Final Project for Systems Security – Protect and Harden a Server

This is your final project and will be worth 35% 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 IDS/IPS to protect the server***. In addition, logging from the vulnerable servers should be reported back to the firewall.

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

Phase 1: Enumerate the vulnerabilities and services to protect (due 4/15) – 10% of project grade

- Use nmap and explore the services offered on the machine. You must keep these services running. (E.g., making the system more secure should not involve taking the services down or blocking them. If they are insecure services by default, you will need to think outside the box on how to protect them.)
- Use tools you have learned in this class to create a report of the problems you will need to fix. Remember, some vulnerabilities can be caused by poor configuration and may not necessarily show up in a nessus or nikto scan.
- Create a Google doc in your group Final Project folder called "Phase 1 -- *Initial Vulnerabilities and Services*" and place this information in there.

Phase 2: Division of Labor (due 4/15) – 10% of project grade

- After you have completed step 1, you must decide who will work on what part of the project. Create a plan with specific tasks delegated to team members, with dates for completion.
- 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…				

- Create a Google doc in your Final Project folder called "Phase 2 – *Division of Labor*" and place this information in there.

Phase 3: Midway point check-in (due 4/24) – 5% of project grade

- Fill in your Phase 2 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 4: Final documentation and presentation (due 5/3) – 40%, 20% of grade

- Create a Google doc in your Final Project folder called "*Documentation*"
- The final documentation should be divided into 3 parts
    - 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.
    - Run vulnerability scans against your secured machine. Report what issues were still found, if any.
    - Report citations/outside resources used as well as the link to your recorded presentation (see below).
    - The more detailed you are, the better.

- The presentation should take around 20 minutes. You will be recording the presentation on a computer screen with either an additional audio track, text track (someone typing in notepad or CC), or both. All group members should take part. You do not need to create a powerpoint presentation if you are comfortable talking in front of your documentation. You should discuss:
    - Vulnerabilities you initially found
    - Steps you took to harden the machine
    - Steps you took to configure sensible firewall/IDS/IPS rules
    - Did everything get secured?
    - Challenges encountered

P**hase 6: Finishing up (due 5/9) – 15% of grade**

- Each individual student will be assigned to watch two random group presentations during finals week and answer some questions. (Form forthcoming on eLearning) – **10% of grade**
- Groups must also fill out a peer-review (as normal) – **5 % of grade**

In summary, here is a breakdown of the different phases and how much everything is worth.

Phase	**Due Date**	**Percentage of Project Grade**
Phase 1: Enumerate the vulnerabilities and services to protect	4/15	10%

Phase 2: Division of labor	4/15	10%
Phase 3: Midway point check-in	4/24	5%
Phase 4: Final documentation	5/3	40%
Phase 4: Recorded presentation	5/3	20%
Phase 5: Confidential review of 2 random presentations (assigned to you)	5/9	10%
Phase 5: Peer review	5/9	5%

You do not need to meet for a final. Be sure you turn in everything by the due date.