System Security Group Project #5

Research a family of defensive security tools/concepts. This project is worth around 5% of your grade.

Directions:

Each team should pick a topic to research in preparation for a 15 minute presentation on your chosen presentation day and a 500 word wiki documentation document due by 3/30.

The presentation

You can present directly from the wiki documentation page or on a separate powerpoint. Your presentation needs to be able to be displayed on Diesburg's computer, so you can use PowerPoint, LibreOffice, or the Google Drive equivalent (no Mac software).

The documentation

The documentation will serve as official class notes for students looking for an explanation of this class of tools. Remember, soon we will be using these tools, so be as descriptive as possible while still explaining at the level of someone just learning about the tool. The documentation should contain a minimum of 500 words (about 2 pages of words on a typical 12-point/double-spaced paper), but it should also contain links, screenshots of the tools, and diagrams of how things work (if applicable). Remember to cite any sources from which you find information, and I will count wikipdedia as a valid source. You need 3 sources cited as a minimum. Citations, links, and pictures do not count towards the word count.

Create a wiki page called "Project 5" and place your documentation in there.

Scope

In both your projects and documentation, you will want to discuss:

- What is the general tool or concept? Be sure to define vocabulary.
- Where and when is this used?
- Links and descriptions of the most popular examples of the tool/concept.
- Neat/interesting things the tool/concept accomplishes.
- Places where you can find more information.

Topics

Your group will be assigned one unique topic:

- Intrusion detection/prevention systems (Snort)
- Prevention of SQL injection attacks
- Prevention of XSS (cross-site scripting) attacks
- Honeypots (LaBrea Tarpit)
- Firewalls (PFSense and Shorewall)
- Use of DMZs
- Proxy servers and reverse-proxy servers (used in security and anonymity-preserving contexts)

Grading

Individual grades will be assigned based on:

- Quality of presentation
- Quality of documentation
- Inner-peer review of group (assigning work % done to each other)