Red text is for passwords
Courier New text is for `files and commands`
Bold is **important**

Kevin Clark
Saint Cloud State University
MN State CCDC 2018

CentOS 5.9 Configuration Guide: First 15 Minutes

1. Log in -- root:changeme
2. Check website status – Enter localhost in Firefox browser
3. Open root terminal
4. Remove backdoor malware:
   - `mv /tmp/.ICE/.sys.so /tmp/.ICE/sys.so.BAK`
   - `crontab -r`
   - `kill -9 $(ps -ef | grep -i .sys.so | grep -v grep | awk '{print $2}')`
5. Change root password and write it down here:_____
6. Change administrator password and write here:_____
7. Change mysql account to nologin: `usermod -s /sbin/nologin mysql`
8. Change tomcat account to nologin: `usermod -s /sbin/nologin tomcat`
9. Back up web root to /opt directory: `cp -R /var/www/html /opt/html.BAK.1`
10. Add the line: `nameserver 8.8.8.8` to the top of `/etc/resolv.conf`
11. Decide on a new mysql password and record it here:_____
12. Change mysql password -- Do the following:

    ON THE UBUNTU DNS MACHINE:
    - Change password to allow local login: `mysqladmin -u root password 'NewSQLPassword'`
    - Log in: `mysql -u root -p mysql` Enter new password at prompt
    - At mysql prompt: `update user set password=PASSWORD("NewSQLPassword") where user='root';`
    - `flush privileges;`

    ON THE CENTOS MACHINE:
    - Edit the following lines of `/var/www/html/configuration.php`
    - `var $host = '172.20.240.23';`
    - `var $password = 'NewSQLPassword';`
13. Fix the yum repositories:
    - Check the repolist: `yum repolist` Status 0 is bad, anything greater than 0 is good.
    - Open `/etc/yum.repos.d/CentOS-Vault.repo`
    - For each section -- Base, Updates, Extras, Plus (**Only version 5.8**): `enabled = 1`
    - Check repolist again. Hope for numbers greater than 0: `yum repolist`
    - Disable all other repos that give results of 0.
    - Install something to test yum: `yum install nmap`
14. Iptables: This may depend on the services being scored. In general, allow only ports 80 and 443.
    - See my RedHat notes for details on how to use iptables.
    - Remeber **Stateful rule**, **ip6tables**, and to **save the rules** with `/etc/init.d/iptables save`

Reference:

Httpd and joomla versions: `apachectl -V`
`cat /var/www/html/libraries/joomla/version.php | grep '$RELEASE'`

CentOS Ecom:	`172.20.240.11`	Debian Email:	`172.20.241.39`
Ubuntu DNS:	`172.20.240.23`	2003 FTP:	`172.20.241.9`
2008 AD/DNS:	`172.20.241.27`	2012 Web Apps:	`172.20.241.3`