Visudo – will show users who have sudo permission

Firewall-cmd – runs firewall commands

Location of certs – “/etc/httpd/ssl/certs”

“w”

“who”

git clone [url]

Netstat commands

netstat -atu

netstat -plant

netstat -planu

top to view processes

ps aux | less

ps -u lists all commands run by a specific user

crontab -l lists cronjobs for a specific user

history can help with finding commands that were run on the host machine

systemctl --type=service will list services running

firewall-cmd - -reload reloads the firewall

firewall-cmd - -zone=public - - add-service=https - - permanent

jobs -p shows current jobs along with PID

kill %<job-id> will kill the job

check /etc/hosts file

change /etc/resolv.conf file

fix base repo in /etc/yum.repos.d to reflect “vault” on ALL links (delete any comments)

install mod\_ssl via yum install mod\_ssl

restart httpd

change /etc/httpd/conf.d/ssl.conf to include the path to the .crt and .key files

check /etc/httpd/conf/httpd.conf and make sure ServerName is set to 127.0.0.1

in httpd.conf, documentroot should be set to /var/www/html

in /etc/httpd/conf.d/welcome.conf comment everything out

in httpd.conf, change DirectoryIndex to match /prestashop/index.php

things to add into httpd.conf: ServerSignature Off, TraceEnable Off, ServerTokens Prod, Header set X-XSS-Protection “1; mode=block”, Header set X-Frame-Options: “SAMEORIGIN”

Basic Hardening Steps

1. log in credentials: root:changeme sysadmin:changeme

ccdcadmin1.morainevalley.edu

ccdc.cit.morainevalley.edu

v1u1,v1u2…

2. wget/curl localhost

sudo passwd [username] – to change password

check /etc/passwd (grep bash)

check for apache user /etc/passwd | grep apache – make sure file is not writable

lock accounts with sudo passwd -L [username]

3. change root password

4. change sysadmin password

5. change accounts to no login: usermod -s /sbin/nologin [username]

6. backup /var/www/html to /opt/html.BAK.1 using: cp -R /var/www/html /opt/html.BAK.1

7. change mysql password: mysqladmin password “[newpassword}”, mysql -u root -p should change password

8. fix yum repos (located above how to do this)

Change /etc/resolv.conf

After yum update, reboot

9. clone github from <https://github.com/SCSU-Cyber-Competition-Club/SCSU_CCDC2023-2024_PUBLIC.git>

10. run InitialScript.sh to fix firewall rules. This will also run a lynis scan and disable some services on the computer

InitialScript has been changed, and should be safe to run now

11. configure apache server (some steps are above), main things to look out for are in /etc/httpd and /var/www.

Reload apache

12. make sure the ownership of the /var/www is apache: sudo chown -R apache:apache /var/www

After this, reload apache

13. sudo yum update ca-certificates to update certs

14. find running services: systemctl list-unit-files –type=service | grep enabled

This is outputted in the Initial script

15. make user of sudo netstat -plant and sudo netstat -planu

16. crontab -l and crontab -u, also crontab -e to edit

17. top or ps to view processes

18. kill -9 [pid] to kill process

19. set up splunk forwarder in E-Comm folder. Run nohup python3 main.py &

This is not working right now

Mysql -u root to gain access

Mysqladmin

Obfuscate admin directory for web server

Uninstalling ssh and ssh-server is done in the initial script, there is another script to re-enable it

Check /etc/init.d/rc3.d

“mysqld\_safe –skip-grant-tables &”

/var/log/messages

“openssl version”

“install openssl”

“openssl genrsa -out ca.key 2048”

“openssl req -x509 -new -nodes -key ca.key -subj “/(N=<name>)” -days 7300 -out ca.crt”