EC-Council

Report generated on : 18 Dec 2023 01:58 AM

Player Details

User	**James5309**
Lab Id	7140549902561972484
Lab name	DFEv1 Module 12 Malware Forensics
Score	**30**
Possible score	30
Date played	13 Dec 2023 03:56 AM

Flag Details

Name	Course	Task	Status	Hints used	Score
In the Windows Server 2019 machine, run the Pestudio tool to analyze the suspect file (njrat.exe) available at C:\DFE-Tools\Evidence Files. Enter the remote IP address through which the file tries to communicate with the network on execution.	Digital Forensics Essentials v1	Perform Static Malware Analysis	Completed	0	**10/10**
Analyze a Microsoft Word document that contains an Emotet downloader. Use the Wireshark tool to analyze the Emotet malware artifacts file (Emotet Network Activities.pcap) available at Z:\DFE-Tools\Evidence Files\Emotet Malware\Artifacts in the Windows 10 machine. Enter the website URL (up to .br) through which Emotet malware downloads the malicious payload.	Digital Forensics Essentials v1	Perform System Behavior Analysis	Completed	0	**10/10**
Examine the malicious Word document (Infected.docx) available at C:\DFE-Tools\Evidence Files using the OffVis tool on the Windows Server 2019 machine. Enter the website URL through which the malicious file downloaded the files test.exe and counter.php onto any system when any suspect opens the file (website URL up to .ec).	Digital Forensics Essentials v1	Analyze Suspicious Word Documents	Completed	0	**10/10**

Target Details

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