CSCE 410/611 Homework #5
Operating System Hardening
Due 2359 (11:59 pm) Thursday 31 March 2022

Alexia Perez
alexia_perezv@tamu.edu
List of people you worked with on homework – None.

PE 1. Identify the specific version of Ubuntu in your assigned VM, then list the steps necessary for hardening the OS.

```
user@box:~$ lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 20.04.4 LTS
Release:        20.04
Codename:       focal
user@box:~$
```

To harden Ubuntu 20.04:

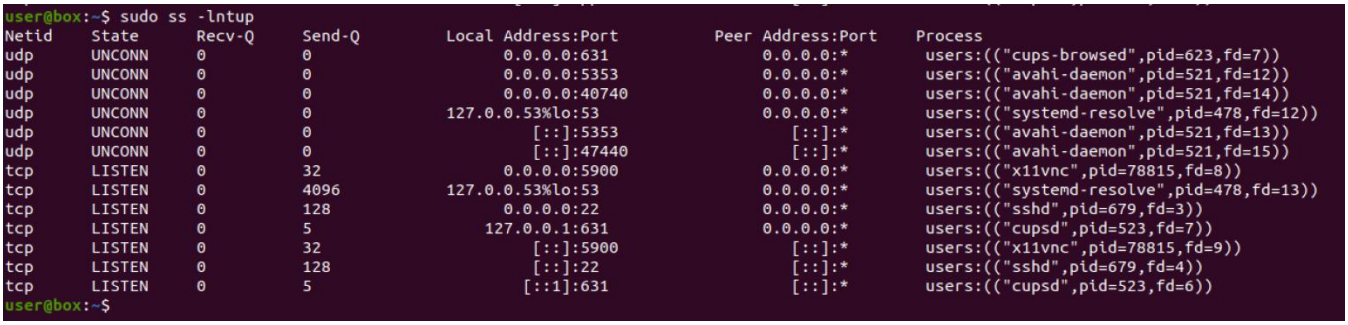
1- Upgrade system
2- Add user account, then add user to sudo group
3- Enable secure ssh server
    a. Change default ssh port and make sure to disable the remote root ssh login (edit file ssh_config).
4- Set ket-based ssh
    a. Generate ssh key
    b. Copy public key (.ssh/id_rsa.pub) to server file (~/.ssh/authorized_keys) and login without a password
5- Configure firewall
    a. Install firewalld
    b. Start and enable firewalld services

Resource: Guide To Initial Server Setup on Ubuntu 20.04 - Linux Windows and android Tutorials (osradar.com)

PE 2. In HW4, you updated the OS to install all necessary patches. In your VM, how do you check for patches to application software?

Run command: “sudo apt-get update”

PE 3. List the ports currently listening in your system. List any ports that can be safely shutdown and list the command sequence for doing so.



```
user@box:~$ sudo ss -lntup
Netid     State      Recv-Q     Send-Q         Local Address:Port          Peer Address:Port    Process
udp       UNCONN     0          0                    0.0.0.0:631                0.0.0.0:*        users:(("cups-browsed",pid=623,fd=7))
udp       UNCONN     0          0                    0.0.0.0:5353               0.0.0.0:*        users:(("avahi-daemon",pid=521,fd=12))
udp       UNCONN     0          0                    0.0.0.0:40740              0.0.0.0:*        users:(("avahi-daemon",pid=521,fd=14))
udp       UNCONN     0          0             127.0.0.53%lo:53                  0.0.0.0:*        users:(("systemd-resolve",pid=478,fd=12))
udp       UNCONN     0          0                       [::]:5353                  [::]:*        users:(("avahi-daemon",pid=521,fd=13))
udp       UNCONN     0          0                       [::]:47440                 [::]:*        users:(("avahi-daemon",pid=521,fd=15))
tcp       LISTEN     0          32                   0.0.0.0:5900               0.0.0.0:*        users:(("x11vnc",pid=78815,fd=8))
tcp       LISTEN     0          4096          127.0.0.53%lo:53                  0.0.0.0:*        users:(("systemd-resolve",pid=478,fd=13))
tcp       LISTEN     0          128                  0.0.0.0:22                 0.0.0.0:*        users:(("sshd",pid=679,fd=3))
tcp       LISTEN     0          5                  127.0.0.1:631                0.0.0.0:*        users:(("cupsd",pid=523,fd=7))
tcp       LISTEN     0          32                      [::]:5900                  [::]:*        users:(("x11vnc",pid=78815,fd=9))
tcp       LISTEN     0          128                     [::]:22                    [::]:*        users:(("sshd",pid=679,fd=4))
tcp       LISTEN     0          5                     [::1]:631                    [::]:*        users:(("cupsd",pid=523,fd=6))
user@box:~$
```

Ports that are currently listening but not connected to any application are able to be safely shutdown. To shutdown a specific port, run command: “call close($pid)”