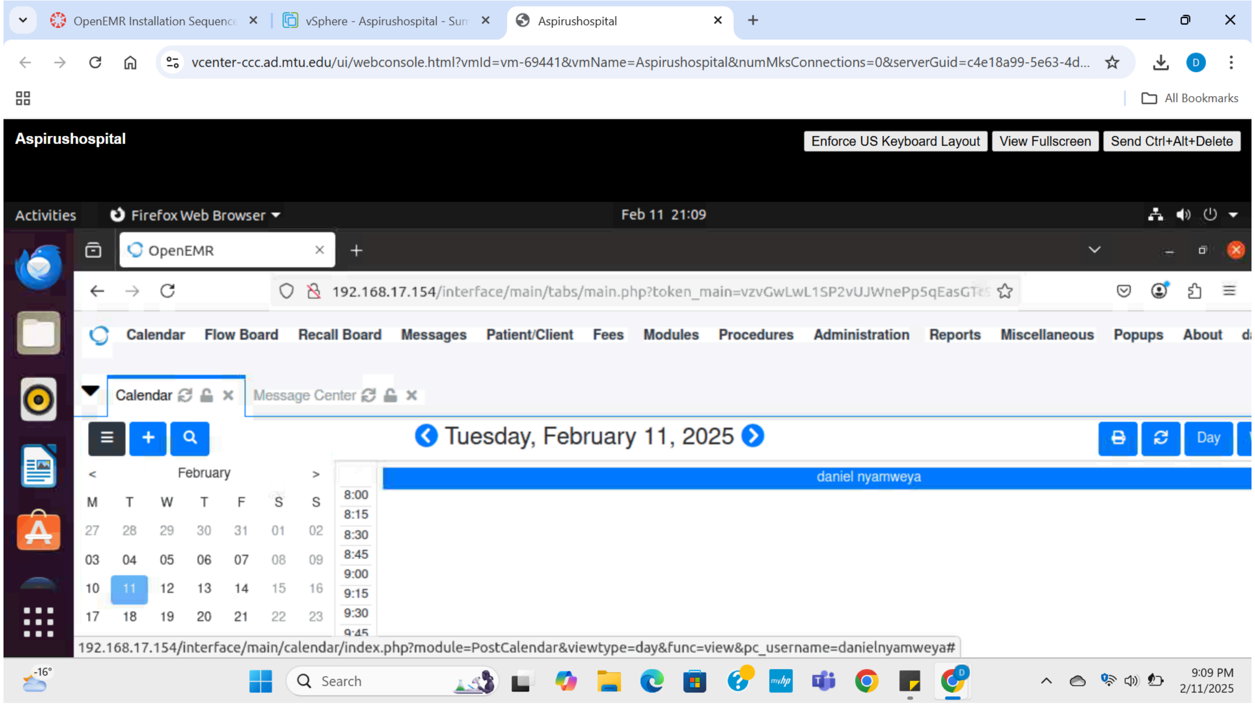
Architecture assignment part 2: Installation and security of openEMR

A. Web page screenshot (the screen shot must include the IP_Address of each hospital) of the each hospital's successful installation of OpenEMR

The following is the complete installation of openEMR in all the 4 hospitals(IP address can be seen on the URL bar)

1. Aspirus Hospital

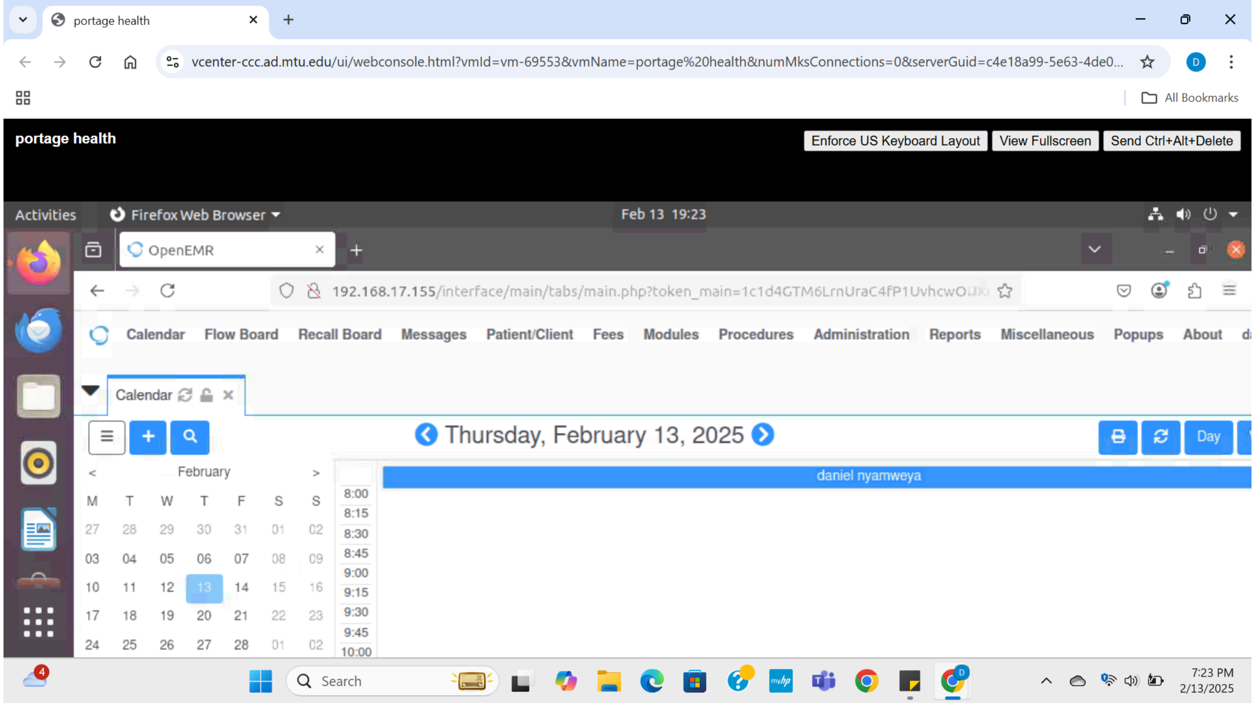


vcenter-ccc.ad.mtu.edu/ui/webconsole.html?vmId=vm-69441&vmName=Aspirushospital&numMksConnections=0&serverGuid=c4e18a99-5e63-4d...

192.168.17.154/interface/main/tabs/main.php?token_main=vzvGwLwL1SP2vUJWnePpSqEasGT

192.168.17.154/interface/main/calendar/index.php?module=PostCalendar&viewtype=day&func=view&pc_username=danielnyamweya#

2. Portage Health Hospital



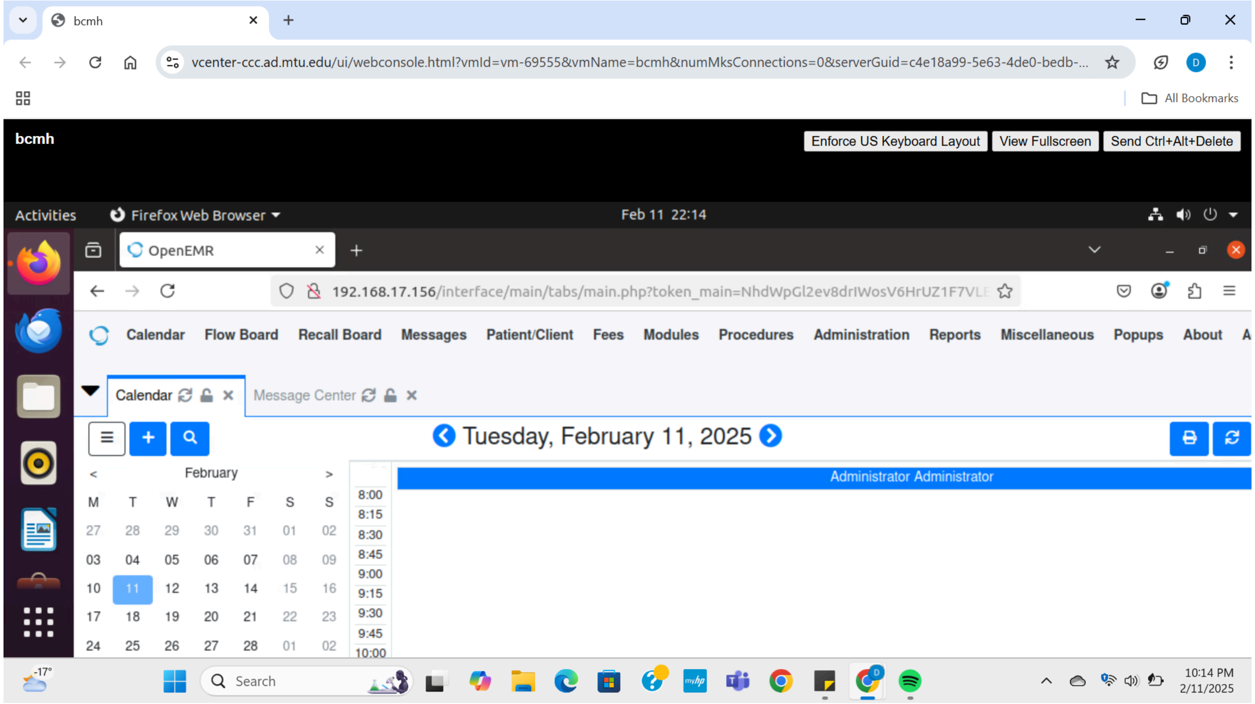
vcenter-ccc.ad.mtu.edu/ui/webconsole.html?vmId=vm-69553&vmName=portage%20health&numMksConnections=0&serverGuid=c4e18a99-5e63-4de0...

192.168.17.155/interface/main/tabs/main.php?token_main=1c1d4GTM6LrnUraC4fP1UvhcwO...

Thursday, February 13, 2025

daniel nyamweya

3. Baraga County Memorial Hospital (BCMH)



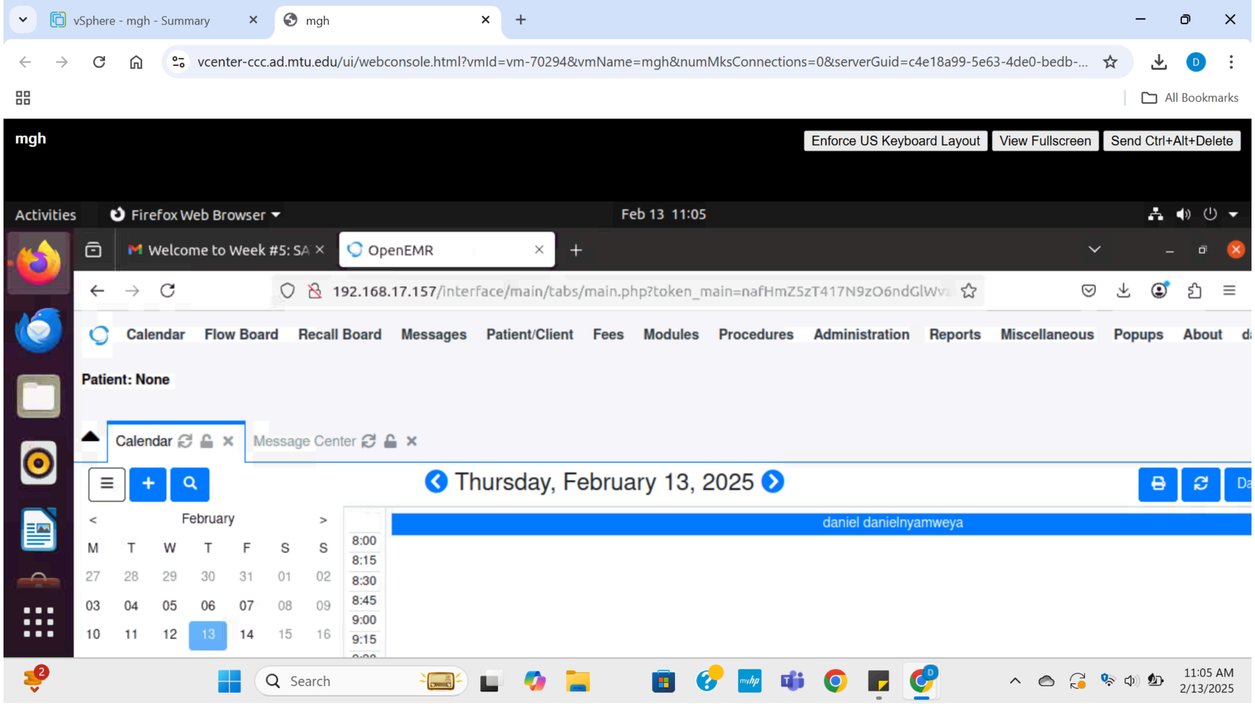
vcenter-ccc.ad.mtu.edu/ui/webconsole.html?vmId=vm-69555&vmName=bcmh&numMksConnections=0&serverGuid=c4e18a99-5e63-4de0-bedb-...

192.168.17.156/interface/main/tabs/main.php?token_main=NhdWpGl2ev8drIWosV6HrUZ1F7VL...

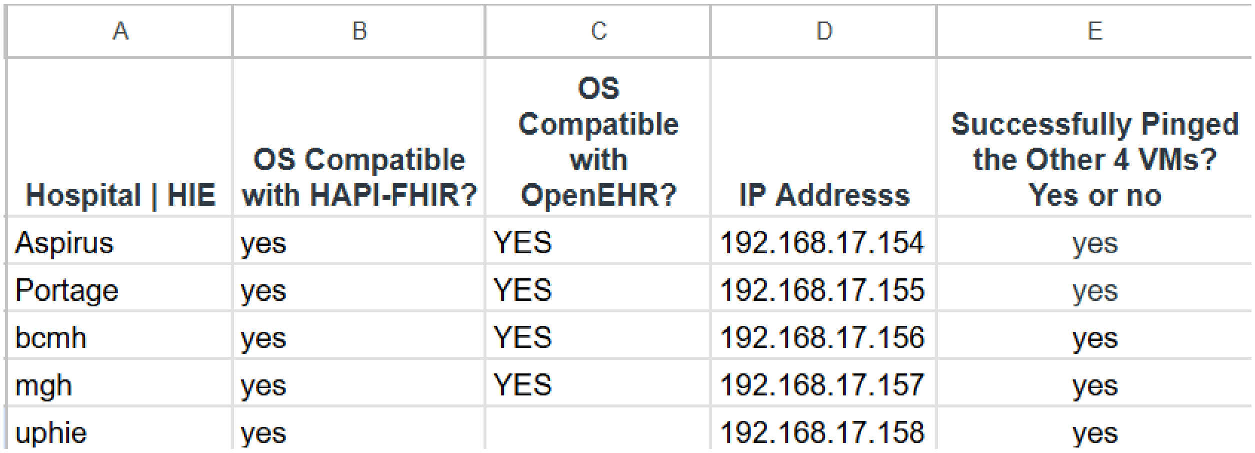
Tuesday, February 11, 2025

Administrator Administrator

4. Marquette General Hospital (MGH)



Summary table



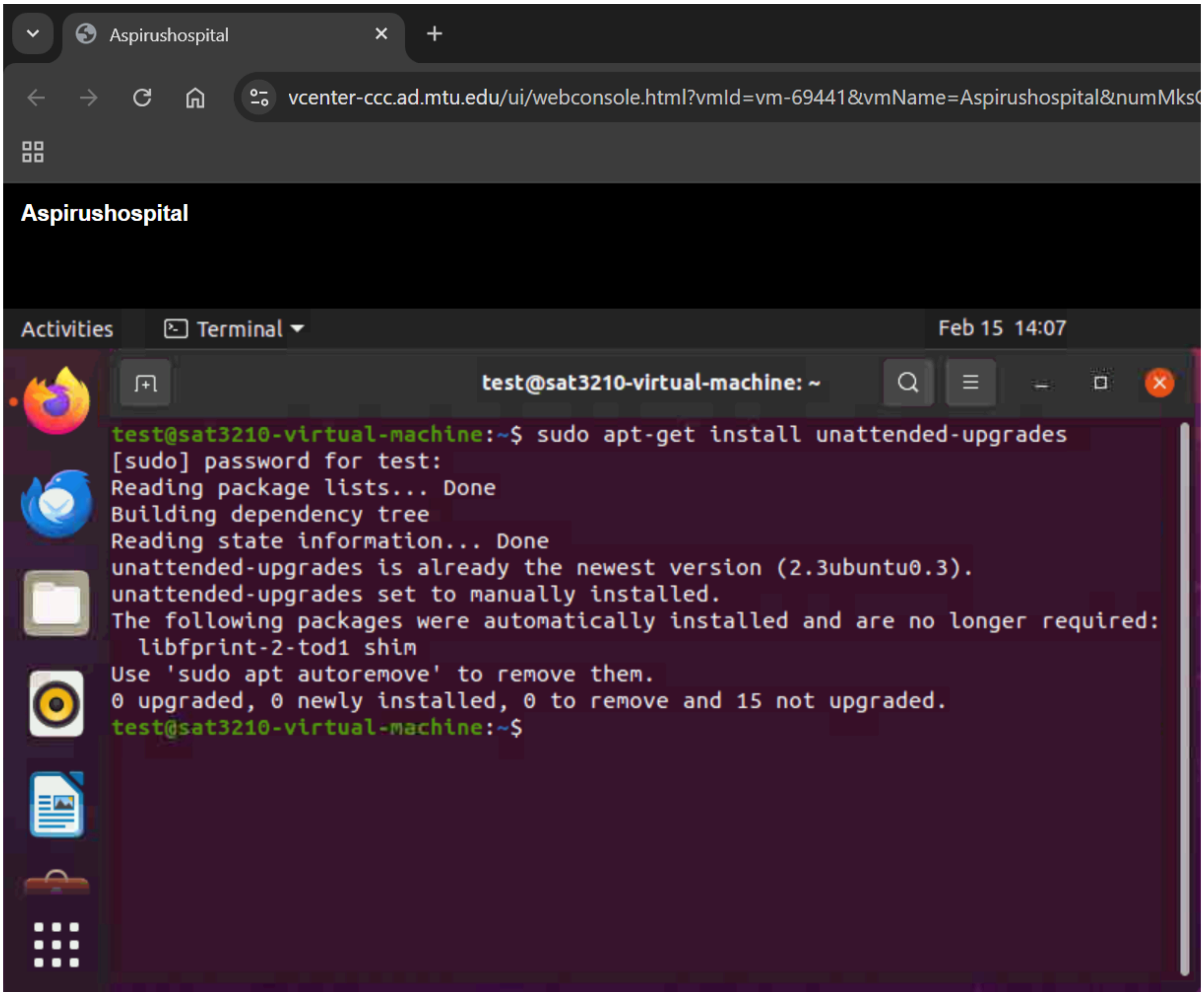
A	B	C	D	E
Hospital | HIE	OS Compatible with HAPI-FHIR?	OS Compatible with OpenEHR?	IP Addresss	Successfully Pinged the Other 4 VMs? Yes or no
Aspirus	yes	YES	192.168.17.154	yes
Portage	yes	YES	192.168.17.155	yes
bcmh	yes	YES	192.168.17.156	yes
mgh	yes	YES	192.168.17.157	yes
uphie	yes		192.168.17.158	yes

B. Show the steps and commands you used to secure OpenEMR

The following steps were taken to secure openEMR (these steps screenshots are for Aspirus only, they do however reflect what was done in all the other 3 hospitals):-

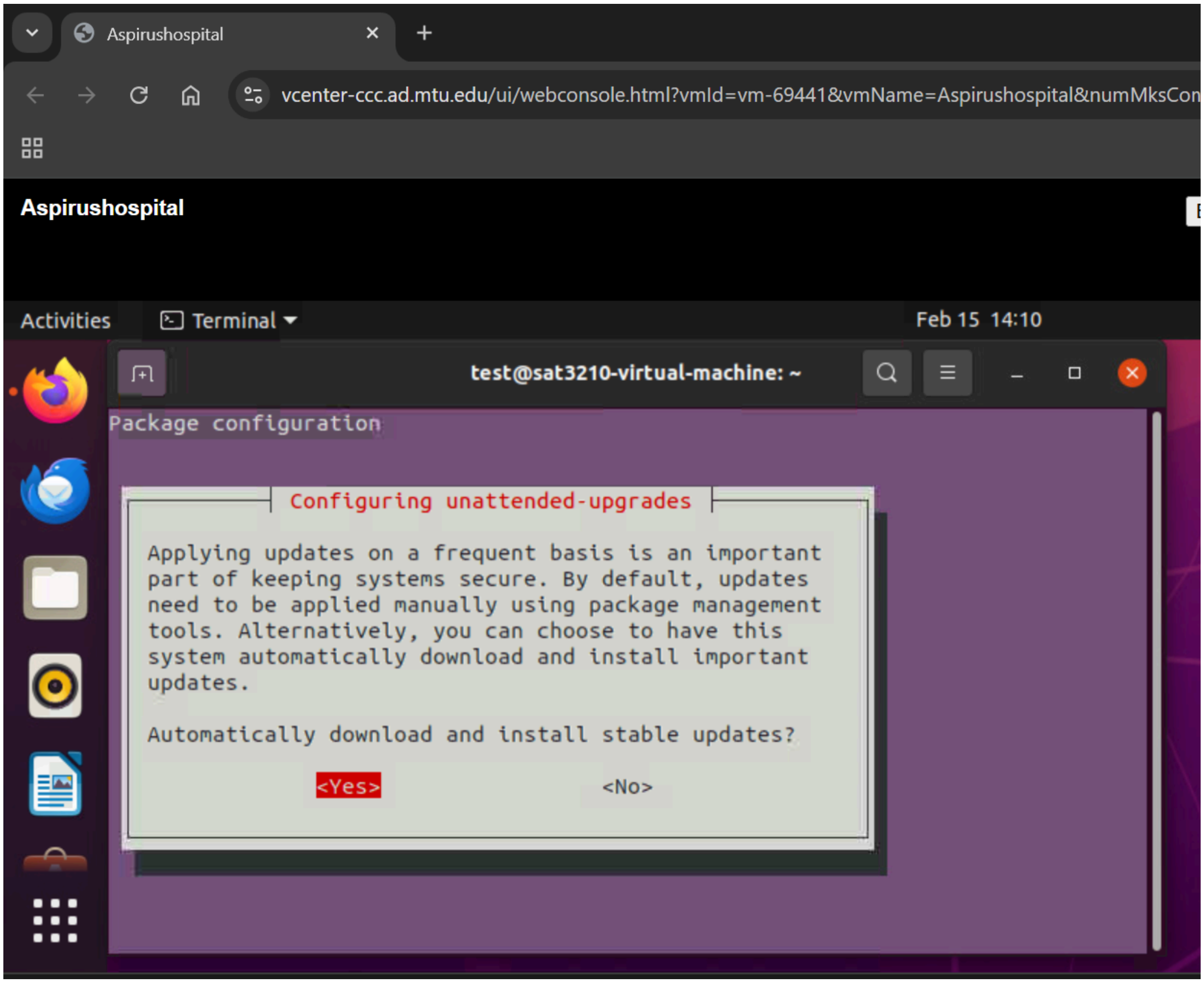
1. Installing and enabling automatic security updates. This is good since security is never 100%, it keeps updating all the time. This will ensure openEMR does not miss any security updates. Used this commands:

sudo apt-get install unattended-upgrades


Aspirushospital
vcenter-ccc.ad.mtu.edu/ui/webconsole.html?vmId=vm-69441&vmName=Aspirushospital&numMks
Aspirushospital
Activities
Terminal
Feb 15 14:07
test@sat3210-virtual-machine: ~

```
test@sat3210-virtual-machine:~$ sudo apt-get install unattended-upgrades
[sudo] password for test:
Reading package lists... Done
Building dependency tree
Reading state information... Done
unattended-upgrades is already the newest version (2.3ubuntu0.3).
unattended-upgrades set to manually installed.
The following packages were automatically installed and are no longer required:
  libfprint-2-tod1 shim
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 15 not upgraded.
test@sat3210-virtual-machine:~$
```

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

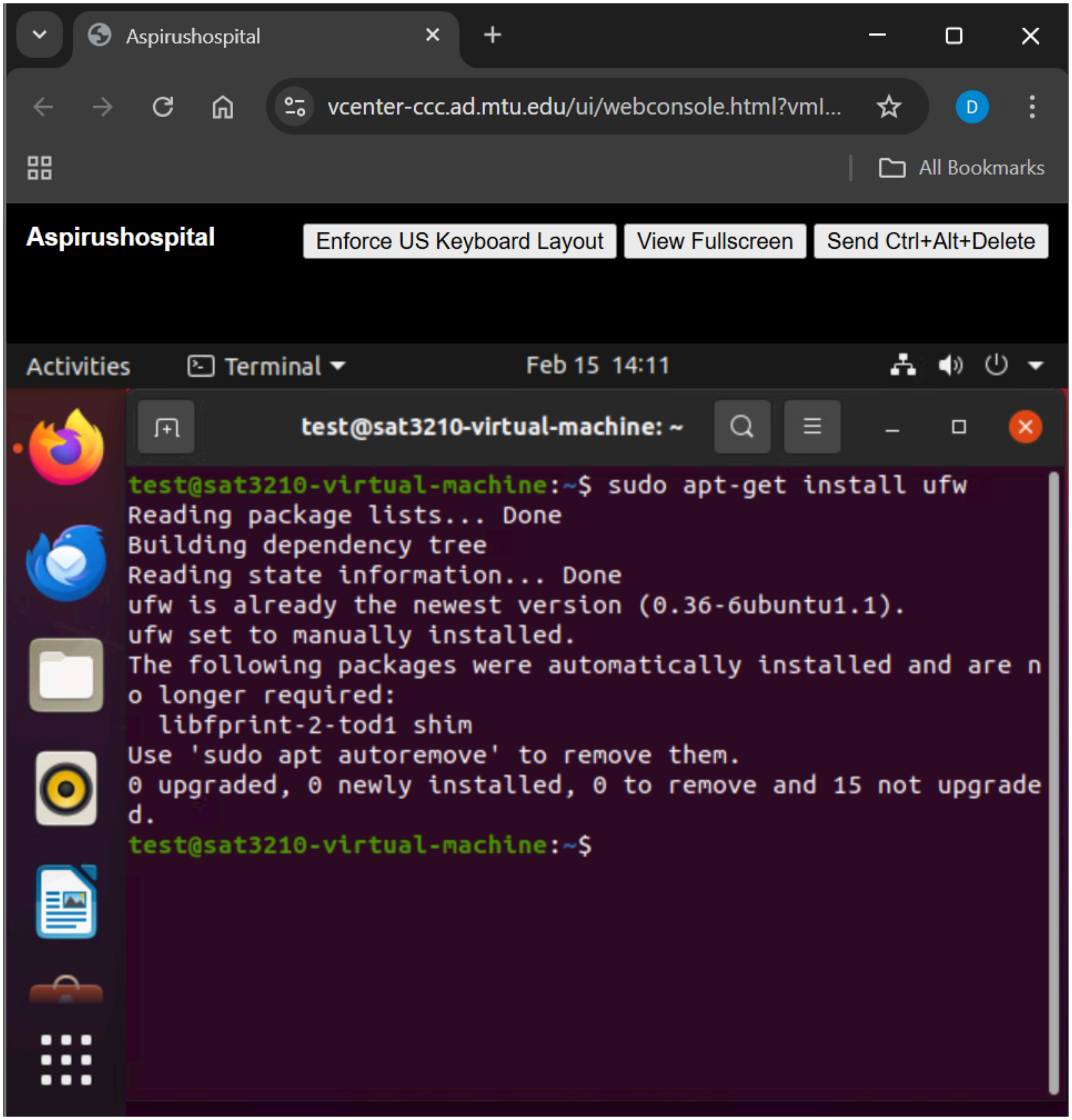


Aspirushospital
vcenter-ccc.ad.mtu.edu/ui/webconsole.html?vmId=vm-69441&vmName=Aspirushospital&numMksCon
Aspirushospital
Activities
Terminal
Feb 15 14:10
test@sat3210-virtual-machine: ~

```
Package configuration

         Configuring unattended-upgrades

 Applying updates on a frequent basis is an important
 part of keeping systems secure. By default, updates
 need to be applied manually using package management
 tools. Alternatively, you can choose to have this
 system automatically download and install important
 updates.

 Automatically download and install stable updates?

             <Yes>                  <No>
```

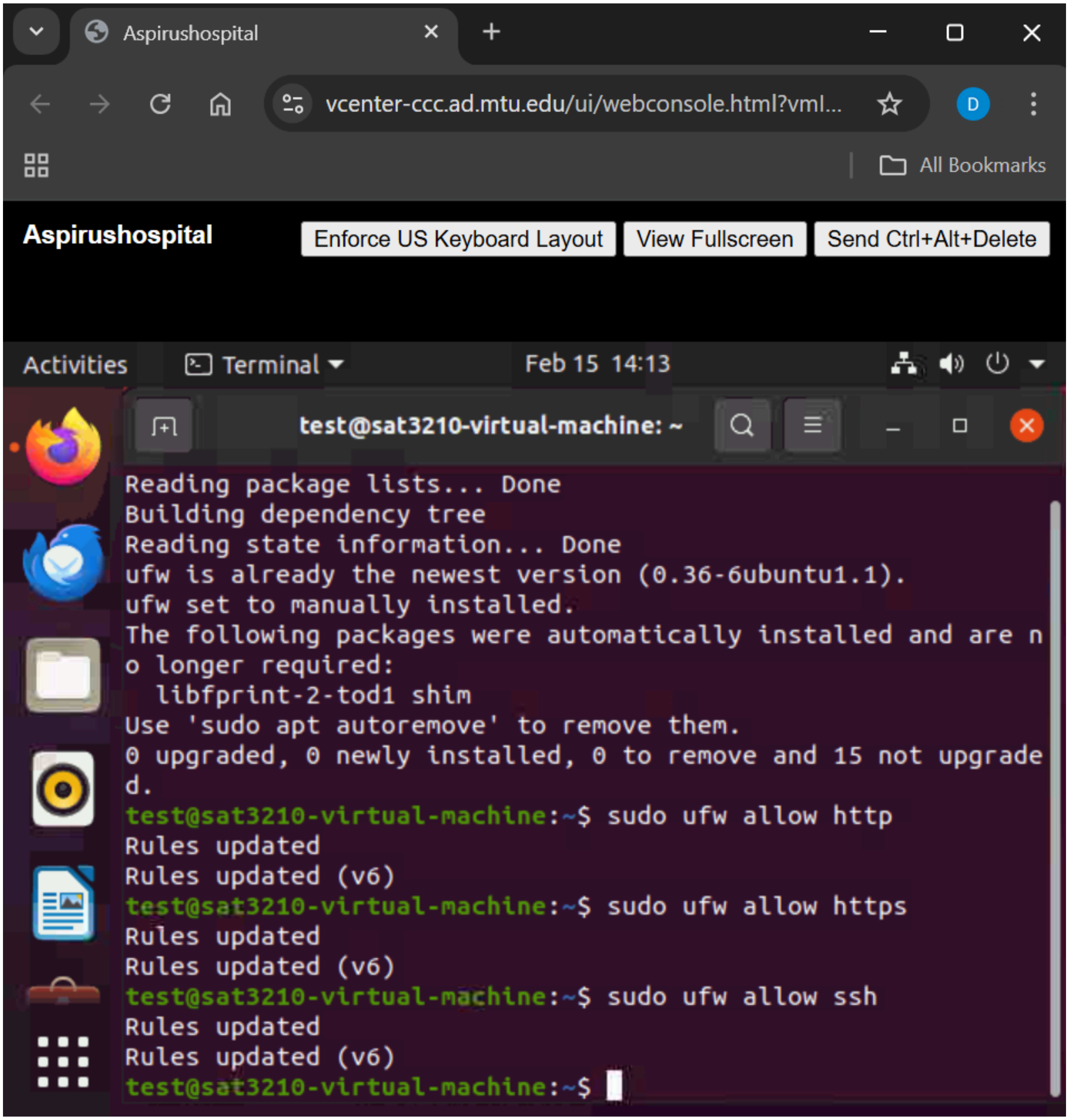
2. Configuring a firewall. Network security system that monitors and controls incoming and outgoing network traffic based on configurable security rules.

sudo apt-get install ufw



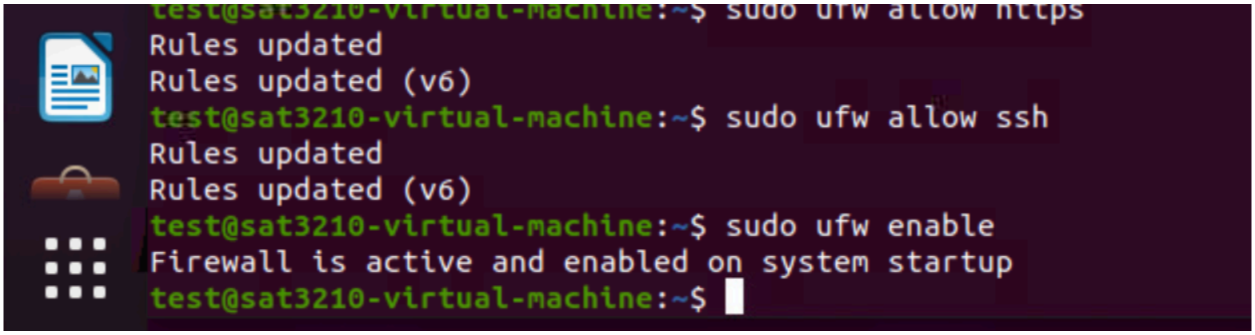
```
test@sat3210-virtual-machine:~$ sudo apt-get install ufw
Reading package lists... Done
Building dependency tree
Reading state information... Done
ufw is already the newest version (0.36-6ubuntu1.1).
ufw set to manually installed.
The following packages were automatically installed and are n
o longer required:
  libfprint-2-tod1 shim
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 15 not upgrade
d.
test@sat3210-virtual-machine:~$
```

Allowing HTTP, HTTPS, and SSH traffic



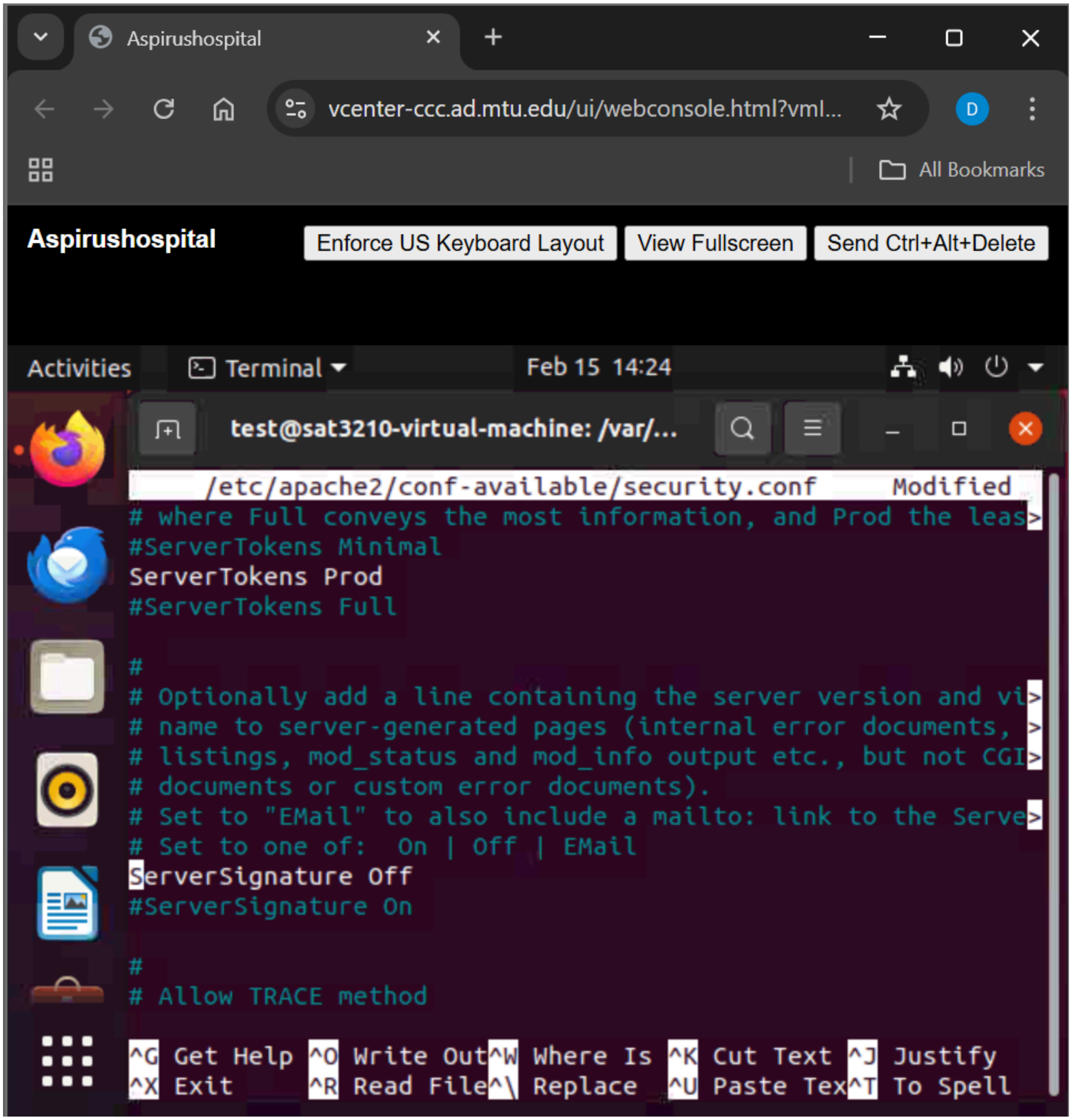
```
Reading package lists... Done
Building dependency tree
Reading state information... Done
ufw is already the newest version (0.36-6ubuntu1.1).
ufw set to manually installed.
The following packages were automatically installed and are n
o longer required:
  libfprint-2-tod1 shim
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 15 not upgrade
d.
test@sat3210-virtual-machine:~$ sudo ufw allow http
Rules updated
Rules updated (v6)
test@sat3210-virtual-machine:~$ sudo ufw allow https
Rules updated
Rules updated (v6)
test@sat3210-virtual-machine:~$ sudo ufw allow ssh
Rules updated
Rules updated (v6)
test@sat3210-virtual-machine:~$
```

Activating the firewall.



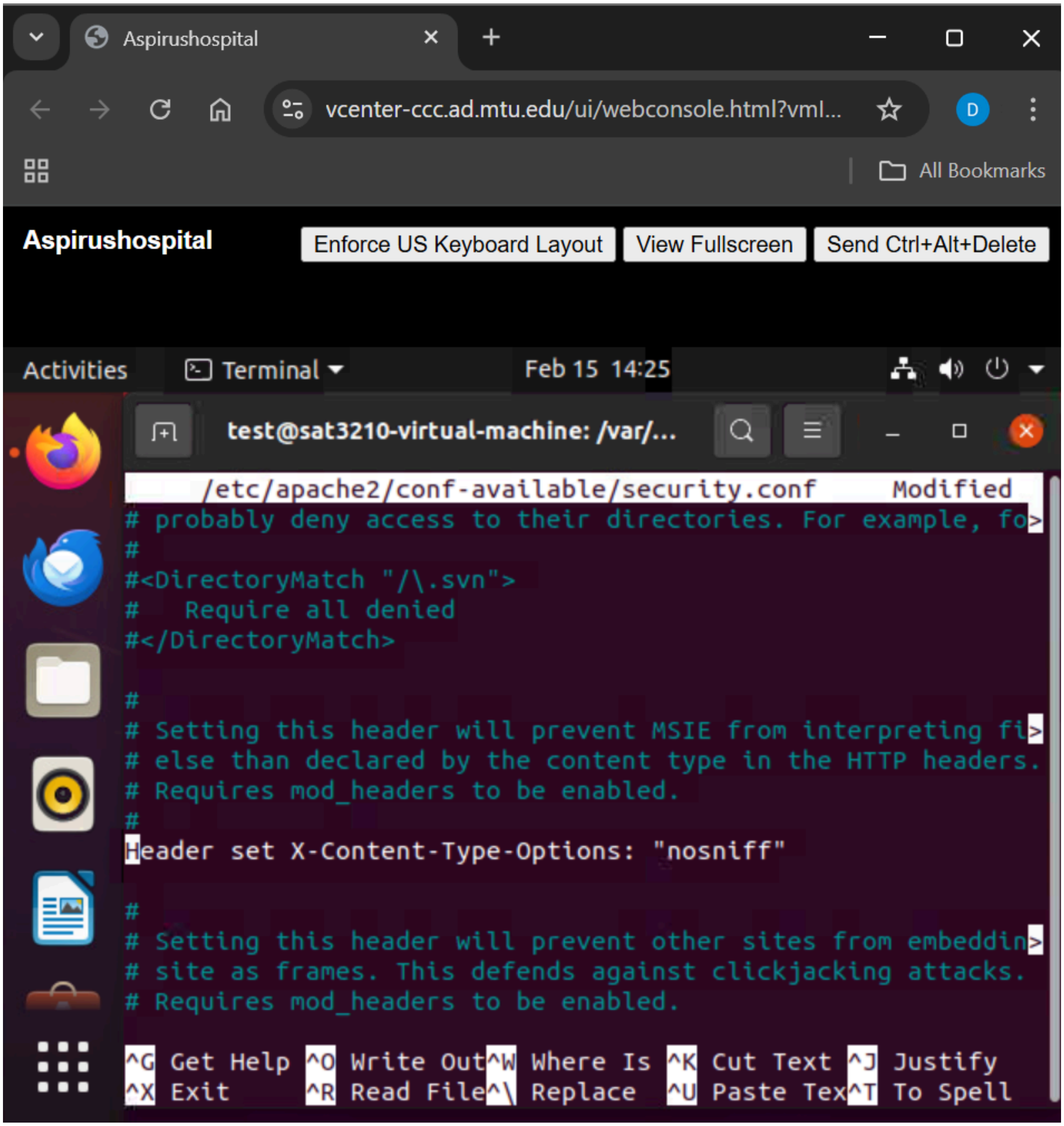
```
test@sat3210-virtual-machine:~$ sudo ufw allow https
Rules updated
Rules updated (v6)
test@sat3210-virtual-machine:~$ sudo ufw allow ssh
Rules updated
Rules updated (v6)
test@sat3210-virtual-machine:~$ sudo ufw enable
Firewall is active and enabled on system startup
test@sat3210-virtual-machine:~$
```

3. Securing Apache. Here we modified the security configuration to secure Apache from various attacks.



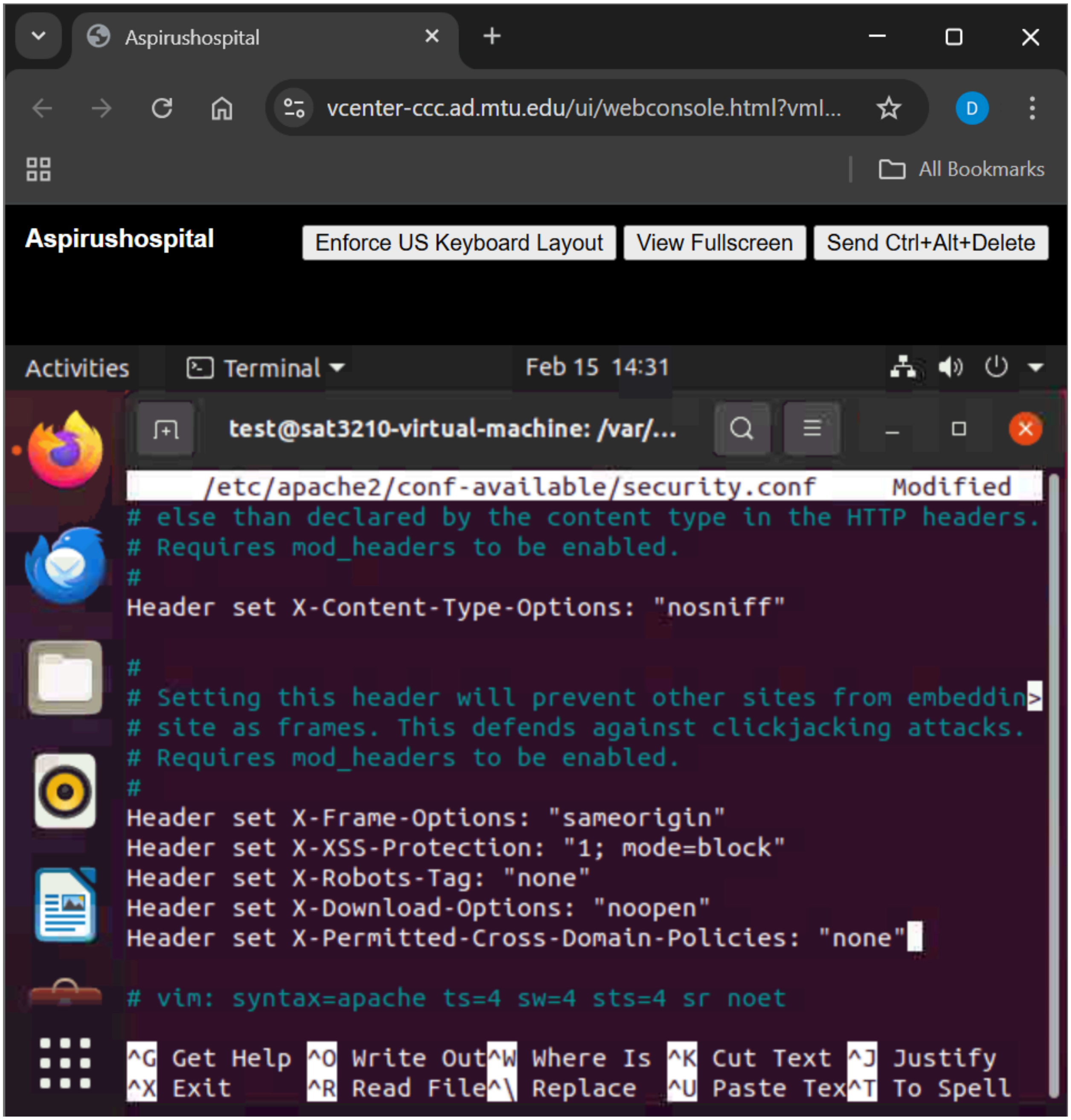
Aspirushospital
vcenter-ccc.ad.mtu.edu/ui/webconsole.html?vml...
All Bookmarks
Aspirushospital
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Activities
Terminal
Feb 15 14:24
test@sat3210-virtual-machine: /var/...

```
      /etc/apache2/conf-available/security.conf      Modified
# where Full conveys the most information, and Prod the leas>
#ServerTokens Minimal
ServerTokens Prod
#ServerTokens Full

#
# Optionally add a line containing the server version and vi>
# name to server-generated pages (internal error documents, >
# listings, mod_status and mod_info output etc., but not CGI>
# documents or custom error documents).
# Set to "EMail" to also include a mailto: link to the Serve>
# Set to one of:  On | Off | EMail
ServerSignature Off
#ServerSignature On

#
# Allow TRACE method

^G Get Help  ^O Write Out^W Where Is  ^K Cut Text  ^J Justify
^X Exit      ^R Read File^\ Replace   ^U Paste Tex^T To Spell
```



Aspirushospital
vcenter-ccc.ad.mtu.edu/ui/webconsole.html?vml...
All Bookmarks
Aspirushospital
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Activities
Terminal
Feb 15 14:25
test@sat3210-virtual-machine: /var/...

```
     /etc/apache2/conf-available/security.conf     Modified
# probably deny access to their directories. For example, fo>
#
#<DirectoryMatch "/\.svn">
#   Require all denied
#</DirectoryMatch>

#
# Setting this header will prevent MSIE from interpreting fi>
# else than declared by the content type in the HTTP headers.
# Requires mod_headers to be enabled.
#
Header set X-Content-Type-Options: "nosniff"

#
# Setting this header will prevent other sites from embeddin>
# site as frames. This defends against clickjacking attacks.
# Requires mod_headers to be enabled.

^G Get Help  ^O Write Out^W Where Is  ^K Cut Text  ^J Justify
^X Exit      ^R Read File^\ Replace   ^U Paste Tex^T To Spell
```


Aspirushospital
vcenter-ccc.ad.mtu.edu/ui/webconsole.html?vml...
All Bookmarks
Aspirushospital
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Activities
Terminal
Feb 15 14:31
test@sat3210-virtual-machine: /var/...

```
     /etc/apache2/conf-available/security.conf      Modified
# else than declared by the content type in the HTTP headers.
# Requires mod_headers to be enabled.
#
Header set X-Content-Type-Options: "nosniff"

#
# Setting this header will prevent other sites from embeddin>
# site as frames. This defends against clickjacking attacks.
# Requires mod_headers to be enabled.
#
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"

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet

^G Get Help  ^O Write Out^W Where Is  ^K Cut Text  ^J Justify
^X Exit      ^R Read File^\ Replace   ^U Paste Tex^T To Spell
```

4. Password Authentication.
   All users are required to create strong passwords for their openEMR accounts making it harder to hack from the front-end.

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

1. **Denial of Service (DoS/DDoS) -** Attackers could overwhelm the OpenEMR server with excessive requests, making it unavailable for legitimate users.
2. **Data Leakage & Unencrypted Storage -** If patient data is stored without encryption or sent over unencrypted connections, attackers could intercept or steal sensitive medical information.
3. **SQL Injection (SQLi)-** Since OpenEMR relies on a database (usually MySQL or MariaDB), poorly sanitized inputs can allow attackers to execute malicious SQL queries, potentially exposing or modifying patient records.