EC-Council

Report generated on : 18 Dec 2023 01:52 AM

Player Details

User	**James5309**
Lab Id	7140555137384943876
Lab name	DFEv1 Module 06 Windows Forensics
Score	**40**
Possible score	40
Date played	13 Dec 2023 04:16 AM

Flag Details

Name	Course	Task	Status	Hints used	Score
Use Windows Server 2019 as the host machine and Windows 10 as a locally connected machine to collect volatile information from a live Windows machine. Use PsTools and LogonSessions tools available at C:\DFE-Tools\DFE Module 06 Windows Forensics\Volatile Data Acquisition Tools to collect the volatile information. Enter the utility, which will help you retrieve information pertaining to all the open shared files.	Digital Forensics Essentials v1	Collect Volatile and Non-Volatile Information	Completed	0	**10/10**
Use Redline utility in the Windows Server 2019 machine to examine Windows memory dumps file Windows_RAM.mem available at C:\DFE-Tools\Evidence Files\Forensic Images. Enter the PID of calc.exe, which is a child process of spoolsv.exe.	Digital Forensics Essentials v1	Perform Windows Memory and Registry Analysis	Completed	0	**10/10**
Use ChromeCacheView, ChromeHistoryView, and ChromeCookiesView tools on Windows Server 2019 to investigate and extract web browser artifacts such as browsing history, cookies, and cache. Tools are available at C:\DFE-Tools\DFE Module 06 Windows Forensics\Browser Analysis Tools\Google Chrome. (No answer is required. Write skip as an answer to skip this flag)	Digital Forensics Essentials v1	Examine Cache, Cookie, and History Recorded in Web Browsers	Completed	0	**10/10**
Use the Process Explorer tool available at C:\DFE-Tools\DFE Module 06 Windows Forensics\Windows Forensics Tools\Process Explorer on the Windows Server 2019 machine to examine information pertaining to loaded processes on the Windows Server 2019. (No answer is required. Write skip as an answer to skip this flag)	Digital Forensics Essentials v1	Examine Windows Files and Metadata	Completed	0	**10/10**

Target Details

Name	Operating System
DFEv1 Ubuntu Suspect	Linux
DFEv1 Ubuntu Forensics	Linux
DFEv1 Windows 10	Windows