CSE 8349 – Quiz #1

January 29, 2015

Name: \_\_\_Tyler Jackson\_\_\_\_\_

• [1 pts] Describe the difference between a *threat*, a *vulnerability*, and a *risk*.

A threat is who or what might want to cause harm to what you have of value (actor). Where as a vulnerability is a weakness that a threat can use to exploit an access. The risk is the likelihood of an attack multiplied by the impact an attack on this asset would have. For example, a threat to a small strawberry jam business might be a disgruntled employee. A vulnerability might be if the strawberry jam storage freezer wasn’t kept locked. The risk would be the likelihood of an attack on the strawberry jam storage multiplied by the impact that attack would have. For example, someone stealing all the jam would have a huge impact, because the jam is really important to the business. The likelihood would vary based on the disgruntled employee.

• [1 pt] Consider Risk Management as it relates to Security:

• What is the primary goal of Risk Management?

To protect the company, and its ability to be successful.

• If you were asked, “What one thing would you fix?” What criteria would you use to determine your answer?

I would tell them to fix the thing that would save them the most money.

• [1 pt] Consider ARP:

• What is the primary purpose of ARP?

To get a hardware address from a protocol address. For example, requesting a MAC address from an IP address. And then the corresponding ARP response.

• What addresses would be present in an ARP request?

The destination MAC address would be FFFFFFFF, and the source MAC address would be the MAC address corresponding to the machine sending the request. There would be no IP header. Then the payload would say who has the IP address corresponding to X.

• [2 pts] Assume each network has a network mask of 255.255.255.0 and the following three machines contain network interfaces with the following IP addresses and the following MAC addresses:

• 192.168.5.3 - 01:3e:7f:d4:7a:6c

• 10.10.30.4 - 01:3e:7f:d4:7a:6d

• 192.168.5.1 - 01:3e:7f:d4:7a:61; 10.10.30.1 - 01:3e:7f:d4:7a:62

Draw the Network:

Comp. Comp. Comp.

A <————————> C <—————————> B

192.168.5.3 192.168.5.1 10.10.30.1 10.10.30.4

01:3e:7f:d4:7a:6c 01:3e:7f:d4:71:61 01:3e:7f:d4:7a:62 01:3e:7f:d4:7a:6d

If machine “a” were to send a packet to machine “b”, give the source and destination IP and MAC addresses for the first hop.

DEST SRC Type DEST IP SRC IP Payload

01:3e:7f:d4:71:61 01:3e:7f:d4:7a:6c 800 10.10.30.4 192.168.5.3 Hey B, its A.

If IP