CYBERPATRIOT

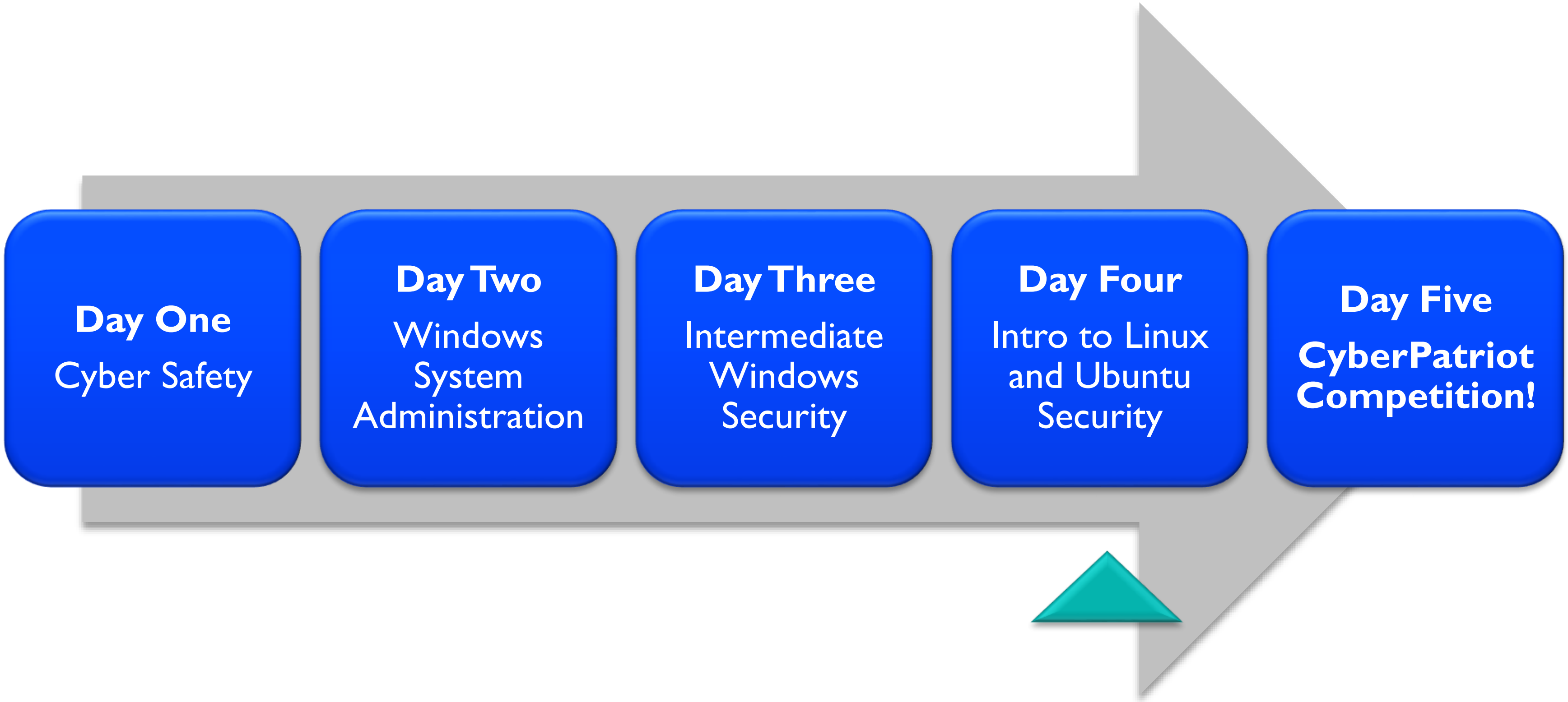
INTEGRITY, SERVICE, EXCELLENCE

NATIONAL YOUTH CYBER EDUCATION PROGRAM

AFA CyberCamp

Module 4

AFA CyberCamp Format



Day One
Cyber Safety

Day Two
Windows System Administration

Day Three
Intermediate Windows Security

Day Four
Intro to Linux and Ubuntu Security

Day Five
CyberPatriot Competition!

Module Four Learning Objectives

1. **Ubuntu Terminology and Concepts**

   - Become familiar with important vocabulary and navigating the Ubuntu interface

2. **Basic GUI Security**

   - Apply key security principles to an Ubuntu system in the Graphic User Interface

3. **Intro to Command Line**

   - Understand command line syntax and explore making commands through code

4. **Basic Command Line Security**

   - Use command line to make account management settings

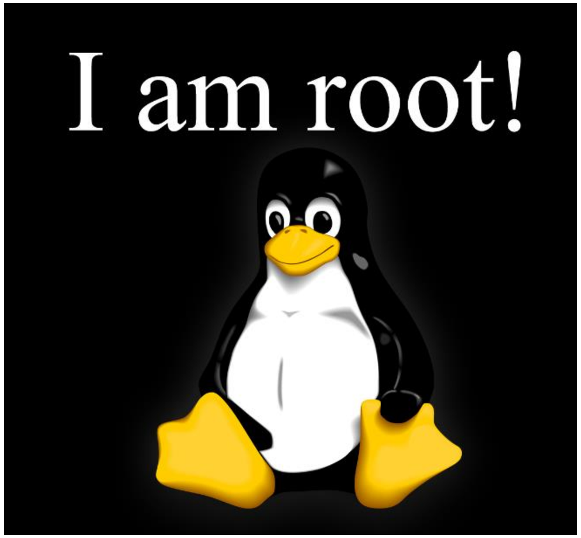
5. **Intermediate Ubuntu Security**

   - Make intermediate security settings using command line and the GUI

Ubuntu Terminology and Concepts

The Root Account

- Account types: **User** and **root**
- **root** - Linux Administrator account
- Requires password in GUI and command line
- **Authentication**
- **Authorization**



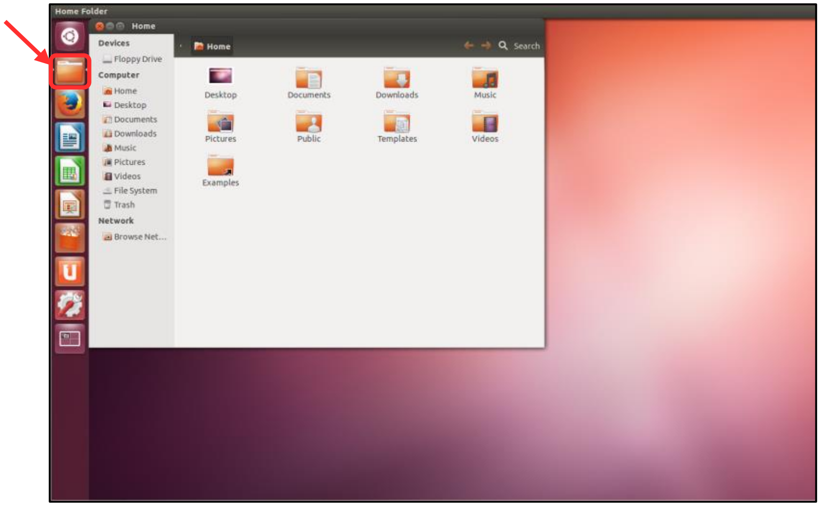
Source: http://eswalls.com/wp-content/uploads/2014/01/i-am-root.png

File system

- Different than Windows
- Example:
  - **Windows:**

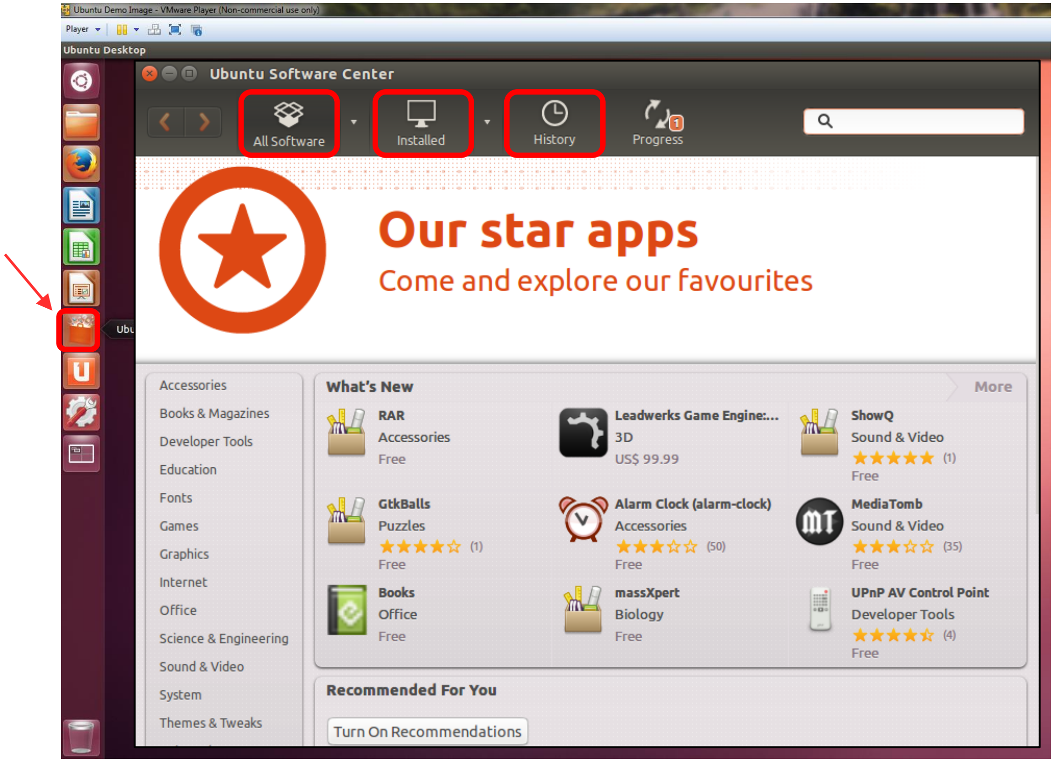
    C:\Documents\hello.txt
  - **Linux:**

    /home/CyberPatriot/hello.txt
- Log in to the image
  - User: **cyberpatriot**
  - Password: **CyberPatriot!**
- Important folders:
  - /home
  - /boot



Adding and Removing Software

- Software is bundled into **packages**
- Packages are managed by **package managers**
- Click the Ubuntu Software Center in the left-hand menu



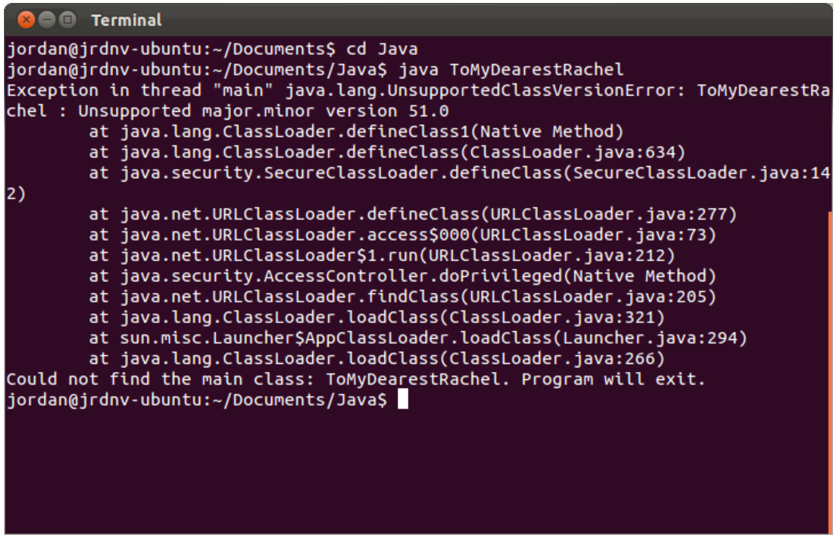
Command Line (Terminal)

Cons

- Not as user-friendly
- Harder to multitask

Pros

- Provides the user more control
- Only option for some tasks
- Just need a keyboard
- Uses fewer resources
- Can be made easier with scripting



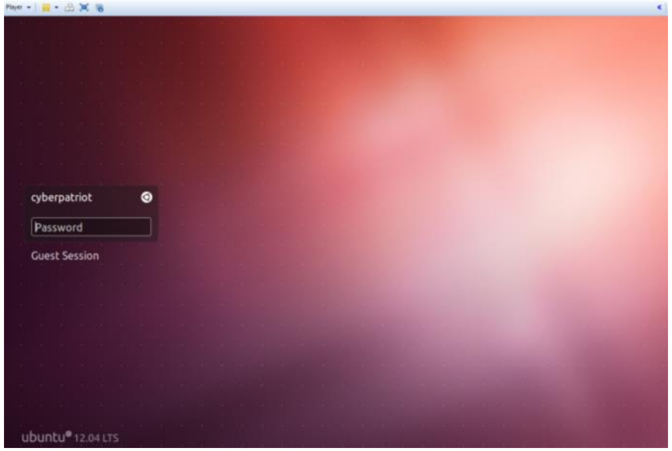
```
jordan@jrdnv-ubuntu:~/Documents$ cd Java
jordan@jrdnv-ubuntu:~/Documents/Java$ java ToMyDearestRachel
Exception in thread "main" java.lang.UnsupportedClassVersionError: ToMyDearestRa
chel : Unsupported major.minor version 51.0
        at java.lang.ClassLoader.defineClass1(Native Method)
        at java.lang.ClassLoader.defineClass(ClassLoader.java:634)
        at java.security.SecureClassLoader.defineClass(SecureClassLoader.java:14
2)
        at java.net.URLClassLoader.defineClass(URLClassLoader.java:277)
        at java.net.URLClassLoader.access$000(URLClassLoader.java:73)
        at java.net.URLClassLoader$1.run(URLClassLoader.java:212)
        at java.security.AccessController.doPrivileged(Native Method)
        at java.net.URLClassLoader.findClass(URLClassLoader.java:205)
        at java.lang.ClassLoader.loadClass(ClassLoader.java:321)
        at sun.misc.Launcher$AppClassLoader.loadClass(Launcher.java:294)
        at java.lang.ClassLoader.loadClass(ClassLoader.java:266)
Could not find the main class: ToMyDearestRachel. Program will exit.
jordan@jrdnv-ubuntu:~/Documents/Java$
```

Source: http://i.stack.imgur.com/2hBJf.png

Activity 4-1: Linux Familiarization Lab

Instructions (Workbook Pages 17-18):

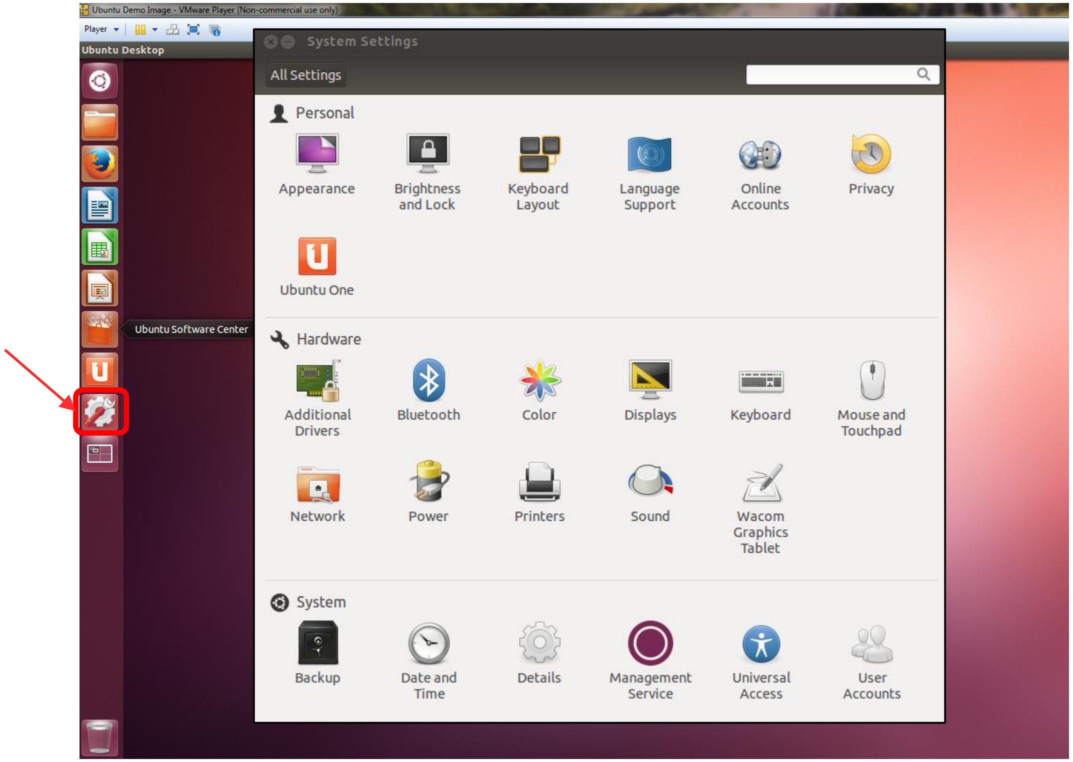
- Open the Ubuntu Demo Image in VMware Player
  - User: **cyberpatriot**
  - Password: **CyberPatriot!**
- Complete the tasks outlined in your workbooks
- Do not change any passwords or user account settings



Basic GUI Security

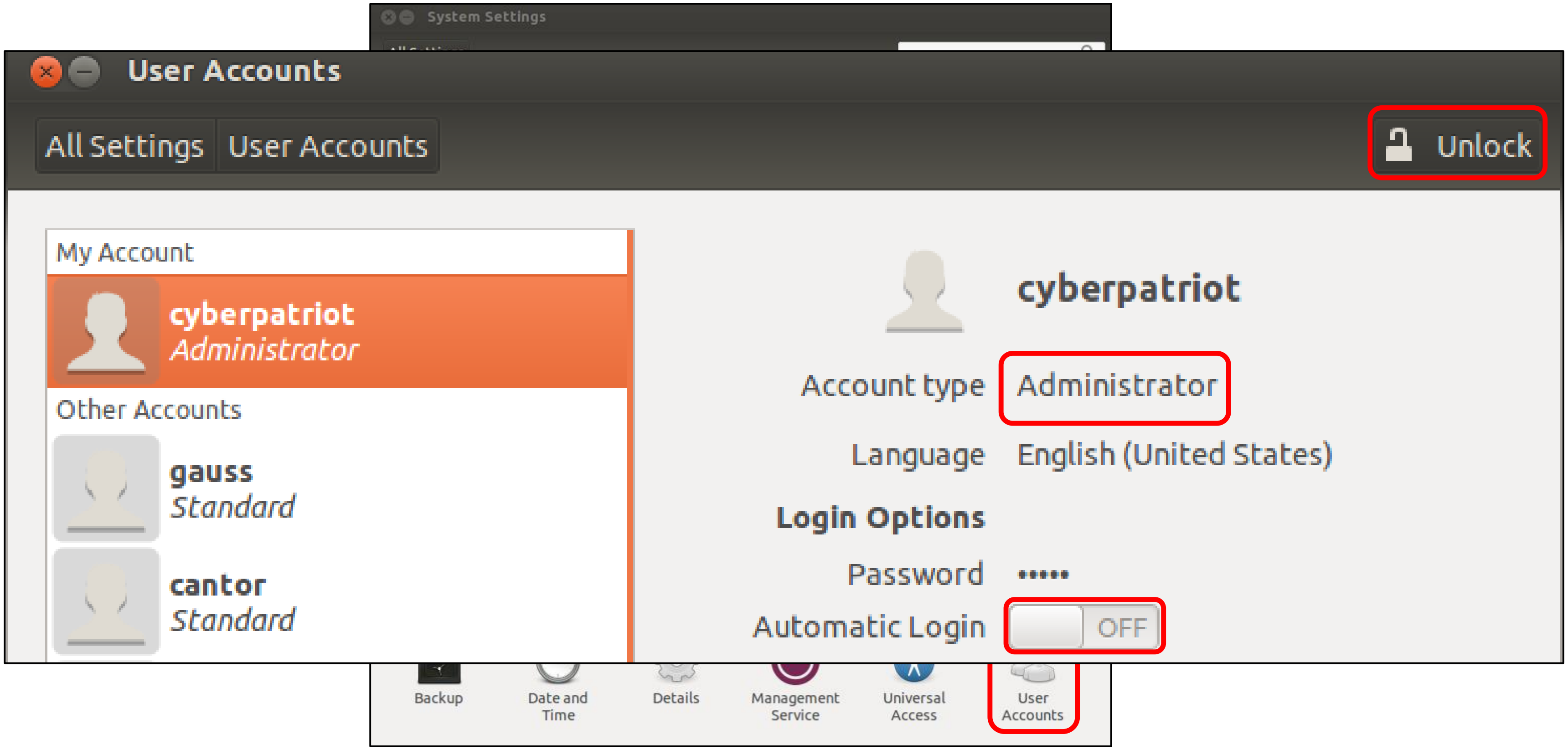
Basic Linux Security

- No Control Panel like in Windows
- Click the System Settings in the left-hand menu



User Accounts

- Click User Accounts
- To Change User Type, click the field next to Account Type



User Accounts

All Settings | User Accounts

Unlock

My Account

cyberpatriot
Administrator

Other Accounts

gauss
Standard

cantor
Standard

cyberpatriot

Account type: Administrator

Language: English (United States)

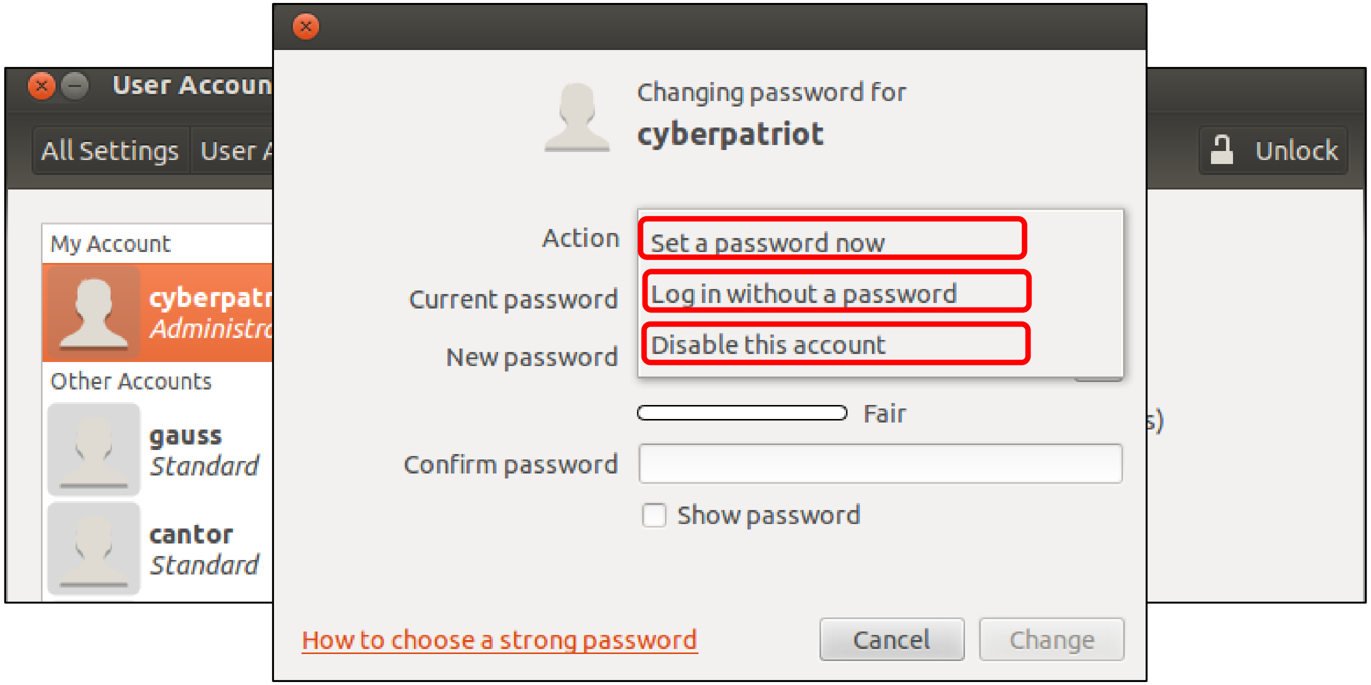
Login Options

Password: •••••

Automatic Login: OFF

User Account Passwords

- Click the field next to Password
- Click the first option next to Action to change a user's password
- Do not use the second option
- Click the third option to disable a user's account



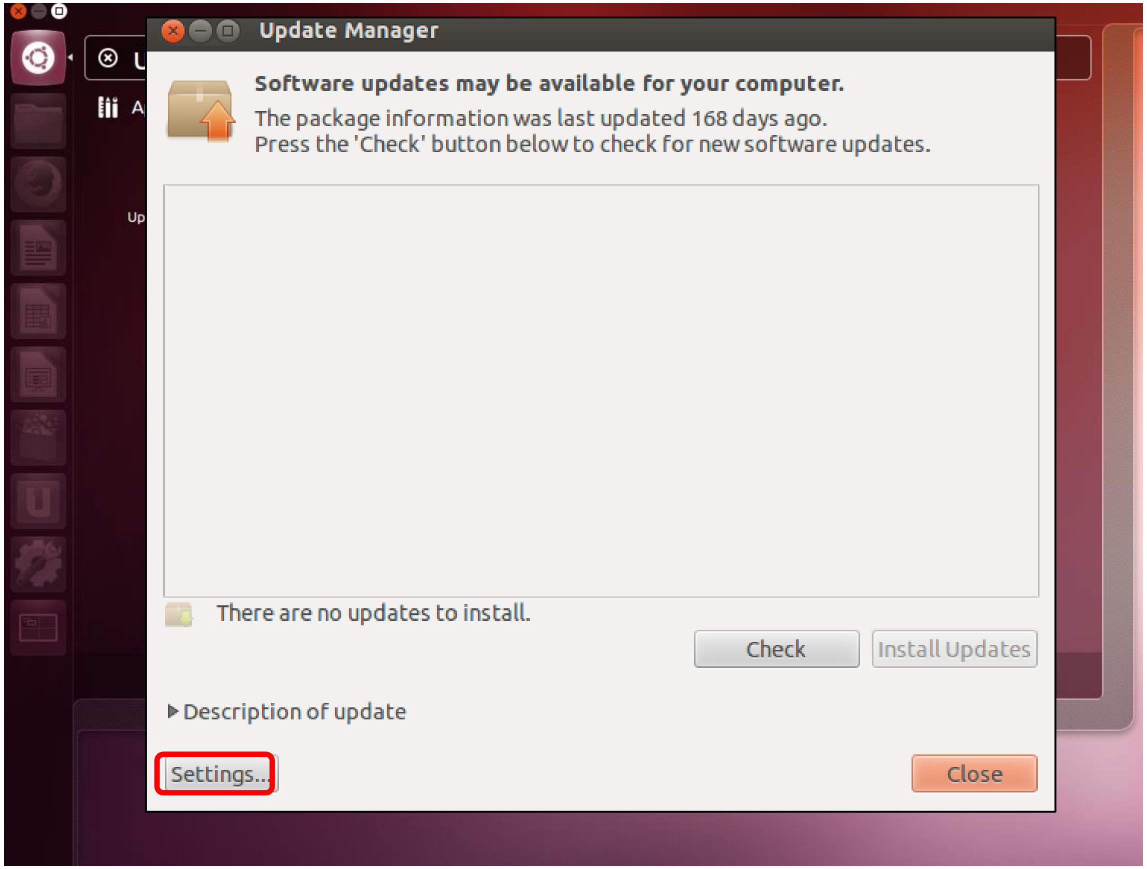
Changing password for

cyberpatriot

Action: Set a password now / Log in without a password / Disable this account

Installing Updates

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



Update Manager

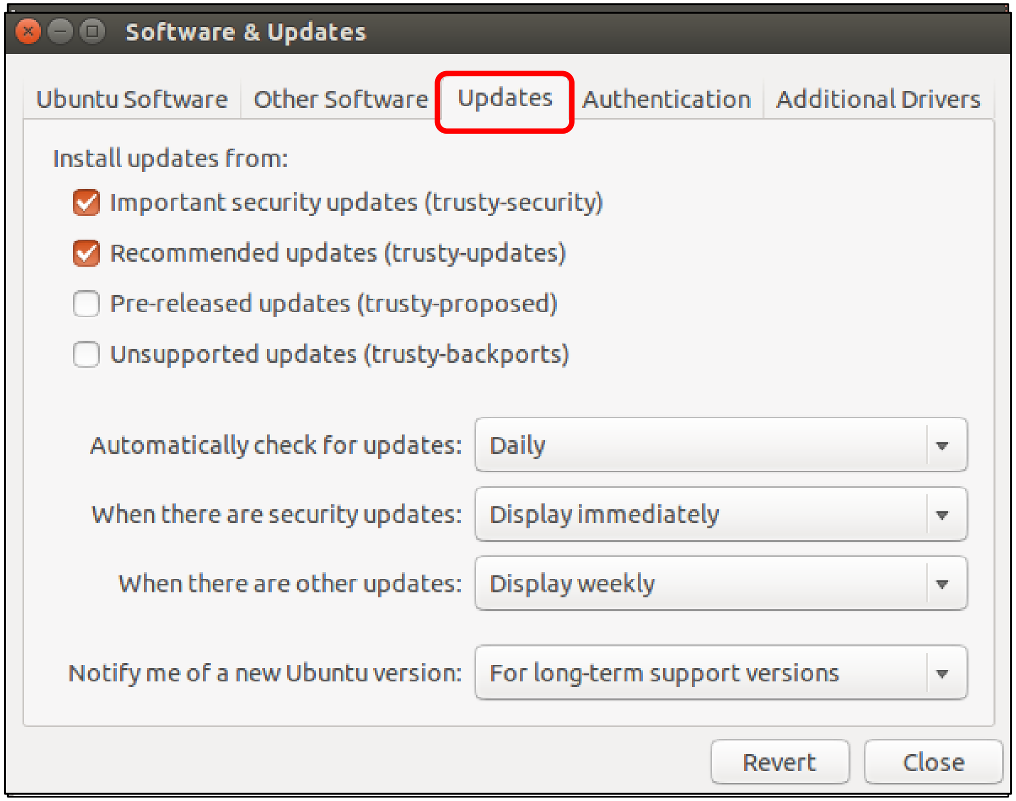
Software updates may be available for your computer.

The package information was last updated 168 days ago.
Press the 'Check' button below to check for new software updates.

There are no updates to install.

Update Policy

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



Install updates from:

☑ Important security updates (trusty-security)

☑ Recommended updates (trusty-updates)

□ Pre-released updates (trusty-proposed)

□ Unsupported updates (trusty-backports)

Automatically check for updates: Daily

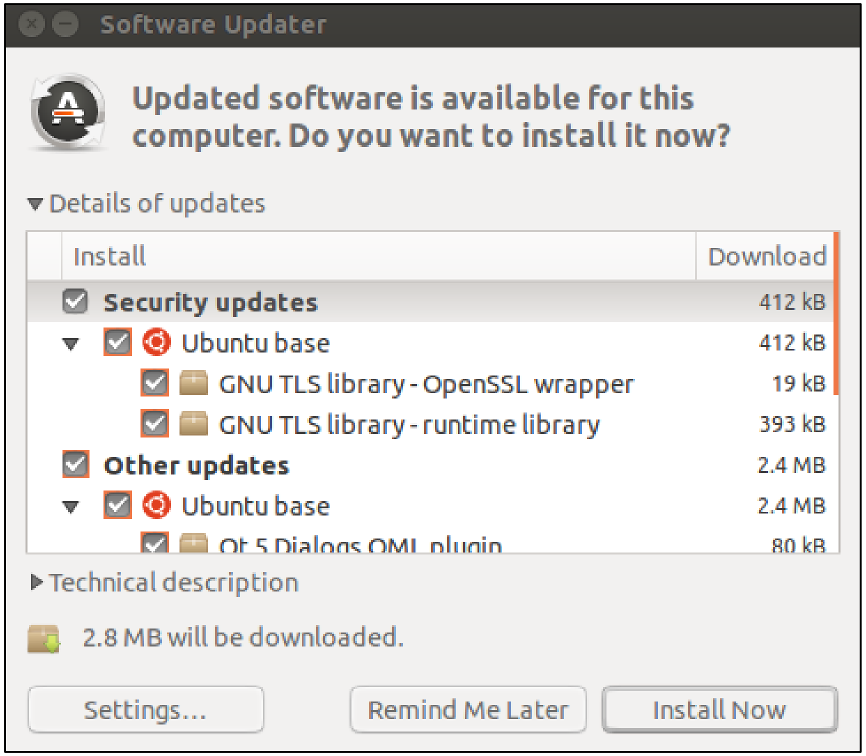
When there are security updates: Display immediately

When there are other updates: Display weekly

Notify me of a new Ubuntu version: For long-term support versions

Update Policy

- Manual Selection of Updates
- Install Updates



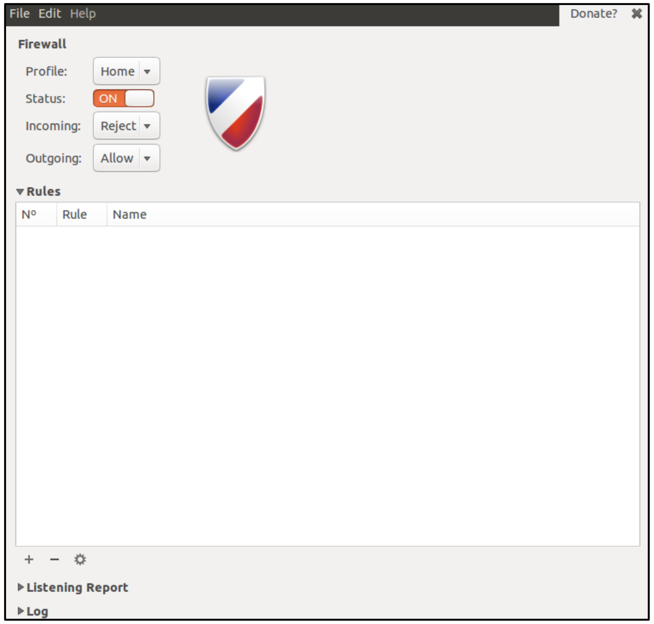
Updated software is available for this computer. Do you want to install it now?

Install	Download
☑ **Security updates**	412 kB
▼ ☑ Ubuntu base	412 kB
☑ GNU TLS library - OpenSSL wrapper	19 kB
☑ GNU TLS library - runtime library	393 kB
☑ **Other updates**	2.4 MB
▼ ☑ Ubuntu base	2.4 MB
☑ Qt 5 Dialogs QML plugin	80 kB

2.8 MB will be downloaded.

Local Firewall

- Built-in Firewall (UFW)
- Not activated by default
- Command line interface
- Gufw



Firewall

Profile: Home

Status: ON

Incoming: Reject

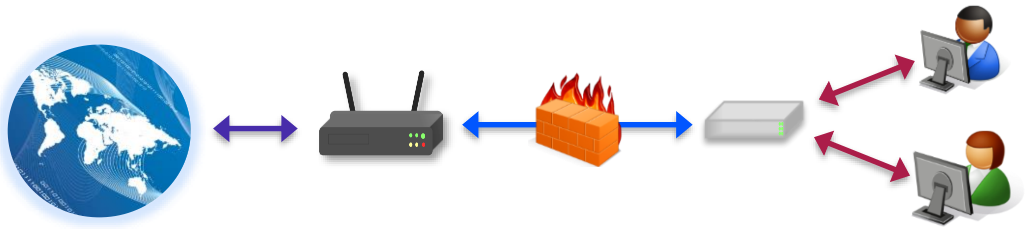
Outgoing: Allow

Rules

Nº	Rule	Name

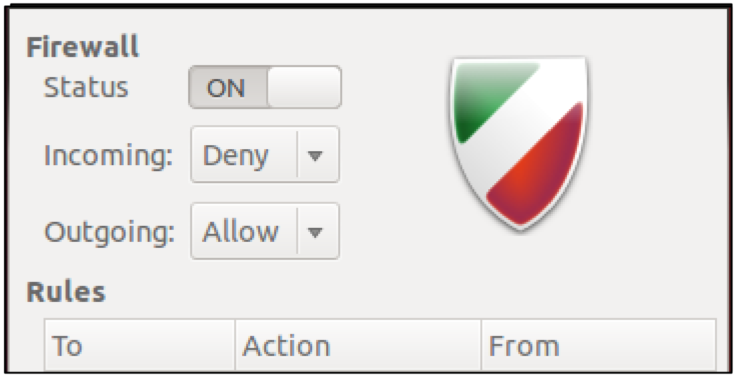
Listening Report

Log



GUFW – Customizing Settings

- Search → Firewall Configuration → Unlock → Status On
- Default:
  - Deny all incoming traffic--silently discards all incoming or outgoing packets
  - Allow all outgoing traffic
- Reject--sends an error packet to the sender of the incoming packets
- Preconfigured Rules



Firewall

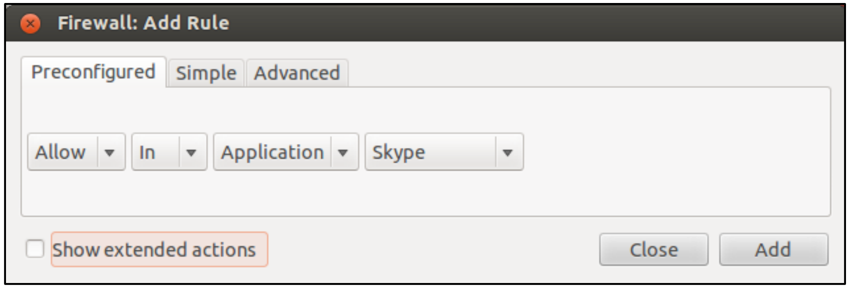
Status: ON

Incoming: Deny

Outgoing: Allow

Rules

To	Action	From



Firewall: Add Rule

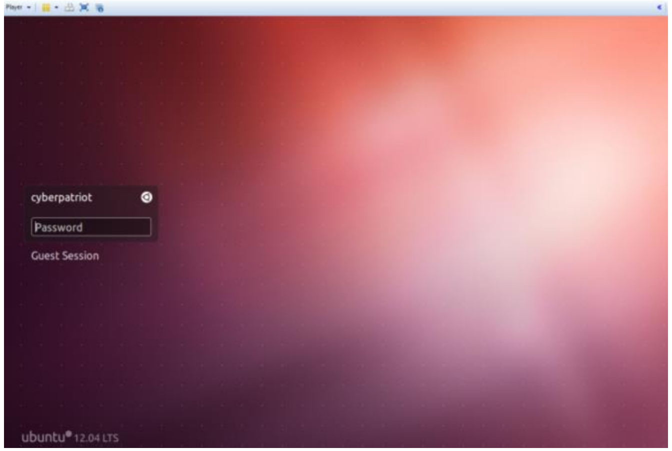
Allow | In | Application | Skype

☐ Show extended actions

Activity 4-2: GUI Security Lab

Instructions (Workbook Page 19):

- Open the Ubuntu Demo Image in VMware Player
  - User: **cyberpatriot**
  - Password: **CyberPatriot!**
- Complete the tasks outlined in your workbooks
- Do not change any passwords or user account settings



CYBERPATRIOT

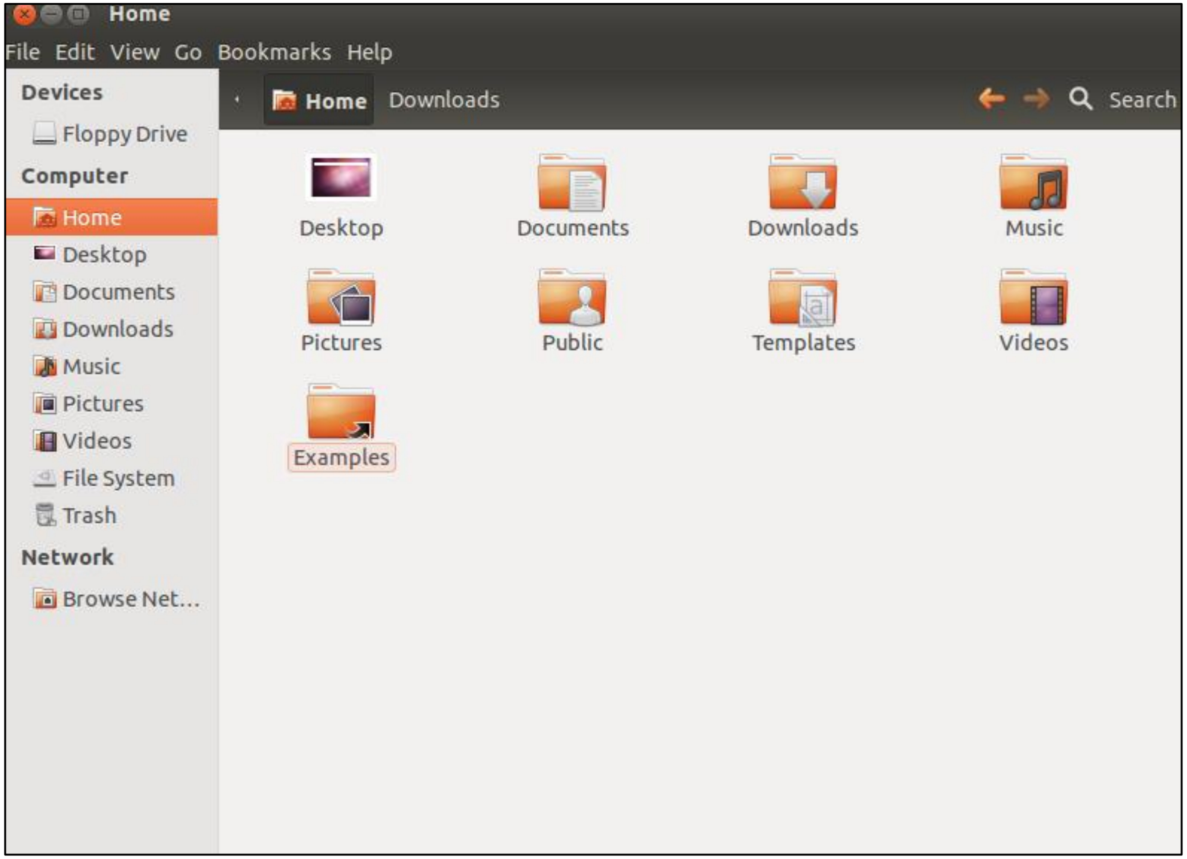
INTEGRITY, SERVICE, EXCELLENCE

NATIONAL YOUTH CYBER EDUCATION PROGRAM

Intro to Command Line

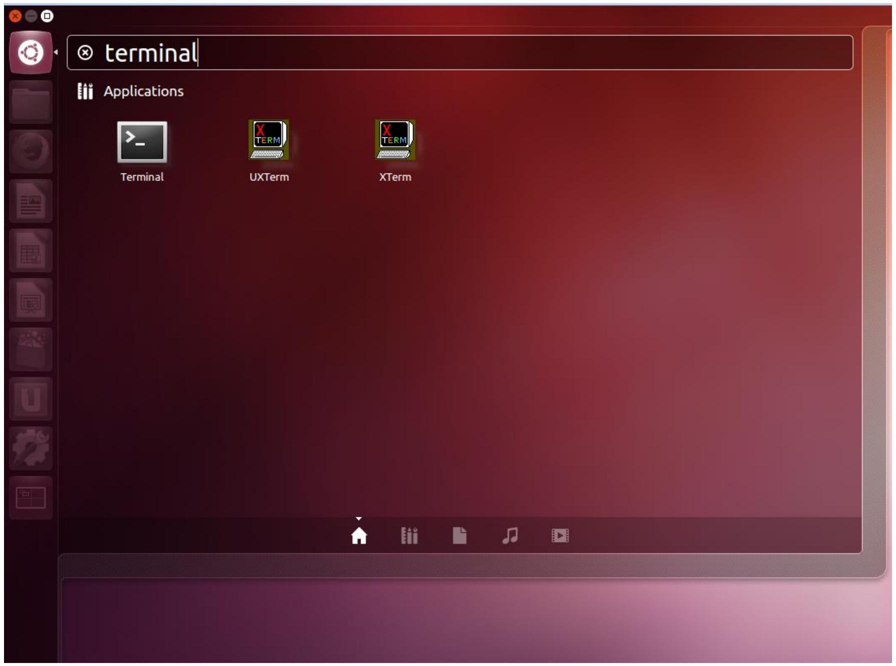
First Command Line Walkthrough

- Open the Home folder



1. Open the Terminal

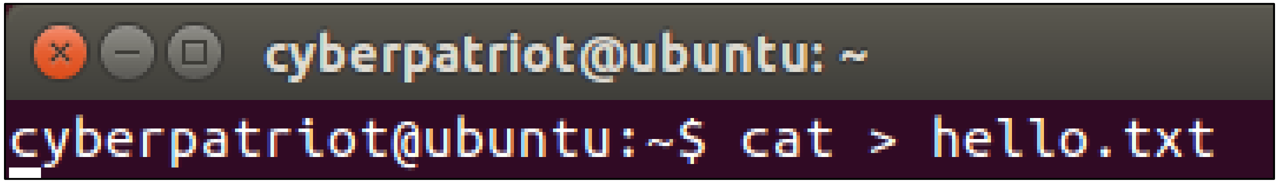
- Close the Home folder
- Click Ubuntu Button at top of left-nav menu → Search "Terminal" → Open Terminal



terminal

2. Create Text Document

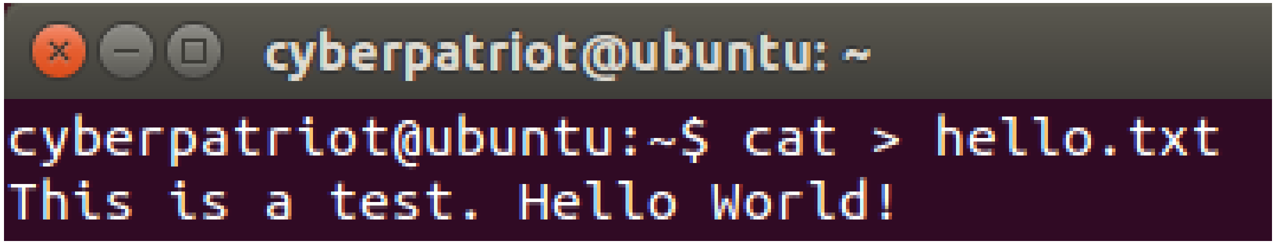
- Type `cat > hello.txt`
- Hit Enter



```
cyberpatriot@ubuntu:~$ cat > hello.txt
```

3. Add Text to Document

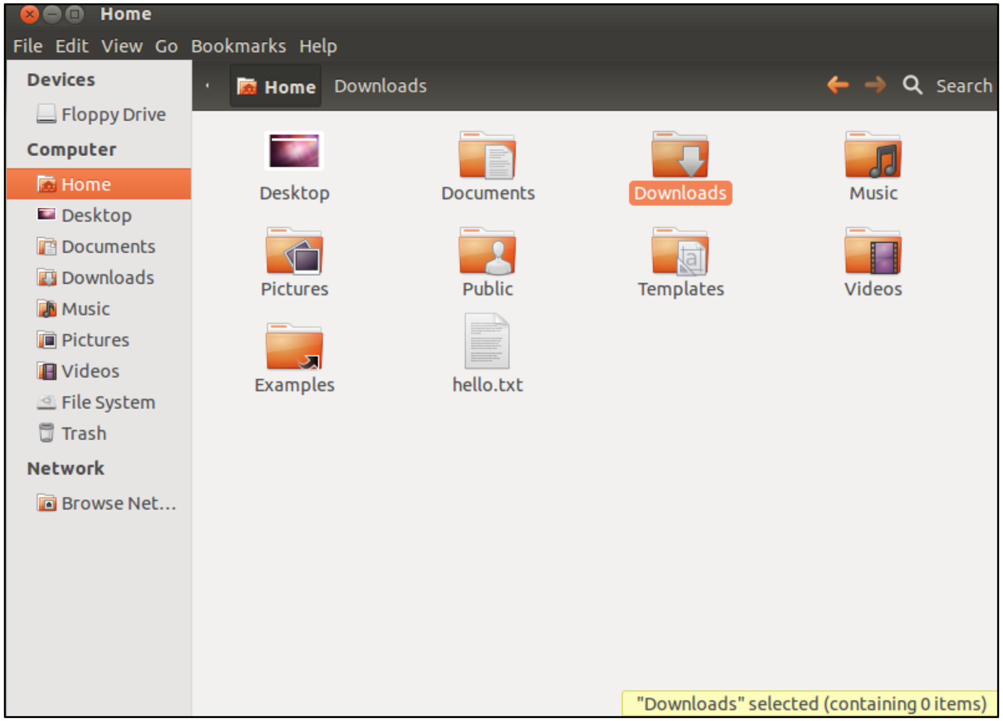
- Type `This is a test. Hello World!`
- Type `Ctrl+D`



```
cyberpatriot@ubuntu:~$ cat > hello.txt
This is a test. Hello World!
```

4. View Document in the GUI

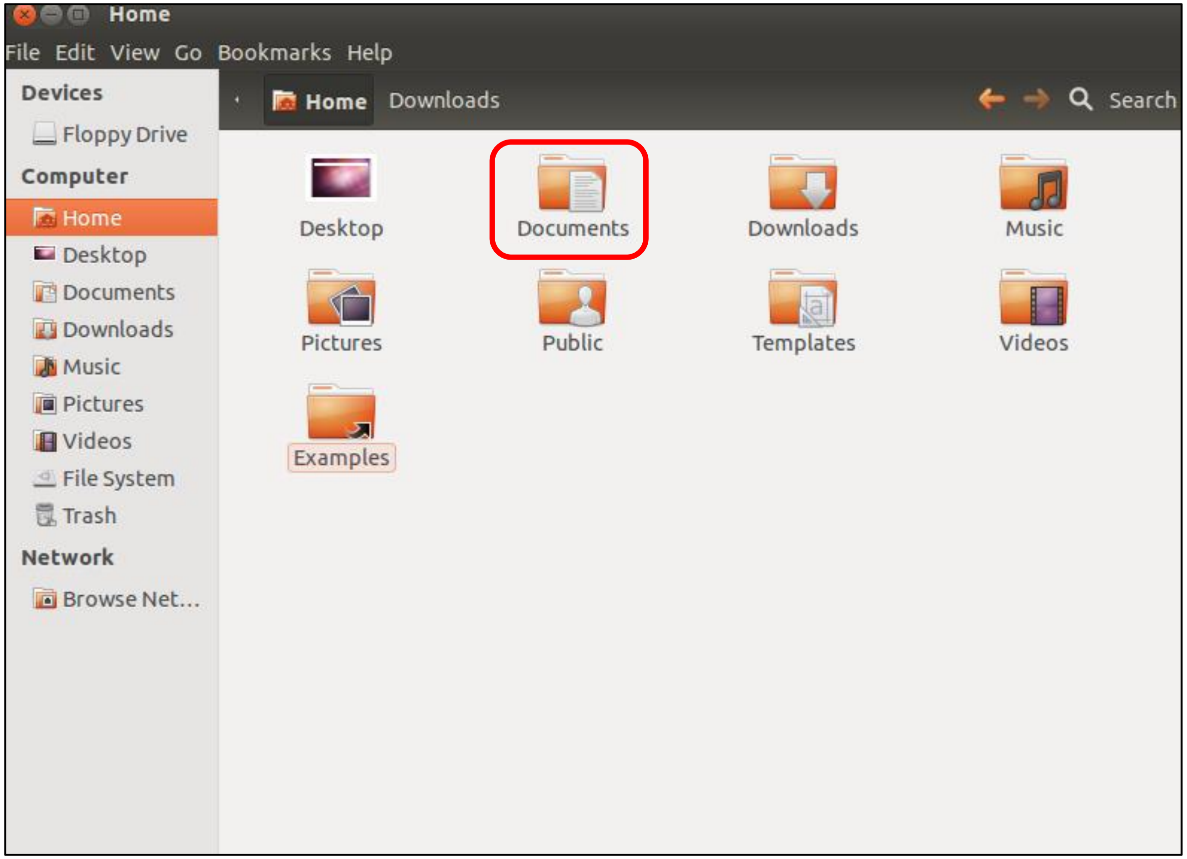
- Close the Terminal
- Open the Home Folder
- Double-click the hello.txt file



"Downloads" selected (containing 0 items)

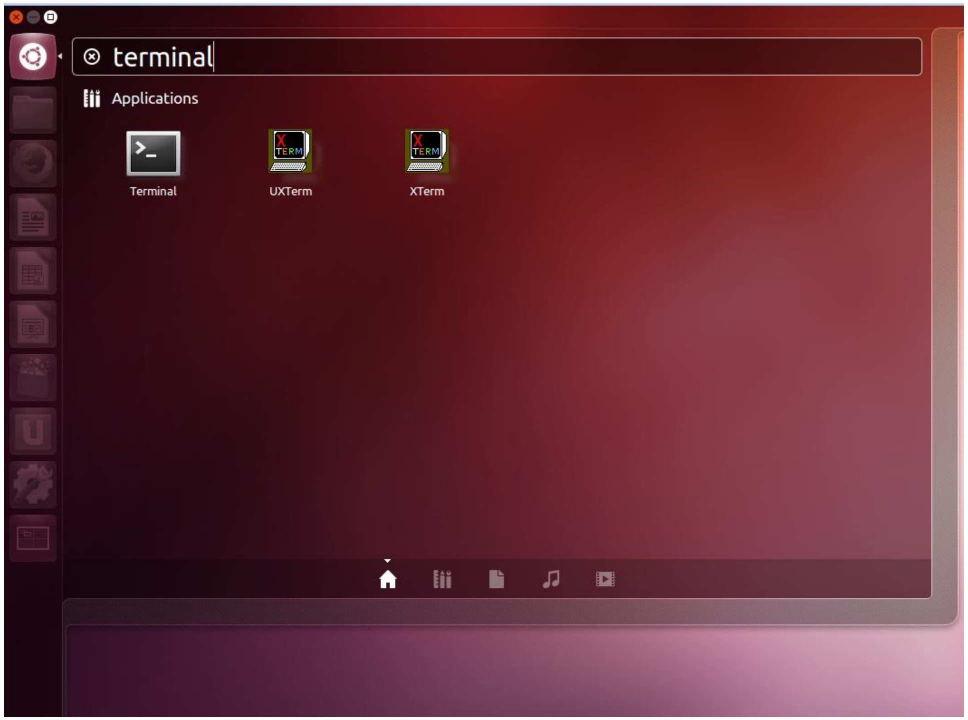
Second Command Line Walkthrough

- Open the Documents folder



1. Open the Terminal

- Close the Home folder
- Click the Ubuntu button in the left-hand menu and search for Terminal



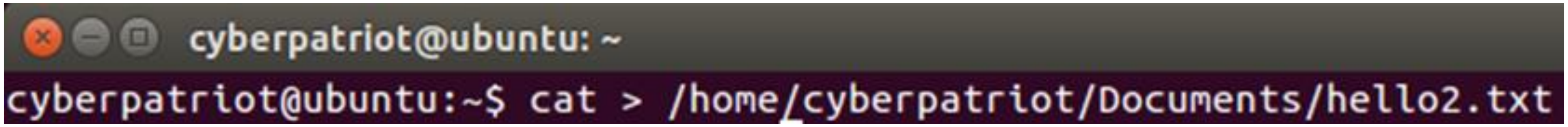
terminal

2. Create Text Document

- Type

```
cat -n > /home/cyberpatriot/Documents/hello2.txt
```

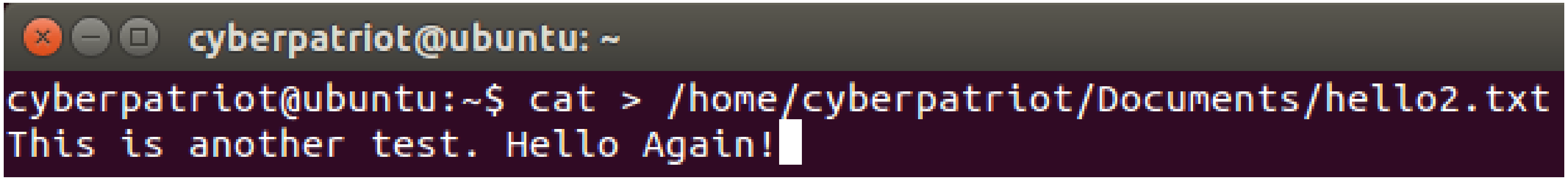
- Hit Enter



```
cyberpatriot@ubuntu:~$ cat > /home/cyberpatriot/Documents/hello2.txt
```

3. Add Text to Document

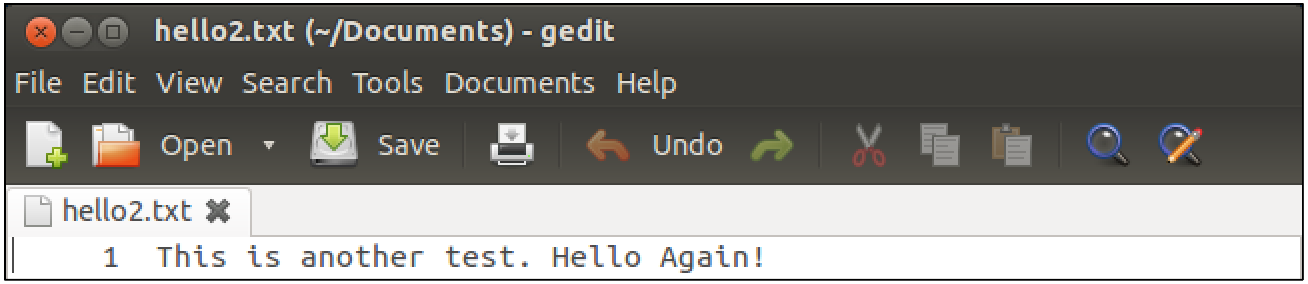
- Type `This is another test. Hello Again!`
- Hit Enter
- Type `Ctrl+D`



```
cyberpatriot@ubuntu:~$ cat > /home/cyberpatriot/Documents/hello2.txt
This is another test. Hello Again!
```

4. Open Document in the GUI

- Close the Terminal
- Open the Home Folder
- Navigate to the Documents folder
- Double-click the .txt file


hello2.txt (~/Documents) - gedit
File Edit View Search Tools Documents Help
Open
Save
Undo
hello2.txt

```
1  This is another test. Hello Again!
```

Command Syntax

- Rules that govern how command are written
- Similar to English grammar

```
The boy pet the dog.
```

- Subject – `The boy`
- Verb – `pet`
- Object – `the dog.`

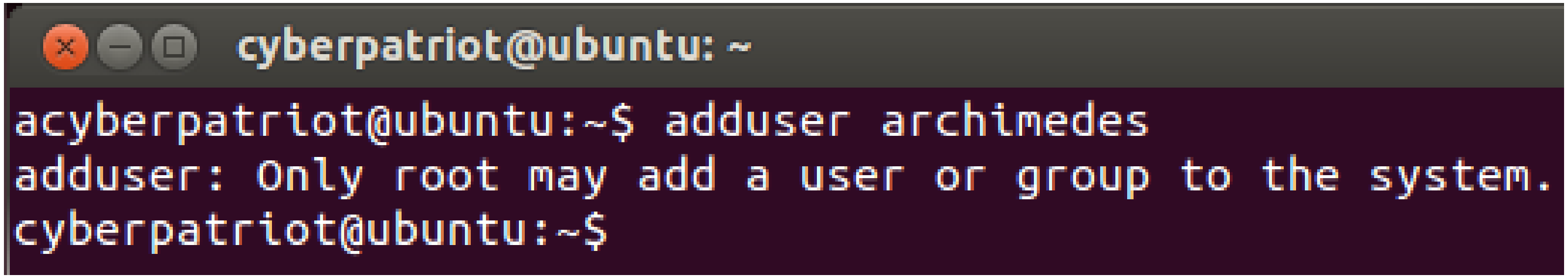
Command Syntax

```
cat -n > /home/cyberpatriot/Documents/hello2.txt
```

- Command: `cat`
- Option: `-n`
- Operator: `>`
- File Name/Location: `/home/cyberpatriot/Documents/hello2.txt`
- Format depends on the command

The sudo Command

- This command must be used to perform administrative tasks
- Example: adding a user
  - Type `adduser archimedes`
  - Hit `Enter`



```
acyberpatriot@ubuntu:~$ adduser archimedes
adduser: Only root may add a user or group to the system.
cyberpatriot@ubuntu:~$
```

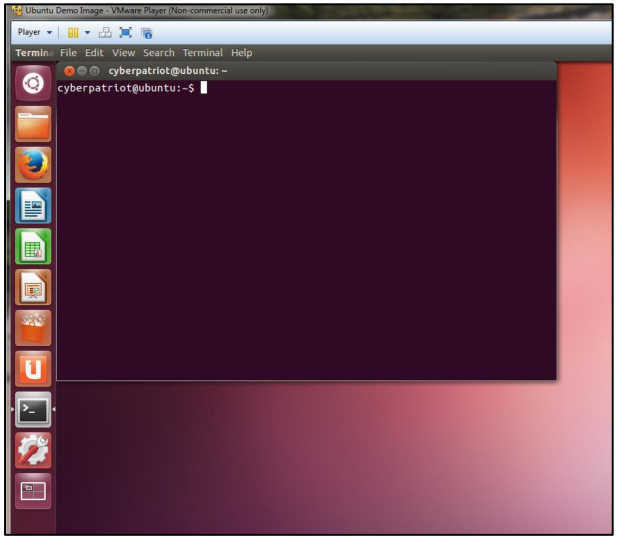
sudo Command Options

- **Sudo Command Option 1:**
  - Type `sudo adduser archimedes`
  - Hit `Enter` and Authenticate
  - Type a password for the user. You can add the other details but they are unnecessary.
  - Hit `Enter`
- **Sudo Command Option 2:**
  - Type `sudo su`
  - Hit `Enter` and Authenticate
  - Type `adduser riemann`
  - Hit `Enter`
  - Type a password for the user. You can add the other details but they are unnecessary.
  - Hit `Enter`

Activity 4-3: Command Line Lab

Instructions (Workbook Page 20):

- Complete the tasks outlined in your workbooks
- Do not change or delete anything not listed in your workbooks

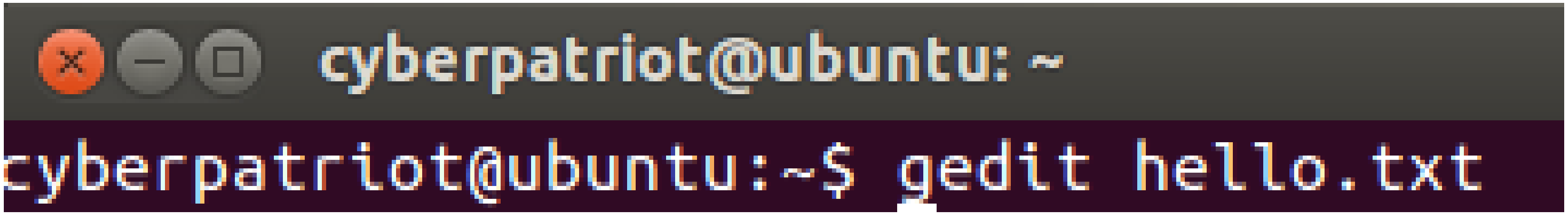


```
cyberpatriot@ubuntu:~$
```

Basic Command Line Security

The gedit Command

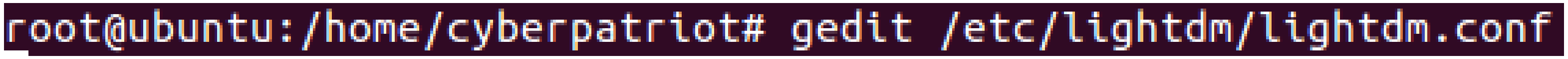
- One of many text editors
- Syntax: gedit [filepath]
- Root permissions occasionally required
- Type gedit hello.txt



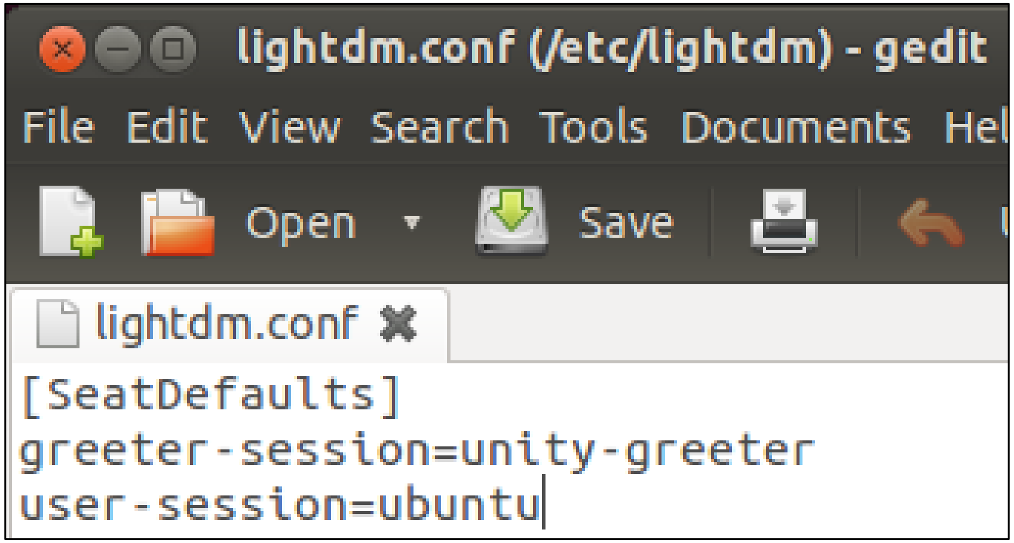
```
cyberpatriot@ubuntu:~$ gedit hello.txt
```

Turn off the Guest Account

- Turned on by default
- LightDM: display manager controlling the login screen
- Type `gedit /etc/lightdm/lightdm.conf`
  - Notice, sudo was <u>not</u> used
- Add the line `allow-guest=false` to the file



```
root@ubuntu:/home/cyberpatriot# gedit /etc/lightdm/lightdm.conf
```



```
[SeatDefaults]
greeter-session=unity-greeter
user-session=ubuntu
```

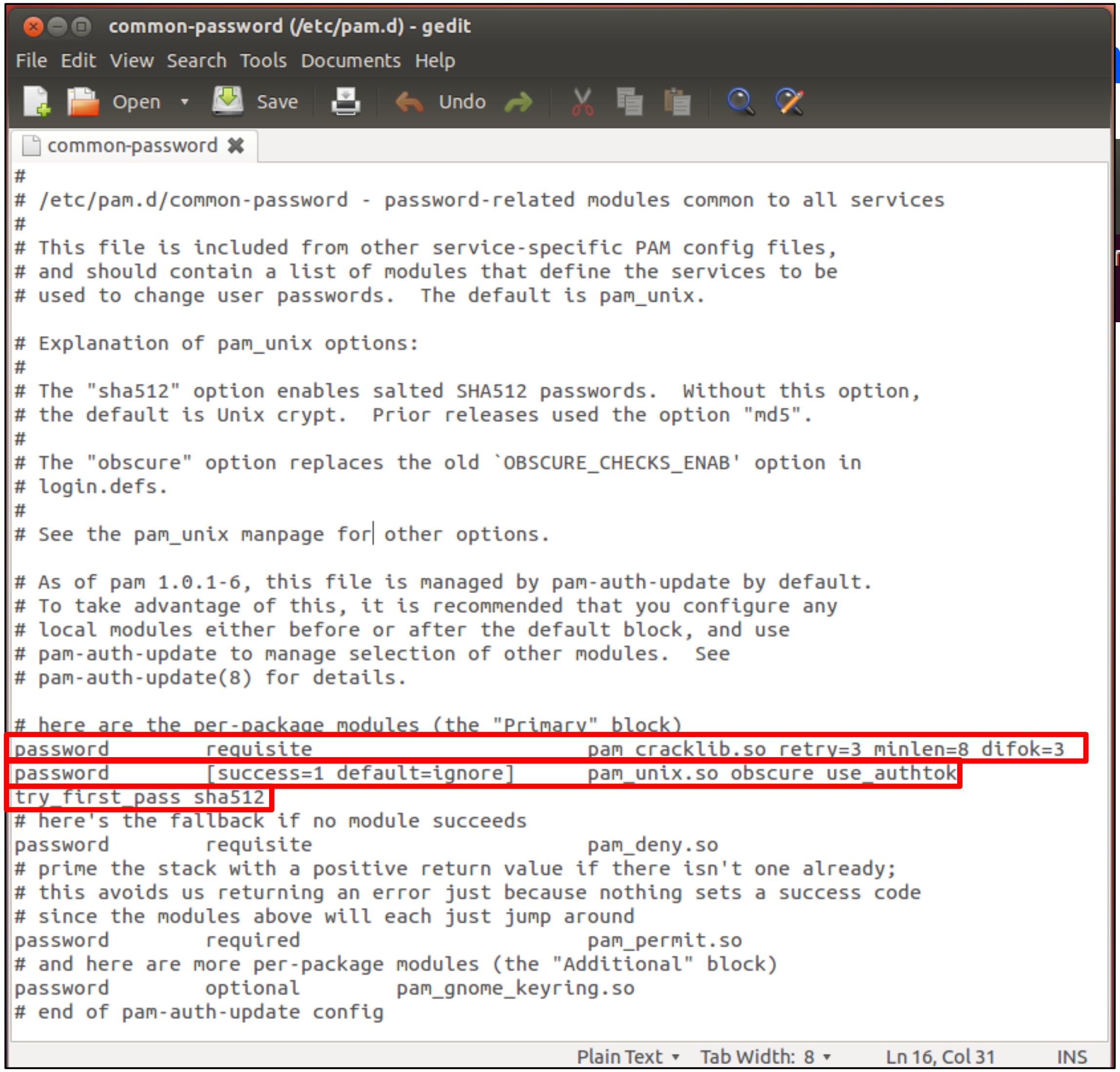
PAM (Pluggable Authentication Modules) Files

- Used for logon and applications
- Simplifies user authentication
- 4 types:
  - Account
  - Authentication
  - Password
  - Session

http://i.walmartimages.com/i/p/00/06/41/44/03/000641440303l_500X500.jpg

The Password File

Can you identify the error on the slide?



common-password (/etc/pam.d) - gedit
File Edit View Search Tools Documents Help
Open
Save
Undo
common-password

```
#
# /etc/pam.d/common-password - password-related modules common to all services
#
# This file is included from other service-specific PAM config files,
# and should contain a list of modules that define the services to be
# used to change user passwords.  The default is pam_unix.

# Explanation of pam_unix options:
#
# The "sha512" option enables salted SHA512 passwords.  Without this option,
# the default is Unix crypt.  Prior releases used the option "md5".
#
# The "obscure" option replaces the old `OBSCURE_CHECKS_ENAB' option in
# login.defs.
#
# See the pam_unix manpage for other options.

# 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)
password        requisite                       pam_cracklib.so retry=3 minlen=8 difok=3
password        [success=1 default=ignore]      pam_unix.so obscure use_authtok
try_first_pass sha512
# here's the fallback if no module succeeds
password        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
password        required                        pam_permit.so
# and here are more per-package modules (the "Additional" block)
password        optional        pam_gnome_keyring.so
# end of pam-auth-update config
```

on-password

rd

Password history:

Add "remember=5" to the end of this line.

Password length:

Add "minlen=8" to the end of this line.

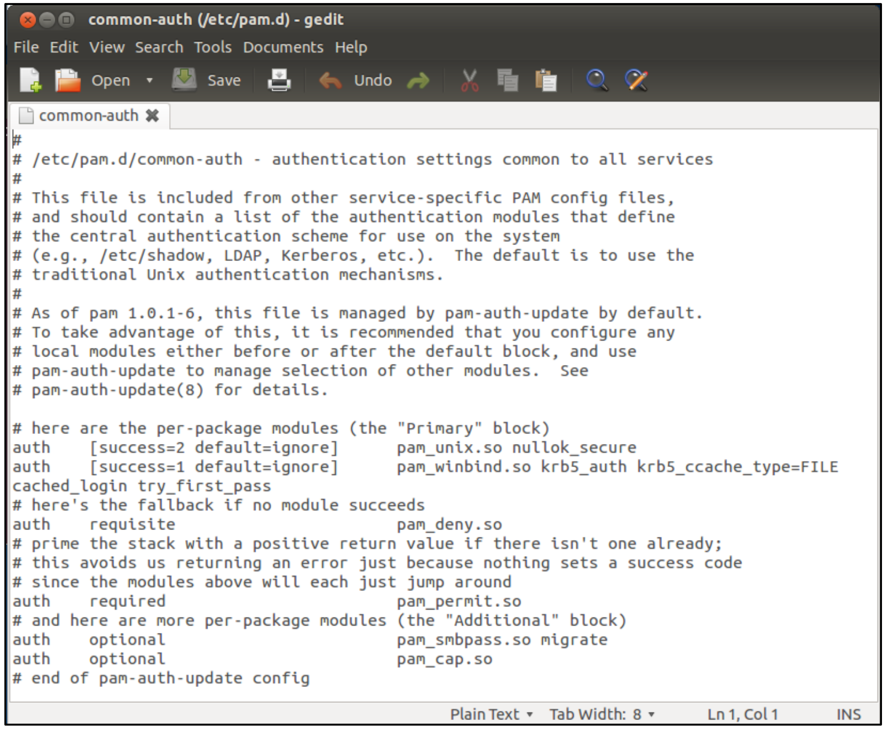
Password complexity:

Add "ucredit=-1 lcredit=-1 dcredit=-1 ocredit=-1" to the end of this line.

The Password File, cont.

- Password Complexity:
  - Add “ucredit=-1 (uppercase)
  - lcredit=-1 (lowercase)
  - dcredit=-1 (number)
  - ocredit=-1” (other characters !)
  - to the end of this line.
- **Note**: -1 means require one character of this type
- Information: **man pam_cracklib**

Account Policy: Number of Unsuccessful Login Attempts



```
#
# /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_winbind.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
```

- Type `gedit /etc/pam.d/common-auth`
- Add this line to the end of the file:

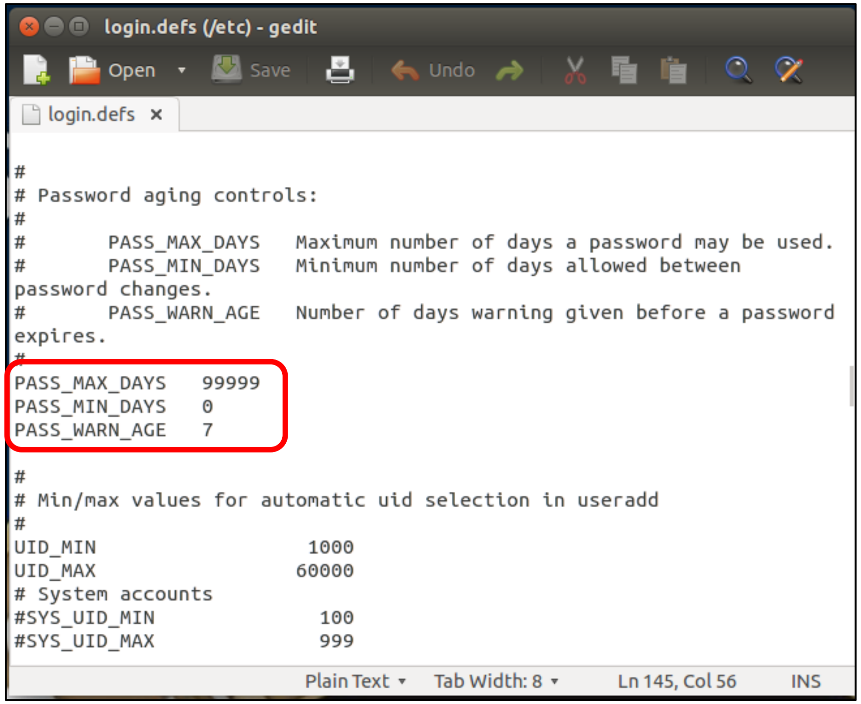
  `auth required pam_tally2.so deny=5 onerr=fail unlock_time=1800`

  `(30 minutes)`

More Password Policy

- Type `gedit /etc/login.defs`

Maximum Password Duration:	`PASS_MAX_DAYS`	`90`
Minimum Password Duration:	`PASS_MIN_DAYS`	`10`
Password Warning Before Expiration:	`PASS_WARN_AGE`	`7`



```
#
# 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
```

CYBERPATRIOT

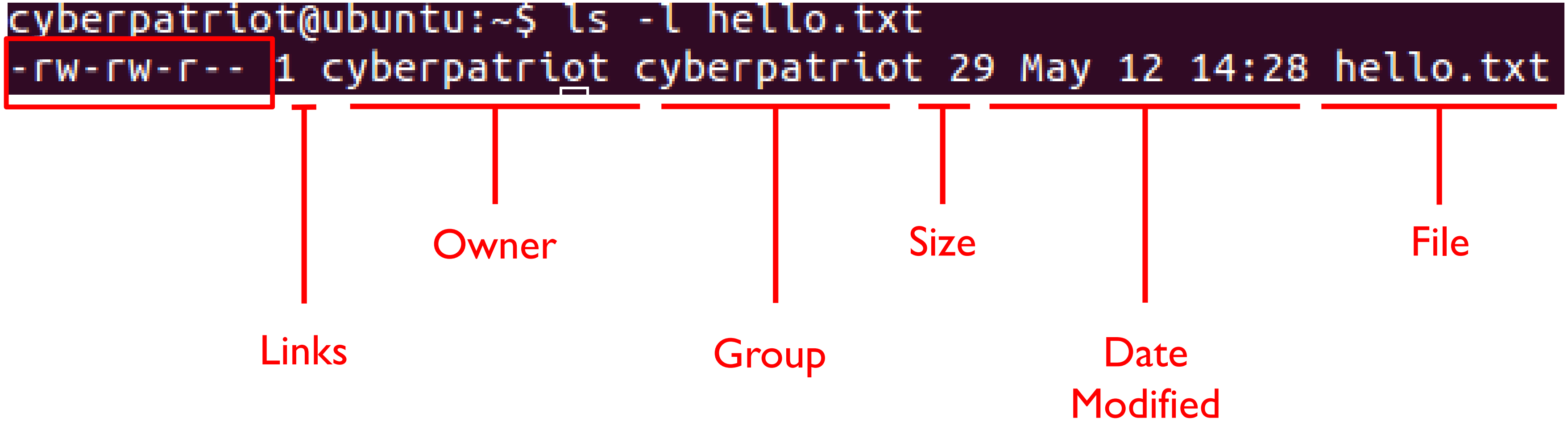
INTEGRITY, SERVICE, EXCELLENCE

NATIONAL YOUTH CYBER EDUCATION PROGRAM

Intermediate Ubuntu Security

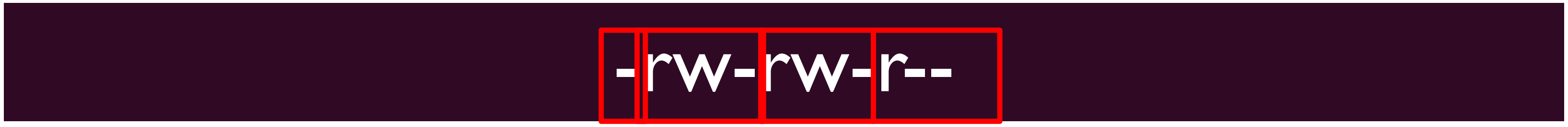
The ls Command

- Lists the contents and properties of a file or directory
- Syntax: `ls [option] [filepath]`
- `-l` option
- Type `ls -l hello.txt`



```
cyberpatriot@ubuntu:~$ ls -l hello.txt
-rw-rw-r-- 1 cyberpatriot cyberpatriot 29 May 12 14:28 hello.txt
```

Files Permissions

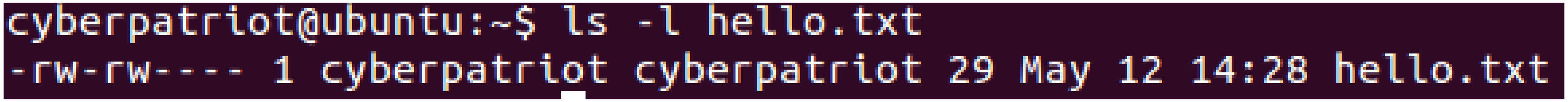


```
-rw-rw-r--
```

- 10 characters
  - **1. File Type**
    - Directory – d
    - File – ‘-’
  - **2-4. Owner File Permissions**
    - (Blank 2) Read - r
    - (Blank 3) Write/modify - w
    - (Blank 4) Execute – x
  - **5-7. Group File Permissions**
  - **8-10. Other File Permissions**

The chmod Command

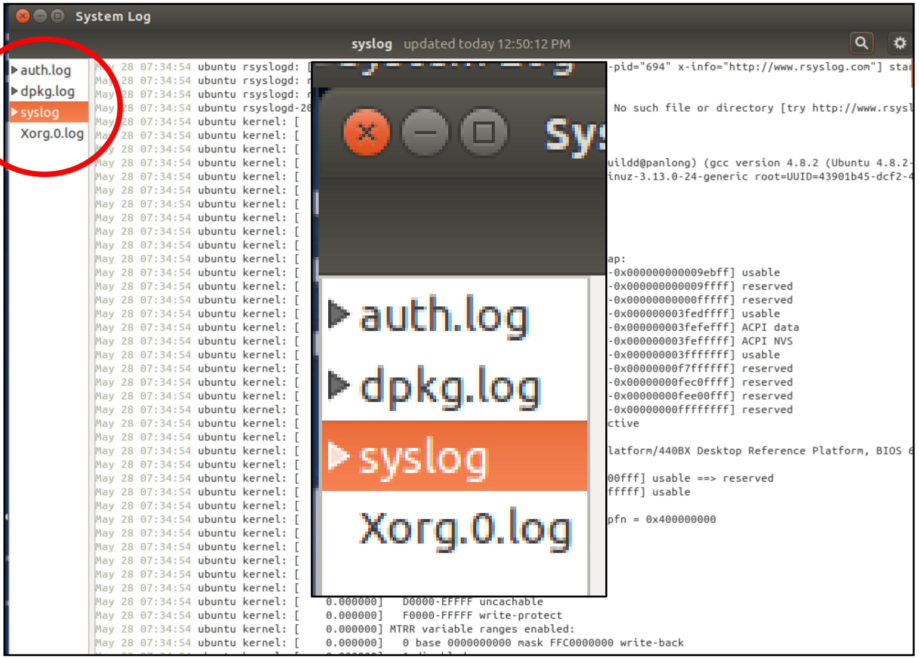
- Allows you to change file permissions
- Syntax `chmod [u,g or o]  [+ or -] [r,w or x] [filepath]`
- Type `chmod o-r hello.txt`
- Type `ls –l hello.txt`



```
cyberpatriot@ubuntu:~$ ls -l hello.txt
-rw-rw---- 1 cyberpatriot cyberpatriot 29 May 12 14:28 hello.txt
```

System Logs

- Similar to Windows Event Viewer
- From the Search field, type Log File Viewer
- Four types of logs
  - **auth.log:** Tracks authentication events
  - **dpkg.log:** Tracks software events
  - **syslog:** Tracks operating system events
  - **Xorg.0.log:** Tracks desktop events
- Can add different types of logs



syslog updated today 12:50:12 PM

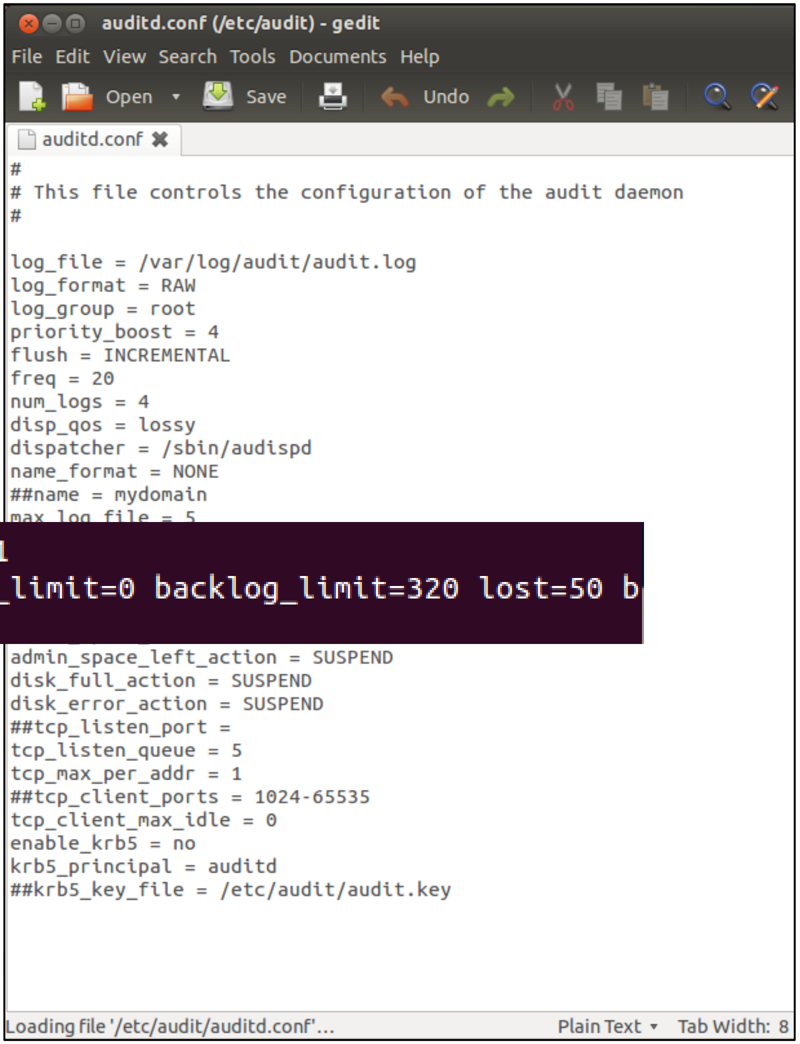
```
May 28 07:34:54 ubuntu rsyslogd: [                      -pid="694" x-info="http://www.rsyslog.com"] sta
May 28 07:34:54 ubuntu rsyslogd: r
May 28 07:34:54 ubuntu rsyslogd: r
May 28 07:34:54 ubuntu rsyslogd-20                       No such file or directory [try http://www.rsysl
May 28 07:34:54 ubuntu kernel: [
May 28 07:34:54 ubuntu kernel: [
May 28 07:34:54 ubuntu kernel: [
May 28 07:34:54 ubuntu kernel: [                        uildd@panlong) (gcc version 4.8.2 (Ubuntu 4.8.2-
May 28 07:34:54 ubuntu kernel: [                        inuz-3.13.0-24-generic root=UUID=43901b45-dcf2-4
May 28 07:34:54 ubuntu kernel: [
May 28 07:34:54 ubuntu kernel: [
May 28 07:34:54 ubuntu kernel: [
May 28 07:34:54 ubuntu kernel: [
May 28 07:34:54 ubuntu kernel: [
May 28 07:34:54 ubuntu kernel: [                        ap:
May 28 07:34:54 ubuntu kernel: [                        -0x000000000009ebff] usable
May 28 07:34:54 ubuntu kernel: [                        -0x000000000009ffff] reserved
May 28 07:34:54 ubuntu kernel: [                        -0x00000000000fffff] reserved
May 28 07:34:54 ubuntu kernel: [                        -0x000000003fedffff] usable
May 28 07:34:54 ubuntu kernel: [                        -0x000000003fefefff] ACPI data
May 28 07:34:54 ubuntu kernel: [                        -0x000000003fefffff] ACPI NVS
May 28 07:34:54 ubuntu kernel: [                        -0x000000003fffffff] usable
May 28 07:34:54 ubuntu kernel: [                        -0x00000000f7ffffff] reserved
May 28 07:34:54 ubuntu kernel: [                        -0x00000000fec0ffff] reserved
May 28 07:34:54 ubuntu kernel: [                        -0x00000000fee00fff] reserved
May 28 07:34:54 ubuntu kernel: [                        -0x00000000ffffffff] reserved
May 28 07:34:54 ubuntu kernel: [                        ctive
May 28 07:34:54 ubuntu kernel: [
May 28 07:34:54 ubuntu kernel: [                        latform/440BX Desktop Reference Platform, BIOS 6
May 28 07:34:54 ubuntu kernel: [
May 28 07:34:54 ubuntu kernel: [                        00fff] usable ==> reserved
May 28 07:34:54 ubuntu kernel: [                        fffff] usable
May 28 07:34:54 ubuntu kernel: [
May 28 07:34:54 ubuntu kernel: [                        pfn = 0x400000000
May 28 07:34:54 ubuntu kernel: [
May 28 07:34:54 ubuntu kernel: [
May 28 07:34:54 ubuntu kernel: [
May 28 07:34:54 ubuntu kernel: [
May 28 07:34:54 ubuntu kernel: [
May 28 07:34:54 ubuntu kernel: [    0.000000]   D0000-EFFFF uncachable
May 28 07:34:54 ubuntu kernel: [    0.000000]   F0000-FFFFF write-protect
May 28 07:34:54 ubuntu kernel: [    0.000000] MTRR variable ranges enabled:
May 28 07:34:54 ubuntu kernel: [    0.000000]   0 base 0000000000 mask FFC0000000 write-back
```

Audit Policies

- Unlike Windows, auditing is <u>not</u> set up by default in Ubuntu
- Three step process
  - To install, type `apt-get install auditd`
  - To enable, type `auditctl -e 1`

```
[sudo] password for cyberpatriot:
root@ubuntu:/home/cyberpatriot# auditctl -e 1
AUDIT_STATUS: enabled=1 flag=1 pid=4229 rate_limit=0 backlog_limit=320 lost=50 b
acklog=0
```

  - To modify, type `gedit /etc/audit/auditd.conf`



auditd.conf (/etc/audit) - gedit
File Edit View Search Tools Documents Help
Open
Save
Undo
auditd.conf

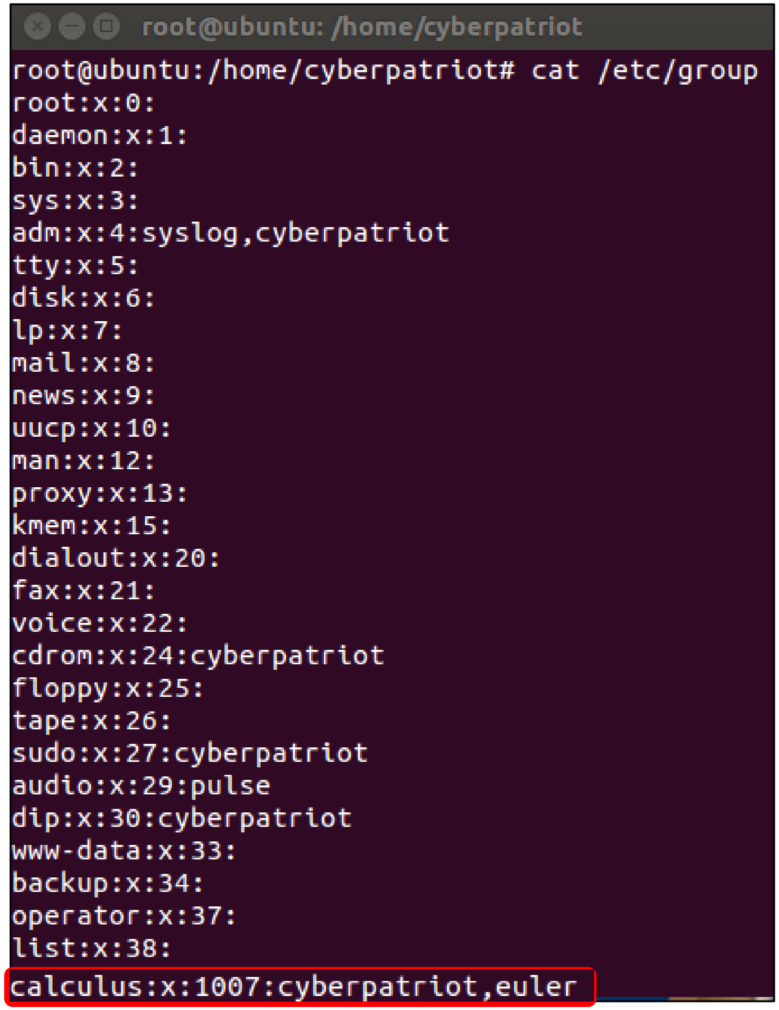
```
#
# This file controls the configuration of the audit daemon
#

log_file = /var/log/audit/audit.log
log_format = RAW
log_group = root
priority_boost = 4
flush = INCREMENTAL
freq = 20
num_logs = 4
disp_qos = lossy
dispatcher = /sbin/audispd
name_format = NONE
##name = mydomain
max_log_file = 5
```

```
admin_space_left_action = SUSPEND
disk_full_action = SUSPEND
disk_error_action = SUSPEND
##tcp_listen_port =
tcp_listen_queue = 5
tcp_max_per_addr = 1
##tcp_client_ports = 1024-65535
tcp_client_max_idle = 0
enable_krb5 = no
krb5_principal = auditd
##krb5_key_file = /etc/audit/audit.key
```

Groups

- Work very similarly to Windows
- To list all groups: `cat /etc/group`
- To add a group: `addgroup [groupname]`
- To add a user to a group: `adduser [username] [groupname]`

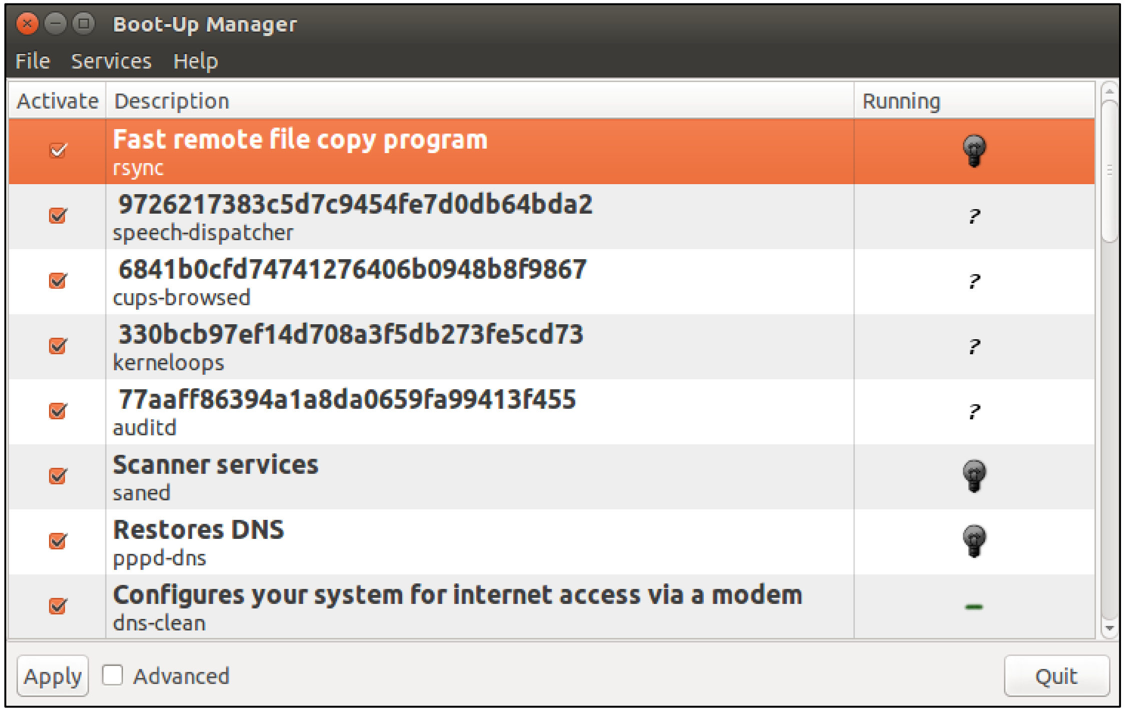


```
root@ubuntu:/home/cyberpatriot# cat /etc/group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:syslog,cyberpatriot
tty:x:5:
disk:x:6:
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
kmem:x:15:
dialout:x:20:
fax:x:21:
voice:x:22:
cdrom:x:24:cyberpatriot
floppy:x:25:
tape:x:26:
sudo:x:27:cyberpatriot
audio:x:29:pulse
dip:x:30:cyberpatriot
www-data:x:33:
backup:x:34:
operator:x:37:
list:x:38:
calculus:x:1007:cyberpatriot,euler
```

Services

- Can be run in the GUI
- To install, type `apt-get install bum`
- To run, type `bum`

Search using boot
Click BootUp-Manager

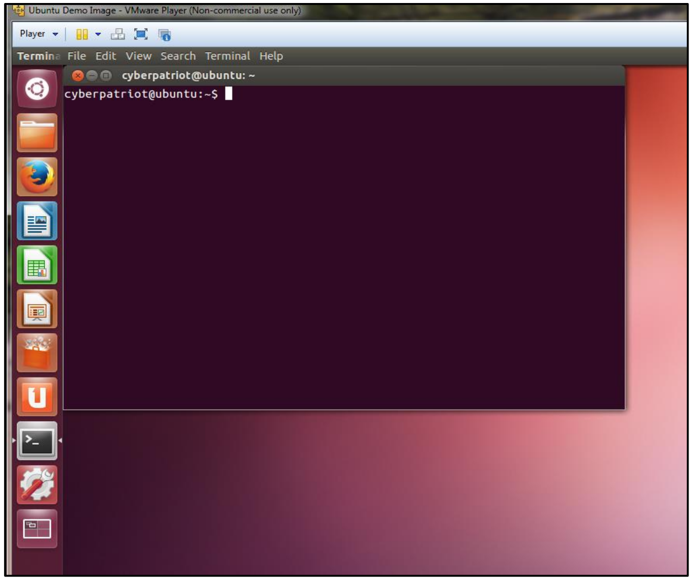


Activate	Description	Running
☑	**Fast remote file copy program** rsync	💡
☑	**9726217383c5d7c9454fe7d0db64bda2** speech-dispatcher	?
☑	**6841b0cfd74741276406b0948b8f9867** cups-browsed	?
☑	**330bcb97ef14d708a3f5db273fe5cd73** kerneloops	?
☑	**77aaff86394a1a8da0659fa99413f455** auditd	?
☑	**Scanner services** saned	💡
☑	**Restores DNS** pppd-dns	💡
☑	**Configures your system for internet access via a modem** dns-clean	–

Activity 4-4: Command Line Security Lab

Instructions (Workbook Page 21):

- Complete the tasks outlined in your workbooks
- Do not change or delete anything not listed in your workbooks



```
cyberpatriot@ubuntu:~$
```

Linux Conclusion

- Ubuntu and other Linux operating systems are both very similar and very different to Windows operating systems
- Ubuntu is vulnerable to many of the same problems as Windows systems
- Securing Ubuntu requires some knowledge of the command line environment