CYBV 326: Introductory Methods of Network Analysis Analysis
Final Exam
The University of Arizona, CAST
Fall, 2020

Instructor: Jordan VanHoy
Email: javanhoy@arizona.edu
Cell Phone: 910-585-3626

Final Project

The final project is designed to test your application of the knowledge you have gained from this course. You will need to develop a network architecture, describe what happens as a request for a resource travels through the network, and research and analyze potential attacks at each network layer and determine how to stop that from happening. You may use any resources or notes but may not copy/duplicate/plagiarize anyone's work. You will ensure that you cite all sources using APA format. You may start working on the project anytime throughout the course. **This assignment is due December 11, 2020 at 1159.**

Instructions

1. **Network Architecture:** You will develop a network architecture consisting of the following components:
    a. Minimum of 5 hosts (one of which will be a wireless host). Hosts can be laptops, desktops, tablets, or smartphones.
    b. Divide the hosts into at least two different networks
    c. Use a minimum of two switches
    d. Use a minimum of one router
    e. Use a minimum of one firewall
    f. Use a minimum of two public servers that you are trying to connect to
    g. Annotate a public network
    h. You will place the appropriate addressing scheme with each object in the diagram (host, switch, router). Addressing must be formatted correctly. You may use any IP addresses you want, but ensure that the IP address is appropriate for the device that you are assigning the IP to (Public facing vs Private).
    i. Use common network architecture symbology.
    j. The network architecture will be incorporated to the final document (cut and paste or screen capture). Ensure that it is legible; easily read. You

may use any applicable tool to create your diagram. Some examples are packet tracer, PowerPoint, Microsoft Visio, Draw.IO.

2. **Resource Request:** Using a theme such as sending an email or transferring a file, you will discuss 20 concepts that allow your data to move from your host to the resource you are requesting and back again. Do not cut and paste from another source. Use your own words and understanding of the concepts to explain the process. If you reference or use a quote to provide clarity to a concept, you must reference your source. This will be prose not fill in the blank or in list format. This section will consist of the following:
    a. Minimum of 20 concepts along the "path" of the resource request. Each layer of the TCP/IP model (Chapters 2, 3, 4/5, 6) will have a minimum of five concepts explained (5 x 4 = 20). Each concept is worth two points.
    b. Each step will consist of the following:
        i. Concept
        ii. Concept Definition
        iii. Applicable Port and Protocol
        iv. Applicable data unit (Data, Segment, Datagram, Frame)
        v. What this concept provides the user
        vi. For each concept you use you will label your network diagram with where that concept takes place
        vii. Example: Bob would like to access a webpage at www.example.com. His computer does not currently have an IP address so his computer creates a DHCP message request. The DHCP server is a network management protocol that dynamically assigns IP address to network devices. It uses two ports 67 for the server and 68 for the client. This message is contained within a UDP segment which will be encapsulated within an IP datagram. When DHCP provides Bob's computer with an IP address the computer will be able to communicate networked resources.

3. **Research and Analysis:** You will research four attacks; one at each layer of the TCP/IP stack. Each attack is worth 25 Points. **You cannot use any of the attacks that you have researched from previous assignments.**
    a. You will answer the following questions for each of these attacks:
        i. What was the attack? Provide what layer the attack typically occurs at and description of what the attack does.
        ii. How is the attack carried out?
        iii. What does the attack hope to achieve? Relate this to the CIA triad.
        iv. What network vulnerability does the attack take advantage of?
        v. What recommendations would you make to senior management? (i.e. What can be done to mitigate the attack?)
    b. For each of the four attacks you will use a different source for a minimum of four cited sources. You will use academic resources such as peer-reviewed journals, scholarly articles, textbooks, etc.

4. **Paper Guidelines:**
    a. Project will be a minimum of 1500 words (not including the network architecture)
    b. Project will use APA format
    c. Project will include a cover page
    d. Project will include a reference page
    e. To reiterate: the network architecture will be incorporated to the final document (cut and paste or screen capture). Ensure that it is legible; easily read. You may use any applicable tool to create your diagram. Some examples are packet tracer, PowerPoint, Microsoft Visio, Draw.IO.

5. **Grading Rubric:** See attached grading rubric for a detailed breakdown for this assignment. In general, your assignment will be graded as follows:
    a. **Content:**
        i. **Architecture:** 40 Points
        ii. **Resource Request:** 40 Points
        iii. **Research and Analysis:** 100 Points (25 Points for each attack/layer)
    b. **Structure:**
        i. **Formatting, Grammar, Research Elements:** 20