Cyber Defense Organization

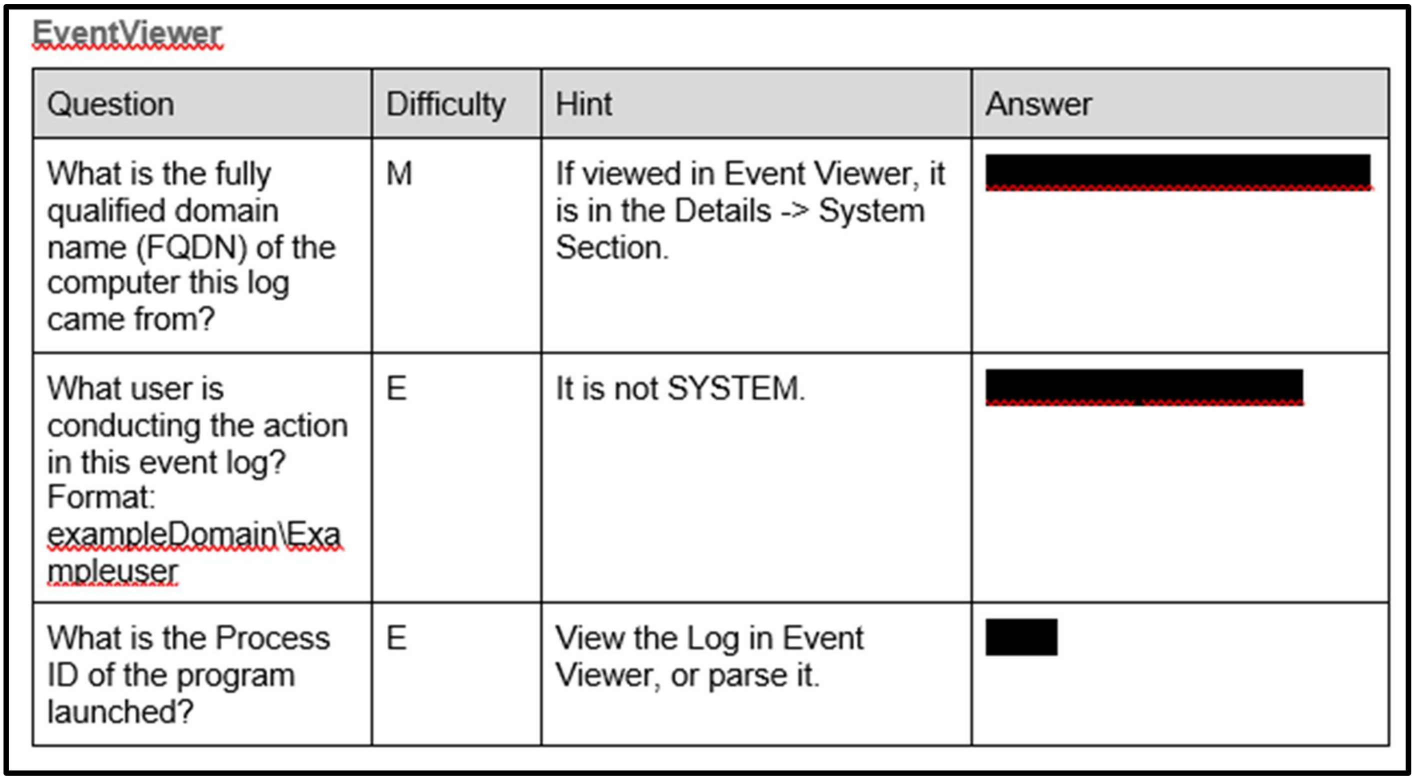
Windows Forensics - Liam Smith - 2020-06-03

Scenario

- On 2019-10-21 the weakadmin user logged into the WEAKSERVER Windows Server noticed “owned.txt” on the desktop.
- They told the incident response team, and user IncidentResponder logged in a confirmed the existence of the file. They then used CyLR to collect forensically relevant artifacts for analysis.
- They usalized KAPE to parse the artifacts and generate a few reports.

Option 1: Capture the Flags

Downloads\weakserver\WEAKSERVER\DraftOne_Challenges_CTF

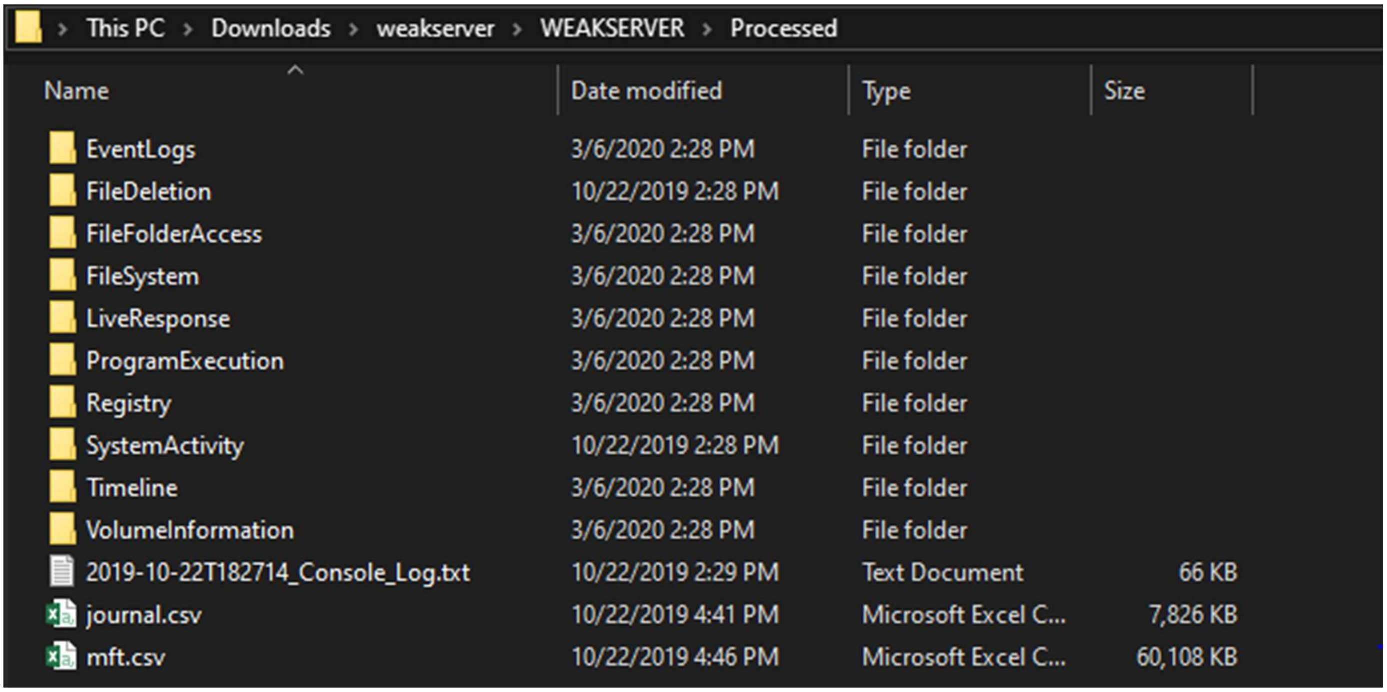


EventViewer

Question	Difficulty	Hint	Answer
What is the fully qualified domain name (FQDN) of the computer this log came from?	M	If viewed in Event Viewer, it is in the Details -> System Section.	[redacted]
What user is conducting the action in this event log? Format: exampleDomain\Exampleuser	E	It is not SYSTEM.	[redacted]
What is the Process ID of the program launched?	E	View the Log in Event Viewer, or parse it.	[redacted]

Option 2: Use the Parsed Artifacts

\Downloads\weakserver\WEAKSERVER\Processed



This PC › Downloads › weakserver › WEAKSERVER › Processed

Name	Date modified	Type	Size
EventLogs	3/6/2020 2:28 PM	File folder	
FileDeletion	10/22/2019 2:28 PM	File folder	
FileFolderAccess	3/6/2020 2:28 PM	File folder	
FileSystem	3/6/2020 2:28 PM	File folder	
LiveResponse	3/6/2020 2:28 PM	File folder	
ProgramExecution	3/6/2020 2:28 PM	File folder	
Registry	3/6/2020 2:28 PM	File folder	
SystemActivity	10/22/2019 2:28 PM	File folder	
Timeline	3/6/2020 2:28 PM	File folder	
VolumeInformation	3/6/2020 2:28 PM	File folder	
2019-10-22T182714_Console_Log.txt	10/22/2019 2:29 PM	Text Document	66 KB
journal.csv	10/22/2019 4:41 PM	Microsoft Excel C...	7,826 KB
mft.csv	10/22/2019 4:46 PM	Microsoft Excel C...	60,108 KB

Option 3: Parse it All Yourself

Download the Zimmerman tools - here.

1. Unzip the folder.
2. Open an Administrative powershell session.
    a. cd <Path to Zimmerman Tools>
    b. Set-ExecutionPolicy Bypass
    c. .\Get-ZimmermanTools.ps1