Detecting Lateral Movement through Tracking Event Logs (Version 2)

JPCERT/CC

December 05, 2017

Table of Contents

1. Introduction

Many recent cyberattacks have been confirmed in which malware infects a host and in turn spreads to other hosts and internal servers, resulting in the whole organization becoming compromised. In such cases, many points need to be investigated. Accordingly, an approach for quickly and thoroughly investigating such critical events, ascertaining the overall picture of the damage as accurately as possible, and collecting facts necessary for devising remedial measures is required.

While the configuration of the network that is targeted by an attack varies depending on the organization, there are some common patterns in the attack methods. First, an attacker that has infiltrated a network collects information of the host it has infected using "ipconfig", "systeminfo", and other tools installed on Windows by default. Then, they examine information of other hosts connected to the network, domain information, account information, and other information using "net" and other tools. After choosing a host to infect next based on the examined information, the attacker obtains the credential information of the user using "mimikatz", "pwdump", or other password dump tools. Then, by fully utilizing "net", "at", or other tools, the attacker infects other hosts and collects confidential information.

For such conventional attack methods, limited set of tools are used in many different incidents. The many points that need to be investigated can be dealt with quickly and systematically by understanding typical tools often used by such attackers, and what kind of and where evidence is left.

For such use of tools, the Japan Computer Emergency Response Team Coordination Center (JPCERT/CC) extracted tools used by many attackers by investigating recently confirmed cases of targeted attacks. Then, a research was conducted to investigate what kind of logs were left on the server and clients by using such tools, and what settings need to be configured to obtain logs that contain sufficient evidential information. This report is a summary of the results of this research.

The outline of this report is as follows. First, Chapter 2 describes the environment and the tools used for this research. Next, Chapter 3 describes the "Tool Analysis Result Sheet" created based on the results of this research. Then, Chapter 4 explains how to investigate an incident based on this research results described in Chapter 3.

2. Research Method

This chapter describes the method that was used for this research.

2.1. Approach

The research aims to provide basic information which is useful in log analysis by investigating evidence of tools used by many attackers. More specifically, this report aims to be a dictionary that can be used as a guide for effective log analysis by identifying which tools were used based on logs or which log is recorded when a certain tool is executed.

In this research, tools that are used by many attackers were investigated. The specific tools that JPCERT/CC knows are used by many attackers are described in the next section. The following log items, including event logs and execution history, were investigated so that persons who are not experts in incident investigation can analyze more easily: Note that it was confirmed that traces of tool execution is most likely to be left in event logs. Accordingly, examination of event logs is the main focus in this report.

- Event log
- Execution history
- Prefetch
- USN journal
- MFT
- UserAssist
- Packet Capture

Note that a sufficient amount of event logs cannot be acquired with the default Windows settings. In this research, logs that are recorded with the following settings were examined:

- Audit policy enabled
- Sysmon installed

The audit policy is a default Windows setting for acquiring detailed logs about logon, logoff, file access, etc. The audit policy can be confirmed and its settings can be changed from the local group policy.

Sysmon is a tool provided by Microsoft that enables process startup, network communication, file

changes, etc., to be recorded in event logs. Installing Sysmon enables recorded logs from Event Viewer to be checked as shown below.

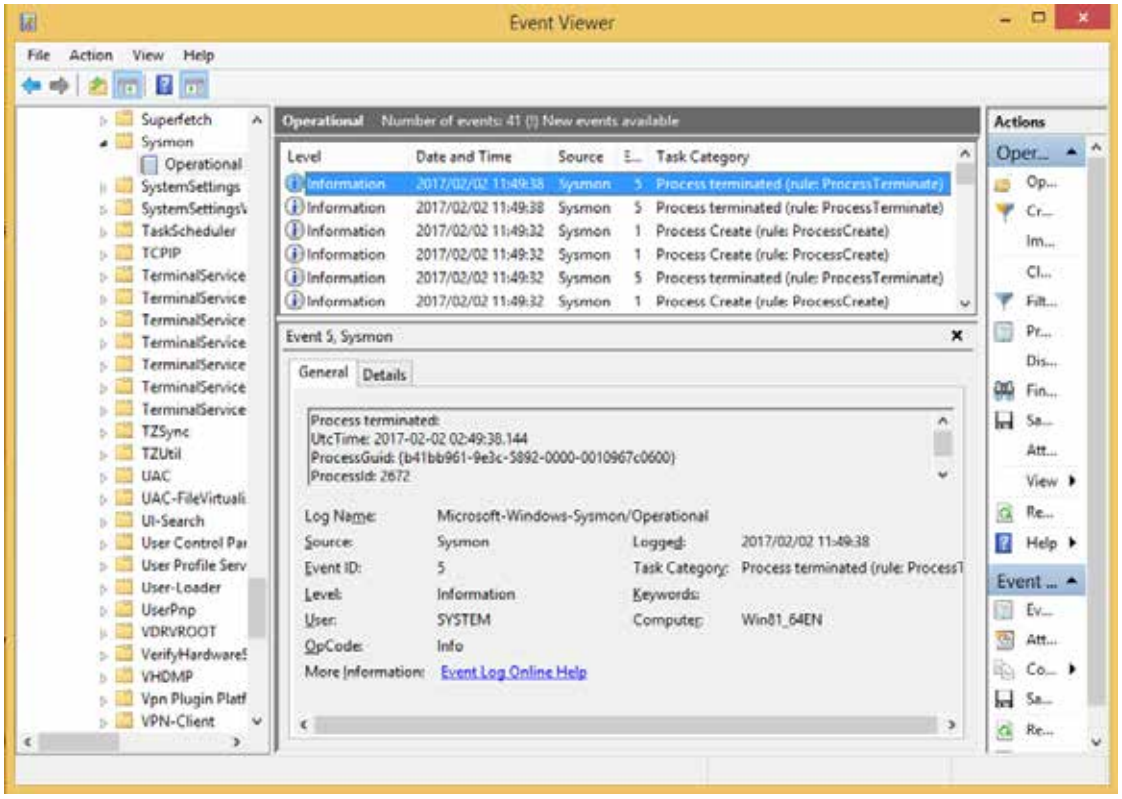


Fig. 2-1: Checking Sysmon Logs from Event Viewer

In this research, the tools listed in Section 2.2 were actually executed on a virtual network made up of Windows Domain Controller and a client. By checking changes in the system before and after executing each tool, logs recorded in the OS were examined. The network environment used for this research are described in detail in Section 2.3.

2.2. Tested Tools

Among tools observed in multiple incidents JPCERT/CC handled, 49 tools that are directly related to attack operations were selected as typical tools, such as command execution, obtaining password hash, and remote login, were selected as tools used by many attackers. Table 2-1 shows these tools grouped by the attackers' purpose of use.

Table 2-1: List of Tested Tools

Attacker's Purpose of Using Tool	Tool
Command execution	PsExec
	wmic
	schtasks

	wmiexec.vbs
	BeginX
	WinRM
	WinRS
	BITS
Password and hash dump	PWDump7
	PWDumpX
	Quarks PwDump
	Mimikatz (Password and hash dump lsadump::sam)
	Mimikatz (Password and hash dump sekurlsa::logonpasswords)
	Mimikatz (Ticket acquisition sekurlsa::tickets)
	WCE
	gsecdump
	lslsass
	AceHash
	Find-GPOPasswords.ps1
	Get-GPPPassword (PowerSploit)
	Invoke-Mimikatz (PowerSploit)
	Out-Minidump (PowerSploit)
	PowerMemory (RWMC Tool)
	WebBrowserPassView
Malicious communication relay (Packet tunneling)	Htran
	Fake wpad
Remote Login	RDP
Pass-the-hash **Pass-the-ticket**	WCE (Remote login)
	Mimikatz (Remote login)
Escalation to SYSTEM privilege	MS14-058 Exploit
	MS15-078 Exploit
	SDB UAC Bypass
Capturing domain administrator rights account	MS14-068 Exploit
	Golden Ticket (Mimikatz)
	Silver Ticket (Mimikatz)
Adding or deleting local user and group	net user

File sharing	net use
Deleting evidence	sdelete
	timestomp
	klist purge
	wevtutil
Information collection	ntdsutil
	vssadmin
	csvde
	ldifde
	dsquery
	dcdiag
	nltest
	nmap

2.3. Research Environment

A simplified system with a client and server, was built on a virtual network as a target. The selected tools were executed in the environment to observe changes to files and registries resulting from the execution. By installing the following versions of Windows OS on the server and client, the system was tested. In each system configuration, Active Directory service was configured on the server to manage the client computer.

- OS installed on the client
  - Windows 7 Professional Service Pack 1
  - Windows 10
- OS installed on the server
  - Windows Server 2012 R2

3. Research Results

In this research, the tools listed in Section 2.2 were actually executed on a virtual network. By checking changes in the system before and after executing each tool, execution history, event logs, registry entry, and file system records were examined. In addition, for tools that perform a distinctive pattern of communication, packet captures were also examined. The results of the research were published on the following website.

Tool Analysis Result Sheet: https://jpcertcc.github.io/ToolAnalysisResultSheet/

The above website summarizes the basic information including functionality of the tools tested in this research and log information recorded when the relevant tools were executed. The research results also describe the details of logs that can be acquired when the settings described in section 2.1 are configured. (Note that how to set up the audit policy and how to install Sysmon are described in Chapter 7.)

3.1. Structure of Tool Analysis Result Sheet

The Tool Analysis Result Sheet describes the results of analyzing 49 tools. The analysis results for each tool are described in a table format. The content described for each item is explained as follows:

① Tool Overview

- Ø An explanation of the tool and an example of presumed tool use during an attack are described.

② Tool Operation Overview

- Ø Privileges for using the tool, communication protocol, and related services are described.

③ Information Acquired from Log

- Ø An overview of logs acquired at tool execution with the default settings (standard settings) as well as when an audit policy is set or Sysmon is installed is described.

④ Evidence that can be confirmed when execution is successful

- Ø The method to confirm successful execution of the tool.

⑤ Main Information Recorded at Execution

- Ø Important information that can be used for the investigation of records in the target event logs, registry, USN Journal, MFT, and so on.

⑥ Details

- Ø All logs to be recorded, except ones included in (5), are described.

⑦ Remarks

- Ø Any logs that may be additionally recorded and items confirmed during verification are described.

4. Acquiring Additional Logs

This chapter describes the importance of acquiring detailed logs that cannot be obtained with the default settings as stated in the findings, and matters that should be taken into consideration when acquiring additional detailed logs.

4.1. Importance of Acquiring Additional Logs

This research found that the tools installed by default in Windows leave execution traces of evidence in event logs, but most tools that are not installed in Windows do not leave execution traces of evidence anywhere. For example, Remote Desktop Protocol (RDP), a tool for remote login, and "at", a tool for scheduling tasks, leave evidence of execution in the event logs Microsoft¥Windows¥TerminalServices-LocalSessionManager¥Operational and Microsoft¥Windows¥TaskScheduler¥Operational, respectively, indicating that the tools have been executed.

Conversely, in an environment where the audit policy is enabled and Sysmon is installed for acquiring additional logs, evidence of execution of most tools can be acquired. For example, by configuring audit policy settings, when a temporary file is created, it can be recorded in the event log. As a result, if an attacker attempts to collect account information by using "csvde", the temporary file that is created, C:¥Users¥[User_Name]¥AppData¥Local¥Temp¥csv[Random_Number].tmp, is recorded in the event log. To investigate the execution of tools, these settings need to be configured in advance to acquire detailed logs.

Note that detailed logs can be acquired with audit software (such as asset management software) without enabling the audit policy and installing Sysmon. When such software monitors the following Windows OS operations, it can be recorded in a similar manner as in an environment where the audit policy is enabled and Sysmon is installed:

- Executing processes
- Writing files

4.2. Precautions When Changing the Additional Log Acquisition Settings

The increase in the amount of logs should be considered in advance when acquiring additional detailed logs. Because the amount of logs increases when the audit policy is enabled, log rotation accelerates, and older logs are maintained for a shorter period of time. Therefore, when enabling the audit policy, consider changing the maximum size of event logs at the same time. The maximum size of event logs can be changed with Event Viewer or the "wevtutil" command.

Note that changing the maximum size of event logs may exhaust storage capacity. JPCERT/CC recommends that storage capacity be evaluated before changing the maximum size of event logs.

5. How to Use the Tool Analysis Result Sheet in Incident Investigation

This chapter describes how the Tool Analysis Result Sheet can be used through same incident investigation examples.

5.1. Incident Investigation Using This Report

The Tool Analysis Result Sheet was created on the assumption that it will be used when identifying tools that might be executed as part of incident investigations. Searching for keywords, such as an event ID and file name of a characteristic event log and a registry entry found during incident investigation, can find out possible tools that were executed.

An incident investigation often checks any suspicious logs in the "Security" event log. Then, if "Event ID: 4663 (An attempt was made to access an object)" is found for example, it is assumed that there is evidence that the file 192.168.100.100-PWHashes.txt was created temporarily (recorded when the audit policy is enabled). Searching the Tool Analysis Result Sheet for the distinctive text PWHashes.txt finds it is a file created when PWDumpX is executed.

Further proceeding with the investigation while referring to the Tool Analysis Result Sheet finds that "PWDumpX" is a command attackers execute to acquire a password hash. Additionally, the fact that the temporary file [Destination_Address]-PWHashes.txt was created implies that the attacker had completed the purpose of acquiring the password hash on the server with IP address 192.168.100.100.

Investigating the server with IP address 192.168.100.100 explains that the file C:¥Windows¥System32¥DumpSvc.exe was created and executed, and the fact that the service "PWDumpX Service" was installed is recorded as "Event ID: 7045 (A service was installed in the system)." This allows for determining that the attacker acquired the password hash for the IP address 192.168.100.100.

Section 3.2 describes how to verify that each tool was executed. Referring to the section for planning an investigation strategy in advance of commencing an incident investigation is encouraged as it shows information recorded by each tool in a list.

6. Conclusion

As it is becoming apparent that many organizations have suffered damage due to targeted attacks, the importance of incident investigations to further examine such damage is increasing. This report and the Tool Analysis Result Sheet summarize and present evidence suggesting the execution of tools and their corresponding relationship with tools, which are the key to a successful incident investigation.

Many tools do not leave evidence of having been executed with the default Windows settings, which may cause incident investigations to remain unsolved. To analyze what the attacker did in detail, an environment that allows for more logs to be collected than those obtained with the default settings needs to be prepared in advance.

Under the current circumstances where it is difficult to prevent infiltration of a network, it is important to always consider and improve the method for acquiring logs to analyze the amount of damage after an incident occurs in order to prevent the spread of damage and review post-incident security measures. In addition to reviewing and being prepared for responses that are not limited to the method for acquiring additional logs using Windows standard functionality as shown in this report, also use other methods that combine the use of audit software or similar. Moreover, JPCERT/CC recommends that this report be used to identify evidence of tool execution by attackers in the event of a suspicious incident. JPCERT/CC hopes that this report will be of help in early detection and accurate response to targeted attacks, which are becoming more sophisticated.

7. Appendix A

This appendix describes how to install Sysmon and how to enable the audit policy. Note that it has been confirmed that setting up the audit policy and installing Sysmon will increase the amount of event logs. Before enabling the setting and installing the tool, it is recommended to verify its impact.

7.1. How to Install Sysmon

1. Download Sysmon from the following site:

   https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon

2. Execute the command prompt as a user with administrator privileges and execute the following command:

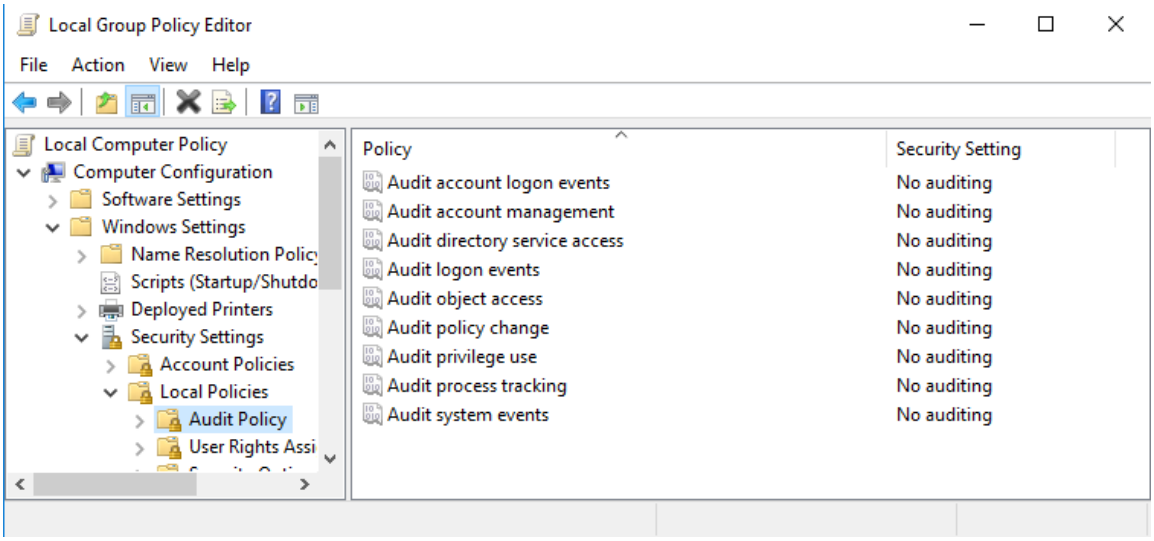
```
> Sysmon.exe -i
```

* Although adding the option "-n" enables network connection logs to be acquired, network connection should be dealt with in the audit policy.

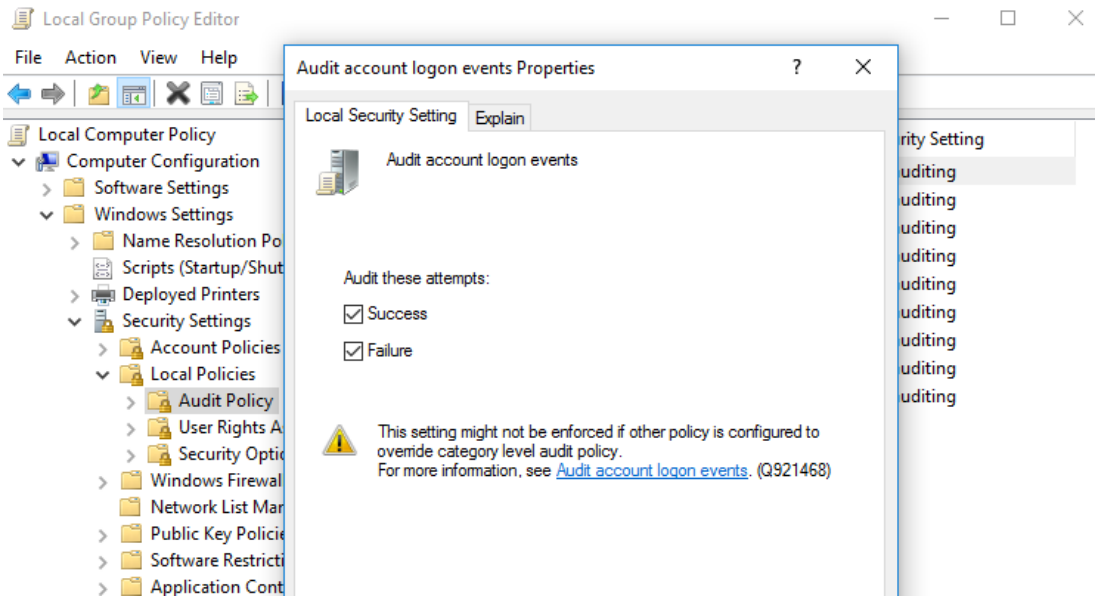
7.2. How to Enable the Audit Policy

The following describes how to enable the audit policy on a local computer. Note that the following shows settings in Windows 10.

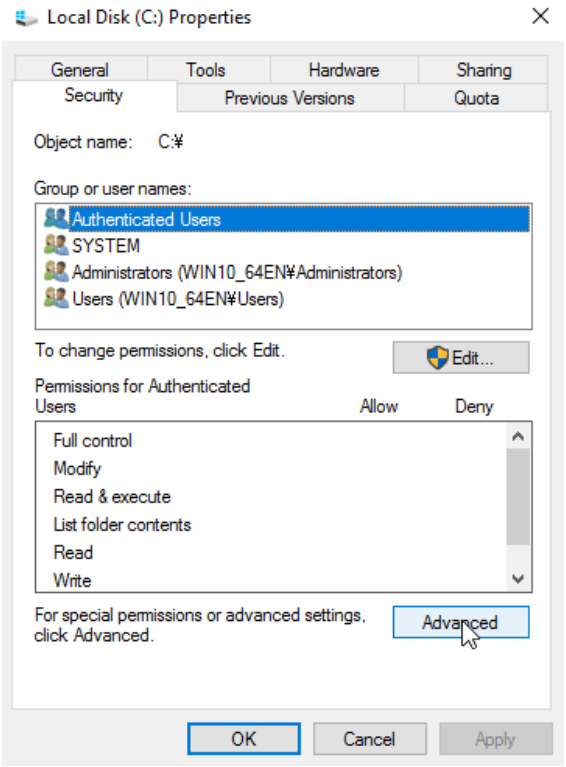
1. Open the Local Group Policy Editor. (Enter "gpedit.msc" into the [Search] box and execute it.)



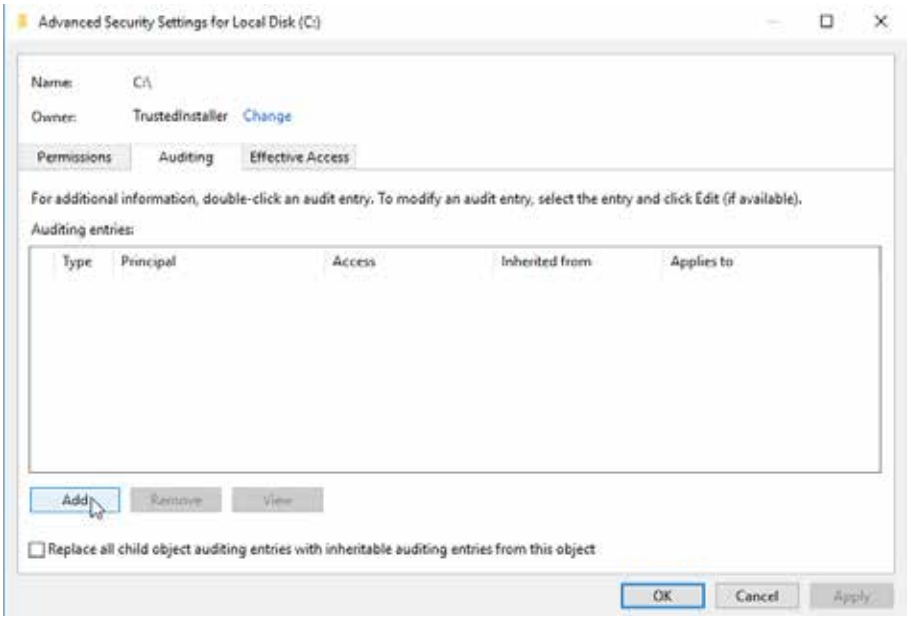
2. Select [Computer Configuration]→[Windows Settings]→[Security Settings]→[Local Policies]→[Audit Policy], and enable "Success" or "Failure" for each policy.



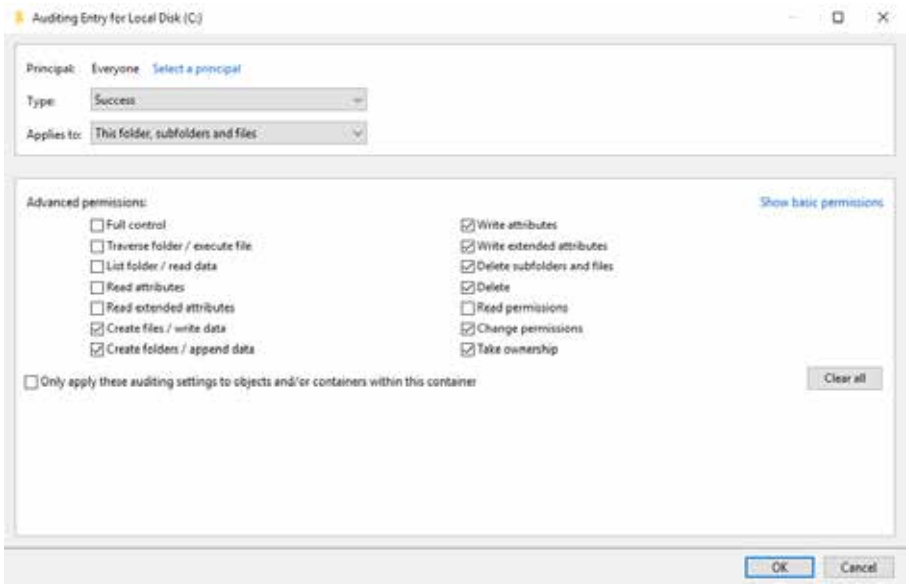
3. Select [Local Disk (C:)]→[Properties]→[Security] tab→[Advanced].



4. On the [Auditing] tab, add an object to be audited.



5. As shown below, select the user to be audited and access method to be audited.



The "Permissions" set here are as follows. (Although recording file read enables a more detailed investigation, it is excluded as doing so will increase the amount of logs.)

- Create files / write data
- Create folders / append data
- Write attributes
- Write extended attributes
- Delete subfolders and files
- Delete
- Change permissions

l Take ownership

Although configuring the above settings displays many errors as shown below, select "Continue."