EC-Council

Report generated on : 18 Dec 2023 01:54 AM

Player Details

User	**James5309**
Lab Id	7140551920725430532
Lab name	DFEv1 Module 07 Linux and Mac Forensics
Score	**20**
Possible score	20
Date played	13 Dec 2023 04:04 AM

Flag Details

Name	Course	Task	Status	Hints used	Score
Install Volatility Framework tool on the Ubuntu Forensics machine and examine a Linux RAM dump file (Linux_RAM.dd) to extract information that can be useful for investigation. Identify the malicious communication that has occurred on the machine using the netstat plugin. Enter the port number of process apache2 that established connection with external IP address 10.0.0.32 over port 1234.	Digital Forensics Essentials v1	Demonstrate Memory Forensics	Completed	0	**10/10**
Retrieve data from a memory dump file (Linux_RAM.dd) using the PhotoRec tool on the Ubuntu Forensics machine. Navigate to the location where you have extracted the contents of the memory dump and open the recup_dir.1 folder. Enter the file name with the .tar extension (file name without file extension).	Digital Forensics Essentials v1	Demonstrate Memory Forensics	Completed	0	**10/10**

Target Details

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