cit470

Task: Above-and-Beyond 2

Complete an optional project that creatively goes "above and beyond" the tasks you and your partner(s) are working on in your team projects.

Students that achieve a passing grade with each of their team tasks and peer evaluations will pass the course with a C grade. Above-and-beyond tasks are projects that students may accomplish individually. There are eight Above-and-beyond opportunities in this course.

Tools

On one or more of your team's virtual machines, install Wireshark, a software utility for capturing and analyzing network traffic.

- Wireshark features a Graphical User Interface application, useful for interactive packet-captures and packet-analysis. It also includes a terminal-based command-line utility, tshark, which complements Wireshark; for some tasks it is more practical than the GUI application.
- Most Linux distributions' default installations provide the command-line utility tcpdump. Learn to use this tool too; you'll likely use it often in your future careers.

Requirements

Write a brief tutorial showing how you used Wireshark and tshark (or tcpdump) to solve two of the problems you encountered while working on any of your other tasks in this course. Write your tutorial as if it could be a supplement or appendix to another of your other project task reports. Here's an example outline that might be helpful:

- Identify a network or security problem that, with the help of Wireshark, you were able to troubleshoot and solve.
  - Show how Wireshark helped you diagnose and fix that problem.
  - Where appropriate, include a couple of illustrative screen captures of Wireshark in action.
- Identify a network or security problem that, with the help of tcpdump or tshark, you were able to troubleshoot and solve.
  - Show how the tool helped you diagnose and fix that problem.

- Where appropriate, include console text output (or screencaptures) of your command-line tool in action.

Deliverable

Upload an illustrated tutorial, in which you explain what you did and how you accomplished it.

- Your document should be clear enough that one of your peers would be able to follow your instructions and accomplish the same tasks.
- Identify any difficult or challenging parts of the project, and clearly explain how you diagnosed and overcame your obstacles.
- Include a few cropped screen captures where appropriate.

Scoring Rubric

- If your tutorial satisfies every requirement outlined above, you will earn a passing score (one point).
- If your tutorial does not satisfy one or more of the above requirements, you will earn no points. Your must then address any deficiencies and re-upload corrected documents until you earn the passing score.

Hints

If one of your VMs is unable to access the Internet while you are working on a project, you will not be able to download a traffic analyzer such as Wireshark to that VM. Instead, you may be forced to find and use whatever tools were installed by default during that VM's initial installation. Many Linux distributions include tcpdump by default.