Final Project for Systems Security – Protect and Harden a Server

This is your final project and will be worth 30% of your class grade.

Description:

A mysterious company has given you a server to harden and protect so full of holes it may as well be swiss cheese! Use the knowledge you have learned in this class to discover the vulnerabilities and fix the issues, all while making sure all services still work and are available to the users of the server. Specifically, you need to

1. ***Secure the vulnerable virtual machine while not breaking any existing working services***. This means actually fixing the problems with the services themselves. The server should be secured enough to withstand attacks without the second piece (see below).
2. ***Creating a second layer of defense by installing/configuring a Firewall and Intrusion Detection System to protect the server***.

To receive the minimum passing grade, you should at the very least do the following without breaking any services:

1. Add modsecurity to apache
2. Configure pfSense, move the CTF9 server "behind it"
3. Update the php code to version 8.1 and secure it using the mysqli library

(Smaller groups of 2 must do at least two of these things.)

To earn more points, you should do more things. Take a look at the "Final-Project-Hints.pdf" for more things you can do to secure the server. The list is not exhaustive.

The documentation

Create a document in your group Google Folder by the due date using the following format:

Section	Description
Title Page	Project name, student names, creation date, last edit date
Overview Page	2-3 sentences about what this final project 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.
Chapter 1: Summary of Services on CTF9	What are you trying to secure? At minimum, please explain (1) the OS type/version of the server, (2) services running on the server, and (3) version numbers of the services. Your services should include information about the LAMP stack being used – Linux version, apache version, mysql (mariadb) version, and php version. Since ssh is running, also discuss the ssh version and protocols.

Chapter 2: Initial Vulnerability Report	Using project 4 as a guide, briefly discuss the vulnerabilities you found on the server that you found scanning it with Nikto, Nessus, and SQLMap (or similar). To earn more than the minimum passing grade, also discuss vulnerabilities you found through other methods (such as XSS, permissions, etc.)
Chapter 3: Table of Defensive Deliverables	This is your main deliverable table for the client. What will you do, and who will do it? See the explanation in a later section for details.
Chapter 4: Defensive Deliverable	For each deliverable in the Division of Labor table, discuss what you had to do to fix/harden/protect the issue/problem/service. Include screenshots. Include screenshots of configurations. Each defensive deliverable should be its own subsection.
Chapter 5: Final Vulnerability Report	After you have completed your defensive deliverables, rerun nessus, nikto, and SQLMap (or similar). Discuss how the results now differ from Chapter 2. To earn more than the minimum passing grade, also discuss how you can tell other vulnerabilities not necessarily found by nessus, nikto, and SQLmap are no longer vulnerable to a hacker (e.g. XSS, permissions, etc.)
Chapter 6: Future Work	(Optional but highly recommended) If you didn't finish securing everything you wanted to secure, what would you do in the future and why?
Technical Sources Used	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.

The presentation

Each group will present a 20 minute Google Slides presentation live to the class. 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).

Slide Type	Description
Title Slide	Project name, student names, presentation date
Overview Slide	2-3 summary bullet points about what your final project is about.

Outline Slide	What are you covering next in your presentation?
Background Slides	Use a slide or two to ***briefly*** discuss a list of the vulnerabilities you found and needed to fix before securing the server. I'm expecting 1-2 slides and not more than 30 seconds discussing this section.
Content	This is the bulk of your presentation. Summarize each of your defensive deliverables (from Chapter 4) here. Note: It is acceptable here to not make slides of this portion and instead open your documentation and present from it if you are comfortable doing so. When you are done discussing the defensive deliverables, be sure to go back to the slides for future work and further reading.
Future Work	Did you accomplish everything you set out to do? Did you run out of time? If you had more time, what would you do?
Further Reading Slides	This is your bibliography area. 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.

Deadlines and Project Rubric

I've broken this final project into phases below with deadlines.

Phase 1: Chapters 1-3 (due 4/12) – 20% of project grade

- I'll be stopping by each group to check that you've gotten most of chapters 1-2 written. These sections should not take long or be very long, since most of this information can be found from project 4 and summarized/paraphrased.
- You must decide who will work on what part of the project. **This is important.** Create a plan with specific tasks delegated to team members, with dates for completion. I will be checking to make sure you have a good plan for your group.
- Your table might look something like this:

Task	Deliverable	Person	Date	Done? (Notes)
Firewall	Investigate best firewall	Person1	4/13	
Firewall	Install and document firewall settings	Person1	4/16	
SQL injection	Investigate php code to harden against sql injections	Person2	4/13	
SQL injection	Create documentation of changes to harden php	Person2	4/16	
Permissions	Check system permissions	Person3	4/16	
Etc…				

- It is expected that this table will change like a living document throughout the remainder of the project.

Phase 2: Midway point check-in (due 4/24) – 5% of project grade

- Update your division of labor table with what is done and what is still left to do. I will be going around and talking to each group based on this update.

Phase 3: Final documentation written and frozen (due 4/29) – 40% of grade

- The final documentation needs to be done by this day at 11:59pm.

Final Presentation and finishing up (4/26 or 4/29) – 35% of grade

- The presentation should take around 20 minutes. You will be recording the presentation on a computer screen. This will be recorded on Panopto for departmental outcome assessment purposes, so those who are currently speaking must stand behind the podium in front of the computer for the audio to be recorded properly. All group members should take part. Each group member should be available to answer questions based on their contributions. **– 20% of grade**
- All students must watch group presentations during finals week and answer some questions. Questions are due at the end of finals week. (Form forthcoming on eLearning) – **10% of grade**
- Groups must also fill out a peer-review (as normal) – **5 % of grade**