SY205 – Net: OPS & Analysis Name(s): _____

Alpha(s): _____

Assignment Type:	Assignment	Collaboration Policy:	Default
Assignment Title:	Networking Infrastructure		

Capture & Collect: Hub

1. (5) Complete the below network configuration information for the `eth0` interface of your Raspberry Pi.

   a. [3 / __ / 0] Enter your IPv4 address (*inet addr*) in dotted quad format.

   b. [1 / __ / 0] Enter your IPv4 network mask (*Mask*) in dotted quad format.

   c. [1 / __ / 0] Enter your IPv4 broadcast address (*Bcast*) in dotted quad format.

2. [5 / __ / 0] Before sending a direct communication to another group member. How many ARP entries are in your ARP cache table for the `eth0` interface?

3. (5) Complete the below based on the round-robin pings.

   a. [1 / __ / 0] How many entries are listed in the ARP cache for the `eth0` interface?

   b. [4 / __ / 0] Complete the below table based on the entries in your ARP cache. The below table may have extra lines.

Role Name	MAC Address	IPv4 Address

4. (8) Complete the following based on the collective `ping` results from the *Packet Storm* activity.

a. [4 / __ / 0] Complete the below table.

Role	Packets Transmitted	Packets Received	Packet Loss (%)

b. [4 / __ / 0] Explain whether you were collectively able to overwhelm the network or not. Explain why you think that; i.e. what evidence supports your statement. Use complete sentences, spelling and grammar count.

5. (8) Complete the following based on the collective ping results from the *Targeted Attack* activity.

a. [4 / __ / 0] Complete the below table.

Role	Packets Transmitted	Packets Received	Packet Loss (%)

b. [4 / __ / 0] Explain whether you were collectively able to overwhelm the Bob or not. Explain why you think that; i.e. what evidence supports your statement. Use complete sentences, spelling and grammar count.

Capture & Collect: Switch

6. (5) Complete the below network configuration information for the `eth0` interface of your Raspberry Pi.

a. [3 / __ / 0] Enter your IPv4 address (*inet addr*) in dotted quad format.

b. [1 / __ / 0] Enter your IPv4 network mask (*Mask*) in dotted quad format.

c. [1 / __ / 0] Enter your IPv4 broadcast address (*Bcast*) in dotted quad format.

7. [5 / __ / 0] Before sending a direct communication to another group member. How many ARP entries are in your ARP cache table for the `eth0` interface?

8. (5) Complete the below based on the round-robin pings.

a. [1 / __ / 0] How many entries are listed in the ARP cache for the `eth0` interface?

b. [4 / __ / 0] Complete the below table based on the entries in your ARP cache. The below table may have extra lines.

Role Name	MAC Address	IPv4 Address

Intermission

Upload and download captures within your group.

Analysis: Protocols in Action

9. [5 / __ / 0] Draw a high level protocol sequence diagram of the ARP and ICMP traffic resulting from the first `ping` command; i.e. the first time you pinged when connected to the Ethernet hub. Being a high level diagram, your Role name should be on the left, your target should be on the right, you don't need to depict packet details other than protocol and message summary; e.g. *HTTP GET index.html*.

10. [5 / __ / 0] Draw a high level protocol sequence diagram of the `nc` messages sent between the hosts on the network, draw at least three message exchanges per hosts communicating. Draw one diagram for the communication you participated in; draw a separate diagram for the communication you did not participate in. Just depict the `nc` messages.

Participated In	Did Not Participate In

Analysis: Network Architecture

12. [5 / __ / 0] Draw a network diagram depicting the hosts your host knows at this point and the networking hardware connecting the hosts. Note: A host always knows about itself.

13. [5 / __ / 0] Draw a network diagram depicting the hosts your host knows at this point and the networking hardware connecting the hosts.

14. [5 / __ / 0] Draw a network diagram depicting the hosts your host knows at this point and the networking hardware connecting the hosts.

Analysis: Collision Domain

15. [5 / __ / 0] Modify your drawing in Question 14 by drawing a dashed circle around the hosts and hardware devices that are in the same collision domain; i.e. each represent each collision domain as a collection of hosts surrounded by a dashed circle.

Analysis: Broadcast Domain

16. [2 / __ / 0] Draw a network diagram depicting the hosts your host knows at this point and the networking hardware connecting the hosts. Note: A host always knows about itself.

17. [3 / __ / 0] Draw a network diagram depicting the hosts your host knows at this point and the networking hardware connecting the hosts.

18. (5) Complete the following based on the Somethings Missing activity.

My Role Name:	

a. [2 / __ / 0] List the IPv4 addresses that communicated via TCP based on *your* own ethSwitch pcap.

b. [3 / __ / 0] Discuss what TCP communication your host did not see, but you know did take place based on your own and your group member's pcap files. Use a complete sentence, spelling and grammar count; you may use role names in your discussion (e.g. Alice, Carlos).

19. (5) Update your network diagram in Question 17 per the below.

a. [3 / __ / 0] Draw a dashed circle around the hosts and hardware devices that are in the same *collision* domain.

b. [2 / __ / 0] Draw a solid circle around the hosts and hardware devices that are in the same *broadcast* domain.

Analysis: A Jump to Conclusions Mat

20. (4) Complete the below regarding the networking hardware (hub or switch), and the pillars of cyber security.

a. [1 / __ / 0] Which networking hardware device is better at supporting confidentiality?

b. [1 / __ / 0] Which networking hardware device is better at supporting integrity?

c. [2 / __ / 0] Which networking hardware device is better at supporting availability?

21. [5 / __ / 0] You are designing a network for your organization. Discuss which networking hardware you would use when setting up local area networks. Discuss the function/characteristic of the networking hardware that enables supporting the pillars of cyber security from the previous question. Use complete sentences, spelling and grammar count.
