CYBV 326: Introductory Methods of Network Analysis

Analysis 2: TCP / UDP and Lower-Level Protocols

The University of Arizona

College of Applied Science and Technology (CAST)

Research and Critical Thinking

From the lectures and the reading use what you have learned to answer the following questions. Each answer requires at least one academic source and should be written following APA style. A general style guide can be found within the classroom and if you have any questions please feel free to contact me if this resource is unable to help you. The minimum word count for this analysis paper is 1000 words.

Write an analysis paper answering the following:

- Describe three vulnerabilities associated with TCP or UDP. What can be done to mitigate or prevent these vulnerabilities from being exploited?
- Describe the benefits of using TCP over UDP. Why is there a need to use UDP?
- Compare and contrast two ways in which a TCP connection ends (graceful vs abrupt shutdown).
- Identify an attack that uses ICMP. Describe the attack and how it is implemented. What can be done to mitigate this type of attack?
- Describe three reasons why a ping command would not work when trying to reach a destination.
- Identify one attack that uses ARP or attacks the network's Link Layer. Describe these attacks and provide a real-world example for each of these attacks. A real-world example means that it has occurred.
- Research how you could change the MAC address on a system. Describe the following:
    - The process for changing the MAC address.
    - How would an attacker use this for nefarious purposes?
    - Describe a situation where this has occurred. This is another example of an attack that has occurred in the lab or in the wild.