CPE457/557 Software Reverse Engineering

**07 – Network Protocols**

# lab

**Lab Description:** When performing reverse engineering activities, it often required to view network communication to gain a better understanding of your target software. This lab will focus on analyzing application-layer protocols through PCAP files.

**Lab Environment:** Students will need to be able to run the latest version of Wireshark to analyze the lab PCAP files.

**Lab Files that are Needed:** The provided PCAP files associated with this lab:

* dns.pcap
* http.pcap
* ftp.pcap

**Answer the Following Questions**

The following network traffic was generated from a sample of CryptoLocker, which utilized a domain-generation algorithm (DGA). Provide detailed answers to the following question, utilize *dns.pcap* for this section. Your goal is to understand what protocols this malware used and how it utilized them.

1. What protocols did this malware use? List them and provide discussion about the relevance of each one.
2. How many DNS queries did this malware generate?
3. What *user-agent* string did the malware use when making HTTP requests? What is the significance of this?
4. This malware is attempting to establish connection with a command and control node, was it able to do that? Support your answer with specific evidence from the PCAP file.

The following network traffic was generated by a malicious Microsoft Word document and used to gain an initial foothold onto a system. Your goal is to analyze how the malware used application layer protocols to further it’s attack. Use *http.pcap* for this section.

1. What domain was used in this attack? What was the IP address returned from the query?
2. What resource was requested from the malware? This is the first HTTP request that was made. What was provided as a response?

The following network traffic utilized an application layer protocol. Your goal is to understand what happened based off of the network traffic. Use *unk.pcap* for this section.

1. What protocol was captured in this PCAP?
2. What port was used for this session?
3. What was the username/password used to authenticate?
4. What did the user do?

## What to submit

Submit a Microsoft Word document or PDF that includes answers to the questions posed along with screenshots demonstrating the installation of the virtual machine.