System Security Group Project #1

Research a family of offensive security tools. 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 due on 1/19 and a 500 word wiki documentation document due by 1/22.

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.

Please remember to put notes in your weekly journal as you work on this research. It serves as a record of what you are doing individually. Once you are done, you can individually use information from your journal notes to put the group documentation and presentation together as a group.

Scope

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

- How the tools/attack works.
- Where and when are the tools/attacks used?
- Links and descriptions of the most popular examples of the tool/attack.
- Neat/interesting things the tool/attack accomplishes.
- Places where you can find more information.

Topics

Your group needs to pick one unique topic:

- Password cracking, including rainbow tables and john the ripper software
- SQL injection attacks
- XSS (cross-site scripting) attacks
- Network enumeration tools (be sure to include the software called nmap and try to find one more software tool example)

- Vulnerability enumeration tools (be sure to discuss Nessus and Nikto)
- Rootkits (be sure to talk about both a Linux and Windows example)
- The metasploit framework (be sure to give at least three specific examples of something it can do)
- Iowa State Cyber Defense Competition (only for group actively signed up). Instead of giving a presentation on a tool or attack, instead briefly discuss how the competition works and what you've been working on. You still need to provide documentation and a presentation. It's ok if you did a lot of work on something and it isn't completely finished. Instead, present on what you've learned about what you are doing.

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)