letsdefend.io

INTRODUCTION TO

EVENT LOG ANALYSIS

for SOC Analysts

LetsDefend

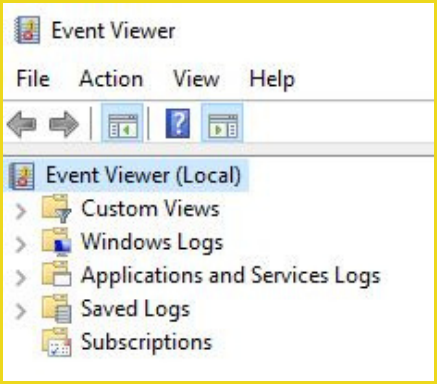
TABLE OF CONTENTS

LetsDefend

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.



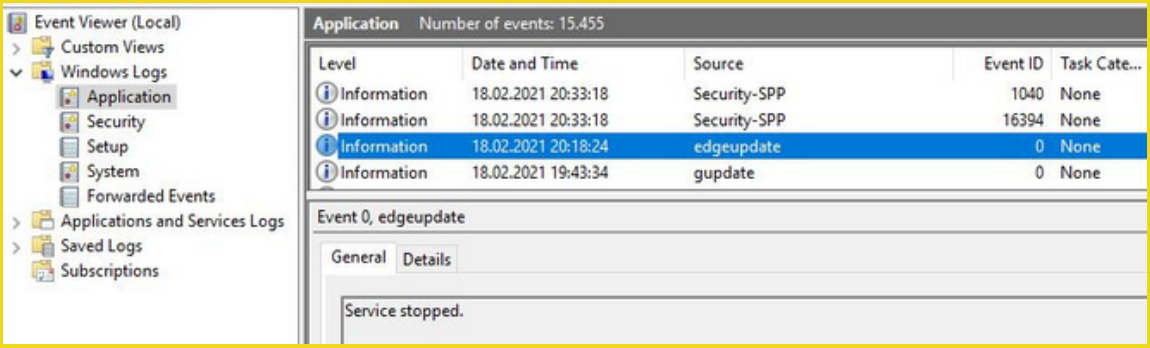
It is often possible to obtain the following evidence with event log analysis:
-Service start, stop
-RDP activity
-Changing user privileges
-Failed login activities
These actions are among the most basic actions seen in any cyber attack. Therefore, event log analysis is really important to find the root cause of the cyber attack.
In Windows systems, there are three main event log titles as Application, System and Security.

LetsDefend

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:



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.

LetsDefend

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/encyclopedia/default.aspx

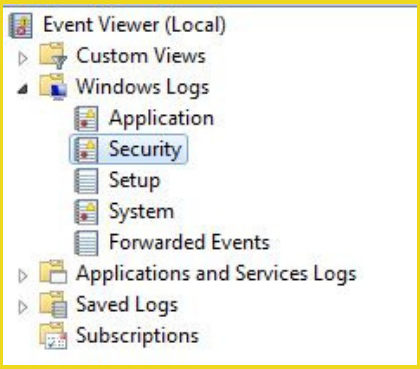
Investigation of Login Records

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".

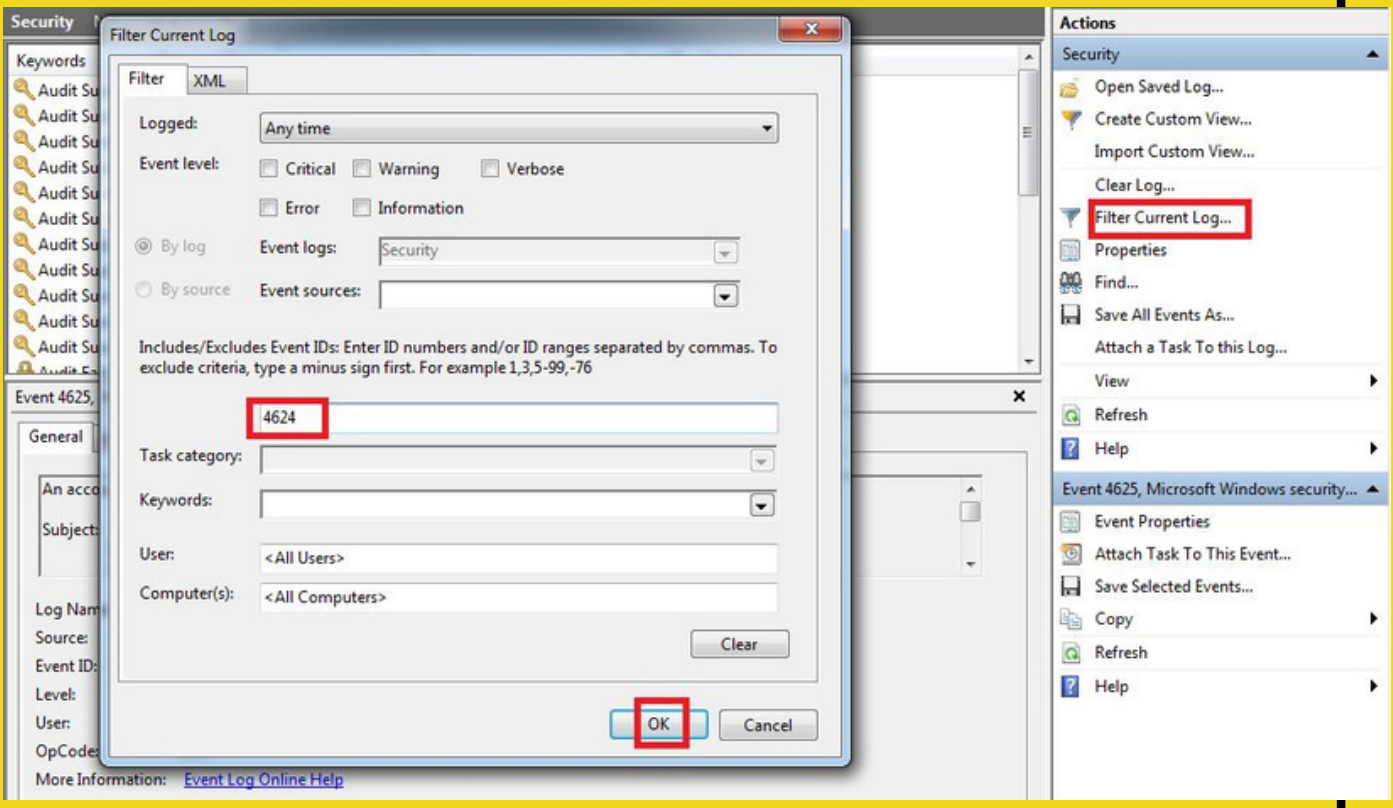
Log file for lesson:
Log_File.zip Pass=321
To reach the result, we open the "Event Viewer" and select "Security" logs.
https://app.letsdefend.io/academy/lesson/Analysis-Successful-Logon-Events/

LetsDefend

ANALYSIS SUCCESSFUL LOGON EVENTS



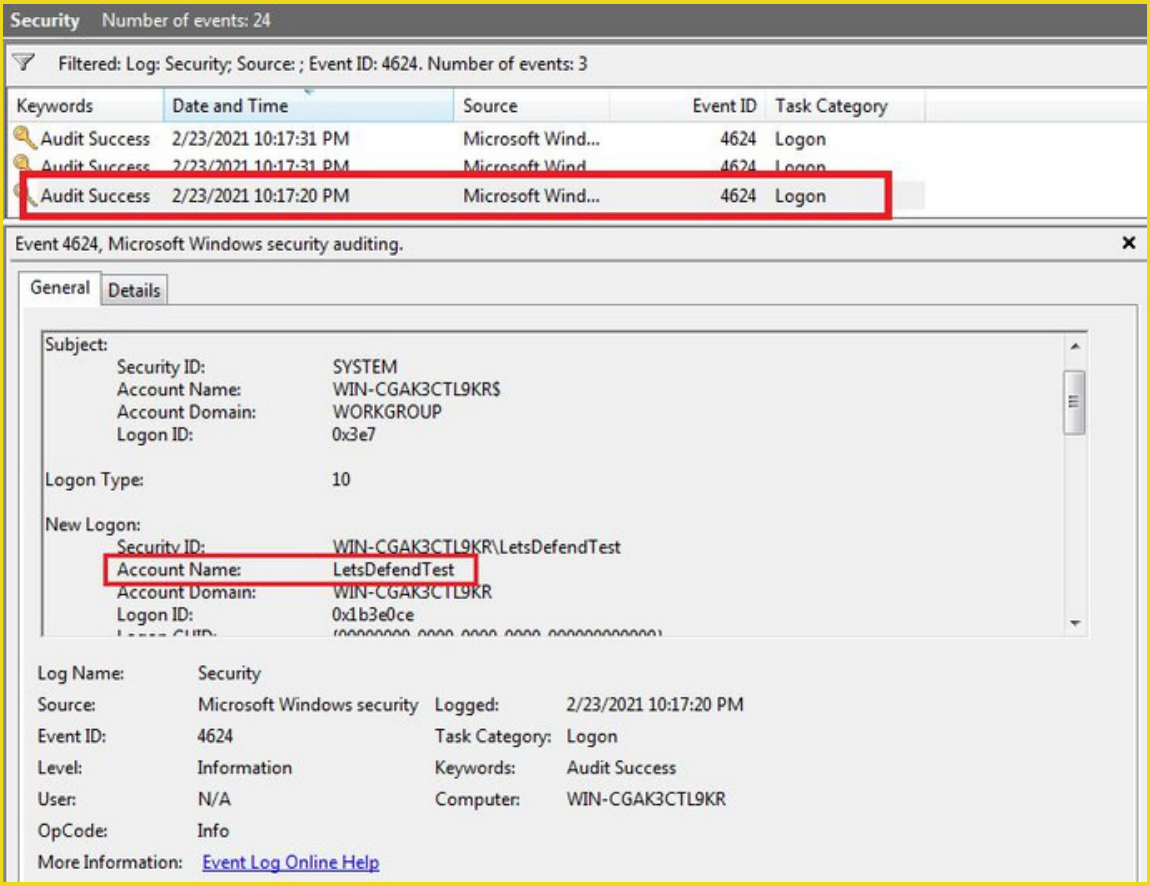
Then we create a filter for the “4624” Event ID.



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.

LetsDefend

ANALYSIS SUCCESSFUL LOGON EVENTS



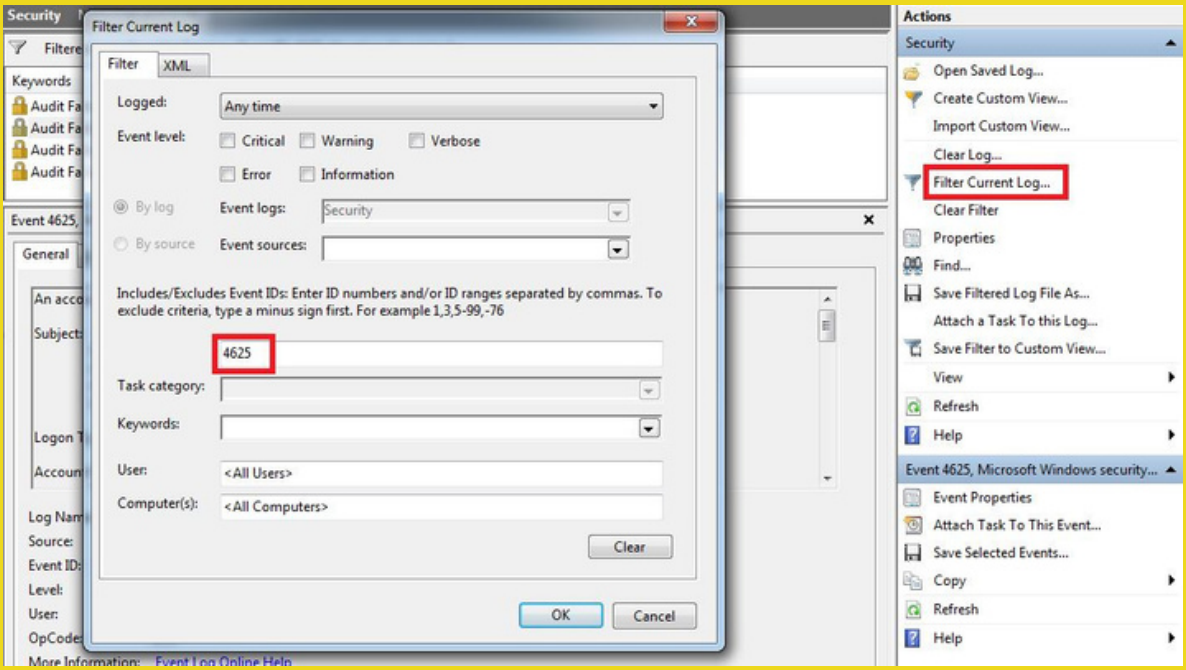
Even when we look at the "Logon Type" field, we see the value 10. This indicates that you are logged in with "Remote Desktop Services" or "Remote Desktop Protocol".
You can find the meaning of the logon type values on Microsoft's page.
https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4624
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/

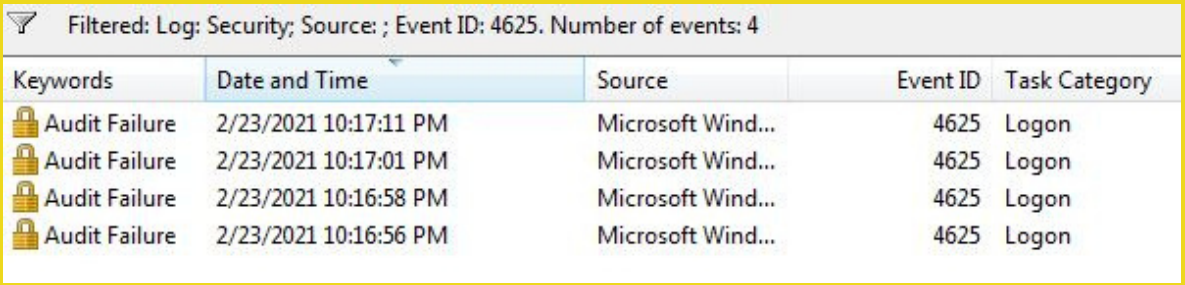
When an unsuccessful login operation is made on RDP, the "Event ID 4625 - An account failed to log on" log is generated. If we follow this log, we can track down the attacker.



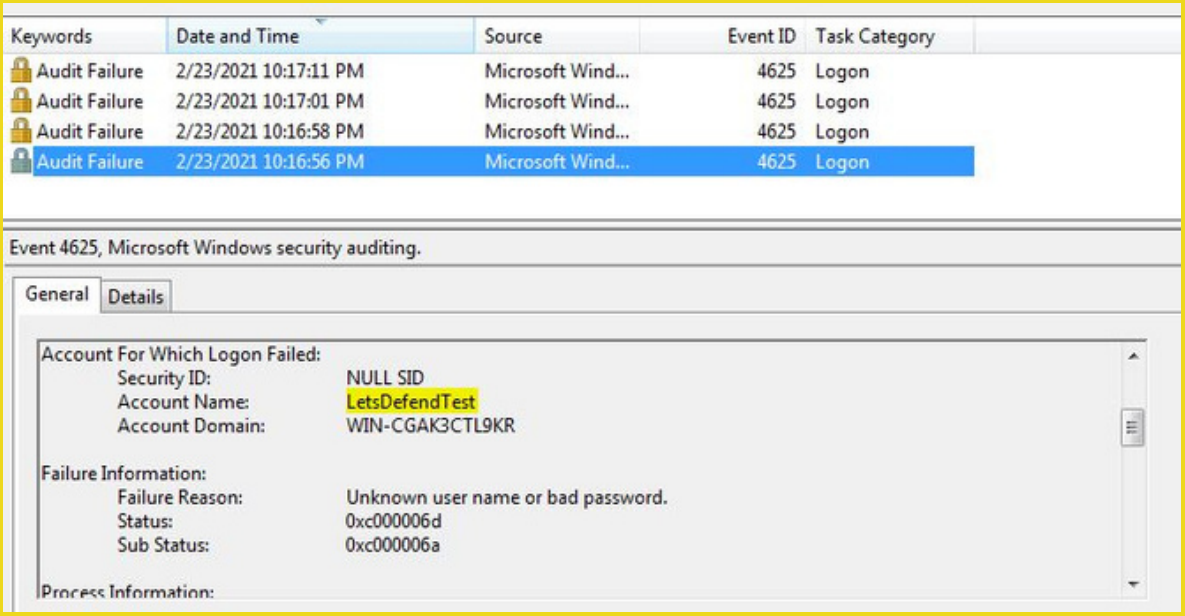
LetsDefend

DETECTING BRUTE FORCE

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



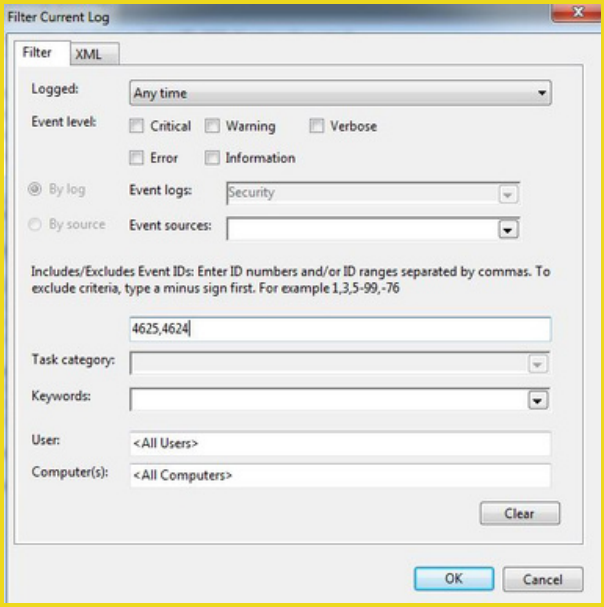
When we look at the dates, we see that the logs are formed one after the other. When we look at the details, it is seen that all logs are created for the "LetsDefendTest" user.

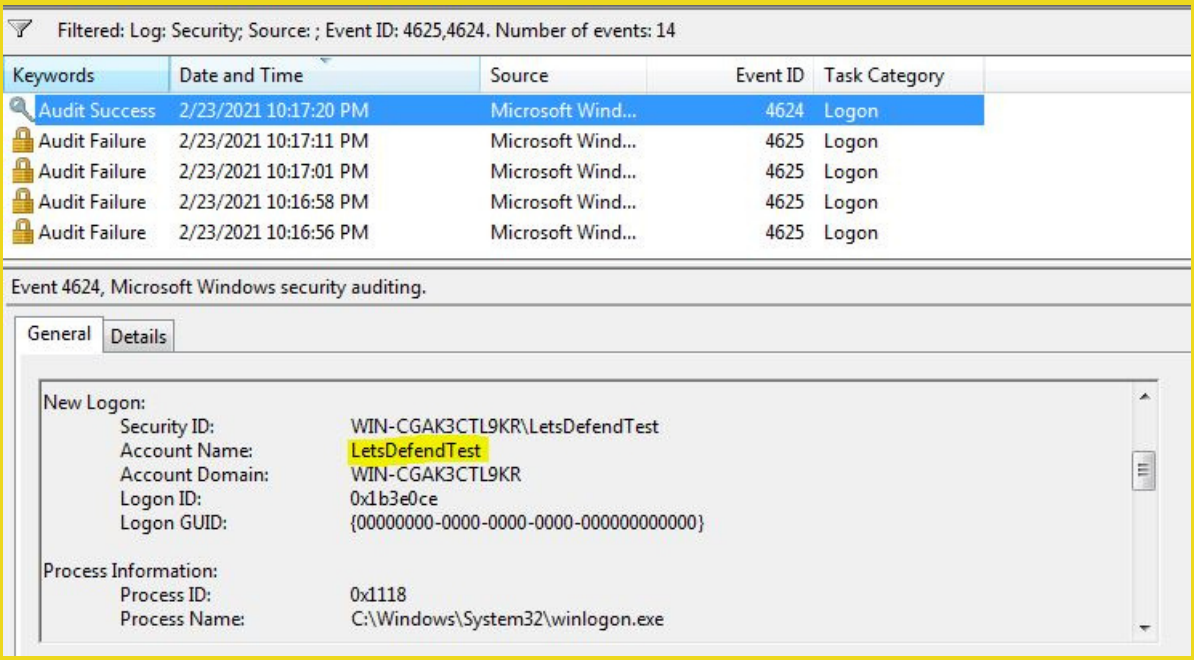


As a result, we understand that the attacker has unsuccessfully attempted to login 4 times. To understand whether the attack was successful or not, we can search for the 4624 logs we saw in the previous section.

LetsDefend

DETECTING BRUTE FORCE





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

LetsDefend

letsdefend.io

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".

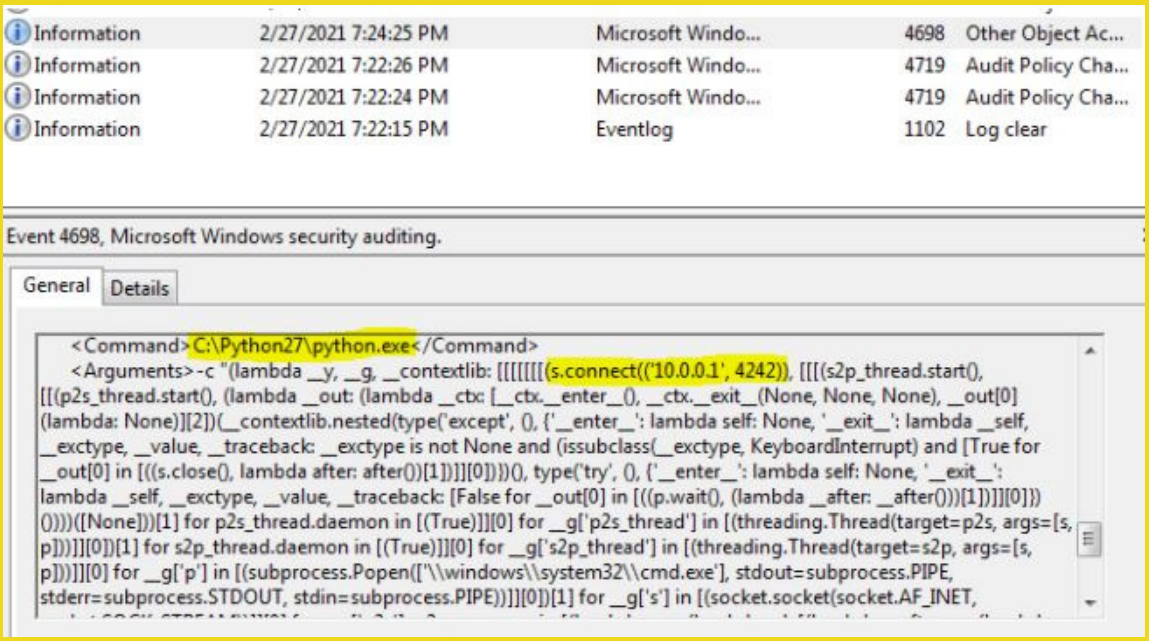
Log file for lesson: persistence.zip Pass=321

- 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.



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.