Milestone 5: Systems Set Up

Objective:

Configure the:

- Web server
- Database server
- File server
- Mail server

Instructions:

Step 1: Web Server

1. Evaluate and secure the code for the given website
2. Create a secure web server config file for your chosen web server Apach2, Nginx, etc.
3. Set up any other security measure you deem necessary
4. Set up the website on the server
5. Make sure it is accessible through the internal BYU IP that you have been assigned

Step 2: Database server

1. Evaluate the code for the given website and see what tables and columns you'll need
2. Create a secure database server config file for your chosen database MySQL, MariaDB, etc.
3. Set up any other security measure you deem necessary
4. Set up the database on the server

Step 3: File server

1. Set up your central file server on one of the Linux VMs
2. Set access rights to the different directories and files
3. Connect all the workstation computers to the central file server
4. Test CRUD operations from the workstation computers on the file server

Step 4: Mail server

1. Set up your mail server on one of the Linux VMs
2. Create email accounts for all the users listed in Milestone 1
3. Connect to the mail server using an email client on a Windows GUI VM
4. Connect to the mail server using an email client on a Linux GUI VM

Step 5: Vulnerability Scanning

1. Install OpenVas or another vulnerability scanning tool on a Kali VM
2. Scan all your VMs, document the results and any vulnerabilities you may need to fix

Requirements

☐ 15 Points - Webserver
- The webserver has been set up and is accessible from the CSRL network
- Users can use the website without any errors
- The Webserver has a secure config
- The Website code has been secured

☐ 15 Points – Database
- Database has been setup
- The database has a secure config
- The database has the correct tables for the website

☐ 15 Points - File Server
- The file server has been setup
- The file server has a secure config
- The file server can be accessed from the workstations
- Users can perform CRUD operations on the folders and files within their permission group

☐ 15 Points - Mail server
- The mail server has been setup
- The mail server has a secure config
- The mail server can be accessed from the workstations
- Users can send and receive emails

☐ 5 Points - A vulnerability scanning tool has been installed

☐ 5 Points - Vulnerability Scanning of all VMs and workstations has been completed

☐ 30 Points - Document all the config files and explain and security principles and practices used

The lab pass-off will be done with a TA and the documentation should be uploaded to Learning Suite. Documentation must be submitted as a PDF.