System Security Group Project #1

Research a family of offensive security tools. This project is worth around 5% of your grade. Due 2/5.

Directions

Each team should pick a topic to research in preparation for

- **(Group of 3)** a 15-minute Google Slides presentation due on your assigned day and a 2000 word Google document
- **(Group of 2)** a 10-minute Google Slides presentation due by your assigned day and a 1500 words Google document (talk to professor on what can be trimmed)

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

Each group will present a Google Slides presentation live to the class. (Zoom can be used for extraordinary circumstances, but the presentation should be a live presentation.) 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 (found on Blackboard).

Please refer to the presentation example.

Slide Type	Description
Title Slide	Project name, student names, presentation date
Overview Slide	2-3 summary bullet points about what your tool/technique is about.
Outline Slide	What are you covering next in your presentation?
Background Slides	Before jumping into the tool/technique, the audience may need to understand some background information. For example, if you are discussing SQL injection attacks, the audience may need a quick tutorial on what is SQL. Be sure to introduce any new vocabulary you are going to use. Only assume that students have taken the direct prerequisites to this course. (For example, may assume students have Networking knowledge, but you cannot assume they have taken the Database class.) In this section, you can also give a general overview of when the tools/techniques.
Content Slides	Depending on your topic and group size, you will give 2-3 examples of project tools/techniques. You do not have to install or run these yourself. Rather, research these techniques and feel free to pull information/graphics from official project resources and tutorials. However, be sure to cite these materials (see next section).
Further Reading Slides	This is your bibliography area. Since this is technical documentation, you do not have to use inline citations. However, you do need to list every source you used to create your presentation. See the example presentation for an example. You should be prepared to say a sentence about each source when presenting, so make sure they are good sources. (Bad sources are usually personal blogs. Good sources come

	from official project pages or organization learning resources.) You should have at least 8 sources.
Question Slide	This is just a placeholder slide to let the audience know it is time to ask questions.

In addition, professional presentations should:

- Contain page numbers for all but the title slide. (In this way, audience members can refer to a slide by a page number if they have a question.)
- Not contain "walls" of text. Please use bullet points. Screenshots/pictures/diagrams are also encouraged.
- Not contain any text below 14pt font. (The people in the back need to read, too.)
- Not contain misspellings or grammatical errors
- The "notes" area under the presentation can be filled in, but this is not required.

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 2000 words, 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 (but not an AI, yet). You need 8 sources cited as a minimum. Citations, links, and pictures do not count towards the word count. Each student should work equally on the documentation.

Please refer to the documentation example.

Section	Description
Title Page	Project name, student names, creation date, last edit date
Overview Page	2-3 sentences about what your tool/technique is about.
Table of Contents	Be sure to use the Google Docs table of contents tool. To use this tool well, be sure to format your headings using the heading tool so that the table of contents can be automatically generated and refreshed.
Background	Before jumping into the tool/technique, the audience may need to understand some background information. For example, if you are discussing SQL injection attacks, the audience may need a quick tutorial on what is SQL. Be sure to introduce any new vocabulary you are going to use. Only assume that students have taken the direct prerequisites to this course. (For example, may assume students have Networking knowledge, but you cannot assume they have taken the Database class.) In this section, you can also give a general overview of when the tools/techniques.
Content	Depending on your topic and group size, you will give 2-3 examples of project tools/techniques. You do not have to install or run these yourself. Rather, research these techniques and feel free to pull information/graphics from official project resources and tutorials. However, be sure to cite these materials (see next section).

Further Reading	This is your bibliography area. Since this is technical documentation, you do not have to use inline citations. However, you do need to list every source you used to create your documentation. See the example documentation for an example. You should be prepared to say a sentence about each source when presenting, so make sure they are good sources. (Bad sources are usually personal blogs. Good sources come from official project pages or organization learning resources.) You should have at least 8 sources.

In addition, professional technical documentation should:

- Contain page numbers for all but the first page.
- Contain a header with the project title for all but the first page.
- Contain last access dates for all references. (In this way, readers can get an idea if the link is getting stale.)
- Contain complete sentences and have correct grammar.
- Contain page breaks in-between sections.

Offensive Topics

Your group will be assigned one unique topic:

- SQL injection attacks – be sure to discuss the classic and blind attacks. Discuss how syntax of different flavors of sql can influence/thwart attacks. Do not assume audience has taken the database class.
- XSS (cross-site scripting) attacks – be sure to discuss stored, reflected, and DOM-based attacks.
- Network vulnerability scanning tools - be sure to discuss Nmap, Nessus, and Nikto.
- Metasploit – be sure to give at least 3 examples of different things it can do.
- Attack Proxy – be sure to demonstrate how they are used in general to allow packet modification. Be sure to discuss ZAP and Burp Suite. (Ignore the vulnerability scanning plugins and concentrate on how these proxies can modify packets to send malicious attacks to servers and analyze responses.)
- Reverse Shells – Be sure to discuss the concept of ssh, reverse shells and what netcat can do.
- Linux/Apache/MySQL/PHP (LAMP) Stack – What is a LAMP stack, what are each of the pieces, briefly touch on 1-2 popular alternatives. (This background is important, as we'll want to understand what we are attacking in the next module.)

Can I use AI?

AI can be used as a tool to help you do the following:

- Personally learn about a concept
- Find more resources
- Make your writing flow better

Keep in mind that the purpose of this project is for you to create reference documentation for your classmates. That means you need to learn about the tool/technique yourself and decide how best to present that information that aligns with your own style, the skill level of this class, and what the

professor is expecting. If you use AI to generate your documentation and presentation but don't learn anything, it'll become brutally obvious when (1) paragraphs/sections don't make sense, and (2) you can't answer questions about your own topic. My grading heavily takes these two things into account.

Grading

Individual grades will be assigned based on:

- Quality of the presentation – 40%
- Quality of the documentation – 40%
- Inner-peer review of group (assigning work % done to each other) – 10%
- Rating of other classmate's presentations – 10%