Assignment 4

When I first started this assignment, I had planned to use my virtual lab that I created during the semester, containing PFSense, Windows 10, and Kali Linux virtual machines. Due to issues that will be discussed in this document, I was unable to perform this analysis on a working virtual environment. In consequence, the analysis will be more hypothetical than literal, and the process will be discussed in the context of what I would've done had my lab setup worked properly. I will instead use evidence samples found on the internet to conduct my work.

Because I feel my issues in this project are important to discuss, I thought it would be best to talk about them first, then discuss my analysis at a later point in the document. I had initially stored my virtual lab drives on a NAS device residing on my home network, but the virtual machines were unable to efficiently communicate with these drives and would frequently lose connection. This NAS is running from a Raspberry Pi 4 with 2 GB of RAM, so this issue could have stemmed from the Pi being unable to handle the access requests without compromising bandwidth. I had not run a speed test, but it's likely that the bandwidth was too congested. It's also possible that VirtualBox did not have proper permissions to access the files it needed, as I've commonly run into similar issues with my current setup. This provided an unsafe environment for the integrity of the data stored on those virtual drives, as disconnection can result in corruption to the drives. Ultimately, the best course of action was to use my old external drive that I used to use for VMs to keep all of my virtual drives. I reinstalled all of the operating systems onto the external drive, but they were still inconsistent. My host machine also kept crashing and restarting, hindering my productivity. I assume this was because my host machine only has 8 GB of RAM and each virtual machine running was just drawing just too much power, causing the system to halt. This was when I made the ultimate decision to use evidence captures found online instead of trying to force my host machine to handle a workload that it wasn't designed for. Before I discovered these issues, I had actually gathered some evidence before I had to scrap it and restart. To make sure my browsing did not infect my home network, I connected the PFSense box to a VPN server using ExpressVPN. This way, all traffic from the virtual network will not go directly though my home router, protecting my other devices. First, I used the integrated packet capture feature of PFSense to begin capturing all packets coming into and leaving the network. I then booted into the Windows 10

machine and began looking to get it infected. I started browsing the web for anything that might get my machine infected. Two main viruses that I know of are BonziBuddy and Wave Browser, as I've encountered these in the wild. I installed these onto the windows machine. Unfortunately, I lost the PCAP of the machine trying to access the website after I had to reinstall the operating system. As I mentioned, I instead opted to follow a guide online that provides a PCAP to analyze.

After downloading the sample PCAP from Xplico, I used NetMiner to analyze the packets and try to find any evidence of infection throughout them. Upon opening the file in NetMiner, I was presented with a list of hosts and their respective operating systems. I also found current sessions and information about those sessions under the hosts tab. If a device is expanded, I can also see what websites and domains that device accessed, external or internal. This view also shows the NIC manufacturer, as well as attributes such as age, drivers, and open ports. It appears the internal network IP address is 10.0.2.0, as most of the hosts are communicating from that address space. This can provide useful information for attackers trying to perform reconnaissance on an internal network, which in turn creates a threat to the organization. According to the capture's structure, there are 280 hosts, 743 files, 372 images, 3 messages, 222 credentials, 626 sessions, 1390 DNS queries, and 21072 parameters present in the PCAP. This shows a lot of useful information for network forensics investigators and may provide clues as to what events and threats are present on the network. NetMiner also shows the MAC addresses, IP addresses, hostnames, and protocols used by the clients communicating throughout the network. Under the files tab, NetMiner allows you to view files transmitted throughout the capture, which can narrow down the possible threats and vulnerabilities that may have caused harm or may cause harm in the future. Inside this tab, multiple JPEG and HTML files can be found and viewed. It seems that many devices in this capture are contacting a server with the IP address of 200.57.7.194 requesting an HTML file named jav.SAXParserFactory.html. In the credentials tab, investigators can make sure authentication security practices are functioning properly and the intended protocols are being followed. If there is any packet that shows an unusual protocol or authentication method, this may raise a red flag and indicate compromise. Under the Sessions tab, the sessions between devices are documented, including the ports, protocols, hots, and IP addresses used.