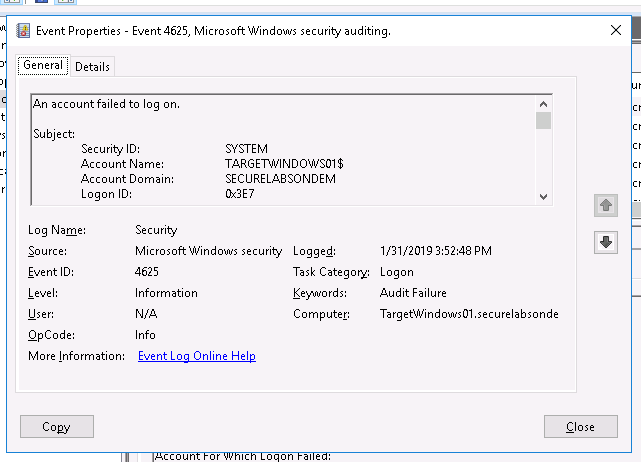
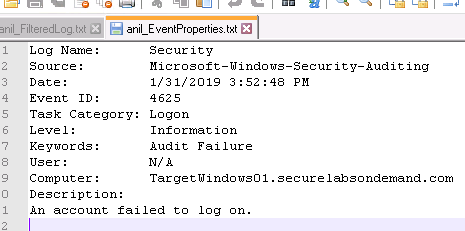
SECTION 1: Hands-On Demonstration

Part 1. Use the Event Viewer to Detect Failed Logons

1. the Event Properties dialog box (screen capture):



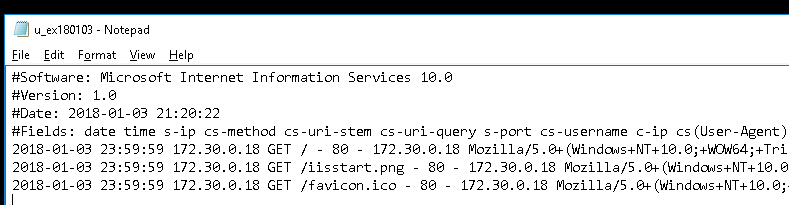
1. summarize your findings in the Filtered Event Viewer Log and recommend a solution for containing and eradicating the incident:



**The security logs are very important for us to be able to identify the source of attacks be it internal or external.**

Part 2. Generate IIS Logon Errors

1. the IIS login errors (screen capture):



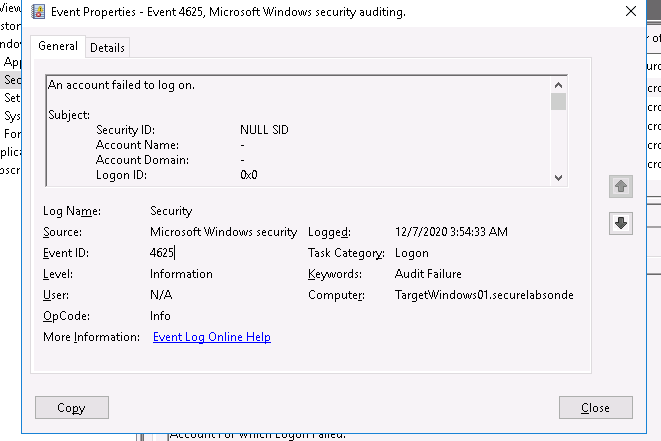
1. summarize the errors and recommend ways to eliminate them:

We can see the date, time, target, http method, path of the file being reached, port, and browser type.

SECTION 2: Applied Learning

Part 1. Use the Event Viewer to Detect Failed Logons

1. the Event Properties dialog box (screen capture):



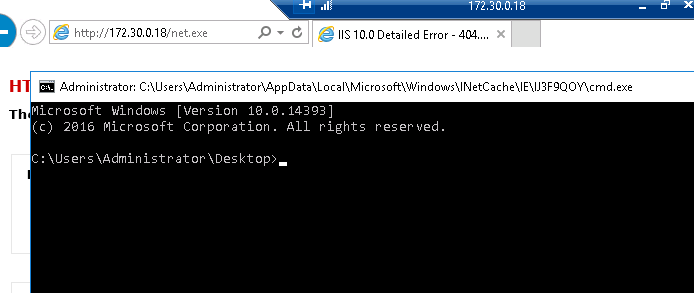
1. document the source name and source network address:

Source: microsoft windows security.

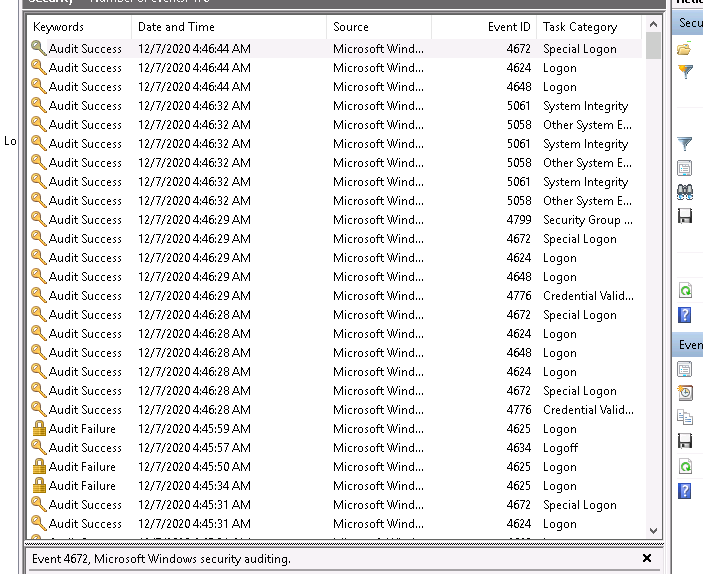
Network: 172.30.0.18

Part 2. Identify Logon Errors in IIS Logs

1. document the results of the executable command:



1. the relevant log entries (screen capture):



1. describe and explain the differences between the two log entries:

After moving the cmd.exe to the relevant folder, we were able to access it and make the succesful call remotely.

SECTION 3: Observation Summary

We RDP into machine1 and access the security logs and save them.

We RDP into machine 1 again. We filter for failed logon audits and open the first one. We save the filtered logs and the event properties to desktop.

We RDP into machine2.