CT6034 Moc PCAP

This lecture is about taking the skills you have learnt with wireshark and applying them to a pcap. The pcap itself is a form of banking trojan that has infiltrated and stolen some user credentials. Your task is to find out what happened by answering the questions below. The purpose of this is to help you with thinking about how to appoah your assignment pcaps.

Wireshark is the main tool, but other ones are applicable such as scapy, netminer and golang

**Part 1 - Basic Information:**

1. **What is the timestamp of the first packet in the capture?**
2. **What is the IP address of the infected machine?**
3. **What are some other IP addresses linked to?**
4. **What ports were used for communication?**

**Part 2 - Traffic & Protocol Analysis:**

1. **What protocol is used for the initial malware download?**
2. **What is the URL used to download the malware?**
3. **What file type was downloaded as part of the infection?**
4. **What are the domain names contacted by the infected machine?**
5. **What is the User-Agent string used during the malicious HTTP request?**
6. **How long does the infected machine communicate with the C2 server?**

**Part 3 - Suspicious Behaviour & Indicators:**

1. **Is there evidence of encrypted traffic? If so, what protocol is used?**
2. **Does the infected machine attempt to resolve suspicious domains?**

**Part 4 - Anomaly Detection**

1. **Does the infected machine scan for open ports on other devices?**
2. **Is there any evidence of lateral movement? What IPs are contacted internally?**
3. **What is the longest TCP session observed in the pcap?**
4. **Is there evidence of data exfiltration? If so, how much data was sent externally?**
5. **Are there any certificates that you can find and if so, what are the issues with them?**
6. **How is persistence achieved with backconnect and vnc?**
7. **Attempt to create a timeline of events from start to finish**
8. **Draw/map out all network-based devices**