**Lesson 2.3 – Server Exploits**

**\*\*Instructions:** Please change the text color of your responses to red text. Please organize the endings to each page.

**Activity 2.3.2 – Stopping the Spread of Malware**

1. Read through steps #1 through #7 – we will not be playing the routing game, but you must read for understanding.
2. Every time you start Wireshark, you need to use the Ethernet 2 interface with the not port 3389 filter. With this configuration, you will not see the network traffic that manages the virtual lab. There will be other network traffic not related to this activity and you will have to filter that accordingly. (Step #11)
3. Document the ping command; summarize what it does and the results it returns. (Step #13)
4. What is the MAC address of the destination host? (Step #18)
5. What is MAC address of the source host? (Step #18)
6. On the Windows host, confirm that Wireshark detected the new network traffic. The source and destination IP addresses for the replies and requests are opposite from the last time you observed this traffic (when you pinged the Linux host from the Windows host). Why do you think that is? (Step #25)
7. Save a screenshot of your Wireshark window that includes both a ping request, shown as Echo (ping) request, and the reply that comes back, shown as Echo (ping) reply. When done with your screenshot, minimize the Wireshark window. (Step #31)
8. How did the routing game accurately reflect the ping flood attack you witnessed in Wireshark? What features of the game did not reflect the actual ping flood? (Step #31)

The routing game introduced many packets (papers) that represented a ping flood and the people acting as servers could not keep up with all of them. The game did not reflect an actual ping flood in that the people acting as servers did not reply to each of the flood packets.

1. From the Linux-based system, issue another ping flood attack. (Step #36)

Students should see that the ping request is going unanswered (no reply is sent).

1. Observe the packets in Wireshark. Using your earlier screenshot, compare this output to the output of your previous session. Note the Info field in Wireshark to confirm that the current session no longer replies to a ping request. Congratulations! Your system is no longer vulnerable to ping flood attacks. Describe what happens to the ping requests instead in Wireshark. (Step #37)
2. In a few sentences, summarize the tasks you performed in this activity and how they relate to the Cybersecurity Lifecycle. (Step #40)

CONCLUSION

1. What do you think is the goal of a ping flood attack? Why would someone use this type of attack vector? Think about the types of hackers on the internet (black/white/gray).
2. How could an attack like a ping flood be harmful to an entire network?