**VM SETUP**

· Install and spin up a new Ubuntu (20.04 LTS) VM

Make sure you can access the VM via SSH

**Application Troubleshooting**

· Install and start Apache Web Server:

a. Apache should start automatically after machine reboot.

b. What is the process ID of apache? Why might this be useful?

9946

Troubleshooting, e.g. ps or netstat output

c. What port is apache running on?

sudo lsof -I gives us ‘http’ which corresponds to well-known port no. 80

Alternatively:

sudo lsof -i -P | grep apache

d. What interaction can systemd have with apache and why might these be useful?

Via the systemctl interface we can start, stop, restart, reload, enable on startup, disable on startup, the Apache service. All useful either for troubleshooting or for testing between configuration changes

e. How can I tell if apache is running correctly through its logs?

Either via systemctl

sudo systemctl status -l apache2

which gives a quick indication of failure to start up

or via journalctl

sudo journalctl -u apache2.service --no-pager

or via the full logs written within /var/log/apache2 for individual Vhosts

**USERS and GROUPS**

· Create accounts for the following users:

1. John – UID 1050, default GID

adduser [options] [--home DIR] [--shell SHELL] [--no-create-home] [--uid ID] [--firstuid ID] [--lastuid ID] [--ingroup GROUP |

--gid ID] [--disabled-password] [--disabled-login] [--gecos GECOS] [--add\_extra\_groups] [--encrypt-home] user

sudo adduser --uid 1050 --force-badname John

b. Andrew – no login shell

sudo adduser --shell /bin/false --force-badname Andrew

c. Bob – account locked

sudo adduser --disabled-login --force-badname Bob

d. David – default settings

sudo adduser --force-badname David

e. Set all passwords to “platform”

sudo passwd username

f. Turn OFF password expiration / aging

sudo passwd -x -1 John

sudo passwd -x -1 Andrew

sudo passwd -x -1 Bob

sudo passwd -x -1 David

· Create ateam group, add John and Bob to it

sudo addgroup ateam

sudo adduser John ateam

sudo adduser Bob ateam

· Create bteam group, add Andrew and David to it

sudo addgroup bteam

sudo adduser Andrew bteam

sudo adduser David bteam

· Allow Bob sudo access

usermod -aG sudo Bob

· Who else is allowed sudo

grep sudo /etc/group

· What is sudo?

**PARTITIONS**

· Create a /share directory

sudo mkdir /share

a. Root should be the owner of group ateam

sudo chown root:ateam /share

ls -ld /share

b. Root and ateam should have read write and execute access

sudo chmod ug+rwx /share

ls -ld /share

c. Others are prohibited to access /share dir

sudo chmod o-rwx /share

ls -ld /share

d. All files created under /share should inherit ateam group (SGID)

sudo chmod g+s /share

ls -ld /share

sudo touch /share/test1

sudo ls -l /share/test1

· Create a new partition:

a. 1G size

b. ext4 file system.

c. mount under /share/data

· Create a 100MB SWAP partition.

a. What would this be useful for?

· How much free disk space does the box have?

· What directory/files are taking up the most space on the system?

**SECURITY**

· Enable AppArmor

a. What does AppArmor do?

b. What does the complain setting mean?

· How many network adapters are configured?

· What is iptables and what is ufw?

a. What are the current rules on iptables?

b. What are the current rules on ufw?

c. Make it so only ssh and http from anywhere are allowed to the box. should you use iptables or ufw?

i.Why might this be useful?

ii.Why might this not be best practice?

**UPDATES and UPGRADES**

· Update all packages on the VM

· Upgrade the VM to the latest release