level:

Information

Keywords:

Audit Success

User:

N/A

Computer:

DESKTOP-7KKG0LU

OpCode:

Info

More Information:

[Event Log Online Help](#)

Task Category: Special Logon

Security ID: System

Account name: System

Account domain: NT Authority

Date: 9/17/2024 2:05:00 PM

Keywords: Audit success

Special privileges assigned to new logon.

### 3. Event ID: 4624

Task Category: Logon

Security ID: System

Account Name: DESKTOP-7KKG0LU\$

Account Domain: WORKGROUP

Date: 9/17/2024 2:05:00 PM

Keywords: Audit Success

An account was successfully logged on.

### 4. Event ID: 1102

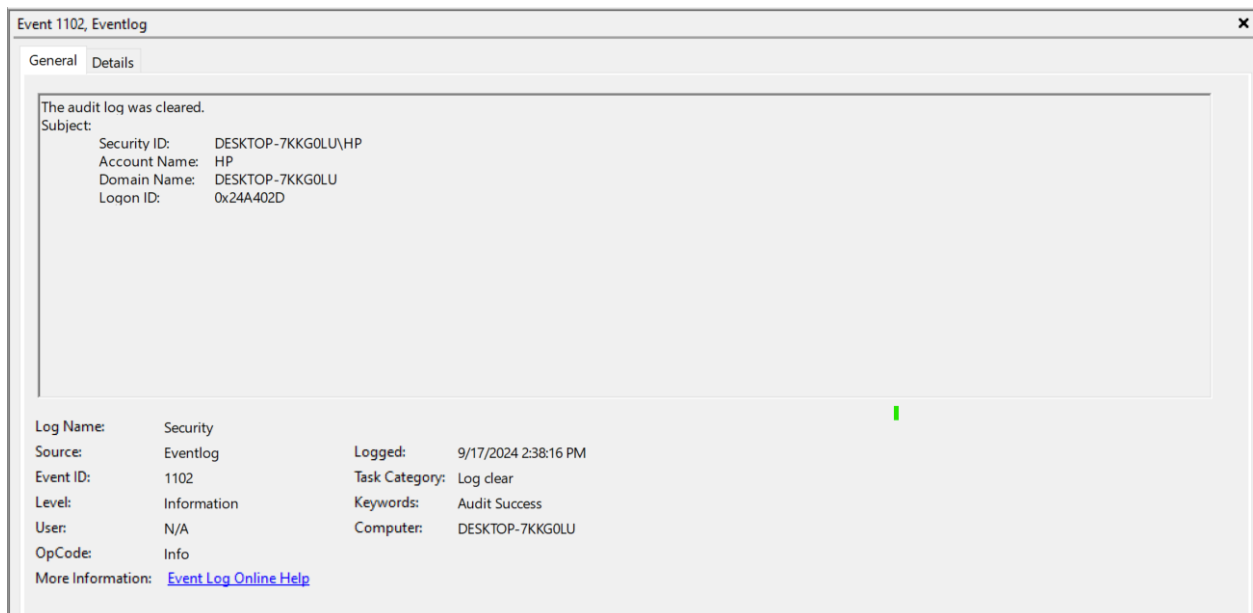
Task Category: Log clear

Security ID: DESKTOP-7KKG0LU\HP

Date: 9/17/2024 2:38:16 PM

Keywords: Audit Success

The audit log was cleared successfully



5. Event ID: 7045

Source: Service Control Manager

Task category: None

Date: 9/17/2024 9:47:58 AM

Event ID: 7045

Keywords: Classic

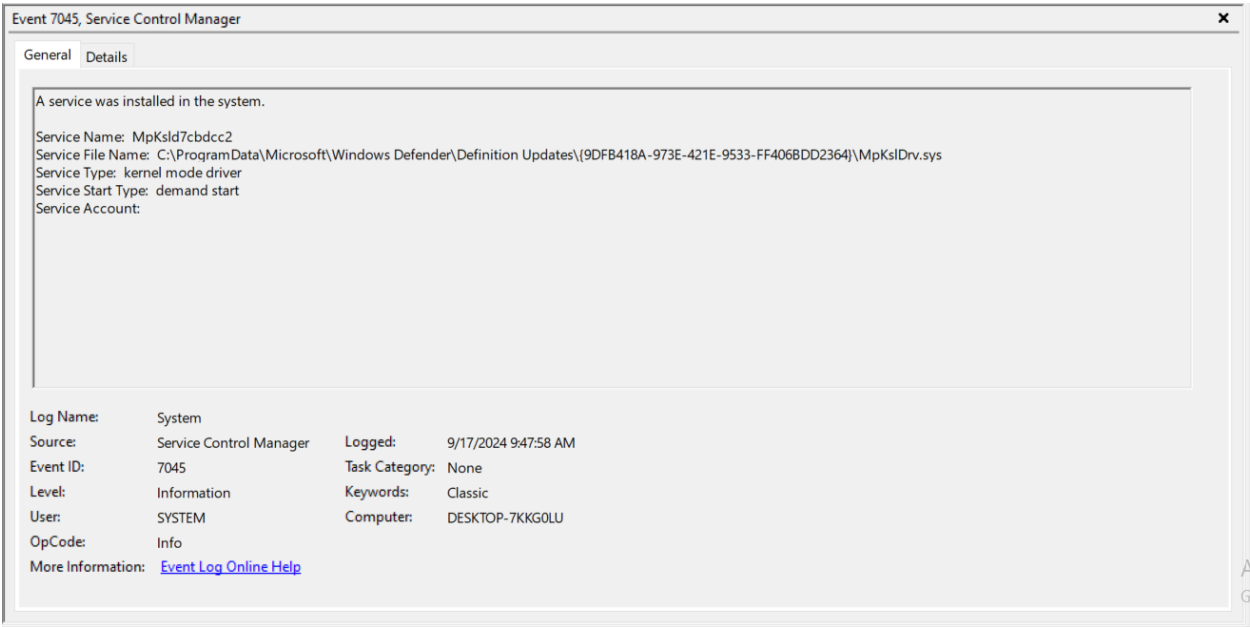
A service was installed in the system.

Service Name: MpKsld7cbdcc2

Service File Name: C:\ProgramData\Microsoft\Windows Defender\Definition Updates\{9DFB418A-973E-421E-9533-FF406BDD2364}\MpKslDrv.sys

Service Type: kernel mode driver

Service Start Type: demand start



Security Posture Assessment

Based on the review of the event IDs and logs above, the host device exhibits a generally healthy security posture with no major vulnerabilities detected. There were no signs of unauthorized access, privilege escalation, or malicious behavior.

## **Recommendations**

Regular auditing using Event Viewer and other monitoring tools should continue to maintain a high level of security and to detect potential threats early.