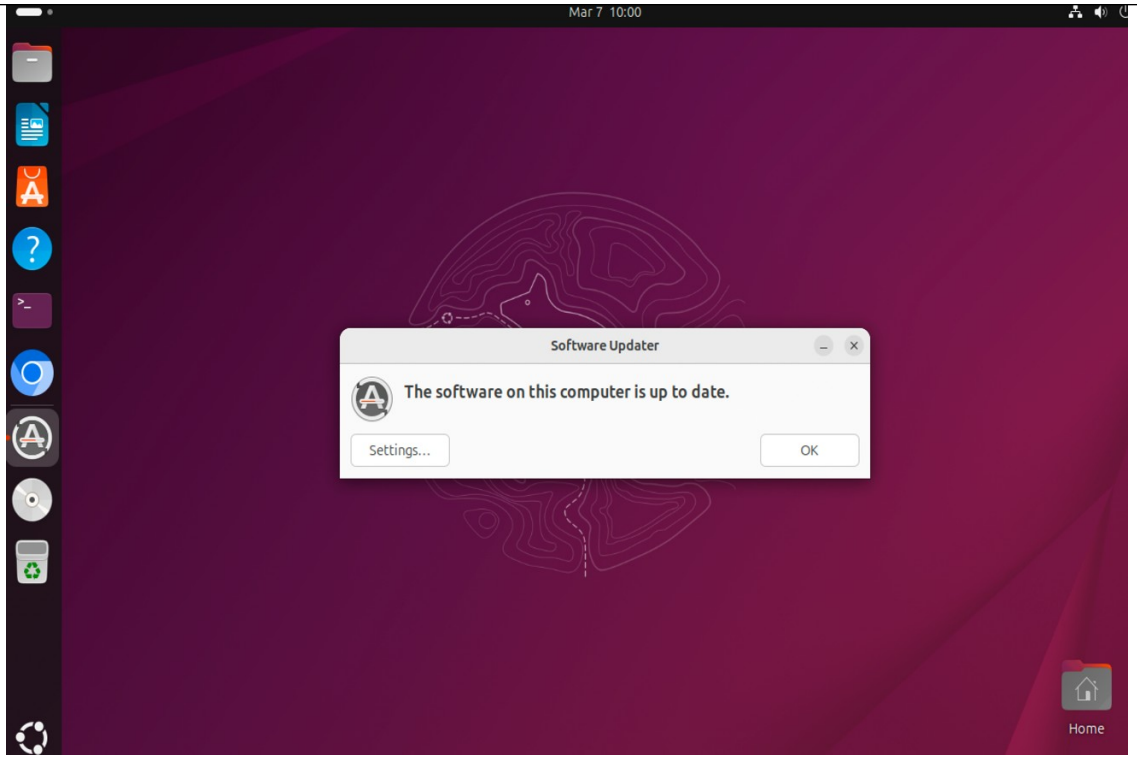
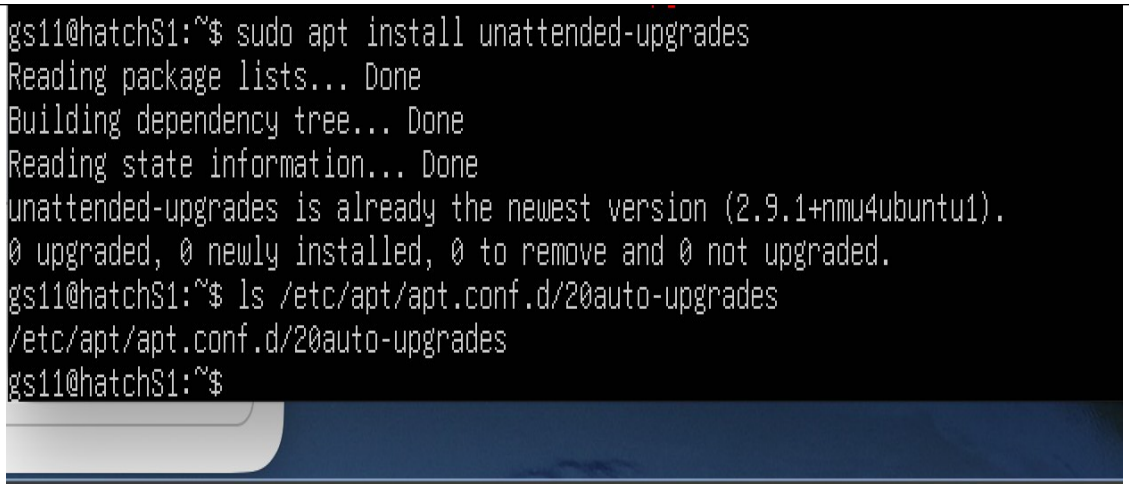
- Software updates are easily installed in the Ubuntu desktop by opening the “Software Updater” application.
- The system will automatically scan for available updates, and provide a button to install if updates are available
- This screenshot shows that the update process has been completed on my Ubuntu Desktop.



- In the Ubuntu server VM, updates can be installed by running the command “Sudo apt update” to install the most recent packages.
- Pair this command with “sudo apt upgrade” to ensure your server is fully up to date.

```
gs11@hatchS1:~$ sudo apt update
[sudo] password for gs11:
Hit:1 http://ports.ubuntu.com/ubuntu-ports noble InRelease
Get:2 http://ports.ubuntu.com/ubuntu-ports noble-updates InRelease [126 kB]
Get:3 http://ports.ubuntu.com/ubuntu-ports noble-backports InRelease [126 kB]
Get:4 http://ports.ubuntu.com/ubuntu-ports noble-security InRelease [126 kB]
Get:5 http://ports.ubuntu.com/ubuntu-ports noble-updates/main arm64 Packages [1,913 kB]
Get:6 http://ports.ubuntu.com/ubuntu-ports noble-updates/main arm64 Components [174 kB]
Get:7 http://ports.ubuntu.com/ubuntu-ports noble-updates/restricted arm64 Components [212 B]
Get:8 http://ports.ubuntu.com/ubuntu-ports noble-updates/universe arm64 Packages [1,527 kB]
Get:9 http://ports.ubuntu.com/ubuntu-ports noble-updates/universe arm64 Components [385 kB]
Get:10 http://ports.ubuntu.com/ubuntu-ports noble-updates/multiverse arm64 Components [212 B]
Get:11 http://ports.ubuntu.com/ubuntu-ports noble-backports/main arm64 Components [3,584 B]
Get:12 http://ports.ubuntu.com/ubuntu-ports noble-backports/restricted arm64 Components [216 B]
Get:13 http://ports.ubuntu.com/ubuntu-ports noble-backports/universe arm64 Components [10.5 kB]
Get:14 http://ports.ubuntu.com/ubuntu-ports noble-backports/multiverse arm64 Components [212 B]
Get:15 http://ports.ubuntu.com/ubuntu-ports noble-security/main arm64 Components [18.4 kB]
Get:16 http://ports.ubuntu.com/ubuntu-ports noble-security/restricted arm64 Components [212 B]
Get:17 http://ports.ubuntu.com/ubuntu-ports noble-security/universe arm64 Components [74.2 kB]
Get:18 http://ports.ubuntu.com/ubuntu-ports noble-security/multiverse arm64 Components [212 B]
Fetched 4,485 kB in 3s (1,584 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
All packages are up to date.
gs11@hatchS1:~$ sudo apt upgrade
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
gs11@hatchS1:~$
```

• The Linux server also provides the option to allow automatic upgrades of the server. • Configure this option with the command “sudo apt install unattended-upgrades”	

Assignment Questions

1) Why should a system administrator review the list of packages after apt update is run?

System administrators need to review the recently installed packages to gain a good understanding of the system’s stability and gauge the uptime for the system. Many updates require a full reboot of the system, which is nothing to worry about in a lab VM for class, but can have huge repercussions in a business setting. Major updates can also introduce new changes that may “break” the system, in the sense that new configuration must be set up to fix the system. Properly reviewing all packages before installation will help to identify the source of any conflict that may come after the system is rebooted.

2) As a Linux system administrator managing patching, what is a key risk to evaluate during implementation, and a single strategy to mitigate it?

The main risk associated with patch implementation is related to the importance of reviewing all packages that was touched on in the first question. This is because new patches can easily cause regression, which is where a security fix or software enhancement accidentally breaks the existing, working system. To mitigate this risk, system administrators should establish a staging or development environment where they can test the updates’ functionality before deploying them to the entire organization.

References

Moody, G. (2025, December 18). *Ubuntu Patch Management Best Practices Guide (2026)*. Action1 | Action1 Risk-Based Patch Management. https://www.action1.com/blog/best-practices-for-ubuntu-patch-management/

Team, T. (2025, January 2). *How AI Can Help Identify and Mitigate Patch Management Risks*. TuxCare. https://tuxcare.com/blog/patch-management-risks/