# Cybersecurity

## Activity 2.3.2 Stopping the Spread of Malware

Copy and paste screenshots and/or answer questions from the activity.

11. Why do we put in the filter text box…not port 3389?

Ignore the traffic from the cyber lab

12. What does the ping command do?

A picture containing text

Description automatically generated

Tests a connection between two machines

14. What information is found in the 3 panes?

Top- Packet List Pane

Middle- Packet Details Pane

Bottom- Packet Bytes Pane

15. a. What is the destination IP Address of each ping request?

172.30.0.6

b. What is the destination IP address of each ping reply?

172.30.0.13

17. a. What information can be gained by looking at the timestamp?

You can discern when traffic happened and if it was valid for said time

b. Why are MAC addresses a valuable piece of information?

Its unique to each device and can be used to identify them

25. Provide a screenshot of the current output. 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?

Graphical user interface, application

Description automatically generated

Graphical user interface

Description automatically generated

31. 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.

Graphical user interface, text, application

Description automatically generated

37. Provide a screenshot of the current output. 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.

Graphical user interface, application

Description automatically generated

40. In a few sentences, summarize the tasks you performed in this activity and how they

relate to the Cybersecurity Lifecycle.

Used wireshark to monitor network traffic, issue a ping flood attack as well as stop it.