

Player Details

User	James5309
Lab Id	7140512146467541252
Lab name	DFEv1 Module 08 Network Forensics
Score	20
Possible score	20
Date played	13 Dec 2023 01:26 AM

Flag Details

Name	Course	Task	Status	Hints used	Score
In the Windows Server 2019 machine, install Wireshark and examine the various network packet capture files available at C:\DFE-Tools\Evidence Files\Wireshark Sample Capture Files\Files for Network Forensics. Investigate the HTTP Traffic.pcapng file and identify traffic for any plain text passwords stored in it. Enter the password found.	Digital Forensics Essentials v1	Investigate Network Traffic	Completed	0	10/10
In the Windows Server 2019 machine, install Wireshark and examine the various network packet capture files available at C:\DFE-Tools\Evidence Files\Wireshark Sample Capture Files\Files for Network Forensics. Investigate the FTP Brute-Force.pcapng file and enter the target machine's IP address, which strongly indicates a brute-force attack.	Digital Forensics Essentials v1	Investigate Network Traffic	Completed	0	10/10

Target Details

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