Lab 12 - Final Project Part 2

Wow! You did such a good job on your report about the company's penetration test that the CIO decided to hire you to implement many of the countermeasures you suggested. However, she had a few concerns, especially when you recommended turning off services completely. While a server that is unplugged from the Internet is secure, it really isn't very usable. So, here is what she is requiring of you for this week's work.

1. **You need to take a snapshot of the system before you start to implement your countermeasure.** This way you can revert back to what you started with if you make a mistake. There is no other backup of the machines and you can't get someone else to just restore the machines for you. You don't really remember how to take a snapshot, but you remember doing this in Lab 7 - OWASP so you know you can look back at those instructions for help. Link to Lab 7. *No snapshot means if it breaks, you could have to start all over from the beginning!*
2. While you suggested removing the cleartext protocols completely from the network, this is not an option. You need to keep the functionality of all cleartext protocols, but do this in a manner that protects the data. So any file transfers, uploads, logins, need to function.
3. Any permissions issues need to be resolved.
4. Any information that is leaked should be redacted or have the correct permissions set. Additional information on this includes Alice and Eve both work in the business office and are the only ones who should be able to see financial information.
5. Any coding issues in applications should be resolved *to the best of your ability*.
6. Any authentication and authorization issues should be resolved. This includes not allowing anonymous users and all users must be authenticated by password.
7. The finance department has decided you **cannot purchase any equipment** for these countermeasures. That means **no network firewalls** can be installed.
8. You may change the passwords, **but they must still be in sync across all boxes and applications.** Plus all services must still function properly!
9. There are only 5 main users: Alice, Bob, Carol, Darrel, and of course, Eve. You are free to modify/remove other user accounts, but you must use caution. You could end up damaging the company's daily business (and lower the amount of cookies you receive) if you prematurely destroy or remove a user account that's being used as a service account. A service account is an account that is used solely for the purpose of running an application.

You decide to start with the information gathered last week in all your tables and then mark what you did to remediate the problem. You may also decide to not remediate the issue, but you have to justify why. Your table that you will turn into the CIO contains the following information.

Host IP	OS	Issue	Remediated? Why/Why not	Deployed Countermeasure
X.X.X.150				
etc.				

Turnin

Please complete the table found in the lab description above. Your lab report is **REQUIRED** to use this table/format, or points will be taken away.