**Lesson 2.2 – Information Architecture**

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

**Activity 2.1.2 – Passive Analysis**

1. Try to complete step #3 with whois amazon.com. To this point it has not worked. If it doesn’t work, please state that fact: (Step #3)

Replace this text with screenshot only if it works! (Step #4)

1. How can Bikes, Boards, and Beyond make use of this type of architecture?
2. Record at least 5 unique remote IP addresses (Step #11 section C)
3. Record the URL’s listed (Step #14)
4. Does the data for the new URL confirm that some domains are part of the Amazon website and others are not? What are some clues? (Step #15)
5. Enter your five (or more) IP addresses from your passive analysis of amazon.com (from step 11). (Step #19)
   1. Do you see a pattern in the domain names? In what way are they similar to amazon's domain? To each other?
   2. Depending on the URLs you chose, some nslookups may return “Non-existent domain”. Why do you think that happens?
   3. You will use nslookup later in this unit, so save a screenshot of your PowerShell window with its results.
6. From your analysis, do you think you’ve seen all the servers and hosts that make up the Amazon ecommerce site? How does Amazon’s architecture affect the security of the site? Consider the hosts you’ve seen that might be private or public facing. (After Step #20)
7. When complete, save a screenshot of the results of tracert. (After Step #21)
8. Save a screenshot of your PowerShell window with your latest netstat data. (After Step #23)
9. Save a screenshot of your PowerShell window with your latest netstat data. (After Step #25)
10. Comparing your baseline data to this new data, you can determine the addresses used to access the web page. Record the full foreign address of the CTS website. (Step #26)
11. Then describe which parts of the network (CTS or your security lab) are using those services. (Step #28)
12. Suppose you want to convert the Cybersecurity Training Site, CTS, to a real ecommerce site. (After Step #28)
    1. What port and web service should the website use? Why?
    2. Should the website architecture include more than one server? Why?
13. Work through the following scenario: suppose you are the victim of a malware attack and you suspect a spoofed website is the problem. Summarize how each tool could help you in your investigation of the website.
    1. Whois
    2. Nslookup
    3. Tracert
    4. netstat