SIT327 - Network Forensics

Pass Task 5: Packet Capture Malware Investigation

Overview

This task synthesizes the concepts covered throughout the term, applying them to a practical scenario. In this case, Company X employs Tom, a manager overseeing a digital forensics expert named Harry. During a visit to a coffee shop, Tom's laptop was infected with malware. Company X has managed to secure a packet capture (pcap) from the compromised laptop. After Harry unexpectedly resigned, the company has enlisted your expertise to analyze the incident. It's important to note that the pcap file contains malicious software. Any analysis or manipulation of the malware should be conducted within a virtual machine (VM) in a secure cyber lab or a VM in your own setup to ensure safety.

Report Submission:

Your report should address the following queries:

- Determine the IP and MAC addresses of Tom's laptop as recorded in the pcap file.
- Identify and describe the network traffic flows found in the pcap data.
- Your report should also investigate any potential command. This involves analyzing the packet capture for any outbound connections from Tom's laptop to suspicious IP addresses, which could reveal how the malware communicates with an attacker's server.