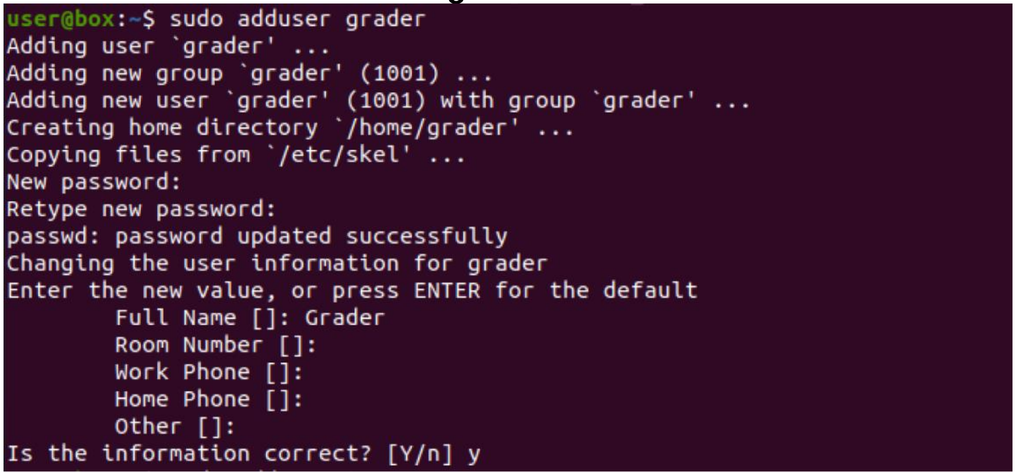
CSCE 410/611 Homework #4
Operating System Administration
Due 2359 (11:59 pm) Thursday 31 March 2022

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

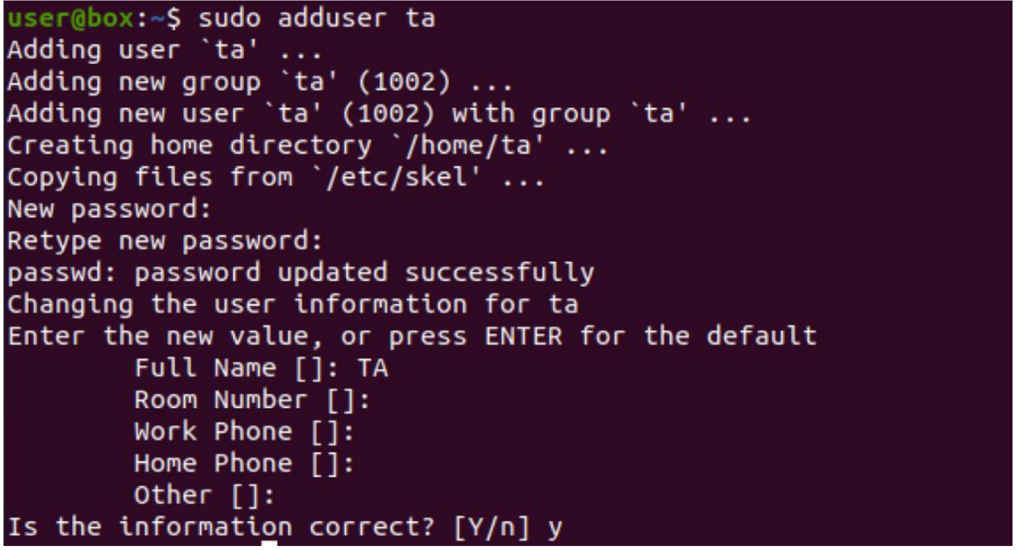
PE 1. Set up user accounts.

1. **Set up 2 new accounts in your VM (if necessary, change the default password policy to accommodate the Last six numbers of your UIN**
   First will be an account with root privileges as follows:
   Username: Grader
   Password: Last six numbers of your UIN
   Second will be an account with user privileges as follows:
   Username: TA
   Password: Last six numbers of your UIN

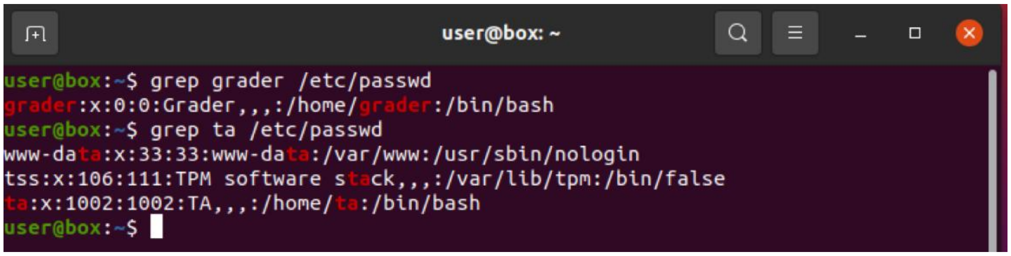
2. **Provide a screenshot showing the successful creation of both accounts.**



```
user@box:~$ sudo adduser grader
Adding user `grader' ...
Adding new group `grader' (1001) ...
Adding new user `grader' (1001) with group `grader' ...
Creating home directory `/home/grader' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for grader
Enter the new value, or press ENTER for the default
        Full Name []: Grader
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
```



```
user@box:~$ sudo adduser ta
Adding user `ta' ...
Adding new group `ta' (1002) ...
Adding new user `ta' (1002) with group `ta' ...
Creating home directory `/home/ta' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for ta
Enter the new value, or press ENTER for the default
        Full Name []: TA
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
```



```
user@box:~$ grep grader /etc/passwd
grader:x:0:0:Grader,,,:/home/grader:/bin/bash
user@box:~$ grep ta /etc/passwd
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
ta:x:1002:1002:TA,,,:/home/ta:/bin/bash
user@box:~$ 
```

Note: I created both users first, then I changed the first user's setting and gave it root privileges, as can be seen in the 3rd screenshot.

PE 2. Configure appropriate authentication policies.

1. **Given the existing architecture of the Texas Cyber Range, describe the authentication measures necessary to access and use your VM.**
    a. First, I must log into the CyberRange VPN: I must provide my "group", my username, and my password followed by a 6-digit code that I must retrieve using the DUO Authentication app.
    b. Then I must connect to my VM using my username and password
        i. If using MobaXterm for SSH access, I simply need to provide the machine's IP address, my username, and my password.
        ii. If connecting via VNCviewer, I must provide the machine's IP address, then the VNC password, and then my username and VM password.
2. **Why does the Texas Cyber Range use a different 2 factor authentication system than TAMU?**
    a. Because the Texas Cyber Range is a separate entity (not associated with TAMU). TAMU simply uses the Cyber Range's resources and has set it up for students to be able to use them with their school credentials, but they do not own the range itself.

PE 3. Configure audit capabilities.

1. **Install the Lynis System and security auditing tool.**
2. **Record the Boot loader files and the directories and files related to logging and auditing and paste the result of both audits into your homework submission.**
    a. Boot loader files:

```
2022-03-31 19:24:43 Action: Performing tests from category: Boot and services
2022-03-31 19:24:43 ===---------------------------------------------------------------===
2022-03-31 19:24:43 Skipped test BOOT-5102 (Check for AIX boot device)
2022-03-31 19:24:43 Reason to skip: Incorrect guest OS (AIX only)
2022-03-31 19:24:43 ===---------------------------------------------------------------===
2022-03-31 19:24:43 Performing test ID BOOT-5104 (Determine service manager)
```

```
2022-03-31 19:24:43 Result: cmdline found = /sbin/initsplash
2022-03-31 19:24:43 Result: cmdline of PID 1 is not a file
2022-03-31 19:24:43 Found: initsplash
2022-03-31 19:24:43 Result: service manager found = SysV Init
2022-03-31 19:24:43 ===---------------------------------------------------------------
===
2022-03-31 19:24:43 Skipped test BOOT-5106 (Check EFI boot file on
Mac OS X/macOS)
2022-03-31 19:24:43 Reason to skip: Incorrect guest OS (macOS only)
2022-03-31 19:24:43 ===---------------------------------------------------------------
===
2022-03-31 19:24:43 Performing test ID BOOT-5108 (Check Syslinux as
bootloader)
2022-03-31 19:24:43 Test: checking if file /boot/syslinux/syslinux.cfg exists
2022-03-31 19:24:43 Result: file /boot/syslinux/syslinux.cfg NOT found
2022-03-31 19:24:43 ===---------------------------------------------------------------
===
2022-03-31 19:24:43 Performing test ID BOOT-5116 (Check if system is
booted in UEFI mode)
2022-03-31 19:24:43 Test: checking if UEFI is used
2022-03-31 19:24:43 Result: UEFI not used, can't find /sys/firmware/efi
directory
2022-03-31 19:24:43 Test: determine if Secure Boot is used
2022-03-31 19:24:43 Result: system not booted with Secure Boot (no
SecureBoot file found)
2022-03-31 19:24:43 ===---------------------------------------------------------------
===
2022-03-31 19:24:43 Performing test ID BOOT-5121 (Check for GRUB
boot loader presence)
2022-03-31 19:24:43 Test: Checking for presence GRUB conf file
(/boot/grub/grub.conf or /boot/grub/menu.lst)
2022-03-31 19:24:43 Result: found GRUB2 configuration file
(/boot/grub/grub.cfg)
2022-03-31 19:24:43 ===---------------------------------------------------------------
===
2022-03-31 19:24:43 Performing test ID BOOT-5122 (Check for GRUB
boot password)
2022-03-31 19:24:43 Found file /boot/grub/grub.cfg, proceeding with tests.
2022-03-31 19:24:43 Test: check if we can access /boot/grub/grub.cfg
(escaped: /boot/grub/grub.cfg)
2022-03-31 19:24:43 Result: file is owned by our current user ID (0),
checking if it is readable
2022-03-31 19:24:43 Result: file /boot/grub/grub.cfg is readable (or
directory accessible).
2022-03-31 19:24:43 Result: Didn't find hashed password line in GRUB
boot file!
```

```
2022-03-31 19:24:43 Suggestion: Set a password on GRUB bootloader to
prevent altering boot configuration (e.g. boot in single user mode without
password) [test:BOOT-5122] [details:-] [solution:-]
2022-03-31 19:24:43 Hardening: assigned partial number of hardening
points (0 of 2). Currently having 0 points (out of 26)
2022-03-31 19:24:43 ===--------------------------------------------------------------
===
2022-03-31 19:24:43 Skipped test BOOT-5124 (Check for FreeBSD boot
loader presence)
2022-03-31 19:24:43 Reason to skip: Incorrect guest OS (FreeBSD only)
2022-03-31 19:24:43 ===--------------------------------------------------------------
===
2022-03-31 19:24:43 Skipped test BOOT-5261 (Check for DragonFly boot
loader presence)
2022-03-31 19:24:43 Reason to skip: Incorrect guest OS (DragonFly only)
2022-03-31 19:24:43 ===--------------------------------------------------------------
===
2022-03-31 19:24:43 Skipped test BOOT-5126 (Check for NetBSD boot
loader presence)
2022-03-31 19:24:43 Reason to skip: Incorrect guest OS (NetBSD only)
2022-03-31 19:24:43 ===--------------------------------------------------------------
===
2022-03-31 19:24:43 Performing test ID BOOT-5139 (Check for LILO boot
loader presence)
2022-03-31 19:24:43 Test: checking for presence LILO configuration file
2022-03-31 19:24:43 Result: LILO configuration file not found
2022-03-31 19:24:43 ===--------------------------------------------------------------
===
2022-03-31 19:24:43 Performing test ID BOOT-5142 (Check SPARC
Improved boot loader (SILO))
2022-03-31 19:24:43 Result: no SILO configuration file found.
2022-03-31 19:24:43 ===--------------------------------------------------------------
===
2022-03-31 19:24:43 Performing test ID BOOT-5155 (Check for YABOOT
boot loader configuration file)
2022-03-31 19:24:43 Test: Check for /etc/yaboot.conf
2022-03-31 19:24:43 Result: no YABOOT configuration file found.
2022-03-31 19:24:43 ===--------------------------------------------------------------
===
2022-03-31 19:24:43 Skipped test BOOT-5159 (Check for OpenBSD boot
loader presence)
2022-03-31 19:24:43 Reason to skip: Incorrect guest OS (OpenBSD only)
2022-03-31 19:24:43 ===--------------------------------------------------------------
===
2022-03-31 19:24:43 Skipped test BOOT-5165 (Check for FreeBSD boot
services)
```

```
2022-03-31 19:24:43 Reason to skip: Incorrect guest OS (FreeBSD only)
2022-03-31 19:24:43 ===------------------------------------------------------------===
2022-03-31 19:24:43 Performing test ID BOOT-5177 (Check for Linux boot and running services)
2022-03-31 19:24:43 Test: checking presence systemctl binary
2022-03-31 19:24:43 Result: systemctl binary found, trying that to discover information
2022-03-31 19:24:43 Searching for running services (systemctl services only)
2022-03-31 19:24:43 Found running service: accounts-daemon
2022-03-31 19:24:43 Found running service: acpid
2022-03-31 19:24:43 Found running service: avahi-daemon
2022-03-31 19:24:43 Found running service: colord
2022-03-31 19:24:43 Found running service: cron
2022-03-31 19:24:43 Found running service: cups-browsed
2022-03-31 19:24:43 Found running service: cups
2022-03-31 19:24:43 Found running service: dbus
2022-03-31 19:24:43 Found running service: fwupd
2022-03-31 19:24:43 Found running service: getty@tty1
2022-03-31 19:24:43 Found running service: irqbalance
2022-03-31 19:24:43 Found running service: kerneloops
2022-03-31 19:24:43 Found running service: lightdm
2022-03-31 19:24:43 Found running service: ModemManager
2022-03-31 19:24:43 Found running service: networkd-dispatcher
2022-03-31 19:24:43 Found running service: NetworkManager
2022-03-31 19:24:43 Found running service: polkit
2022-03-31 19:24:43 Found running service: rsyslog
2022-03-31 19:24:43 Found running service: rtkit-daemon
2022-03-31 19:24:43 Found running service: serial-getty@hvc0
2022-03-31 19:24:43 Found running service: snapd
2022-03-31 19:24:43 Found running service: ssh
2022-03-31 19:24:43 Found running service: switcheroo-control
2022-03-31 19:24:43 Found running service: systemd-journald
2022-03-31 19:24:43 Found running service: systemd-logind
2022-03-31 19:24:43 Found running service: systemd-resolved
2022-03-31 19:24:43 Found running service: systemd-timesyncd
2022-03-31 19:24:43 Found running service: systemd-udevd
2022-03-31 19:24:43 Found running service: udisks2
2022-03-31 19:24:43 Found running service: unattended-upgrades
2022-03-31 19:24:43 Found running service: upower
2022-03-31 19:24:43 Found running service: user@1000
2022-03-31 19:24:43 Found running service: whoopsie
2022-03-31 19:24:43 Found running service: wpa_supplicant
2022-03-31 19:24:43 Found running service: x11vnc
2022-03-31 19:24:43 Found running service: xe-linux-distribution
```

```
2022-03-31 19:24:43 Note: Run systemctl --full --type=service to see all services
2022-03-31 19:24:43 Result: Found 36 enabled services
2022-03-31 19:24:43 Searching for enabled services (systemctl services only)
2022-03-31 19:24:45 Found enabled service at boot: ModemManager
2022-03-31 19:24:45 Found enabled service at boot: NetworkManager-dispatcher
2022-03-31 19:24:45 Found enabled service at boot: NetworkManager-wait-online
2022-03-31 19:24:45 Found enabled service at boot: NetworkManager
2022-03-31 19:24:45 Found enabled service at boot: accounts-daemon
2022-03-31 19:24:45 Found enabled service at boot: anacron
2022-03-31 19:24:45 Found enabled service at boot: apparmor
2022-03-31 19:24:45 Found enabled service at boot: autovt@
2022-03-31 19:24:45 Found enabled service at boot: avahi-daemon
2022-03-31 19:24:45 Found enabled service at boot: bluetooth
2022-03-31 19:24:45 Found enabled service at boot: console-setup
2022-03-31 19:24:45 Found enabled service at boot: cron
2022-03-31 19:24:45 Found enabled service at boot: cups-browsed
2022-03-31 19:24:45 Found enabled service at boot: cups
2022-03-31 19:24:45 Found enabled service at boot: dbus-fi
2022-03-31 19:24:45 Found enabled service at boot: dbus-org
2022-03-31 19:24:45 Found enabled service at boot: dbus-org
2022-03-31 19:24:45 Found enabled service at boot: dbus-org
2022-03-31 19:24:45 Found enabled service at boot: dbus-org
2022-03-31 19:24:45 Found enabled service at boot: dbus-org
2022-03-31 19:24:45 Found enabled service at boot: dbus-org
2022-03-31 19:24:45 Found enabled service at boot: dbus-org
2022-03-31 19:24:45 Found enabled service at boot: dmesg
2022-03-31 19:24:45 Found enabled service at boot: e2scrub_reap
2022-03-31 19:24:45 Found enabled service at boot: getty@
2022-03-31 19:24:45 Found enabled service at boot: gpu-manager
2022-03-31 19:24:45 Found enabled service at boot: grub-common
2022-03-31 19:24:45 Found enabled service at boot: grub-initrd-fallback
2022-03-31 19:24:45 Found enabled service at boot: irqbalance
2022-03-31 19:24:45 Found enabled service at boot: kerneloops
2022-03-31 19:24:45 Found enabled service at boot: keyboard-setup
2022-03-31 19:24:45 Found enabled service at boot: network-manager
2022-03-31 19:24:45 Found enabled service at boot: networkd-dispatcher
2022-03-31 19:24:45 Found enabled service at boot: ondemand
2022-03-31 19:24:45 Found enabled service at boot: openvpn
2022-03-31 19:24:45 Found enabled service at boot: pppd-dns
2022-03-31 19:24:45 Found enabled service at boot: rsync
2022-03-31 19:24:45 Found enabled service at boot: rsyslog
2022-03-31 19:24:45 Found enabled service at boot: secureboot-db
```

```
2022-03-31 19:24:45 Found enabled service at boot: setvtrgb
2022-03-31 19:24:45 Found enabled service at boot: snapd
2022-03-31 19:24:45 Found enabled service at boot: snapd
2022-03-31 19:24:45 Found enabled service at boot: snapd
2022-03-31 19:24:45 Found enabled service at boot: snapd
2022-03-31 19:24:45 Found enabled service at boot: snapd
2022-03-31 19:24:45 Found enabled service at boot: snapd
2022-03-31 19:24:45 Found enabled service at boot: snapd
2022-03-31 19:24:45 Found enabled service at boot: ssh
2022-03-31 19:24:45 Found enabled service at boot: sshd
2022-03-31 19:24:45 Found enabled service at boot: switcheroo-control
2022-03-31 19:24:45 Found enabled service at boot: syslog
2022-03-31 19:24:45 Found enabled service at boot: systemd-pstore
2022-03-31 19:24:45 Found enabled service at boot: systemd-resolved
2022-03-31 19:24:45 Found enabled service at boot: systemd-timesyncd
2022-03-31 19:24:45 Found enabled service at boot: thermald
2022-03-31 19:24:45 Found enabled service at boot: ua-reboot-cmds
2022-03-31 19:24:45 Found enabled service at boot: udisks2
2022-03-31 19:24:45 Found enabled service at boot: ufw
2022-03-31 19:24:45 Found enabled service at boot: unattended-upgrades
2022-03-31 19:24:45 Found enabled service at boot: whoopsie
2022-03-31 19:24:45 Found enabled service at boot: wpa_supplicant
2022-03-31 19:24:45 Found enabled service at boot: x11vnc
2022-03-31 19:24:45 Note: Run systemctl list-unit-files --type=service to see all services
2022-03-31 19:24:45 Result: Found 62 running services
2022-03-31 19:24:45 ===------------------------------------------------------------===
2022-03-31 19:24:45 Performing test ID BOOT-5180 (Check for Linux boot services (Debian style))
2022-03-31 19:24:45 Result: found runlevel 5
2022-03-31 19:24:45 Result: skipping further actions
2022-03-31 19:24:45 ===------------------------------------------------------------===
2022-03-31 19:24:45 Performing test ID BOOT-5184 (Check permissions for boot files/scripts)
2022-03-31 19:24:45 Result: checking /etc/init.d scripts for writable bit
2022-03-31 19:24:45 Test: checking if directory /etc/init.d exists
2022-03-31 19:24:45 Result: directory /etc/init.d found
2022-03-31 19:24:45 Test: checking for available files in directory
2022-03-31 19:24:45 Result: found files in directory, checking permissions now
2022-03-31 19:24:45 Test: checking permissions of file /etc/init.d/acpid
2022-03-31 19:24:45 Result: good, file /etc/init.d/acpid not world writable
2022-03-31 19:24:45 Test: checking permissions of file /etc/init.d/alsa-utils
```

```
2022-03-31 19:24:45 Result: good, file /etc/init.d/alsa-utils not world writable
2022-03-31 19:24:45 Test: checking permissions of file /etc/init.d/anacron
2022-03-31 19:24:45 Result: good, file /etc/init.d/anacron not world writable
2022-03-31 19:24:45 Test: checking permissions of file /etc/init.d/apparmor
2022-03-31 19:24:45 Result: good, file /etc/init.d/apparmor not world writable
2022-03-31 19:24:45 Test: checking permissions of file /etc/init.d/apport
2022-03-31 19:24:45 Result: good, file /etc/init.d/apport not world writable
2022-03-31 19:24:45 Test: checking permissions of file /etc/init.d/avahi-daemon
2022-03-31 19:24:45 Result: good, file /etc/init.d/avahi-daemon not world writable
2022-03-31 19:24:45 Test: checking permissions of file /etc/init.d/bluetooth
2022-03-31 19:24:45 Result: good, file /etc/init.d/bluetooth not world writable
2022-03-31 19:24:45 Test: checking permissions of file /etc/init.d/console-setup.sh
2022-03-31 19:24:45 Result: good, file /etc/init.d/console-setup.sh not world writable
2022-03-31 19:24:45 Test: checking permissions of file /etc/init.d/cron
2022-03-31 19:24:45 Result: good, file /etc/init.d/cron not world writable
2022-03-31 19:24:45 Test: checking permissions of file /etc/init.d/cups
2022-03-31 19:24:45 Result: good, file /etc/init.d/cups not world writable
2022-03-31 19:24:45 Test: checking permissions of file /etc/init.d/cups-browsed
2022-03-31 19:24:45 Result: good, file /etc/init.d/cups-browsed not world writable
2022-03-31 19:24:45 Test: checking permissions of file /etc/init.d/dbus
2022-03-31 19:24:45 Result: good, file /etc/init.d/dbus not world writable
2022-03-31 19:24:45 Test: checking permissions of file /etc/init.d/gdm3
2022-03-31 19:24:45 Result: good, file /etc/init.d/gdm3 not world writable
2022-03-31 19:24:45 Test: checking permissions of file /etc/init.d/grub-common
2022-03-31 19:24:45 Result: good, file /etc/init.d/grub-common not world writable
2022-03-31 19:24:45 Test: checking permissions of file /etc/init.d/hwclock.sh
2022-03-31 19:24:45 Result: good, file /etc/init.d/hwclock.sh not world writable
2022-03-31 19:24:45 Test: checking permissions of file /etc/init.d/irqbalance
2022-03-31 19:24:45 Result: good, file /etc/init.d/irqbalance not world writable
```

```
2022-03-31 19:24:45 Test: checking permissions of file
/etc/init.d/kerneloops
2022-03-31 19:24:45 Result: good, file /etc/init.d/kerneloops not world
writable
2022-03-31 19:24:45 Test: checking permissions of file
/etc/init.d/keyboard-setup.sh
2022-03-31 19:24:45 Result: good, file /etc/init.d/keyboard-setup.sh not
world writable
2022-03-31 19:24:45 Test: checking permissions of file /etc/init.d/kmod
2022-03-31 19:24:45 Result: good, file /etc/init.d/kmod not world writable
2022-03-31 19:24:45 Test: checking permissions of file /etc/init.d/lightdm
2022-03-31 19:24:45 Result: good, file /etc/init.d/lightdm not world writable
2022-03-31 19:24:45 Test: checking permissions of file /etc/init.d/network-
manager
2022-03-31 19:24:45 Result: good, file /etc/init.d/network-manager not
world writable
2022-03-31 19:24:45 Test: checking permissions of file /etc/init.d/openvpn
2022-03-31 19:24:45 Result: good, file /etc/init.d/openvpn not world
writable
2022-03-31 19:24:45 Test: checking permissions of file /etc/init.d/plymouth
2022-03-31 19:24:45 Result: good, file /etc/init.d/plymouth not world
writable
2022-03-31 19:24:45 Test: checking permissions of file
/etc/init.d/plymouth-log
2022-03-31 19:24:45 Result: good, file /etc/init.d/plymouth-log not world
writable
2022-03-31 19:24:45 Test: checking permissions of file /etc/init.d/pppd-
dns
2022-03-31 19:24:45 Result: good, file /etc/init.d/pppd-dns not world
writable
2022-03-31 19:24:45 Test: checking permissions of file /etc/init.d/procps
2022-03-31 19:24:45 Result: good, file /etc/init.d/procps not world writable
2022-03-31 19:24:45 Test: checking permissions of file
/etc/init.d/pulseaudio-enable-autospawn
2022-03-31 19:24:45 Result: good, file /etc/init.d/pulseaudio-enable-
autospawn not world writable
2022-03-31 19:24:45 Test: checking permissions of file /etc/init.d/rsync
2022-03-31 19:24:45 Result: good, file /etc/init.d/rsync not world writable
2022-03-31 19:24:45 Test: checking permissions of file /etc/init.d/rsyslog
2022-03-31 19:24:45 Result: good, file /etc/init.d/rsyslog not world writable
2022-03-31 19:24:45 Test: checking permissions of file /etc/init.d/saned
2022-03-31 19:24:45 Result: good, file /etc/init.d/saned not world writable
2022-03-31 19:24:45 Test: checking permissions of file /etc/init.d/speech-
dispatcher
2022-03-31 19:24:45 Result: good, file /etc/init.d/speech-dispatcher not
world writable
```

```
2022-03-31 19:24:45 Test: checking permissions of file /etc/init.d/spice-vdagent
2022-03-31 19:24:45 Result: good, file /etc/init.d/spice-vdagent not world writable
2022-03-31 19:24:45 Test: checking permissions of file /etc/init.d/ssh
2022-03-31 19:24:45 Result: good, file /etc/init.d/ssh not world writable
2022-03-31 19:24:45 Test: checking permissions of file /etc/init.d/udev
2022-03-31 19:24:45 Result: good, file /etc/init.d/udev not world writable
2022-03-31 19:24:45 Test: checking permissions of file /etc/init.d/ufw
2022-03-31 19:24:45 Result: good, file /etc/init.d/ufw not world writable
2022-03-31 19:24:45 Test: checking permissions of file /etc/init.d/unattended-upgrades
2022-03-31 19:24:45 Result: good, file /etc/init.d/unattended-upgrades not world writable
2022-03-31 19:24:45 Test: checking permissions of file /etc/init.d/uuidd
2022-03-31 19:24:45 Result: good, file /etc/init.d/uuidd not world writable
2022-03-31 19:24:45 Test: checking permissions of file /etc/init.d/whoopsie
2022-03-31 19:24:45 Result: good, file /etc/init.d/whoopsie not world writable
2022-03-31 19:24:45 Test: checking permissions of file /etc/init.d/x11-common
2022-03-31 19:24:45 Result: good, file /etc/init.d/x11-common not world writable
2022-03-31 19:24:45 Test: checking permissions of file /etc/init.d/xe-linux-distribution
2022-03-31 19:24:45 Result: good, file /etc/init.d/xe-linux-distribution not world writable
2022-03-31 19:24:45 Test: checking if directory /etc/rc.d exists
2022-03-31 19:24:45 Result: directory /etc/rc.d not found. Skipping..
2022-03-31 19:24:45 Test: checking if directory /etc/rcS.d exists
2022-03-31 19:24:45 Result: directory /etc/rcS.d found
2022-03-31 19:24:45 Test: checking for available files in directory
2022-03-31 19:24:45 Result: found no files in directory.
2022-03-31 19:24:45 Test: Checking /etc/rc0.d scripts for writable bit
2022-03-31 19:24:45 Test: Checking /etc/rc1.d scripts for writable bit
2022-03-31 19:24:45 Test: Checking /etc/rc2.d scripts for writable bit
2022-03-31 19:24:45 Test: Checking /etc/rc3.d scripts for writable bit
2022-03-31 19:24:45 Test: Checking /etc/rc4.d scripts for writable bit
2022-03-31 19:24:45 Test: Checking /etc/rc5.d scripts for writable bit
2022-03-31 19:24:45 Test: Checking /etc/rc6.d scripts for writable bit
2022-03-31 19:24:45 Hardening: assigned maximum number of hardening points for this item (3). Currently having 3 points (out of 29)
2022-03-31 19:24:45 ===---------------------------------------------------------------===
2022-03-31 19:24:45 Performing test ID BOOT-5202 (Check uptime of
system)
2022-03-31 19:24:45 Uptime (in seconds): 4595
2022-03-31 19:24:45 Uptime (in days): 0
2022-03-31 19:24:45 ===---------------------------------------------------------------
===
2022-03-31 19:24:45 Performing test ID BOOT-5260 (Check single user
mode for systemd)
2022-03-31 19:24:45 Test: Searching
/usr/lib/systemd/system/rescue.service
2022-03-31 19:24:45 Result: file /usr/lib/systemd/system/rescue.service
2022-03-31 19:24:45 Test: checking presence sulogin for single user
mode
2022-03-31 19:24:45 Result: did not find sulogin in rescue.service
2022-03-31 19:24:45 Hardening: assigned partial number of hardening
points (1 of 3). Currently having 4 points (out of 32)
2022-03-31 19:24:45 Suggestion: Protect rescue.service by using sulogin
[test:BOOT-5260] [details:-] [solution:-]
2022-03-31 19:24:45 Checking permissions of
/usr/share/lynis/include/tests_kernel
2022-03-31 19:24:45 File permissions are OK
2022-03-31 19:24:45 ===---------------------------------------------------------------
===
```

b. Logging files:

```
2022-03-31 19:25:13 Action: Performing tests from category: Logging and
files
2022-03-31 19:25:13 ===---------------------------------------------------------------
===
2022-03-31 19:25:13 Performing test ID LOGG-2130 (Check for running
syslog daemon)
2022-03-31 19:25:13 Test: Searching for a logging daemon
2022-03-31 19:25:13 Result: Found a logging daemon
2022-03-31 19:25:13 Hardening: assigned maximum number of hardening
points for this item (3). Currently having 137 points (out of 260)
2022-03-31 19:25:13 ===---------------------------------------------------------------
===
2022-03-31 19:25:13 Performing test ID LOGG-2132 (Check for running
syslog-ng daemon)
2022-03-31 19:25:13 Test: Searching for syslog-ng daemon in process list
2022-03-31 19:25:13 IsRunning: process 'syslog-ng' not found
2022-03-31 19:25:13 Result: Syslog-ng NOT found in process list
2022-03-31 19:25:13 ===---------------------------------------------------------------
===
2022-03-31 19:25:13 Skipped test LOGG-2134 (Checking Syslog-NG
configuration file consistency)
```

```
2022-03-31 19:25:13 Reason to skip: Prerequisities not met (ie missing
tool, other type of Linux distribution)
2022-03-31 19:25:13 ===--------------------------------------------------------------
===
2022-03-31 19:25:13 Performing test ID LOGG-2136 (Check for running
systemd journal daemon)
2022-03-31 19:25:13 Test: Searching for systemd journal daemon in
process list
2022-03-31 19:25:13 IsRunning: process 'systemd-journal' found (236 )
2022-03-31 19:25:13 ===--------------------------------------------------------------
===
2022-03-31 19:25:13 Performing test ID LOGG-2210 (Check for running
metalog daemon)
2022-03-31 19:25:13 Test: Searching for metalog daemon in process list
2022-03-31 19:25:13 IsRunning: process 'metalog' not found
2022-03-31 19:25:13 Result: metalog NOT found in process list
2022-03-31 19:25:13 ===--------------------------------------------------------------
===
2022-03-31 19:25:13 Performing test ID LOGG-2230 (Check for running
RSyslog daemon)
2022-03-31 19:25:13 Test: Searching for RSyslog daemon in process list
2022-03-31 19:25:13 IsRunning: process 'rsyslogd' found (541 )
2022-03-31 19:25:13 Result: Found rsyslogd in process list
2022-03-31 19:25:13 ===--------------------------------------------------------------
===
2022-03-31 19:25:13 Performing test ID LOGG-2240 (Check for running
RFC 3195 compliant daemon)
2022-03-31 19:25:13 Test: Searching for RFC 3195 daemon (alias syslog
reliable) in process list
2022-03-31 19:25:13 IsRunning: process 'rfc3195d' not found
2022-03-31 19:25:13 Result: rfc3195d NOT found in process list
2022-03-31 19:25:13 ===--------------------------------------------------------------
===
2022-03-31 19:25:13 Performing test ID LOGG-2138 (Checking kernel
logger daemon on Linux)
2022-03-31 19:25:13 Test: Searching kernel logger daemon (klogd)
2022-03-31 19:25:13 Result: test skipped, because other facility is being
used to log kernel messages
2022-03-31 19:25:13 ===--------------------------------------------------------------
===
2022-03-31 19:25:13 Performing test ID LOGG-2142 (Checking minilog
daemon)
2022-03-31 19:25:13 Result: Checking for unkilled minilogd instances
2022-03-31 19:25:13 IsRunning: process 'minilogd' not found
2022-03-31 19:25:13 Result: No minilogd is running
```

```
2022-03-31 19:25:13 ===---------------------------------------------------------------===
2022-03-31 19:25:13 Performing test ID LOGG-2146 (Checking logrotate.conf and logrotate.d)
2022-03-31 19:25:13 Test: Checking for /etc/logrotate.conf
2022-03-31 19:25:13 Result: /etc/logrotate.conf found (file)
2022-03-31 19:25:13 Test: Checking for /etc/logrotate.d (directory)
2022-03-31 19:25:13 Result: /etc/logrotate.d found
2022-03-31 19:25:13 Result: logrotate configuration found
2022-03-31 19:25:13 ===---------------------------------------------------------------===
2022-03-31 19:25:13 Performing test ID LOGG-2148 (Checking logrotated files)
2022-03-31 19:25:13 Test: Checking which files are rotated with logrotate and if they exist
2022-03-31 19:25:13 Result: found one or more files which are rotated via logrotate
2022-03-31 19:25:13 Output: File:/var/log/cron.log:does_not_exist
2022-03-31 19:25:13 Output: File:/var/log/daemon.log:does_not_exist
2022-03-31 19:25:13 Output: File:/var/log/debug:does_not_exist
2022-03-31 19:25:13 Output: File:/var/log/lpr.log:does_not_exist
2022-03-31 19:25:13 Output: File:/var/log/mail.err:does_not_exist
2022-03-31 19:25:13 Output: File:/var/log/mail.info:does_not_exist
2022-03-31 19:25:13 Output: File:/var/log/mail.log:does_not_exist
2022-03-31 19:25:13 Output: File:/var/log/mail.warn:does_not_exist
2022-03-31 19:25:13 Output: File:/var/log/messages:does_not_exist
2022-03-31 19:25:13 Output: File:/var/log/ppp-connect-errors:does_not_exist
2022-03-31 19:25:13 Output: File:/var/log/speech-dispatcher/debug-epos-generic:does_not_exist
2022-03-31 19:25:13 Output: File:/var/log/speech-dispatcher/debug-festival:does_not_exist
2022-03-31 19:25:13 Output: File:/var/log/speech-dispatcher/debug-flite:does_not_exist
2022-03-31 19:25:13 Output: File:/var/log/speech-dispatcher/speech-dispatcher-protocol.log:does_not_exist
2022-03-31 19:25:13 Output: File:/var/log/speech-dispatcher/speech-dispatcher.log:does_not_exist
2022-03-31 19:25:13 Output: File:/var/log/ufw.log:does_not_exist
2022-03-31 19:25:13 Output: File:/var/log/user.log:does_not_exist
2022-03-31 19:25:13 Output: File:/var/log/alternatives.log:exists
2022-03-31 19:25:13 Output: File:/var/log/apport.log:exists
2022-03-31 19:25:13 Output: File:/var/log/apt/history.log:exists
2022-03-31 19:25:13 Output: File:/var/log/apt/term.log:exists
2022-03-31 19:25:13 Output: File:/var/log/auth.log:exists
2022-03-31 19:25:13 Output: File:/var/log/boot.log:exists
```

```
2022-03-31 19:25:13 Output: File:/var/log/btmp:exists
2022-03-31 19:25:13 Output: File:/var/log/cron.log:exists
2022-03-31 19:25:13 Output: File:/var/log/cups/access_log:exists
2022-03-31 19:25:13 Output: File:/var/log/cups/error_log:exists
2022-03-31 19:25:13 Output: File:/var/log/daemon.log:exists
2022-03-31 19:25:13 Output: File:/var/log/debug:exists
2022-03-31 19:25:13 Output: File:/var/log/dpkg.log:exists
2022-03-31 19:25:13 Output: File:/var/log/kern.log:exists
2022-03-31 19:25:13 Output: File:/var/log/lightdm/lightdm.log:exists
2022-03-31 19:25:13 Output: File:/var/log/lightdm/seat0-greeter.log:exists
2022-03-31 19:25:13 Output: File:/var/log/lightdm/x-0.log:exists
2022-03-31 19:25:13 Output: File:/var/log/lpr.log:exists
2022-03-31 19:25:13 Output: File:/var/log/mail.err:exists
2022-03-31 19:25:13 Output: File:/var/log/mail.info:exists
2022-03-31 19:25:13 Output: File:/var/log/mail.log:exists
2022-03-31 19:25:13 Output: File:/var/log/mail.warn:exists
2022-03-31 19:25:13 Output: File:/var/log/messages:exists
2022-03-31 19:25:13 Output: File:/var/log/ppp-connect-errors:exists
2022-03-31 19:25:13 Output: File:/var/log/speech-dispatcher/debug-epos-
generic:exists
2022-03-31 19:25:13 Output: File:/var/log/speech-dispatcher/debug-
festival:exists
2022-03-31 19:25:13 Output: File:/var/log/speech-dispatcher/debug-
flite:exists
2022-03-31 19:25:13 Output: File:/var/log/speech-dispatcher/speech-
dispatcher-protocol.log:exists
2022-03-31 19:25:13 Output: File:/var/log/speech-dispatcher/speech-
dispatcher.log:exists
2022-03-31 19:25:13 Output: File:/var/log/syslog:exists
2022-03-31 19:25:13 Output: File:/var/log/ubuntu-advantage-
timer.log:exists
2022-03-31 19:25:13 Output: File:/var/log/ubuntu-advantage.log:exists
2022-03-31 19:25:13 Output: File:/var/log/ufw.log:exists
2022-03-31 19:25:13 Output: File:/var/log/unattended-
upgrades/unattended-upgrades-dpkg.log:exists
2022-03-31 19:25:13 Output: File:/var/log/unattended-
upgrades/unattended-upgrades-shutdown.log:exists
2022-03-31 19:25:13 Output: File:/var/log/unattended-
upgrades/unattended-upgrades.log:exists
2022-03-31 19:25:13 Output: File:/var/log/user.log:exists
2022-03-31 19:25:13 Output: File:/var/log/wtmp:exists
2022-03-31 19:25:13 ===---------------------------------------------------------------
===
2022-03-31 19:25:13 Performing test ID LOGG-2150 (Checking
directories in logrotate configuration)
```

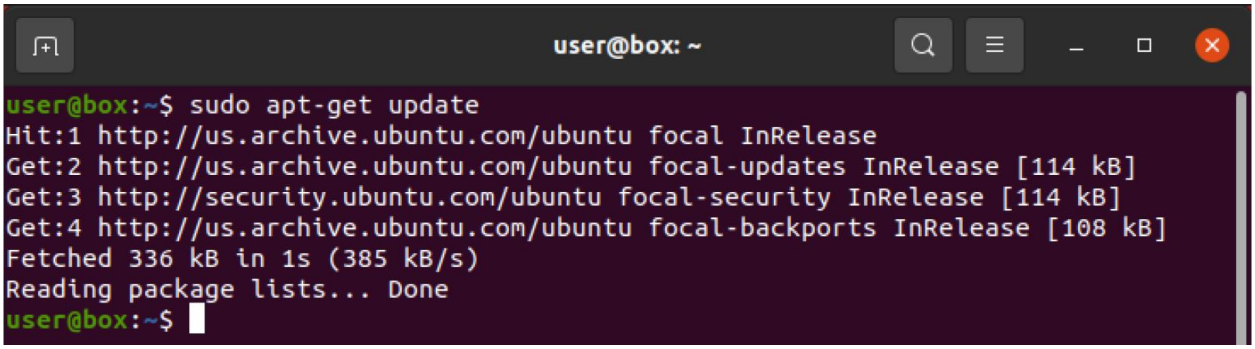
```
2022-03-31 19:25:13 Test: Checking which directories can be found in
logrotate configuration
2022-03-31 19:25:13 Result: found one or more directories (via logrotate
configuration)
2022-03-31 19:25:13 Directory found: /var/log
2022-03-31 19:25:13 Directory found: /var/log/apt
2022-03-31 19:25:13 Directory found: /var/log/cups
2022-03-31 19:25:13 Directory found: /var/log/lightdm
2022-03-31 19:25:13 Directory found: /var/log/speech-dispatcher
2022-03-31 19:25:13 Directory found: /var/log/unattended-upgrades
2022-03-31 19:25:13 ===---------------------------------------------------------------
===
2022-03-31 19:25:13 Skipped test LOGG-2152 (Checking loghost)
2022-03-31 19:25:13 Reason to skip: Incorrect guest OS (Solaris only)
2022-03-31 19:25:13 ===---------------------------------------------------------------
===
2022-03-31 19:25:13 Performing test ID LOGG-2154 (Checking syslog
configuration file)
2022-03-31 19:25:13 Result: test skipped, file /etc/syslog.conf not found
2022-03-31 19:25:13 ===---------------------------------------------------------------
===
2022-03-31 19:25:13 Skipped test LOGG-2160 (Checking
/etc/newsyslog.conf)
2022-03-31 19:25:13 Reason to skip: Prerequisities not met (ie missing
tool, other type of Linux distribution)
2022-03-31 19:25:13 ===---------------------------------------------------------------
===
2022-03-31 19:25:13 Skipped test LOGG-2162 (Checking directories in
/etc/newsyslog.conf)
2022-03-31 19:25:13 Reason to skip: Prerequisities not met (ie missing
tool, other type of Linux distribution)
2022-03-31 19:25:13 ===---------------------------------------------------------------
===
2022-03-31 19:25:13 Skipped test LOGG-2164 (Checking files specified
/etc/newsyslog.conf)
2022-03-31 19:25:13 Reason to skip: Prerequisities not met (ie missing
tool, other type of Linux distribution)
2022-03-31 19:25:13 ===---------------------------------------------------------------
===
2022-03-31 19:25:13 Performing test ID LOGG-2170 (Checking log paths)
2022-03-31 19:25:13 Test: Searching log paths
2022-03-31 19:25:13 Result: directory /var/log exists
2022-03-31 19:25:13 Result: directory /var/adm can't be found
2022-03-31 19:25:13 ===---------------------------------------------------------------
===
2022-03-31 19:25:13 Performing test ID LOGG-2180 (Checking open log
files)
2022-03-31 19:25:13 Test: checking open log files with lsof
2022-03-31 19:25:14 Found logfile: /home/user/.local/share/gvfs-
metadata/home-73bc3d3d.log
2022-03-31 19:25:14 Found logfile: /home/user/.local/share/gvfs-
metadata/root-6013a2fc.log
2022-03-31 19:25:14 Found logfile: /home/user/.local/share/gvfs-
metadata/trash:-c3b13edc.log
2022-03-31 19:25:14 Found logfile: /var/log/Xorg.0.log
2022-03-31 19:25:14 Found logfile: /var/log/auth.log
2022-03-31 19:25:14 Found logfile: /var/log/cups/access_log
2022-03-31 19:25:14 Found logfile: /var/log/kern.log
2022-03-31 19:25:14 Found logfile: /var/log/lightdm/lightdm.log
2022-03-31 19:25:14 Found logfile: /var/log/lightdm/x-0.log
2022-03-31 19:25:14 Found logfile: /var/log/syslog
2022-03-31 19:25:14 Found logfile: /var/log/unattended-
upgrades/unattended-upgrades-shutdown.log
2022-03-31 19:25:14 ===---------------------------------------------------------------
===
2022-03-31 19:25:14 Performing test ID LOGG-2190 (Checking for
deleted files in use)
2022-03-31 19:25:14 Test: checking deleted files that are still in use
2022-03-31 19:25:14 Result: found one or more files which are deleted,
but still in use
2022-03-31 19:25:14 Found deleted file: /home/user/.local/share/gvfs-
metadata/root(gnome-she)
2022-03-31 19:25:14 Found deleted file: /home/user/.local/share/gvfs-
metadata/root-669e3f1c.log(gnome-she)
2022-03-31 19:25:14 Found deleted file: /home/user/snap/snap-
store/common/.cache/gnome-
software/fwupd/remotes.d/lvfs/metadata.xml.gz(snap-stor)
2022-03-31 19:25:14 Found deleted file: /memfd:pulseaudio(pulseaudi)
2022-03-31 19:25:14 Suggestion: Check what deleted files are still in use
and why. [test:LOGG-2190] [details:-] [solution:-]
2022-03-31 19:25:14 ===---------------------------------------------------------------
===
2022-03-31 19:25:14 Performing test ID LOGG-2192 (Checking for open
log files that are empty)
2022-03-31 19:25:14 Result: all opened log files are bigger than zero
bytes in size
2022-03-31 19:25:14 Checking permissions of
/usr/share/lynis/include/tests_insecure_services
2022-03-31 19:25:14 File permissions are OK
2022-03-31 19:25:14 ===---------------------------------------------------------------
===
```

PE 4. Performing back-ups and restoring the system from a backup.

1. **Download and install DejaDup (free version) onto your virtual machine**
2. **List the back-up options provided by DejaDup on your VM.**
   a. Folders to save (in backup), folders to ignore (in backup), storage location (for backup), and backup scheduling. You can also start a backup immediately even if it isn't time for a new backup yet.
3. **Write an appropriate backup policy for student VMs used in semester classes.**
   a. A backup should always be run before disconnecting/turning off a VM
   b. Auto-backups should be enabled (to run every week).
   c. Students should enable the backups to be stored in their Google Drive for ease of access in case of need.

PE 5. Install patches and updates.

1. **List all available patches for your system currently and submit list with this homework.**

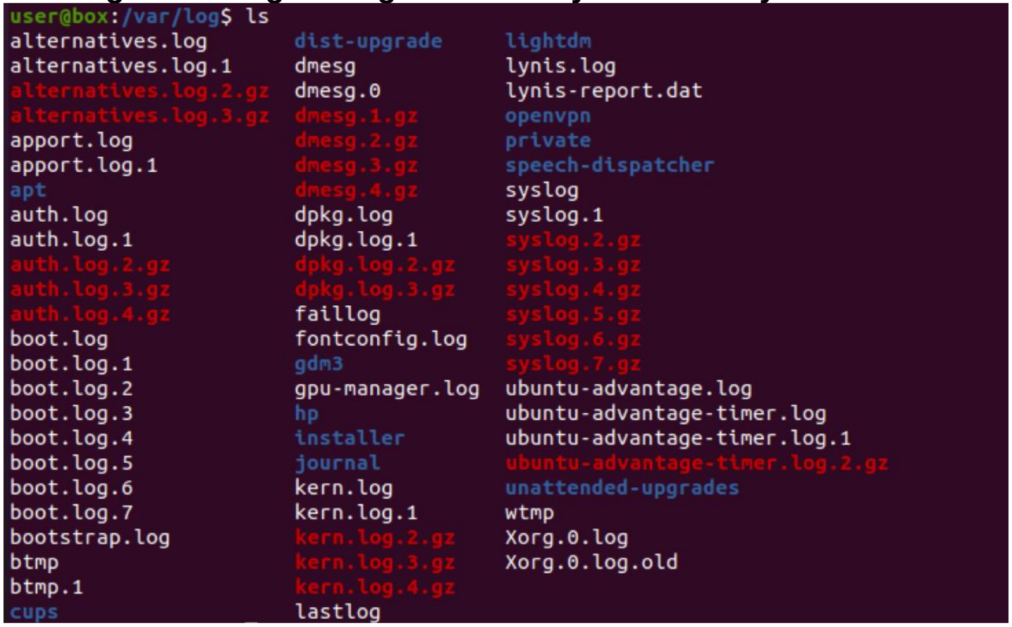


```
user@box:~$ sudo apt-get update
Hit:1 http://us.archive.ubuntu.com/ubuntu focal InRelease
Get:2 http://us.archive.ubuntu.com/ubuntu focal-updates InRelease [114 kB]
Get:3 http://security.ubuntu.com/ubuntu focal-security InRelease [114 kB]
Get:4 http://us.archive.ubuntu.com/ubuntu focal-backports InRelease [108 kB]
Fetched 336 kB in 1s (385 kB/s)
Reading package lists... Done
user@box:~$
```

2. **Install all available patches.**

PE 6. Review security logs.

1. **Investigate the logs being recorded by default on your VM under /var/log.**



```
user@box:/var/log$ ls
alternatives.log       dist-upgrade     lightdm
alternatives.log.1     dmesg            lynis.log
alternatives.log.2.gz  dmesg.0          lynis-report.dat
alternatives.log.3.gz  dmesg.1.gz       openvpn
apport.log             dmesg.2.gz       private
apport.log.1           dmesg.3.gz       speech-dispatcher
apt                    dmesg.4.gz       syslog
auth.log               dpkg.log         syslog.1
auth.log.1             dpkg.log.1       syslog.2.gz
auth.log.2.gz          dpkg.log.2.gz    syslog.3.gz
auth.log.3.gz          dpkg.log.3.gz    syslog.4.gz
auth.log.4.gz          faillog          syslog.5.gz
boot.log               fontconfig.log   syslog.6.gz
boot.log.1             gdm3             syslog.7.gz
boot.log.2             gpu-manager.log  ubuntu-advantage.log
boot.log.3             hp               ubuntu-advantage-timer.log
boot.log.4             installer        ubuntu-advantage-timer.log.1
boot.log.5             journal          ubuntu-advantage-timer.log.2.gz
boot.log.6             kern.log         unattended-upgrades
boot.log.7             kern.log.1       wtmp
bootstrap.log          kern.log.2.gz    Xorg.0.log
btmp                   kern.log.3.gz    Xorg.0.log.old
btmp.1                 kern.log.4.gz
cups                   lastlog
```

2. **List the logs that contain security relevant information and describe what activities are being logged in each log you have identified as a security log.**
    a. auth.log: contains information about authentication related events
    b. syslog: contains information about generic system activity
    c. faillog: contains information about failed login attempts

Resource: https://www.eurovps.com/blog/important-linux-log-files-you-must-be-monitoring/

3. **Explain your rationale for determining which logs captured security relevant information.**
    a. I investigated the log file contents and decided whether the information contained within them could be used to investigate any type of attack on the system. For the auth.log and faillog files, it is obvious that the information can be useful for determining potential brute force attacks (by observing failed login attempts). I also think that taking a close look at the syslog may help in determining if there has been an attack directed to any other part of the system (not login related), and then further information can be extracted by reading the appropriate log the part of the system that has been found to have been attacked by reading the syslog.