Windows Login Brute Force Attack Detection Example

By: Ryan Stewart

Understanding Login Activity in Cyberattacks

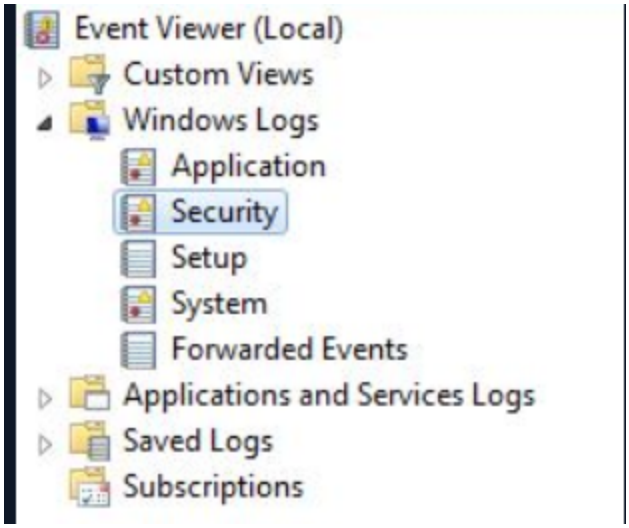
In the context of cyberattacks, login activities are pervasive in both successful and unsuccessful attempts. Attackers often seek to gain control of a system by attempting to log into a server, employing methods such as brute force attacks or using known passwords. In both scenarios; whether the login is successful or unsuccessful; **a log entry is generated.**

Consider an instance where an attacker successfully logs into the server after a brute force attack. To conduct a thorough analysis of the attacker's actions post-entry, it becomes crucial to identify the login date. This information can be extracted by focusing on "**Event ID 4624 – An account was successfully logged on.**"

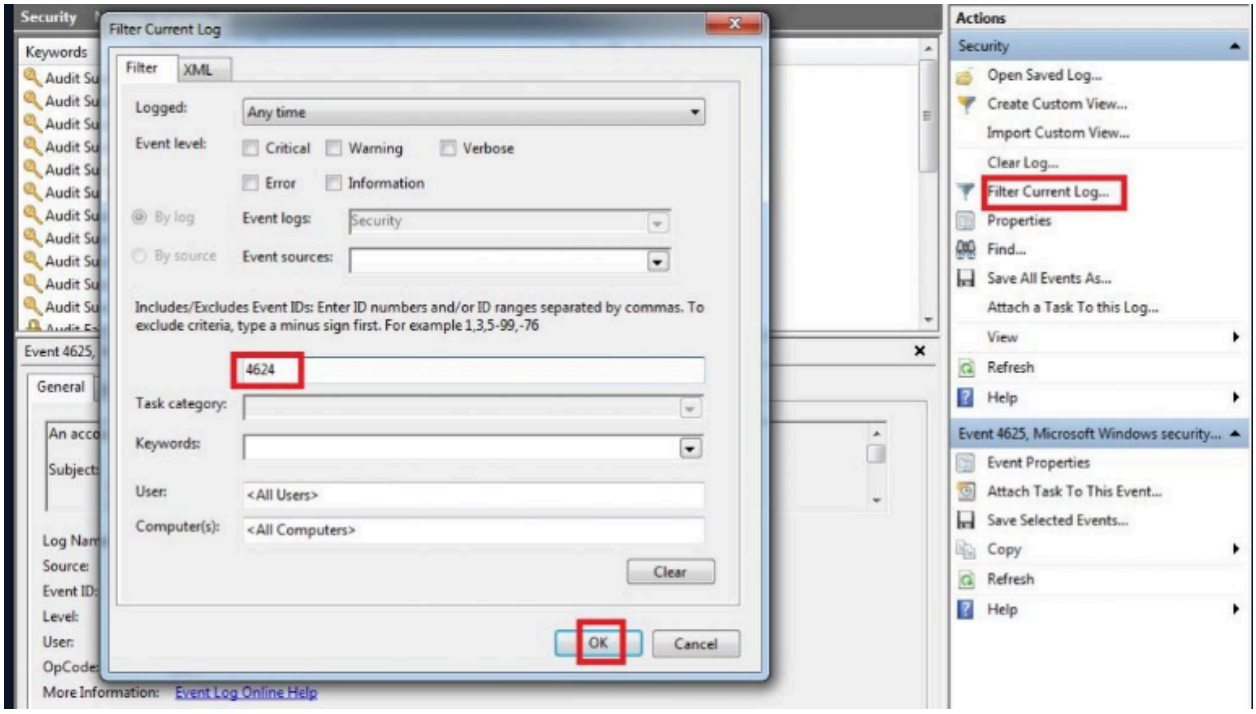
Each event in the log is assigned a unique ID value. Opting to filter, analyze, and search logs based on these ID values simplifies the process, as it offers a more straightforward approach than scrutinizing log titles.

For a comprehensive understanding of the meanings associated with different Event ID values, refer to the details available at the following URL address:
https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/default.aspx

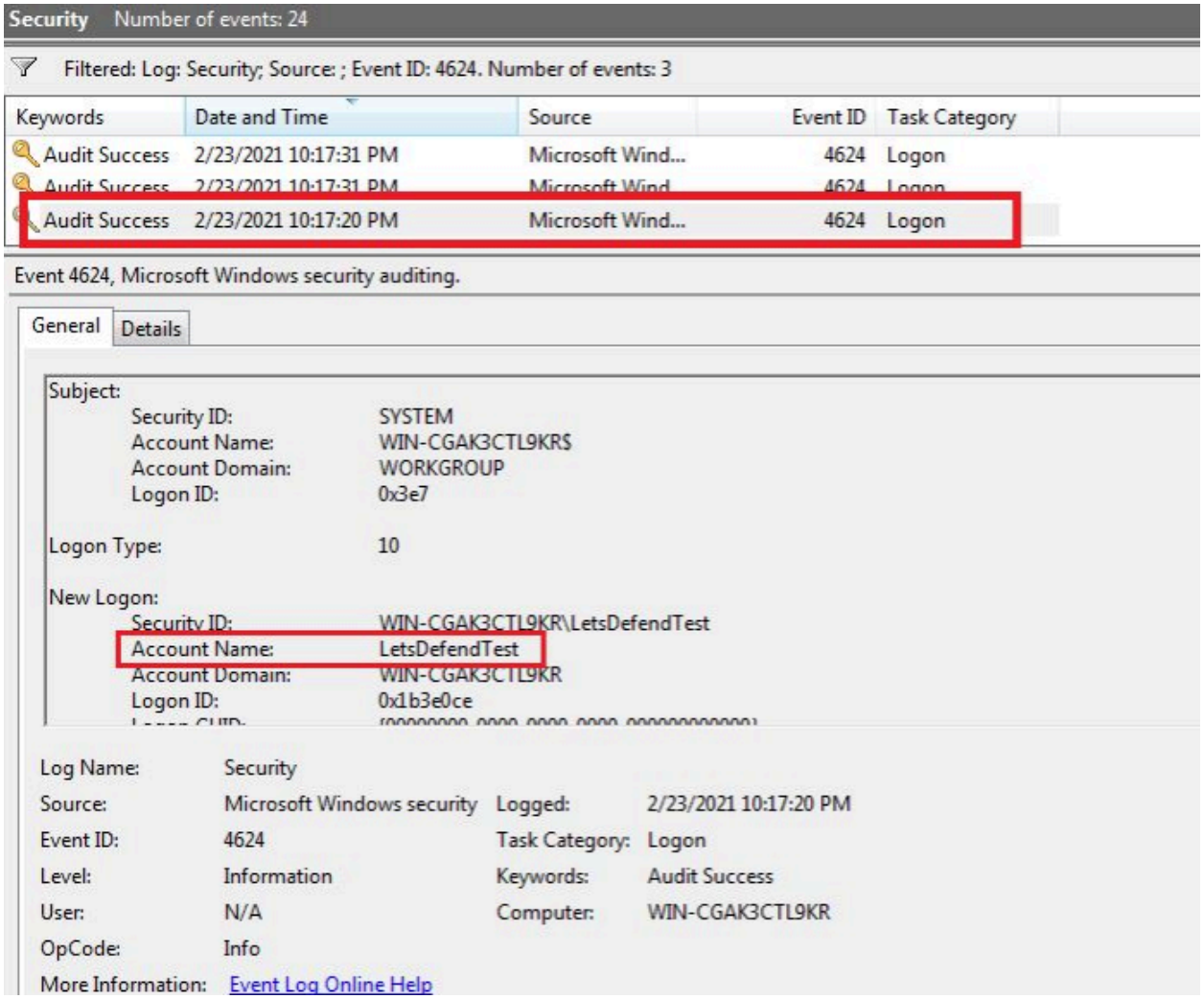
By leveraging Event IDs, cybersecurity professionals can efficiently track and analyze login activities, enhancing their ability to investigate and respond to potential security threats effectively.



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.**



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.

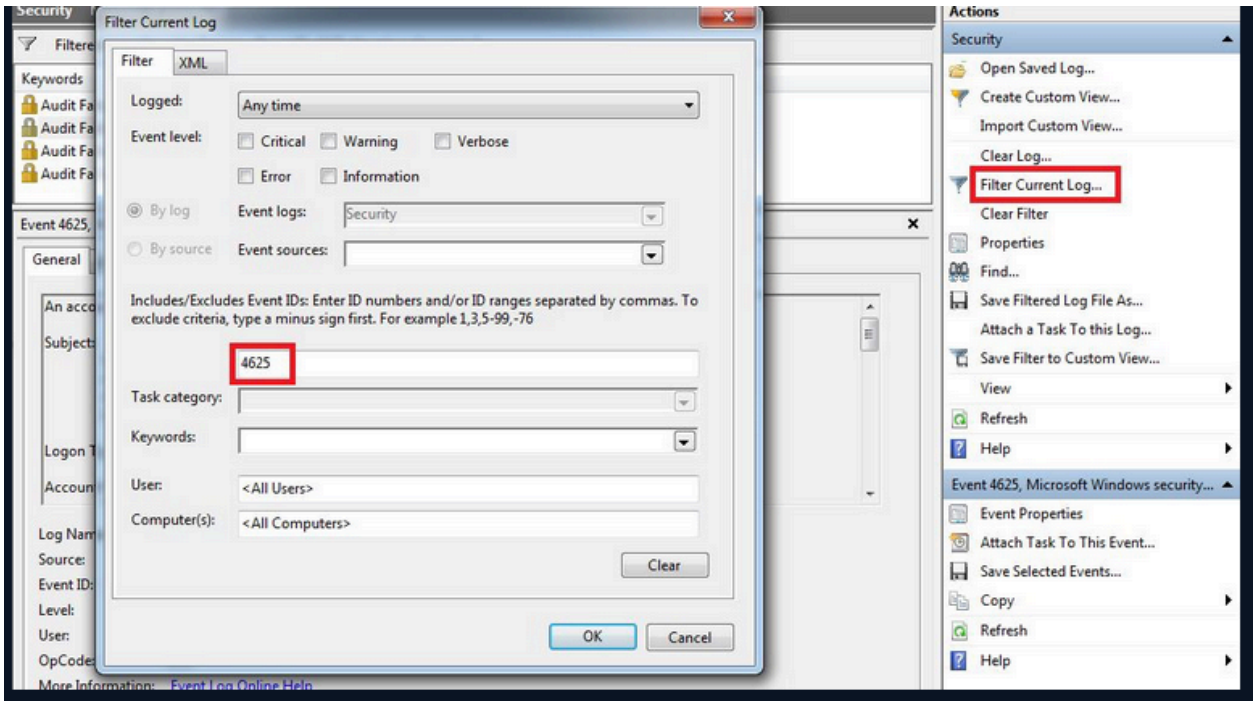
Windows RDP Brute Force Detection

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.

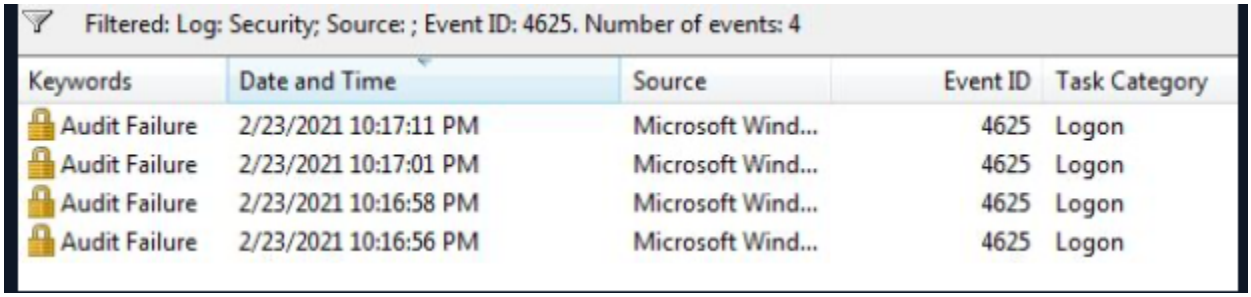
Download log file: Log_File.zip Pass=321

Log_File.zip Pass=321 (https://files-ld.s3.us-east-2.amazonaws.com/Log_File.zip)

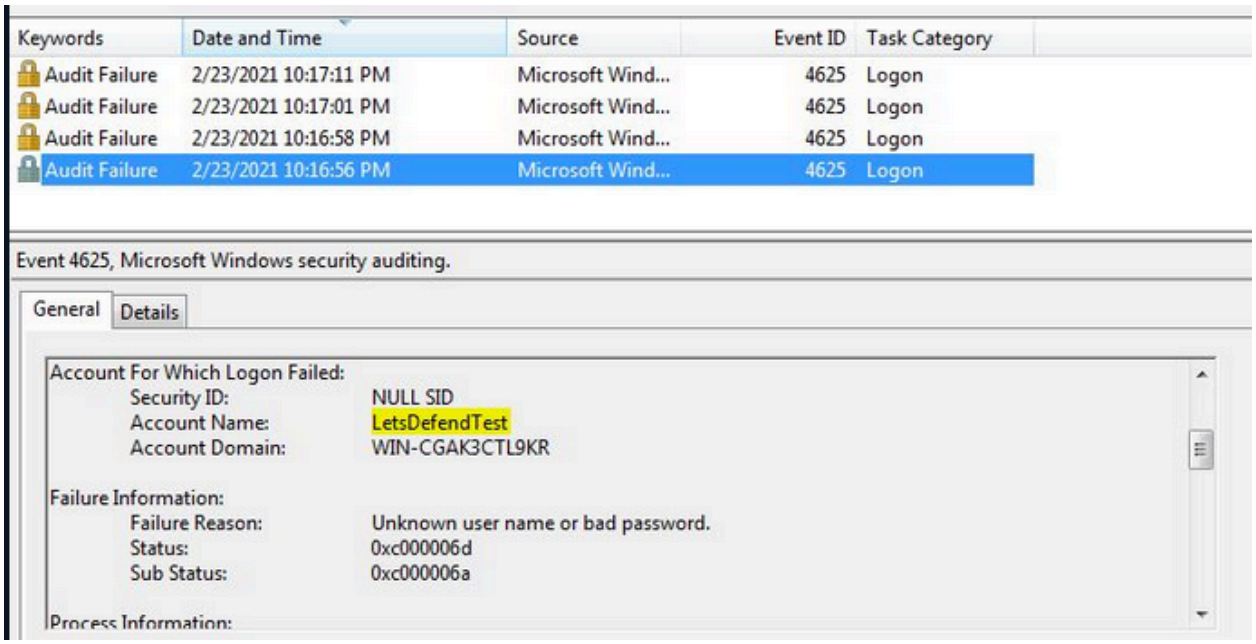
When an unsuccessful login operation is made on RDP, the "Event ID 4625 - An account failed to log on" log is generated. **If we follow this log, we can track down the attacker.**



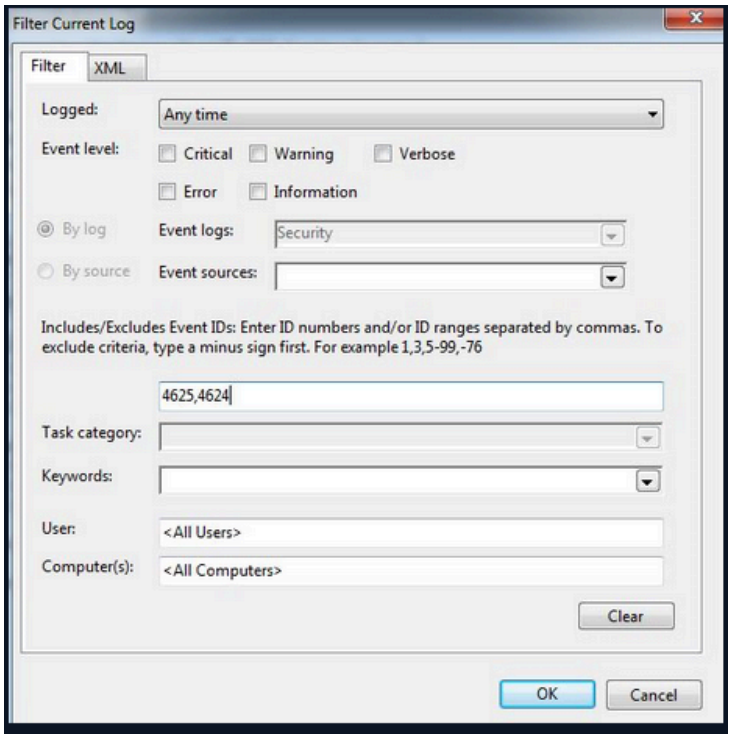
After filtering, we see 4 logs with 4625 Event IDs.

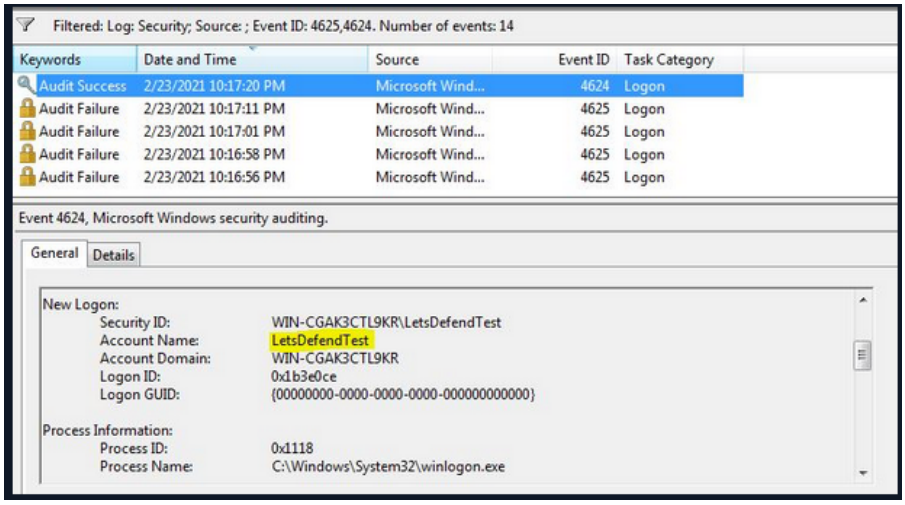


When we look at the dates, we see that the logs are formed one after the other. When we look at the details, it is seen that all logs are created for the "LetsDefendTest" user.



As a result, we understand that the attacker has unsuccessfully attempted to login 4 times. To **understand whether the attack was successful or no**t, we can search for the 4624 logs we saw in the previous section.





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