Computer Hacking Forensic Investigator (CHFI) Project

CCCY 422

Submitted by:

1. Lara Alofi 2110886
2. Taif AlQarni 2111092

30\11\2024

Lab Session Identifiers

1. https://labclient.labondemand.com/LabClient/92f00cca-ce4b-4b26-ba11-2289cc5a3759
2. https://labclient.labondemand.com/LabClient/980daf65-7857-4410-b871-40d47a060412

Username on EC-Council System

1. 2110886@uj.edu.sa
2. 2111092@uj.edu.sa

Part [I]

**Module 09:** Malware Forensics

**Lab 1:**

**Lab 2:**

**Lab 3:**

**Lab 4:**

**Lab 5:**

In this lab, I used internet analysis tools to look at a suspicious Microsoft Word document and see if it was malicious. After I uploaded the document to VirusTotal, it was analyzed by many antivirus engines and found to be dangerous. I went over the specific results, which included the questionable activities, external connections the document attempted to connect to, and contained VBA macros. I also employed hybrid analysis to look more closely at the document's interactions with the system, including the network activity and processes it initiates. In this lab, we learned how to use the internet to learn about the possible dangers of a file and how it affects a system.

**Lab 6:**

In this lab, I investigated the Emotet malware, a very harmful banking Trojan that propagates through phishing emails that contain harmful links or attachments. After being run, Emotet collects private information and downloads more malicious payloads while evading detection by employing obfuscation techniques. Examining a Word document with an embedded macro allowed me to investigate the infection process. This macro retrieves further malware by connecting to distant servers when it is enabled. To learn how the virus endures on compromised systems, I monitored its network activities and system interactions using programs like Wireshark and Process Monitor.  
**Lab 7:**

Part [II]

**Module 13**: Email and Social Media Forensics

**Lab 1:**

In this lab, I examined a suspicious email that falsely claimed to be from Facebook, urging a hotel manager to reset the password for a compromised account. When examined, the suspicious link and attachment in the email pointed to a fake website. I found other indications of tampering by closely examining the email's metadata and structure, including anomalies in the email headers and a suspect URL with an unreliable IP address. The email was confirmed to be a part of a phishing scam when an SPF check failed, and its origin was traced to a Czech datacenter.

**Lab 2:**

I worked with the "Recover My Email" program in this lab to recover deleted emails. Daniel, the suspect in the case, may have deleted important emails connected to a cybercrime. The lab provides insight on how forensic investigators can retrieve these deleted emails from PST files stored in Microsoft Outlook. I examined the emails and their attachments, filtered the results by recipient and subject, then uploaded a PST file. I was able to locate and examine the emails, which might include important evidence for the current inquiry, even though the trial version did not let me store the recovered emails.

**Lab 3:**

I used the "Recovery Toolbox for Outlook" program to work on recovering deleted emails in this experiment. In that case, a brokerage firm employee had been exchanging private information via email, but she deleted all her correspondence to avoid detection. It was my responsibility to recover these deleted emails from the company's Outlook PST files. I stored the recovered emails to a specific location after installing the application and scanning the file for deleted information. This exercise demonstrated how forensic investigators can recover erased emails to find crucial evidence in misconduct cases.

**Lab 4:**

As part of a forensic investigation, I worked in this lab utilizing Python to extract important information from EML files. Analyzing suspicious emails that might be connected to data theft was part of the scenario. My goal was to analyze an EML file and extract important data, like timestamps, sender information, and any threats contained. I improved my knowledge of using Python for email forensics by creating and executing a Python script on an Ubuntu computer that allowed me to extract the relevant data from the email file. This practical experience demonstrated how Python may be used in digital investigations.