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! Surprise – it’s the CTF9 machine! 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).

   **NOTE:** Your boss wants you to upgrade to php 7.2 (already installed on the system) and use the php mysqli library to secure your mysql commands. See video.

2. **Creating a second layer of defense by installing/configuring a Firewall and IDS/IPS to protect the server.** This year, the firewall must be pfSense. See video.

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

**Phase 1: Enumerate the vulnerabilities and services to protect; Division of Labor (due 4/9) – 20% 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 plan with specific tasks delegated to team members, with dates for completion.
- Your table might look something like this:

<table>
<thead>
<tr>
<th>Task</th>
<th>Deliverable</th>
<th>Person</th>
<th>Date</th>
<th>Done? (Notes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall</td>
<td>Investigate pfSense</td>
<td>Person1</td>
<td>4/13</td>
<td></td>
</tr>
<tr>
<td>Firewall</td>
<td>Install and document firewall settings</td>
<td>Person1</td>
<td>4/16</td>
<td></td>
</tr>
<tr>
<td>SQL injection</td>
<td>Investigate php code to harden against sql injections</td>
<td>Person2</td>
<td>4/13</td>
<td></td>
</tr>
<tr>
<td>SQL injection</td>
<td>Create documentation of changes to harden php</td>
<td>Person2</td>
<td>4/16</td>
<td></td>
</tr>
</tbody>
</table>
Investigate good settings

Person3

4/16

- Create a Google doc in your Final Project folder called “Phase 1” and place this information in there.

Phase 2: Midway point check-in (due 4/21) – 5% of project grade

- Update your Phase 2 division of labor table with what is done and what is still left to do. Be prepared to talk to the class instructor about what you have left to do and any problems you are having.

Phase 3: Final documentation and presentation (due 4/30) – 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 recorded presentation should take around 20 minutes. You can record your presentation through the Zoom client or any other method you like. 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

Phase 4: Finishing up (due 5/6) – 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.
<table>
<thead>
<tr>
<th>Phase</th>
<th>Due Date</th>
<th>Percentage of Project Grade</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phase 1: Enumerate the vulnerabilities and services to protect and division of labor</td>
<td>4/9</td>
<td>20%</td>
</tr>
<tr>
<td>Phase 2: Midway point check-in</td>
<td>4/21</td>
<td>5%</td>
</tr>
<tr>
<td>Phase 3: Final documentation</td>
<td>4/30</td>
<td>40%</td>
</tr>
<tr>
<td>Phase 3: Recorded presentation</td>
<td>4/30</td>
<td>20%</td>
</tr>
<tr>
<td>Phase 4: Confidential review of 2 random presentations (assigned to you)</td>
<td>5/6</td>
<td>10%</td>
</tr>
<tr>
<td>Phase 4: Peer review</td>
<td>5/6</td>
<td>5%</td>
</tr>
</tbody>
</table>

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

Note: If you were not able to successfully get root on the CTF9 machine in the previous project, try this command from your Kali machine, replacing the 10.161.x.x with your actual CTF9 IP address. The website was also vulnerable to XSS attacks, and there are other holes as well. You have permission to read private files in home directories and to enforce stronger password requirements/change passwords.

```
sqlmap -u "http://10.161.x.x/admin/index.php" --dbms=MySQL --data="username=test&password=test" --dump -D lampsec -T user
```

Take lots of snapshots of the CTF9 machine so that you can revert if things get messed up!! You must work with your team to coordinate fixes and not step on each other!!