**CSCE 611 600: OPERATING SYSTEMS Homework #5**

**Name:** Rohan Chaudhury

**Email Address:** [rohan.chaudhury@tamu.edu](mailto:rohan.chaudhury@tamu.edu)

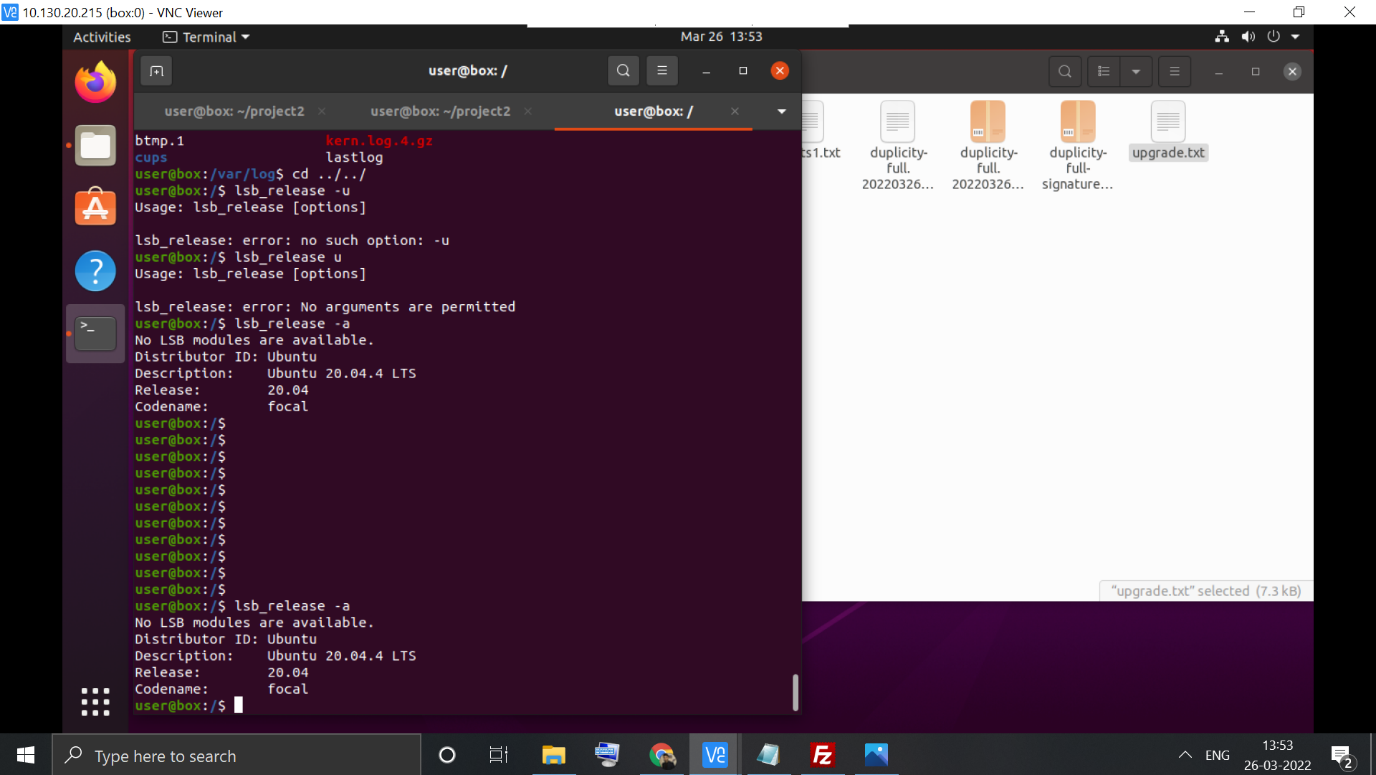
**UIN:** 432001358

**List of people I have worked with:** Abhishek Sinha, Rohit Sah, Shubham Gupta, Sherine Davis Kozhikadan

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

ANSWER PE) 1):

Ubuntu is 20.04.4 LTS is the version of ubuntu. cat /etc/os-release is the command used to see the version of OS installed. (lsb\_release -a can also be used).



A screenshot of a computer

Description automatically generated with medium confidence

The following are available in the log file generated by Linus auditing tool:

1. Steps and suggestions for hardening the OS
2. Hardening index of the system

The complete audit log (**lynis\_audit\_root.log**) is stored in the following drive location which can be accessed via any tamu.edu email account:

<https://drive.google.com/drive/folders/1VwYyDFCUolZnPDrlamT-LSVLfmJG4ltu?usp=sharing>

I have also submitted the log file with the name **lynis\_audit\_root.log** in the canvas portal

From the log file generated by Lynis tool we can see the following suggestions and steps for hardening the OS:

1. Install libpam-tmpdir to set $TMP and $TMPDIR for PAM sessions
2. Install libpam-usb to enable multi-factor authentication for PAM sessions
3. Install apt-listbugs to display a list of critical bugs prior to each APT installation.
4. Install apt-listchanges to display any significant changes prior to any upgrade via APT.
5. Install debian-goodies so that you can run checkrestart after upgrades to determine which services are using old versions of libraries and need restarting.
6. Install needrestart, alternatively to debian-goodies, so that you can run needrestart after upgrades to determine which daemons are using old versions of libraries and need restarting.
7. Install debsecan to generate lists of vulnerabilities which affect this installation.
8. Install debsums for the verification of installed package files against MD5 checksums.
9. Install fail2ban to automatically ban hosts that commit multiple authentication
10. Set a password on GRUB bootloader to prevent altering boot configuration (e.g. boot in single user mode without password)
11. Protect rescue.service by using sulogin
12. Determine why /vmlinuz is missing on this Debian/Ubuntu system. [test:KRNL-5788] [details:/vmlinuz] [solution:-]
13. Check the output of apt-cache policy manually to determine why output is empty [test:KRNL-5788] [details:-] [solution:-]
14. Install a PAM module for password strength testing like pam\_cracklib or pam\_passwdqc [test:AUTH-9262] [details:-] [solution:-]
15. Configure minimum password age in /etc/login.defs [test:AUTH-9286] [details:-] [solution:-]
16. Configure maximum password age in /etc/login.defs [test:AUTH-9286] [details:-] [solution:-]
17. Set password for single user mode to minimize physical access attack surface [test:AUTH-9308] [details:-] [solution:-]
18. Default umask in /etc/login.defs could be more strict like 027 [test:AUTH-9328] [details:-] [solution:-]
19. To decrease the impact of a full /home file system, place /home on a separated partition [test:FILE-6310] [details:-] [solution:-]
20. To decrease the impact of a full /tmp file system, place /tmp on a separated partition [test:FILE-6310] [details:-] [solution:-]
21. To decrease the impact of a full /var file system, place /var on a separated partition [test:FILE-6310] [details:-] [solution:-]
22. Disable drivers like USB storage when not used, to prevent unauthorized storage or data theft [test:STRG-1840] [details:-] [solution:-]
23. Check DNS configuration for the dns domain name [test:NAME-4028] [details:-] [solution:-]
24. Purge old/removed packages (15 found) with aptitude purge or dpkg --purge command. This will cleanup old configuration files, cron jobs and startup scripts. [test:PKGS-7346] [details:-] [solution:-]
25. Install debsums utility for the verification of packages with known good database. [test:PKGS-7370] [details:-] [solution:-]
26. Run apt-get to perform a manual package database consistency check. [test:PKGS-7390] [details:-] [solution:-]
27. Check if system is up-to-date, security updates test (apt-check) gives an unexpected result [test:PKGS-7392] [details:-] [solution:-]
28. Install package apt-show-versions for patch management purposes [test:PKGS-7394] [details:-] [solution:-]
29. Check your resolv.conf file and fill in a backup nameserver if possible [test:NETW-2705] [details:-] [solution:-]
30. Consider running ARP monitoring software (arpwatch,arpon) [test:NETW-3032] [details:-] [solution:-]
31. Access to CUPS configuration could be more strict. [test:PRNT-2307] [details:-] [solution:-]
32. Consider hardening SSH configuration [test:SSH-7408] [details:AllowTcpForwarding (YES --> NO)] [solution:-]
33. Consider hardening SSH configuration [test:SSH-7408] [details:ClientAliveCountMax (3 --> 2)] [solution:-]
34. Consider hardening SSH configuration [test:SSH-7408] [details:Compression (YES --> (DELAYED|NO))] [solution:-]
35. Consider hardening SSH configuration [test:SSH-7408] [details:LogLevel (INFO --> VERBOSE)] [solution:-]
36. Consider hardening SSH configuration [test:SSH-7408] [details:MaxAuthTries (6 --> 2)] [solution:-]
37. Consider hardening SSH configuration [test:SSH-7408] [details:MaxSessions (10 --> 2)] [solution:-]
38. Consider hardening SSH configuration [test:SSH-7408] [details:PermitRootLogin (WITHOUT-PASSWORD --> NO)] [solution:-]
39. Consider hardening SSH configuration [test:SSH-7408] [details:Port (22 --> )] [solution:-]
40. Consider hardening SSH configuration [test:SSH-7408] [details:TCPKeepAlive (YES --> NO)] [solution:-]
41. Consider hardening SSH configuration [test:SSH-7408] [details:X11Forwarding (YES --> NO)] [solution:-]
42. Consider hardening SSH configuration [test:SSH-7408] [details:AllowAgentForwarding (YES --> NO)] [solution:-]
43. Check what deleted files are still in use and why. [test:LOGG-2190] [details:-] [solution:-]
44. Add a legal banner to /etc/issue, to warn unauthorized users [test:BANN-7126] [details:-] [solution:-]
45. Add legal banner to /etc/issue.net, to warn unauthorized users [test:BANN-7130] [details:-] [solution:-]
46. Enable process accounting [test:ACCT-9622] [details:-] [solution:-]
47. Enable sysstat to collect accounting (no results) [test:ACCT-9626] [details:-] [solution:-]
48. Enable auditd to collect audit information
49. Install a file integrity tool to monitor changes to critical and sensitive files
50. Determine if automation tools are present for system management
51. One or more sysctl values differ from the scan profile and could be tweaked [test:KRNL-6000] [details:] [solution:Change sysctl value or disable test (skip-test=KRNL-6000:<sysctl-key>)]
52. Harden compilers like restricting access to root user only
53. Harden the system by installing at least one malware scanner, to perform periodic file system scans [test:HRDN-7230] [details:-] [solution:Install a tool like rkhunter, chkrootkit, OSSEC]

Other than that there are some more suggestions available on the world wide web (<https://linux-audit.com/ubuntu-server-hardening-guide-quick-and-secure/>) to harden the OS:

“**Use strong passwords**

After the first installation steps, the creation of a user account is performed. This user will be added to the administrative group, allowing him or her to become root. For this reason, the password should be a strong password.

**Why a strong password matters**: weak passwords don’t belong on systems. Not during development and especially not for production purposes. This is a serious risk as automated tools can perform many guesses per second, often discover weak passwords in just a few seconds. So system hardening should also apply to the strength of your passwords.

**Tips to enhance your password**: use longer passwords to make brute force password guessing much harder. One trick that is simple and powerful is adding a single character many times to your password (e.g. add 10 dollar signs at the beginning). Besides increasing the length, the variety of used characters is important. Add capitals, numbers, and other characters.

**Use disk encryption**

Enable encrypted LVM volumes during the installation of your Ubuntu desktop or server system. It is a great measure to hardening the system and data in particular. Although it won’t protect against all attacks, it matters for what we call *data at rest*. This means that when your system would get stolen, the data can only be retrieved if the attacker has the related key or passphrase to decrypt the data.

Select the guided partition method with “use entire disk and set up encrypted LVM”.

**Why disk encryption matters**: Your system may be stolen, even if it is a server. Another possibility is that you have to return a broken disk. In both cases, others should not be able to read data stored on the disk.

**Automatic security updates**

Every server needs software packages to fulfill its destiny during the lifetime of the system. Ensure that it gets regularly patched and updated by using *unattended-upgrades*. This is done with the “Install security updates automatically” option during the installation.

**Why applying automatic security updates matters:** almost daily new weaknesses are detected in software packages. This is no different for Ubuntu servers. Although most administrators rather not update their systems automatically, applying only the security updates is a relatively low-risk action. This is because no new features are introduced, only security flaws are patched. After that is done, a new software update is released to solve the related vulnerability. These updates are often linked to a CVE number (Common Vulnerabilities and Exposures), which provides more information about the vulnerability itself. So don’t take risks and apply those automatic security updates.

**Minimal installation**

The Ubuntu installation has been improved over the last years. It already applies the “lean” principle. This way it will only install what is really needed. The administrator can still select additional packages or software groups. There is the possibility to add new software groups at the end of the installation process or do it manually later on. Our security tip is to only select the groups and services which are really needed. For server systems, it makes sense to select the SSH server role. This way OpenSSH and the SSH daemon will be installed.

**Software updates**

During the installation, there was the option to select automatic security updates. If you already had a system running, you can add this component easily by installing the *unattended-upgrades* package

**Configure PAM: pwquality**

PAM is an abbreviation for *pluggable authentication module*. It extends the existing functionality of the authentication steps, allowing for a very fine-grained configuration. PAM is usually a little bit scary for those who are new to its configuration, as there is not a clear path it follows. Files are including each other and have sometimes cryptic names. Still, don’t be scared and test your changes first on a virtual system where you always have root access. Create an additional test user and log in with that, to help with testing.

**Firewall installation and configuration**

Now that we implemented a few measures, it is time to look at the network services. Even systems that are already filtered by a network-based firewall, might still benefit from a local firewall. There are a few options available when it comes to Linux firewalling, including UFW and iptables.

**Firewall options**

The best firewall for Ubuntu is the one that you can actually manage. The most common option is iptables. This filtering engine exists for a while and is rock-solid. Its syntax is not that friendly compared with others like pf on BSD. Still, it does the job and gradually you become better at it. UFW or Uncomplicated FireWall is a good option for those that want to apply some simple rules. UFW will take care of generating the required rules for iptables.

**Security assessment with Lynis**

If you like to learn what can be improved on your system, use the open source security tool [Lynis](https://linux-audit.com/lynis/" \t "_blank). This tool is not restricted to Ubuntu. It performs hundreds of individuals tests to detect possible weaknesses of the system. Besides that, it comes with a report that shows suggestions, or room for security improvements on your system.

”

Reference:

<https://linux-audit.com/ubuntu-server-hardening-guide-quick-and-secure/>

**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?**

**ANSWER:** To check for patches and possible updates to application software we can use the following command:

**sudo apt list --upgradable**

Text

Description automatically generated

**Commands to install all the available patches:**

1. sudo apt-get update
2. sudo apt list --upgradable
3. sudo apt-get upgrade
4. sudo apt-get dist-upgrade

If we want to install only the security patches then we can use the following command:

**sudo apt install unattended-upgrades**

If we want to automatically check for the updates and install manually through a GUI then we can use the following command:

**update-manager -d**

**List of available patches before upgrading:**

alsa-ucm-conf/focal-updates,focal-updates 1.2.2-1ubuntu0.12 all [upgradable from: 1.2.2-1ubuntu0.11]

base-files/focal-updates 11ubuntu5.5 amd64 [upgradable from: 11ubuntu5.4]

command-not-found/focal-updates,focal-updates 20.04.6 all [upgradable from: 20.04.5]

fwupd-signed/focal-updates 1.27.1ubuntu7+1.2-2~20.04.1 amd64 [upgradable from: 1.27.1ubuntu5+1.5.11-0ubuntu1~20.04.2]

fwupd/focal-updates 1.7.5-3~20.04.1 amd64 [upgradable from: 1.5.11-0ubuntu1~20.04.2]

gir1.2-gtk-3.0/focal-updates 3.24.20-0ubuntu1.1 amd64 [upgradable from: 3.24.20-0ubuntu1]

gir1.2-nm-1.0/focal-updates 1.22.10-1ubuntu2.3 amd64 [upgradable from: 1.22.10-1ubuntu2.2]

gtk-update-icon-cache/focal-updates 3.24.20-0ubuntu1.1 amd64 [upgradable from: 3.24.20-0ubuntu1]

initramfs-tools-bin/focal-updates 0.136ubuntu6.7 amd64 [upgradable from: 0.136ubuntu6.6]

initramfs-tools-core/focal-updates,focal-updates 0.136ubuntu6.7 all [upgradable from: 0.136ubuntu6.6]

initramfs-tools/focal-updates,focal-updates 0.136ubuntu6.7 all [upgradable from: 0.136ubuntu6.6]

language-pack-en-base/focal-updates,focal-updates 1:20.04+20220211 all [upgradable from: 1:20.04+20210802]

language-pack-en/focal-updates,focal-updates 1:20.04+20220211 all [upgradable from: 1:20.04+20210802]

language-pack-gnome-en-base/focal-updates,focal-updates 1:20.04+20220211 all [upgradable from: 1:20.04+20210802]

language-pack-gnome-en/focal-updates,focal-updates 1:20.04+20220211 all [upgradable from: 1:20.04+20210802]

libfwupd2/focal-updates 1.7.5-3~20.04.1 amd64 [upgradable from: 1.5.11-0ubuntu1~20.04.2]

libgtk-3-0/focal-updates 3.24.20-0ubuntu1.1 amd64 [upgradable from: 3.24.20-0ubuntu1]

libgtk-3-bin/focal-updates 3.24.20-0ubuntu1.1 amd64 [upgradable from: 3.24.20-0ubuntu1]

libgtk-3-common/focal-updates,focal-updates 3.24.20-0ubuntu1.1 all [upgradable from: 3.24.20-0ubuntu1]

libjcat1/focal-updates 0.1.4-0ubuntu0.20.04.1 amd64 [upgradable from: 0.1.3-2~ubuntu20.04.1]

libnetplan0/focal-updates 0.103-0ubuntu5~20.04.6 amd64 [upgradable from: 0.103-0ubuntu5~20.04.5]

libnm0/focal-updates 1.22.10-1ubuntu2.3 amd64 [upgradable from: 1.22.10-1ubuntu2.2]

linux-firmware/focal-updates,focal-updates 1.187.29 all [upgradable from: 1.187.25]

netplan.io/focal-updates 0.103-0ubuntu5~20.04.6 amd64 [upgradable from: 0.103-0ubuntu5~20.04.5]

network-manager-config-connectivity-ubuntu/focal-updates,focal-updates 1.22.10-1ubuntu2.3 all [upgradable from: 1.22.10-1ubuntu2.2]

network-manager/focal-updates 1.22.10-1ubuntu2.3 amd64 [upgradable from: 1.22.10-1ubuntu2.2]

python-apt-common/focal-updates,focal-updates 2.0.0ubuntu0.20.04.7 all [upgradable from: 2.0.0ubuntu0.20.04.6]

python3-apt/focal-updates 2.0.0ubuntu0.20.04.7 amd64 [upgradable from: 2.0.0ubuntu0.20.04.6]

python3-commandnotfound/focal-updates,focal-updates 20.04.6 all [upgradable from: 20.04.5]

python3-distupgrade/focal-updates,focal-updates 1:20.04.37 all [upgradable from: 1:20.04.36]

python3-update-manager/focal-updates,focal-updates 1:20.04.10.10 all [upgradable from: 1:20.04.10.9]

rsync/focal-updates 3.1.3-8ubuntu0.2 amd64 [upgradable from: 3.1.3-8ubuntu0.1]

ubuntu-advantage-tools/focal-updates 27.6~20.04.1 amd64 [upgradable from: 27.5~20.04.1]

ubuntu-drivers-common/focal-updates 1:0.9.0~0.20.04.5 amd64 [upgradable from: 1:0.9.0~0.20.04.4]

ubuntu-release-upgrader-core/focal-updates,focal-updates 1:20.04.37 all [upgradable from: 1:20.04.36]

ubuntu-release-upgrader-gtk/focal-updates,focal-updates 1:20.04.37 all [upgradable from: 1:20.04.36]

update-manager-core/focal-updates,focal-updates 1:20.04.10.10 all [upgradable from: 1:20.04.10.9]

update-manager/focal-updates,focal-updates 1:20.04.10.10 all [upgradable from: 1:20.04.10.9]

Listing...

alsa-ucm-conf/focal-updates,focal-updates 1.2.2-1ubuntu0.12 all [upgradable from: 1.2.2-1ubuntu0.11]

base-files/focal-updates 11ubuntu5.5 amd64 [upgradable from: 11ubuntu5.4]

command-not-found/focal-updates,focal-updates 20.04.6 all [upgradable from: 20.04.5]

fwupd-signed/focal-updates 1.27.1ubuntu7+1.2-2~20.04.1 amd64 [upgradable from: 1.27.1ubuntu5+1.5.11-0ubuntu1~20.04.2]

fwupd/focal-updates 1.7.5-3~20.04.1 amd64 [upgradable from: 1.5.11-0ubuntu1~20.04.2]

gir1.2-gtk-3.0/focal-updates 3.24.20-0ubuntu1.1 amd64 [upgradable from: 3.24.20-0ubuntu1]

gir1.2-nm-1.0/focal-updates 1.22.10-1ubuntu2.3 amd64 [upgradable from: 1.22.10-1ubuntu2.2]

gtk-update-icon-cache/focal-updates 3.24.20-0ubuntu1.1 amd64 [upgradable from: 3.24.20-0ubuntu1]

initramfs-tools-bin/focal-updates 0.136ubuntu6.7 amd64 [upgradable from: 0.136ubuntu6.6]

initramfs-tools-core/focal-updates,focal-updates 0.136ubuntu6.7 all [upgradable from: 0.136ubuntu6.6]

initramfs-tools/focal-updates,focal-updates 0.136ubuntu6.7 all [upgradable from: 0.136ubuntu6.6]

language-pack-en-base/focal-updates,focal-updates 1:20.04+20220211 all [upgradable from: 1:20.04+20210802]

language-pack-en/focal-updates,focal-updates 1:20.04+20220211 all [upgradable from: 1:20.04+20210802]

language-pack-gnome-en-base/focal-updates,focal-updates 1:20.04+20220211 all [upgradable from: 1:20.04+20210802]

language-pack-gnome-en/focal-updates,focal-updates 1:20.04+20220211 all [upgradable from: 1:20.04+20210802]

libfwupd2/focal-updates 1.7.5-3~20.04.1 amd64 [upgradable from: 1.5.11-0ubuntu1~20.04.2]

libgtk-3-0/focal-updates 3.24.20-0ubuntu1.1 amd64 [upgradable from: 3.24.20-0ubuntu1]

libgtk-3-bin/focal-updates 3.24.20-0ubuntu1.1 amd64 [upgradable from: 3.24.20-0ubuntu1]

libgtk-3-common/focal-updates,focal-updates 3.24.20-0ubuntu1.1 all [upgradable from: 3.24.20-0ubuntu1]

libjcat1/focal-updates 0.1.4-0ubuntu0.20.04.1 amd64 [upgradable from: 0.1.3-2~ubuntu20.04.1]

libnetplan0/focal-updates 0.103-0ubuntu5~20.04.6 amd64 [upgradable from: 0.103-0ubuntu5~20.04.5]

libnm0/focal-updates 1.22.10-1ubuntu2.3 amd64 [upgradable from: 1.22.10-1ubuntu2.2]

linux-firmware/focal-updates,focal-updates 1.187.29 all [upgradable from: 1.187.25]

netplan.io/focal-updates 0.103-0ubuntu5~20.04.6 amd64 [upgradable from: 0.103-0ubuntu5~20.04.5]

network-manager-config-connectivity-ubuntu/focal-updates,focal-updates 1.22.10-1ubuntu2.3 all [upgradable from: 1.22.10-1ubuntu2.2]

network-manager/focal-updates 1.22.10-1ubuntu2.3 amd64 [upgradable from: 1.22.10-1ubuntu2.2]

python-apt-common/focal-updates,focal-updates 2.0.0ubuntu0.20.04.7 all [upgradable from: 2.0.0ubuntu0.20.04.6]

python3-apt/focal-updates 2.0.0ubuntu0.20.04.7 amd64 [upgradable from: 2.0.0ubuntu0.20.04.6]

python3-commandnotfound/focal-updates,focal-updates 20.04.6 all [upgradable from: 20.04.5]

python3-distupgrade/focal-updates,focal-updates 1:20.04.37 all [upgradable from: 1:20.04.36]

python3-update-manager/focal-updates,focal-updates 1:20.04.10.10 all [upgradable from: 1:20.04.10.9]

rsync/focal-updates 3.1.3-8ubuntu0.2 amd64 [upgradable from: 3.1.3-8ubuntu0.1]

ubuntu-advantage-tools/focal-updates 27.6~20.04.1 amd64 [upgradable from: 27.5~20.04.1]

ubuntu-drivers-common/focal-updates 1:0.9.0~0.20.04.5 amd64 [upgradable from: 1:0.9.0~0.20.04.4]

ubuntu-release-upgrader-core/focal-updates,focal-updates 1:20.04.37 all [upgradable from: 1:20.04.36]

ubuntu-release-upgrader-gtk/focal-updates,focal-updates 1:20.04.37 all [upgradable from: 1:20.04.36]

update-manager-core/focal-updates,focal-updates 1:20.04.10.10 all [upgradable from: 1:20.04.10.9]

update-manager/focal-updates,focal-updates 1:20.04.10.10 all [upgradable from: 1:20.04.10.9]

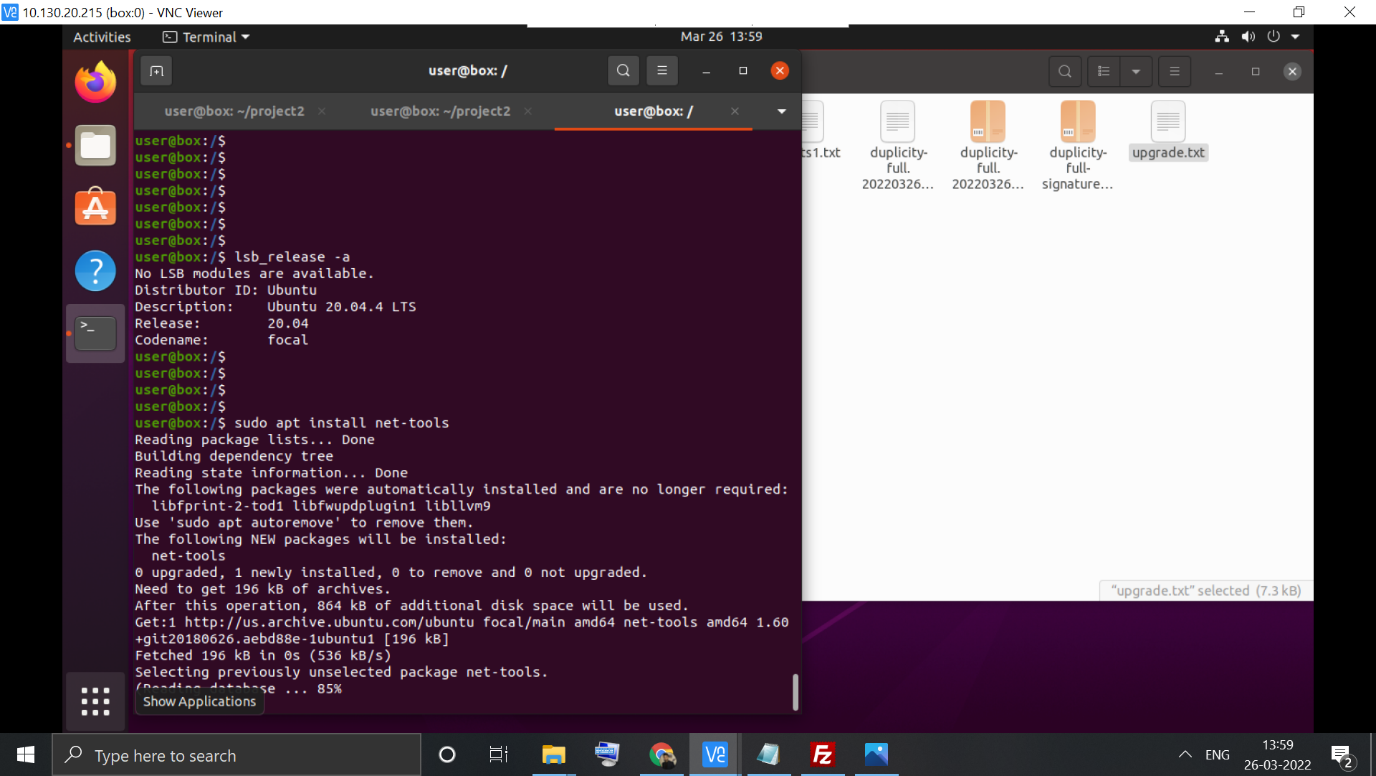
**PE 3. List the ports currently listening in your system. List any ports that can be safely shutdown and list the command sequence for doing so.**

**ANSWER:**

The command to list all the available ports is :

**sudo netstat -lp**

To use that we need to install net-tools using the command: sudo apt install net-tools



A screenshot of a computer

Description automatically generated with medium confidence

All the user level ports can be safely shutdown. Following is the list of ports for my case:

* 1. **cupsd**- “**cupsd** is the scheduler for CUPS. It implements a printing system based upon the Internet Printing Protocol, version 2.1, and supports most of the requirements for IPP Everywhere. If no options are specified on the command-line then the default configuration file */etc/cups/cupsd.conf* will be used.”

As this port “implements a printing system based upon the Internet Printing Protocol” it is not required and we can safely shut it down.

* 1. x11vnc – This is related to the VNC viewer. So shutting it down would shut down the VNC viewer process. Killing this won’t harm the system but inorder to connect to the system via VNC viewer we have to use the following command via ssh: sudo systemctl restart x11vnc.service

sshd is the SSH daemon so closing this would not allow us to ssh to the virtual machine ever again. So this should not be shut down, however shutting it down won’t harm the system.

**Command sequence to shut down a port are as follows:**

“locate the process :

1. netstat -np

You get a source/destination ip:port portstate pid/processname map

locate the the socket's file descriptor in the process

1. lsof -np $pid

You get a list: process name, pid, user,fileDescriptor, ... a connection string.

Locate the matching fileDescriptor number for the connection. It'll be something like "97u" which means "97".

Now connect the process:

1. gdb -p $pid

Now close the socket:

1. call close($fileDescriptor) //does not need ; at end.

example:

1. call close(97)

Then detach gdb:

1. quit

And the socket is closed.

”

Reference:

* 1. <https://linuxize.com/post/check-listening-ports-linux/>
  2. <https://superuser.com/questions/127863/manually-closing-a-port-from-commandline>