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 2000 word Google document due by 4/11. 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. 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.

Defensive Topics

Your group will be assigned one unique topic:

- **Firewalls** – Please focus your discussion on (1) Where firewalls can be placed (e.g. at the border routers and at the individual hosts) and why it is advantages to do so, (2) discuss an example of a packet inspection firewall like PFSense, and (3)discuss a basic port-based/iptables firewall like UFW. Be sure to discuss 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
- **php and apache** –Please give an overview of what php is (server-side code), overview of what apache is (webserver), discussion of where php and apache config files are often stored in Linux, basic example php code that allows users to enter input, introduction to how modsecurity helps protect apache
- **Authentication and Permissions** – (Authentication) Please give an overview of how the /etc/passwd and /etc/shadow files work in Linux and ssh keys. Be sure to talk about the structure of the passwd/shadow files and how ssh keys can be set up to be used instead of passwords. (File Permissions) Please give an overview of how they work in Linux, how to change them, examples of files and directories that need permissions locked down, setuid bit and why it can be dangerous. Please also discuss the setuid bit, why it is used, and why it can be a security problem.
- **Logging** – Please discuss why checking logs are important (in a security context), discuss common Linux logs such as syslog, authlog, and the apache access/error logs, how logrotate works in Linux, and examples of logging software such as Nagios, Splunk, and syslogd (remote syslog).
- **Intrusion Detection and Prevention Systems** – Be sure to talk about the differences between intrusion detection systems (IDS) and intrusion prevention systems (IPS). Please talk about where these appliances may be placed in an organization? (For example, are they placed at the boarders?) Finally, be sure to discuss Snort and Suricata.
- **Prevention of SQL injection attacks** – Please give a small overview of what is an SQL injection attack. Then focus the majority of your presentation on 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** – Please give a small overview of what is a XSS attack. Then focus the majority of your presentation on examples of bad versus good code to

protect against different types of attacks, include libraries and packages that can help (if applicable).

Grading

Individual grades will be assigned based on:

- Quality of presentation (containing required components)
- Quality of documentation (containing required components)
- Inner-peer review of group (assigning work % done to each other)
- Class reviews of presentation