Final Project

Cyber Security Professional Program

Digital Forensics & Incident Response

Final Project

DFIR-11-L1
Forensic Investigation

Project Mission

Study the provided pcap file, discover who attacked the machine, and investigate the attack.

Project Duration

2.5 - 4 hours

Requirements

- Excellent understanding of network forensics.
- Excellent understanding of Windows forensic investigations.
- Excellent understanding of file carving.

Resources

- Environment & Tools
  - SIFT Workstation
  - Flare VM
  - VMware Player (free)
- Files
  - investigate_me.pcap
  - investigate_me2.rar
  - investigate_me3.bin

Project Tasks

Study the provided pcap file (**investigate_me.pcap**), discover from the file who attacked the machine, and investigate the attack.

1 Study the pcap file. Did you find anything suspicious?

2 Use Zeek to extract valuable information from the pcap file.

3 Locate the malicious file in the capture.

4 Identify the nature of the malicious file.

5 Find evidence of malicious activity in the pcap file.

6 Start investigating the infected machine (192.168.23.130) in VMWare Player (download and install the free version). The sequence of the first malicious packet is the password.

7 Identify backdoors the attacker may have left.

8 Investigate the second malware.

9 Follow the hint in the executable.

10 Complete the investigation of the second part.

11 Use the information obtained from the investigation to unlock the last piece of the challenge (**Investigate_me3.bin**).