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 Google Slides presentation due on your presentation day and a 750 word Google document due by 4/8. Both deliverables must be "turned-in" in your assigned group google folder. After the documentation due date, I will make both your presentation and documentation public to the class to serve as notes.

The presentation

You can use a personal laptop or the classroom computer. Each person in the group must have contributed to the presentation, and each member should speak equally (if possible). During your presentation, other members of the class will be filling out a small evaluation form.

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 750 words (about 3 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.

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:

- **File/Directory permissions** – overview of how they work in Linux versus Windows, how to change them, examples of files and directories that need permissions locked down, setuid bit and why it can be dangerous
- **Intrusion detection/prevention systems** – discuss Snort and one other example, discuss where they are placed in the network, types of rules you might employ
- **Prevention of SQL injection attacks** – examples of bad versus good code to protect against different types of attacks, include libraries and packages that can help (if applicable)

- **Prevention of XSS (cross-site scripting) attacks** – examples of bad versus good code to protect against different types of attacks, include libraries and packages that can help (if applicable)
- **Firewalls** - discuss a packet inspection firewall like PFSense and basic port-based/iptables firewall like Shorewall, basic firewall actions like ACCEPT, DROP, REJECT (and what they do at the protocol level), examples of common firewall rules to employ, how the concept of port-forwarding works
- **Logging** – why checking logs are important (in a security context), discuss common Linux logs such as syslog and authlog, where logging occurs in Windows, examples of logging software such as Nagios and Splunk
- **Honeypots** (extra topic if needed) – overview of what it is, discussion of LaBrea Tarpit Honeypot and one other, interesting things a honeypot can catch

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)