



AIR FORCE ASSOCIATION'S

CYBERPATRIOT

NATIONAL YOUTH CYBER EDUCATION PROGRAM

UNIT 10

Ubuntu Security





Learning Objectives

- Participants will understand how to configure major components of Linux/Ubuntu
 - Account management
 - Updates
 - Firewall
- Participants will understand how to implement user-level configurations within Ubuntu
 - Account settings
 - Group configuration
 - Authentication and the PAM file
- Participants will understand commands that will be useful for securing a Linux machine
- Participants will understand system and audit logging
 - Overview
 - Configuration





AIR FORCE ASSOCIATION'S

CYBERPATRIOT

NATIONAL YOUTH CYBER EDUCATION PROGRAM

SECTION 1

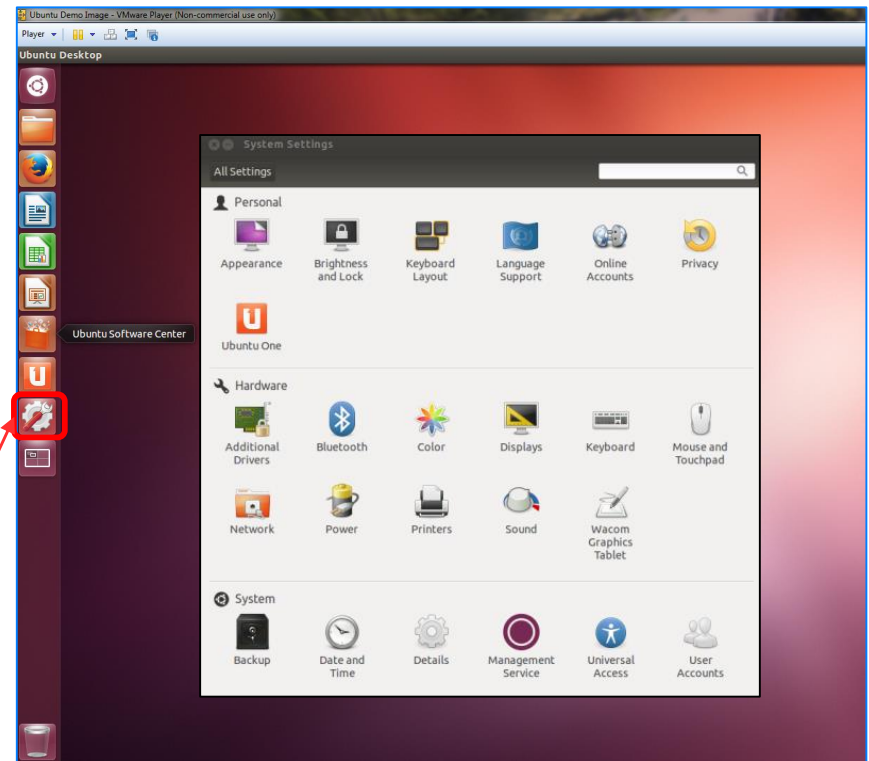
Basic GUI Security





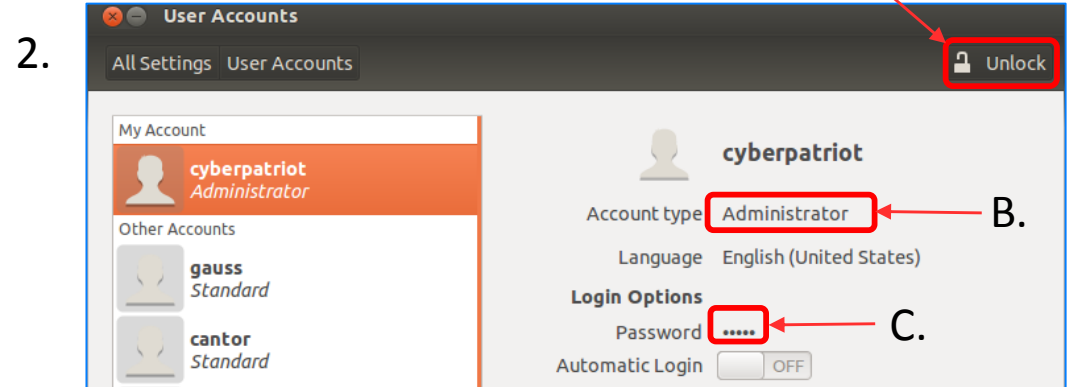
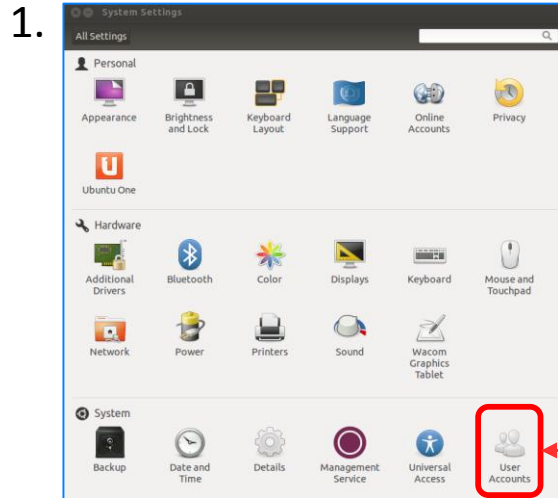
Basic Linux Security

- This unit will show you how to make many of the same security settings you made on Windows in Units 7 and 8
 - Linux has many of the same vulnerabilities, so the fixes are similar
- Linux does not have Settings or Control Panel like in Windows
- The System Settings menu offers limited security tools
- Click the System Settings button in the menu bar





User Accounts Overview



- Click User Accounts in the System Settings window
- As in Windows, it is important to restrict root (Admin) privileges and password protect all accounts
 - A. To make account management changes, you must enact root permissions by clicking Unlock and authenticate yourself by entering your password
 - B. Switch users from Administrator to Standard User by clicking next to Account Type
 - C. Change passwords by clicking the asterisks next to the Password option





User Accounts – Account Type

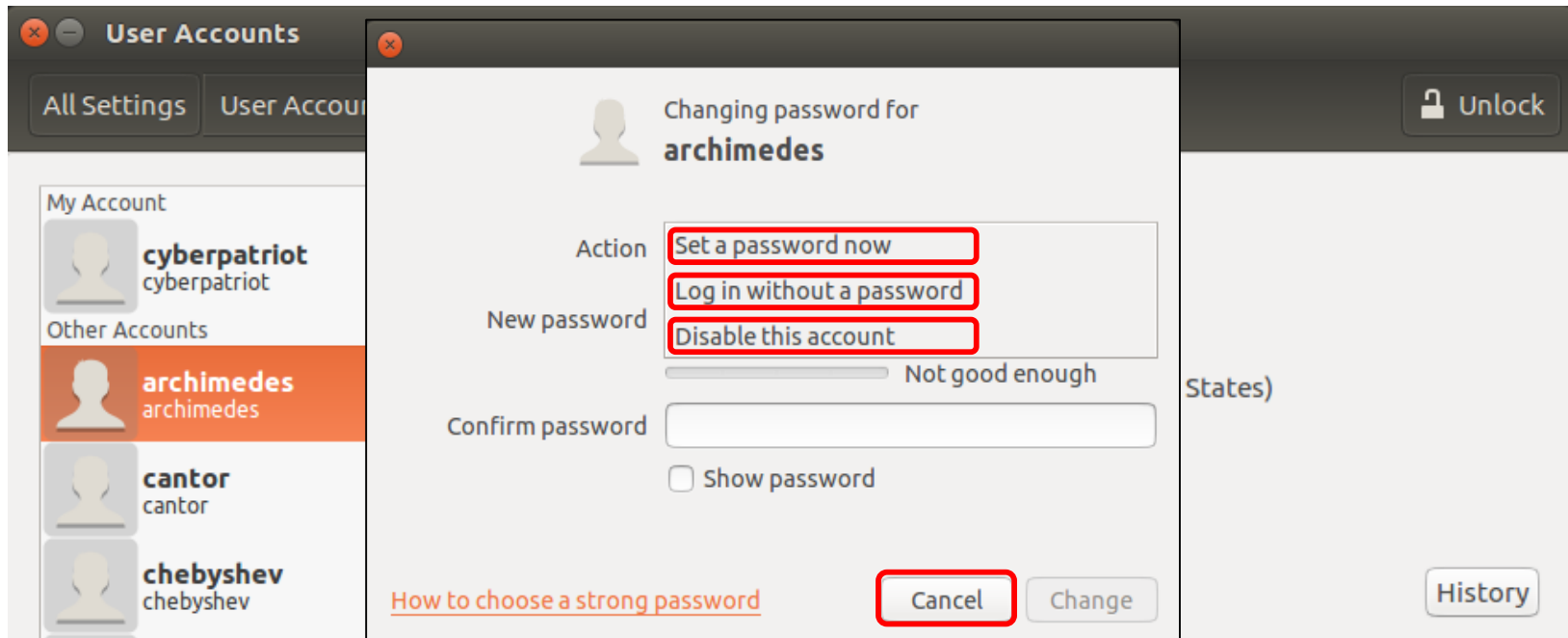
- Select the user **archimedes**
- To make changes, click **Unlock** and authenticate
- Keep **Automatic Login** set to off
- The user account type can be changed by clicking the field next to **Account Type**

The screenshot shows the 'User Accounts' settings interface. At the top, there are tabs for 'All Settings' and 'User Accounts', and an 'Unlock' button with a lock icon, which is highlighted with a red box. Below the tabs, there are two main sections: 'My Account' and 'Other Accounts'. In the 'Other Accounts' section, the user 'archimedes' is selected and highlighted with a red box. To the right, the settings for 'archimedes' are displayed. The 'Account Type' dropdown menu is highlighted with a red box and shows 'Standard' selected. Below it, the 'Language' is set to 'English (United States)'. Under the 'Login Options' section, the 'Automatic Login' toggle is set to 'OFF' and is highlighted with a red box. The 'Last Login' is shown as 'May 9, 20:52' and there is a 'History' button at the bottom right.



User Account -- Passwords

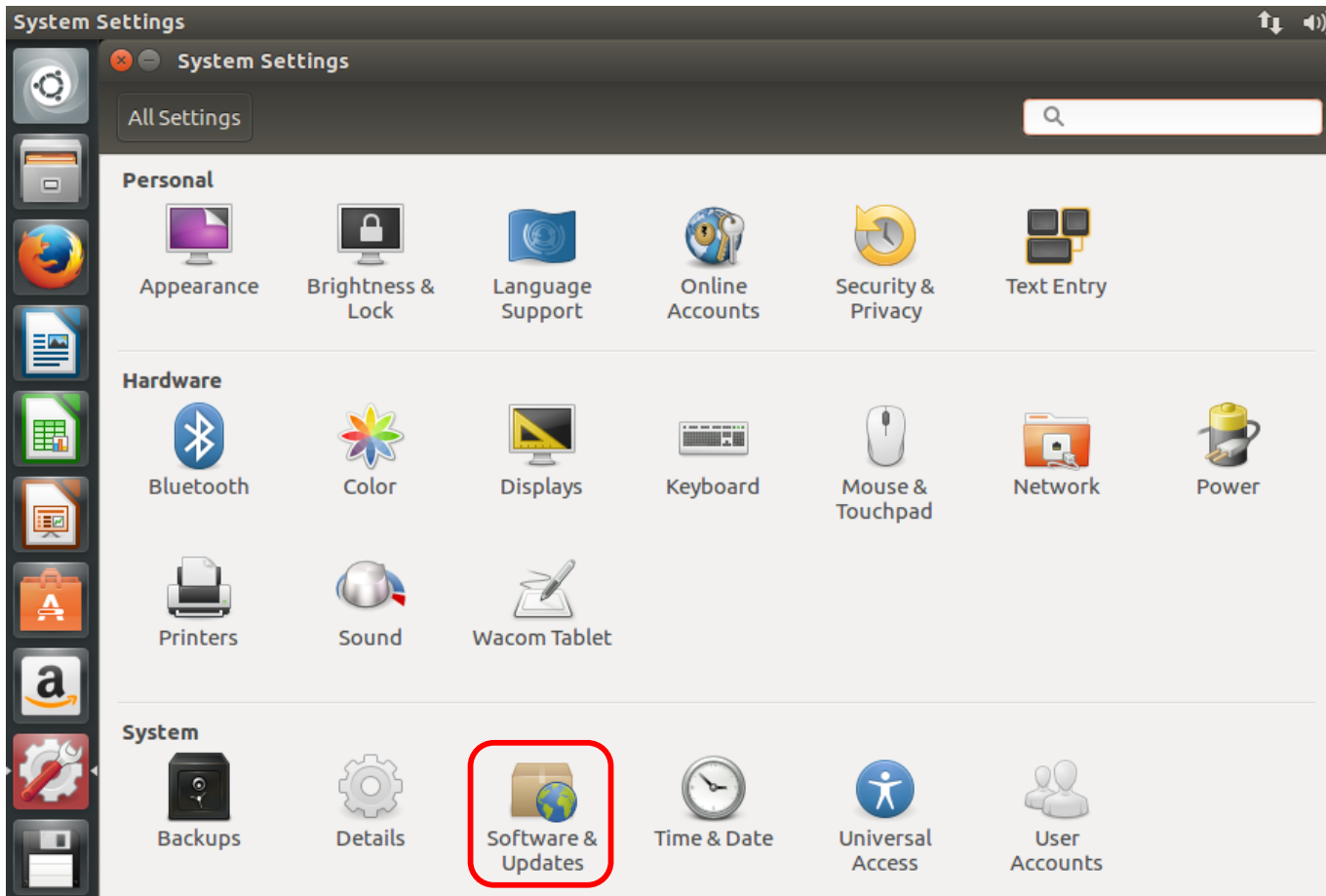
- Click the field next to **Password**
 - **Set a password now** allows you to change a user's password
 - Do not select **Log in without a password**
 - The third option allows you to disable or enable an account
- Press **Cancel** to return to the **User Accounts** windows





Configuring Updates

- Click **Software & Updates** in the System Settings window



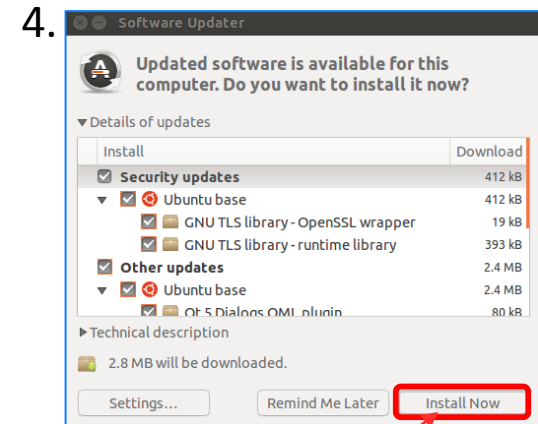
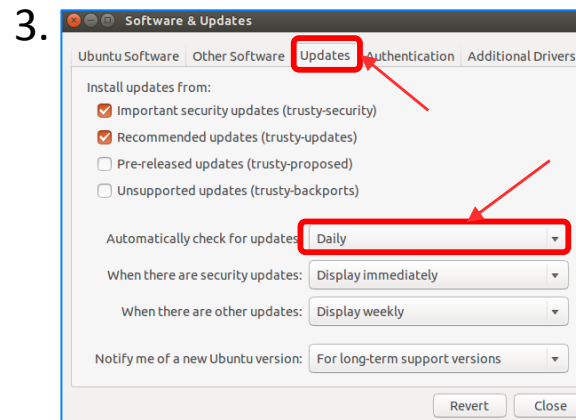
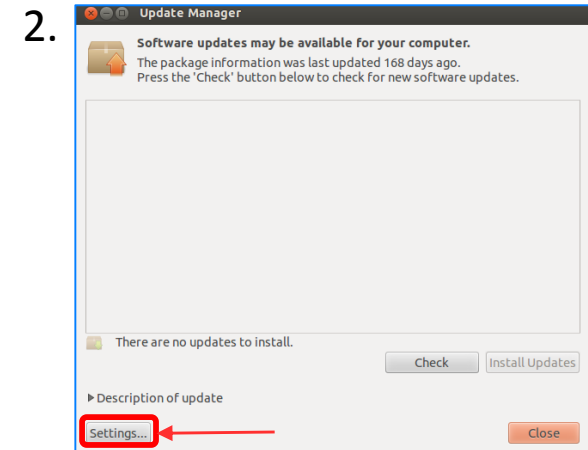
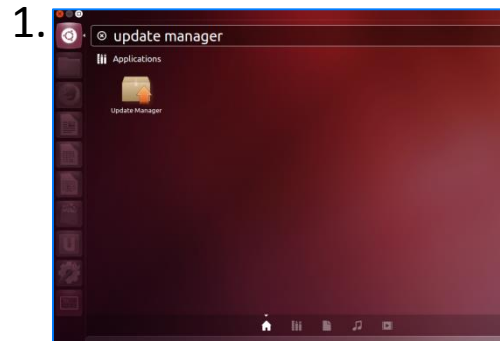


Installing Updates Overview

- The open-source community regularly develops improvements and patches for Ubuntu

- You should install these updates regularly

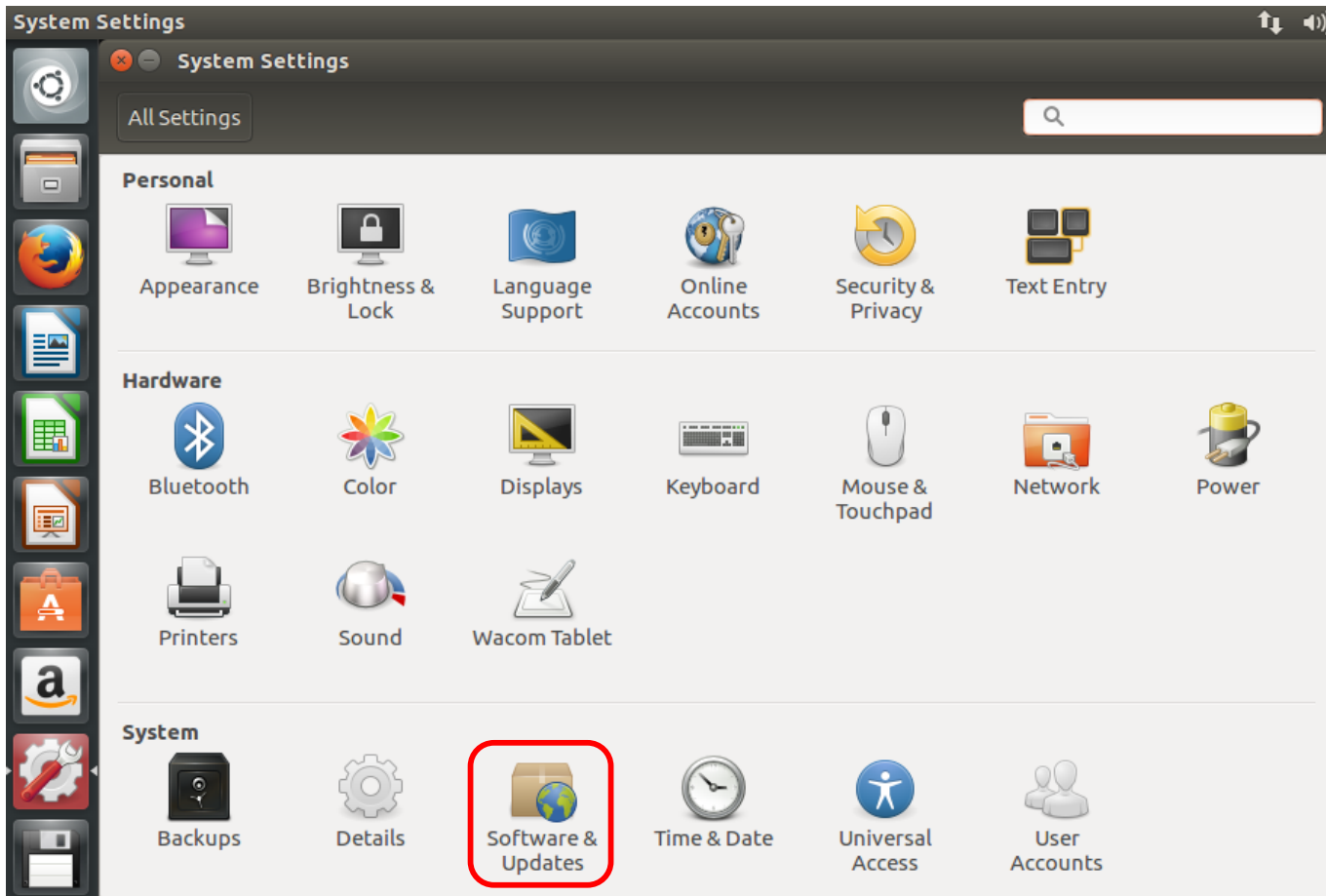
1. Click the Ubuntu button in the menu bar and search for Update Manager
2. Click Settings on the Update Manager Screen
3. To set automatic updates, go to the Updates Tab and make sure “Automatically check for updates” is set to “Daily”
4. After applying the changes, install any available updates from the main Update Manager window





Configuring Updates

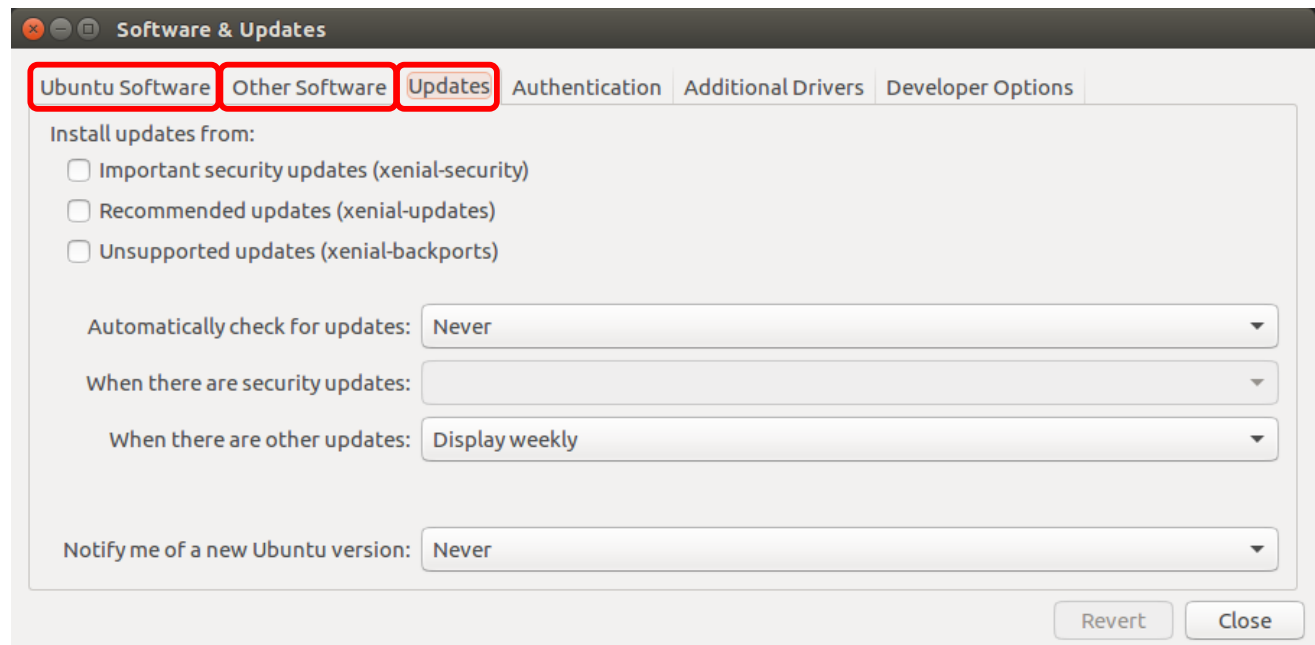
- Click **Software & Updates** in the System Settings window





Update Policy

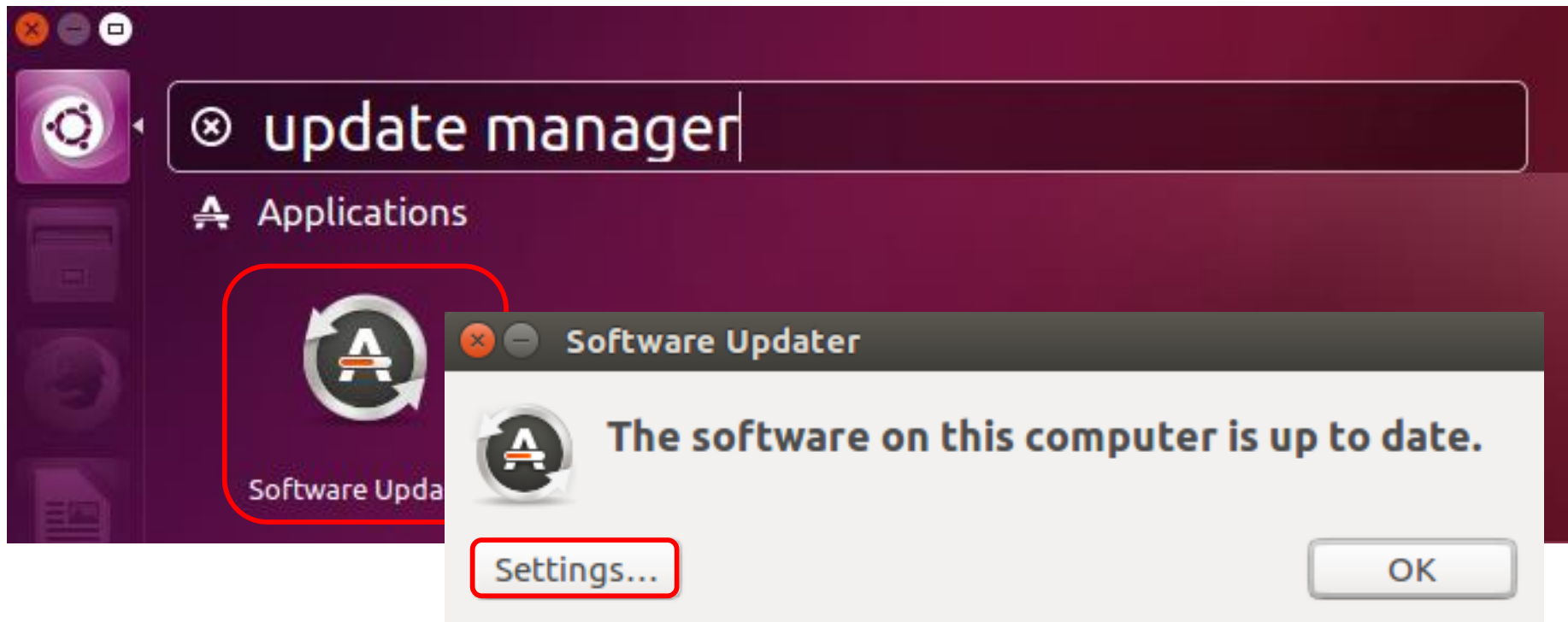
- Three Important Tabs
 - Ubuntu Software
 - Other Software
 - Updates





Installing Updates

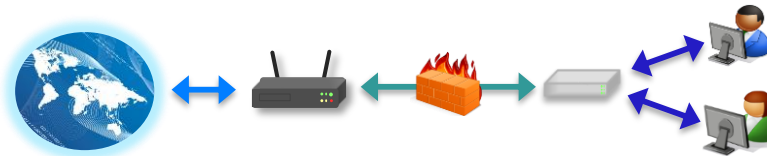
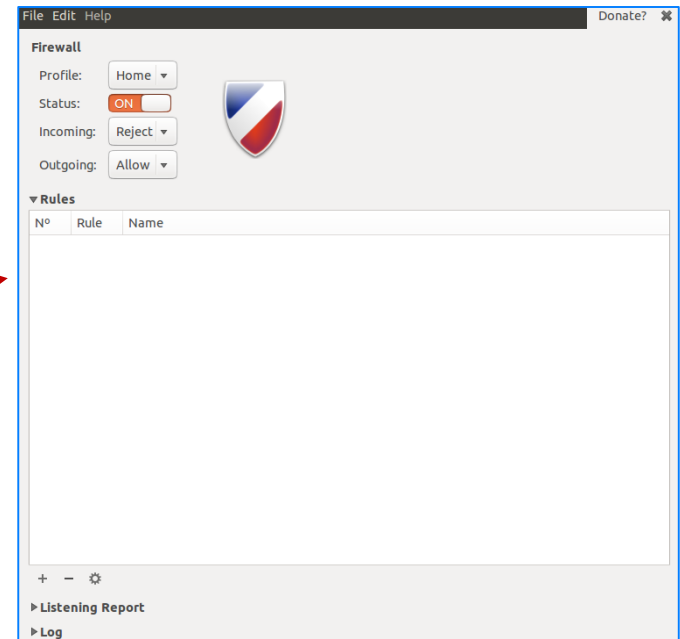
- Click the Ubuntu button in the left-hand menu and search for Update Manager





Enabling the Firewall

- Enable the Ubuntu Built-in Firewall (UFW) to prevent unauthorized access to the computer
 - The UFW is deactivated by default
- By default, UFW is only accessible by command line
- You can download **Gufw**, a graphical firewall interface, from the Software Center and use it to make changes to the UFW in the GUI
 - You might need to install Ubuntu updates before installing Gufw



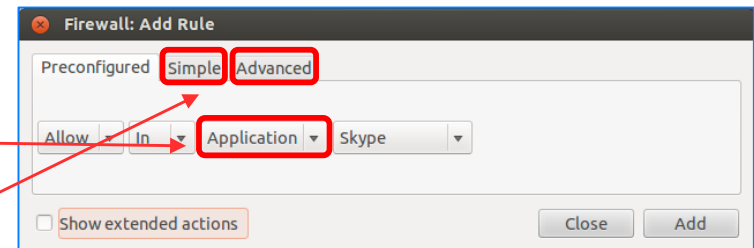
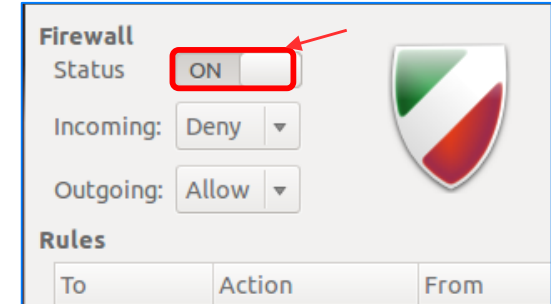
Source: <https://help.ubuntu.com/community/UFW>





Using Gufw

- After downloading Gufw from the Software Center, click the Ubuntu button in your menu bar → Search → Firewall Configuration
- Click the Unlock button on the Gufw window → Enact root permissions by authenticating → Turn Firewall Status On
- The default (and recommended) rules governing traffic are to Deny all incoming traffic and Allow all outgoing traffic
- The Reject option is the same as Deny, but also sends a notification to the sender that connection has been blocked
- The Preconfigured rule panel allows incoming and/or outgoing traffic to be controlled for certain applications or services
 - Similar to the Windows Firewall Exceptions list
 - Open entire ports by clicking the Simple or Advanced tabs



Source: <https://help.ubuntu.com/community/Gufw>





AIR FORCE ASSOCIATION'S

CYBERPATRIOT

NATIONAL YOUTH CYBER EDUCATION PROGRAM

SECTION 2

Basic Command Line Security





The Password file

- /etc/passwd
 - Usually does not contain passwords (anymore)
 - Contains user information
- Type `cat /etc/passwd`

```
cyberpatriot@ubuntu: ~  
cyberpatriot@ubuntu:~$ cat /etc/passwd  
root:x:0:0:root:/root:/bin/bash  
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin  
bin:x:2:2:bin:/bin:/usr/sbin/nologin
```

- Type `man 5 passwd` to view the manual for the password file
 - When you are done, press `q` to quit



The Password File

```
cyberpatriot:x:1021:1021:cyberpatriot:/home/cyberpatriot:/bin/bash
```

User Name

User ID

Password Group ID

- User Name
 - The name associated with this user account
 - This is primarily used by humans to identify a user account
- Password
 - x denotes password is stored in shadow file
- User ID – Numerical user ID, or “UID”
 - The OS internally identifies users using their UID not Username
- Group ID – Numerical primary group ID, or “GID”



The Password File

```
cyberpatriot:x:1021:1021:cyberpatriot:/home/cyberpatriot:/bin/bash
```

User Name

User ID

Password

Group ID

Comment

Home
Directory

Shell

- Comment
 - Typically used to store the users “real name”
- Home Directory
 - The current working directory when this user log in
- Shell
 - The shell (or command) that gets executed when you log in
 - How this user interacts with the computer when logging in on the command line



Listing Users

- Try running the following commands in the terminal:
 - `whoami`
 - Prints your current username
 - `users`
 - Prints the user names of users currently logged in to the current host
 - `who`
 - Prints information about users who are currently logged in
 - `w`
 - Displays information about the users currently on the machine, and their processes

```
cyberpatriot@ubuntu: ~  
cyberpatriot@ubuntu:~$ whoami  
cyberpatriot  
cyberpatriot@ubuntu:~$ users  
cyberpatriot  
cyberpatriot@ubuntu:~$ who  
cyberpatriot tty7          2017-05-03 19:28 (:0)  
cyberpatriot@ubuntu:~$ w  
 20:05:26 up 1 day,  1:46,  1 user,  load average: 0.00, 0.01, 0.05  
USER      TTY      FROM          LOGIN@      IDLE        JCPU       PCPU       WHAT  
cyberpat  tty7     :0            Wed19       25:46m    1:47      0.15s    /sbin/upstart  
cyberpatriot@ubuntu:~$
```



The gedit Command

- Gedit is one of many text editor commands in Ubuntu
 - Syntax: `gedit [filepath]`
 - Unlike with other text editors, using gedit will cause a second window to pop-up where you can easily change the text of a file
 - This command will allow you to edit security policy files
- You need to enact root permissions before using gedit to edit files that cannot be accessed by standard users (e.g. system and security files)
- When using gedit for the first time, go to `Edit → Preferences → Uncheck “Create a backup copy of files”` to avoid saving issues
- Try using gedit by `opening Terminal and entering gedit hello2.txt`
 - You will not be prompted to authenticate because this is a public file

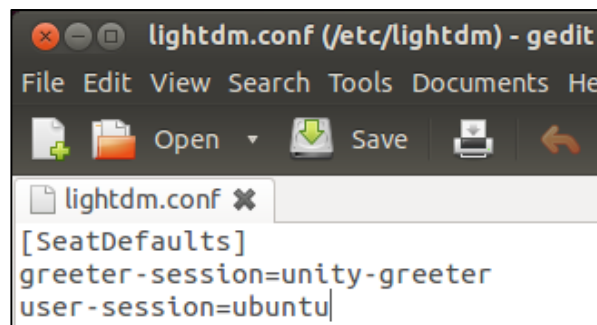




Using gedit to Turn off the Guest Account

- Like in Windows, the Ubuntu guest account is turned on by default
 - You should disable it so people can't access the computer anonymously
- The guest account is controlled by LightDM, the display manager controlling the Ubuntu login screen
- To turn off the guest account, edit the LightDM file:
 - After root authenticating, type `gedit /etc/lightdm/lightdm.conf`

```
root@ubuntu:/home/cyberpatriot# gedit /etc/lightdm/lightdm.conf
```
 - Add the line `allow-guest=false` to the end of the Light DM file that pops up and click `Save`
 - Restart your system and click your username button in the top-right corner of your desktop. The guest account should be disabled.



Sources: <https://help.ubuntu.com/8.04/serverguide/C/user-management.html>,
<http://askubuntu.com/questions/451526/removing-guest-session-at-login-in-ubuntu-14-04>





Using gedit to Edit Password History

- Type `gedit /etc/login.defs`
- This is a much longer file. To easily find the section to edit, type `Ctrl+F` and then “`PASS_MAX_AGE`”
- Modify the following variables to the same recommended settings used in Windows:
 - Maximum Password Duration:
 - `PASS_MAX_DAYS` 90
 - Minimum Password Duration:
 - `PASS_MIN_DAYS` 10
 - Days Before Expiration to Warn Users to Change Their Password:
 - `PASS_WARN_AGE` 7
- Save the file and close it

```
login.defs (/etc) - gedit
login.defs x
#
# Password aging controls:
#
#     PASS_MAX_DAYS   Maximum number of days a password may be used.
#     PASS_MIN_DAYS   Minimum number of days allowed between
password changes.
#     PASS_WARN_AGE   Number of days warning given before a password
expires.
#
PASS_MAX_DAYS   99999
PASS_MIN_DAYS   0
PASS_WARN_AGE   7
#
# Min/max values for automatic uid selection in useradd
#
UID_MIN         1000
UID_MAX         60000
# System accounts
#SYS_UID_MIN    100
#SYS_UID_MAX    999
Plain Text Tab Width: 8 Ln 145, Col 56 INS
```

Sources: <http://xmodulo.com/2013/12/set-password-policy-linux.html>,





Using gedit to Set Account Policy

- Type `gedit /etc/pam.d/common-auth`
- This file allows you to set an account lockout policy
- Add this line to the end of the file:

```
auth required pam_tally2.so deny=5 onerr=fail unlock_time=1800
```

- Save the file and close it

```
common-auth (/etc/pam.d) - gedit
File Edit View Search Tools Documents Help
common-auth
#
# /etc/pam.d/common-auth - authentication settings common to all services
#
# This file is included from other service-specific PAM config files,
# and should contain a list of the authentication modules that define
# the central authentication scheme for use on the system
# (e.g., /etc/shadow, LDAP, Kerberos, etc.). The default is to use the
# traditional Unix authentication mechanisms.
#
# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules. See
# pam-auth-update(8) for details.
#
# here are the per-package modules (the "Primary" block)
auth [success=2 default=ignore] pam_unix.so nullok_secure
auth [success=1 default=ignore] pam_wlnbind.so krb5_auth krb5_ccache_type=FILE
cached_login try_first_pass
# here's the fallback if no module succeeds
auth requisite pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
auth required pam_permit.so
# and here are more per-package modules (the "Additional" block)
auth optional pam_smbpass.so migrate
auth optional pam_cap.so
# end of pam-auth-update config
Plain Text • Tab Width: 8 • Ln 1, Col 1 INS
```

Sets the number of allowed failed login attempts (in this case 5)

Sets the account lockout duration in seconds (in this case, 30 minutes)

Source: http://linux.die.net/man/8/pam_tally





AIR FORCE ASSOCIATION'S

CYBERPATRIOT

NATIONAL YOUTH CYBER EDUCATION PROGRAM

SECTION 3

Advanced Ubuntu Security





Turn off the Guest Account

- Turned on by default
- LightDM: display manager controlling the login screen
- Type `sudo gedit /etc/lightdm/lightdm.conf`
- Add the line `allow-guest=false` under `[Seat:*]`

```
cyberpatriot@ubuntu: ~  
cyberpatriot@ubuntu:~$ sudo gedit /etc/lightdm/lightdm.conf  
(gedit:10875): IBUS-WARNING **: The owner of /home/cyberpatriot  
is not root!  
(gedit:10875) op.DBus.Error: by any .serv  
[Seat:*]  
autologin-user=  
allow-guest=false
```



Password Age Policy

- In a terminal, type `sudo gedit /etc/login.defs`

Maximum Password Duration: `PASS_MAX_DAYS` 90

Minimum Password Duration: `PASS_MIN_DAYS` 5

Password Warning Before Expiration: `PASS_WARN_AGE` 7

```
cyberpatriot@ubuntu: ~  
cyberpatriot@ubuntu:~$ sudo gedit /etc/login.defs  
login.defs /etc  
#  
# Password aging controls:  
#  
#     PASS_MAX_DAYS   Maximum number of days a password may be  
used.  
#     PASS_MIN_DAYS   Minimum number of days allowed between  
password changes.  
#     PASS_WARN_AGE   Number of days warning given before a  
password expires.  
#  
PASS_MAX_DAYS 99999  
PASS_MIN_DAYS 0  
PASS_WARN_AGE 7
```



The chmod Command

- Chmod allows you to change file permissions

Change permissions for
the user, group, or others

Add or subtract
permissions

Specify whether read, write,
or execute privileges are
being changed

- Syntax: `chmod [u,g or o][+ or -][r,w, or x] [filepath]`

– Do not put spaces between the three fields after “chmod”

- Example:

1. Type `chmod o-r hello2.txt`
2. Type `ls -l hello2.txt`
3. If your permissions originally matched those on the last slide, you should see hello2.txt’s new file permissions as shown below

```
cyberpatriot@ubuntu:~$ ls -l hello2.txt
-rw-rw---- 1 cyberpatriot cybercamp 57 May 29 09:34 hello.txt
```

Sources: <http://condor.depaul.edu/dpowebpg/support/chmod.html>,
<https://help.ubuntu.com/community/FilePermissions>





Groups

- Work very similarly to Windows

- Root permissions are required

1. To list all groups:

```
cat /etc/group
```

2. To add a group:

```
addgroup [groupname]
```

3. To add a user to a group:

```
adduser [username] [groupname]
```

```
root@ubuntu: /home/cyberpatriot
root@ubuntu:/home/cyberpatriot# cat /etc/group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:syslog,cyberpatriot
tty:x:5:
disk:x:6:
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
kmem:x:15:
dialout:x:20:
fax:x:21:
voice:x:22:
cdrom:x:24:cyberpatriot
floppy:x:25:
tape:x:26:
sudo:x:27:cyberpatriot
audio:x:29:pulse
dip:x:30:cyberpatriot
www-data:x:33:
backup:x:34:
test:x:1002:cyberpatriot,guest
cybercamp:x:1003:cyberpatriot
root@ubuntu:/home/cyberpatriot#
```



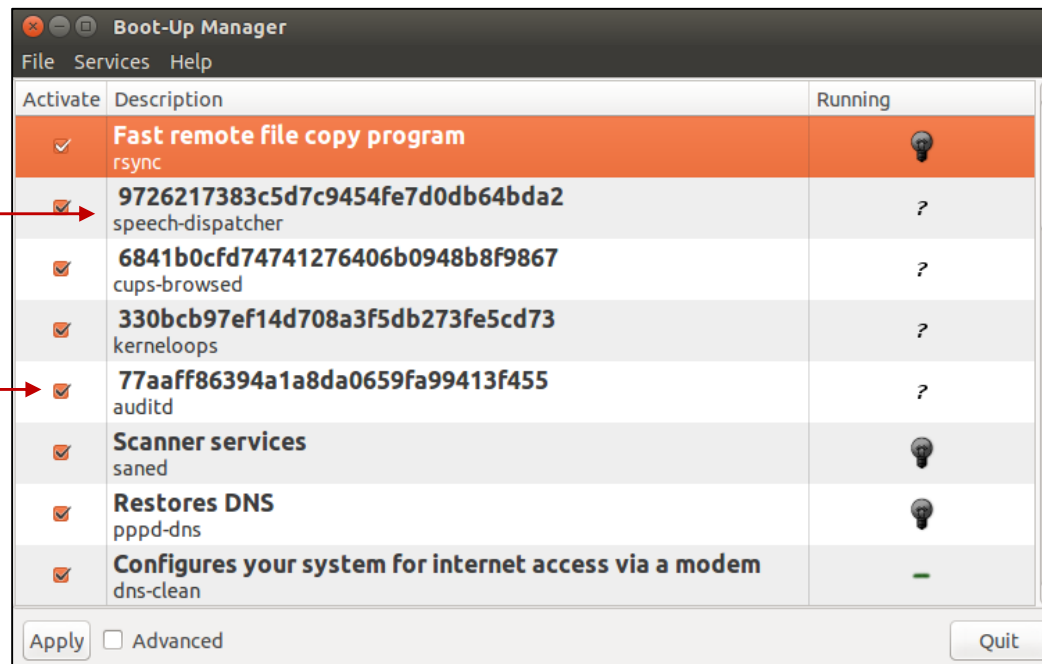


Services

- Can be viewed and managed in the GUI
- To install, type `apt-get install bum` in Terminal
- After installing, type `bum` to run

To start a service, right-click it and select "Start"

To enable a service, check the box next to it



When a service is started, the light bulb will light up. When stopped, the light bulb will be dark.

