A. Web page screenshot *(the screenshort must include the IP_Address of each hospital)* of the each hospital's successful installation of OpenEMR (8 points)

I have attached the screenshots with the name HTML-Hospital name for all four hospitals.

B. Show the steps and commands you used to secure OpenEMR (10 points)

I have attached the screenshots with the name Command-Hospital name for all four hospitals.

C. What other types of attacks would still be susceptible to the OpenEMR platform? (2 points)

Any system is never fully immune to attacks even with proper initial security configurations. Below are a couple of potential attack vectors that OpenEMR could still be susceptible to:

1. SQL Injection Attacks: OpenEMR is a web application that interacts with databases through user input. If input is not properly sanitized i.e use prepared statements and parameterized queries, attackers could exploit SQL injection vulnerabilities to manipulate database queries. This could allow them to access, modify, or delete sensitive data like patient records.

2. Cross-Site Scripting (XSS) Attacks: An attacker injects malicious scripts into web pages viewed by users. This could steal user session data or inject malicious content into the system.

3. Cross-Site Request Forgery (CSRF): A user is tricked into performing unwanted actions on a website where they are authenticated (like OpenEMR). This could result in unauthorized changes to patient data or settings.

4. Brute-Force Attacks: Explanation: Attackers may attempt to guess usernames and passwords through brute-force techniques, especially if weak passwords are used.

5. Man-in-the-Middle (MITM) Attacks: If the communication between the client (browser) and the server is not properly encrypted, attackers could intercept and manipulate the data exchanged between them, potentially stealing sensitive information.

6. Insecure APIs: If OpenEMR is integrated with other systems through APIs, insecure or improperly configured APIs could be exploited by attackers to access sensitive data or perform unauthorized actions.

7. Ransomware and Malware: Like any other software platform, OpenEMR is susceptible to ransomware or malware attacks, particularly if the underlying system is compromised.

Below are few steps to minimize the risks and to detect any suspicious activity early.
1. Update OpenEMR regularly

2. Use secure coding practices

3. Implement security tools

4. Implement intrusion detection systems

5. Secure backups.

6. Monitoring logs

7. Timely auditing access