**SAT5424 – POPULATION HEALTH INFORMATICS**

**PART 2: NETWORK ARCHITECTURE DEVELOPMENT**

Name: Frederick Dampey

1. **OpenEMR, MySQL, Apache2 and other Configurations**

The assignment was to install and open-source electronic health records software applications, openemr on four satellite hospital virtual machines. The hospitals and their IP Addresses are found below:

1. Aspirus Hospital - 192.168.17.67

2. BCMH - 192.168.17.68

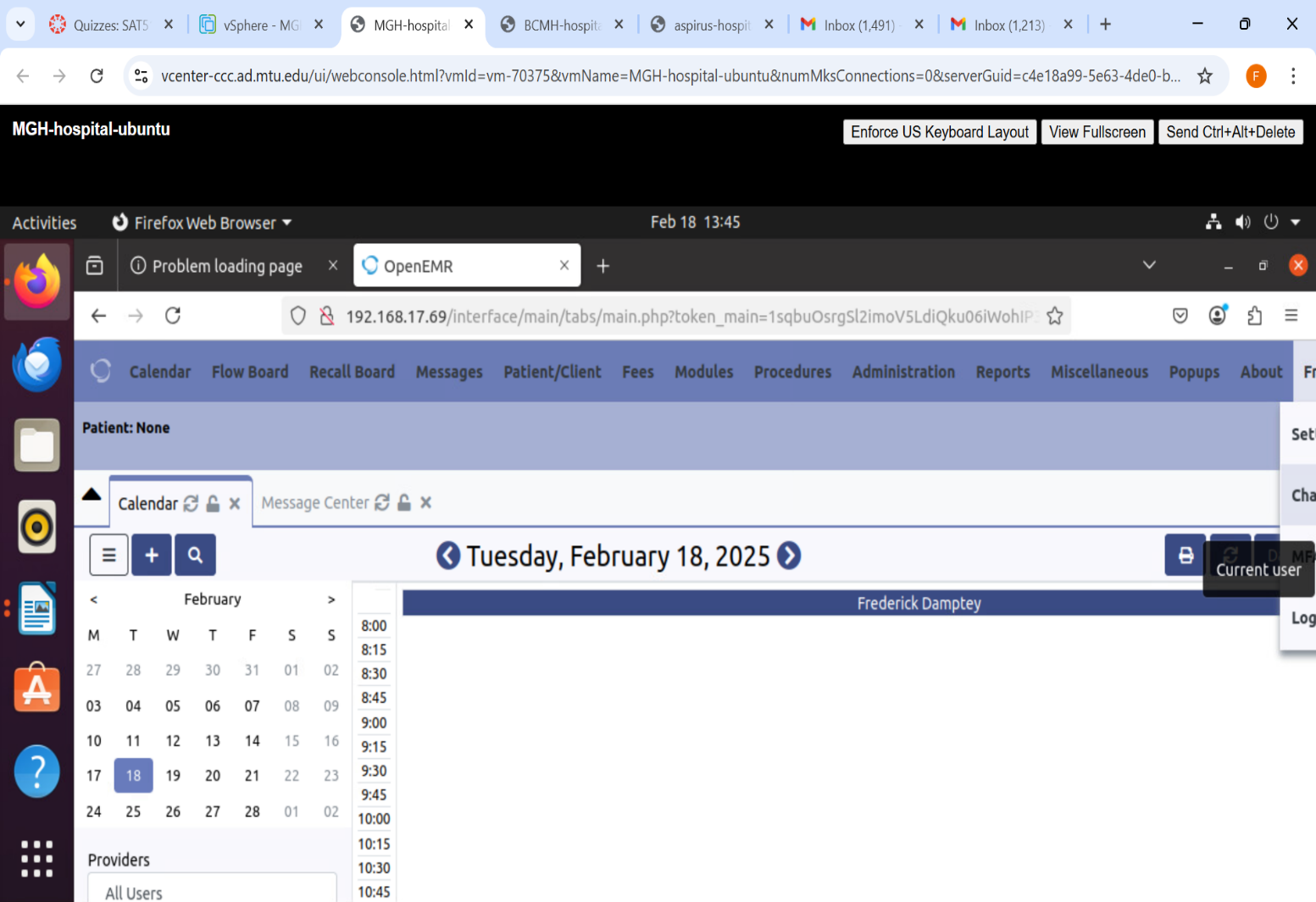
3.BMG - 192.168.17.69

4. Portage Hospital - 192.168.17.70

Screenshots of the various VMs showing the OpenEMR set up are shown below.

**SCREENSHOTS**

**Aspirus Hospital OpenEMR**



**BCMH OpenEMR**

A screenshot of a computer

AI-generated content may be incorrect.

**MGH OpenEMR**

**A screenshot of a computer

AI-generated content may be incorrect.**

**Portage Hospital OpenEMR**

**A screenshot of a computer

AI-generated content may be incorrect.**

**Step-By-Step Guide For Configurations**

The following steps were followed

1. Update and upgrade the VM software, ubuntu for the four health centers software.
2. Download and install MySQL programming language.
3. Create a database for each VM with the name, OpenEMR, account username and password.
4. Test the OpenEMR by using the IP address to launch unto the internet on a secure VPN.
5. Take screenshot of each VM to confirm successful configuration and set up.
6. Lastly, additional security installations, including enabling firewalls, enhancing access permissions and intrusion detection and prevention measures are enabled.
7. **Step-By-Step Guide In Securing OpenEMR**

**VM Password:** P@ssw0rd

1. Update and Upgrade Ubuntu Server

Open the terminal in your Ubuntu Server virtual machine.

* Run the following commands to update and upgrade the system:

sudo apt-get update

sudo apt-get upgrade

2. Enable Automatic Security Updates

Install the required package:

sudo apt-get install unattended-upgrades

Enable automatic updates:

sudo dpkg-reconfigure --priority=low unattended-upgrades

3. Set Up a Firewall

Install UFW (Uncomplicated Firewall):

sudo apt-get install ufw

Allow essential traffic:

sudo ufw allow http

sudo ufw allow https

sudo ufw allow ssh

Enable the firewall:

sudo ufw enable

4. Secure Apache

Open the security configuration file:

sudo nano /etc/apache2/conf-available/security.conf

Modify or add these lines:

ServerTokens Prod

ServerSignature Off

TraceEnable Off

Header set X-Content-Type-Options: "nosniff"

Header set X-Frame-Options: "sameorigin"

Header set X-XSS-Protection: "1; mode=block"

Header set X-Robots-Tag: "none"

Header set X-Download-Options: "noopen"

Header set X-Permitted-Cross-Domain-Policies: "none"

Save the file and exit.

Enable the security settings and restart Apache:

sudo a2enconf security

sudo systemctl restart apache2

5. Use Strong Passwords

Ensure all OpenEMR user accounts have strong, unique passwords.

6. (Optional) Set Up Backups

Regularly back up OpenEMR files and database to prevent data loss.

7. Keep OpenEMR Updated

Always install the latest updates to fix vulnerabilities.

**C) Security Vulnerabilities Of OpenEMR**

* + 1. Phishing attacks: Account user can be tricked with targeted emails with malwares and links to websites containing malwares. This can enable hackers gain unauthorized access to OpenEMR.
    2. SQL injection attacks.
    3. Inadequate account limitations and access controls may lead to unauthorized entries into the system.
    4. Physical security breaches may result in theft of personal health information.
    5. Social engineers may trick account users of OpenEMRs to reveal credentials, gain access and compromise data security and privacy.