280. Securing the i2b2 server

Below are some tips for securing your i2b2 server. Please note that these are only recommendations and not a complete guide. Please consult your IT department if you want to go online with real patient data.

Firewall configuration

It is highly recommended to activate the firewall on your Linux system. For Ubuntu Linux, the firewall software is UFW and can easily be configured. We recommend to block all ports, except those that have to be accessed (SSH, HTTP and maybe JBoss). By default, the firewall blocks all incoming connections. However, to allow incoming traffic on port 22, which is necessary if you use SSH, type:

ufw allow from any to any port 22 (allow all incoming SSH connections)

Respectively, you can also allow:

ufw allow from any to any port 80 (allow HTTP connections, for webclient)
ufw allow from any to any port 9090 (allow JBoss connections)

Please note that allowing connections to JBoss exposes a risk of JBoss being hacked. You should make sure that JBoss is propery secured, e.g. by setting up different passwords for the JBoss web interface. If you're only using the i2b2 webclient, it is not recommended to open the JBoss port 9090. If you're using the Eclipse-based "fat" i2b2 client, opening the JBoss ports is necessary.

To limit connections to certain clients only, you can type:

ufw allow from 123.123.123.123 to any port 22 (where 123.123.123.123 is the allowed IP)

The firewall can be activated by typing:

ufw enable

To enable logging, type:

ufw logging on
tail -f /var/log/syslog

Installing fail2ban

It is also highly recommend to install fail2ban, an intrusion prevention software framework which protects computer servers from brute-force attacks. This handy tool automatically blocks IP addresses that have - unsuccessfully - tried to log into your machine after a couple of attempts. On an Ubuntu machine, type

sudo apt-get install fail2ban

to install fail2ban.