# 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 Google Slides presentation due on 1/25 and a 750 word Google document due by 1/28. 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:

- 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 will be assigned 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)

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)
- Class reviews