Cyber-Security Checklist Linux

By Michael

- **To edit files, run gedit, a graphical editor akin to notepad; nano, a simple command-line editor; or vim, a powerful but less intuitive command-line editor. Note that vim may need to be installed with apt-get install vim. Make sure to add sudo to edit read-only files**

Install Malware Protection

- ❏ ClamAV or ClamTK

Manage Accounts

- ❏ Remove guest user
- ❏ Remove old accounts
- ❏ Ensure all accounts use strong passwords
- ❏ Make sure the correct admins are the only admins

Delete Suspicious Files/Apps

- ❏ Write down file names and locations that were deleted

Enabling the Firewall

- ❏ Services (Also called a daemon)
- ❏ Disable unnecessary services
- ❏ Attach Detection
- ❏ Monitor your processes
- ❏ Port Checks
- ❏ System Logs (syslog)

Installing and Updates

- ❏ Install Updates **sudo apt-get update**
- ❏ **sudo apt-get upgrade**
- ❏ **sudo apt-get dist-upgrade**

1. Read the readme
2. Note down which ports/users are allowed.
3. Do Forensics Questions
4. You may destroy the requisite information if you work on the checklist!
5. Secure root
6. set PermitRootLogin no in /etc/ssh/sshd_config
7. Secure Users
    i. Disable the guest user.
    ii. Go to /etc/lightdm/lightdm.conf and add the line
    iii. allow-guest=false
    iv. Then restart your session with sudo restart lightdm. This will log you out, so make sure you are not executing anything important.
    v. Open up /etc/passwd and check which users
        a. Are uid 0
        b. Can login
        c. Are allowed in the readme
    vi. Delete unauthorized users:
    vii. sudo userdel -r $user
    viii. sudo groupdel $user
    ix. Check /etc/sudoers.d and make sure only members of group sudo can sudo.
    x. Check /etc/group and remove non-admins from sudo and admin groups.
    xi. Check user directories.
        a. cd /home
        b. sudo ls -Ra *
        c. Look in any directories which show up for media files/tools and/or "hacking tools."
    xii. Enforce Password Requirements.
        a. Add or change password expiration requirements to /etc/login.defs.
        b. PASS_MIN_DAYS 7

           PASS_MAX_DAYS 90

           PASS_WARN_AGE 14

        c. Add a minimum password length, password history, and add complexity requirements.
            a. Open /etc/pam.d/common-password with sudo.
            b. Add minlen=8 to the end of the line that has pam_unix.so in it.
            c. Add remember=5 to the end of the line that has pam_unix.so in it.
            d. Locate the line that has pam.cracklib.so in it. If you cannot find that line, install cracklib with sudo apt-get install libpam-cracklib.
            e. Add ucredit=-1 lcredit=-1 dcredit=-1 ocredit=- to the end of that line.
        d. Implement an account lockout policy.
            a. Open /etc/pam.d/common-auth.
            b. Add deny=5 unlock_time=1800 to the end of the line with pam_tally2.so in it.
        e. Change all passwords to satisfy these requirements.
        f. chpasswd is very useful for this purpose.
8. Enable automatic updates
9. In the GUI set Update Manager->Settings->Updates->Check for updates:->Daily.
10. Secure ports
    i. sudo ss -ln
    ii. If a port has 127.0.0.1:$port in its line, that means it's connected to loopback and isn't exposed. Otherwise, there should only be ports which are specified in the readme open (but there probably will be tons more).
    iii. For each open port which should be closed:
        a. sudo lsof -i :$port
        b. Copy the program which is listening on the port. whereis $program
        c. Copy where the program is (if there is more than one location, just copy the first one). dpkg -S $location
        d. This shows which package provides the file (If there is no package, that means you can probably delete it with rm $location; killall -9 $program). sudo apt-get purge $package
        e. Check to make sure you aren't accidentally removing critical packages before hitting "y".
        f. sudo ss -l to make sure the port actually closed.
11. Secure network
    i. Enable the firewall
    ii. sudo ufw enable
    iii. Enable syn cookie protection
    iv. sysctl -n net.ipv4.tcp_syncookies
    v. Disable IPv6 (Potentially harmful)
    vi. sudo echo "net.ipv6.conf.all.disable_ipv6 = 1" >> /etc/sysctl.conf
    vii. Disable IP Forwarding
    viii. sudo echo 0 > /proc/sys/net/ipv4/ip_forward
    ix. Prevent IP Spoofing
    x. sudo echo "nospoof on" >> /etc/host.conf
12. Install Updates
13. Start this before half-way.
    i. Do general updates.
        a. sudo apt-get update.
        b. sudo apt-get upgrade.
    ii. Update services specified in readme.
        a. Google to find what the latest stable version is.
        b. Google "ubuntu install service version".
        c. Follow the instructions.
    iii. Ensure that you have points for upgrading the kernel, each service specified in the readme, and bash if it is vulnerable to shellshock.
14. Configure services
    i. Check service configuration files for required services. Usually a wrong setting in a config file for sql, apache, etc. will be a point.
    ii. Ensure all services are legitimate.
    iii. service --status-all
15. Check the installed packages for "hacking tools," such as password crackers.
16. Run other (more comprehensive) checklists. This is checklist designed to get most of the common points, but it may not catch everything.

AIR FORCE ASSOCIATION'S

CYBERPATRIOT

NATIONAL YOUTH CYBER EDUCATION PROGRAM

UNIT EIGHT

Ubuntu Security

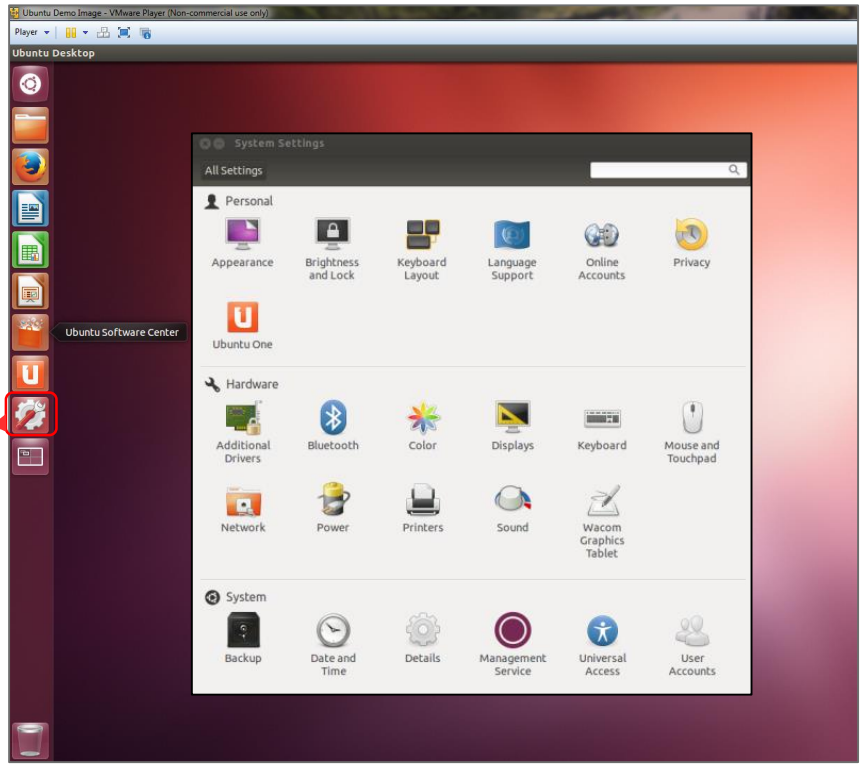
www.uscyberpatriot.org

SECTION ONE

Basic GUI Security

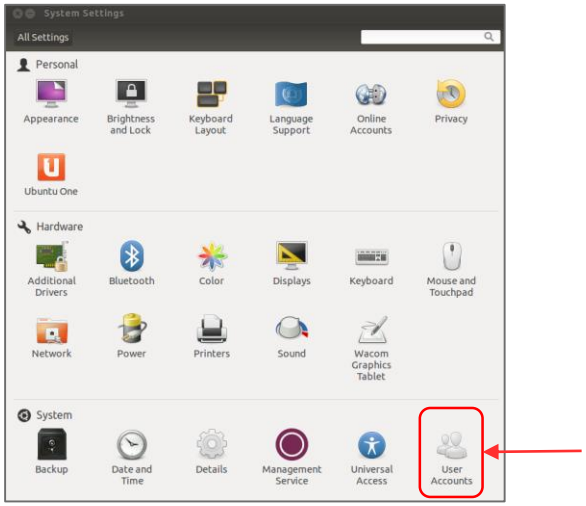
Basic Linux Security

- This unit will show you how to make many of the same security settings you made in Unit 5
  - Linux has many of the same vulnerabilities, so the fixes are similar
- Linux does not have a Control Panel like in Windows
- The System Settings menu offers limited security tools
- Click the System Settings button in the menu bar

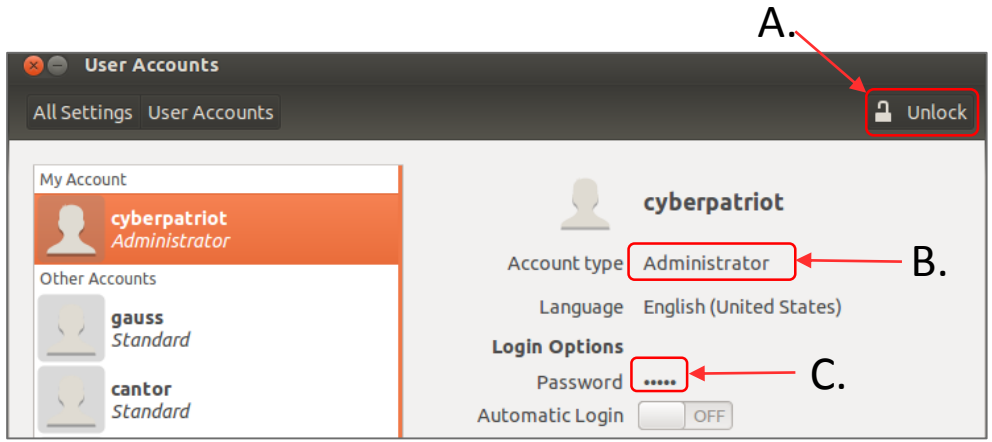


User Accounts

1.



2.



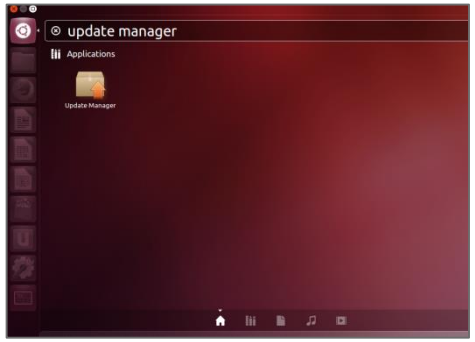
- Click User Accounts in the System Settings window
- As in Windows, it is important to restrict root (Admin) privileges and password protect all accounts
  - A. To make account management changes, you must enact root permissions by clicking Unlock and authenticate yourself by entering your password
  - 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

Installing and Automating Updates

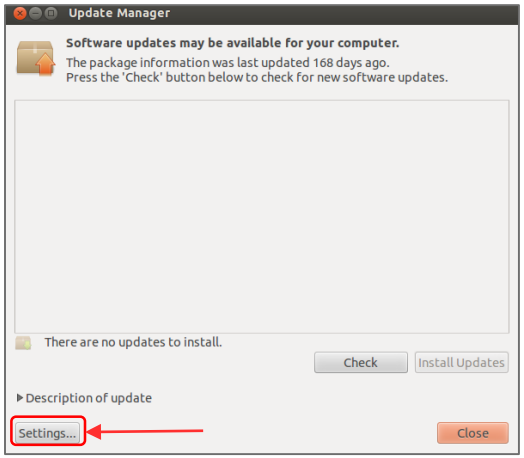
- The open-source community regularly develops improvements and patches for Ubuntu
- You should install these updates regularly

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

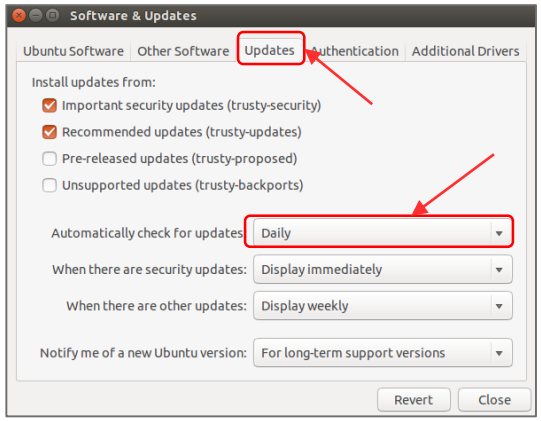
1.



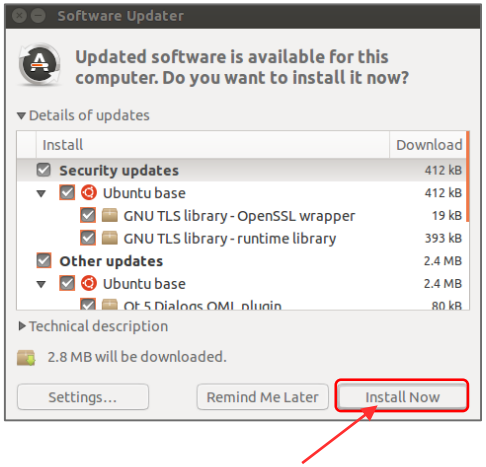
2.



3.

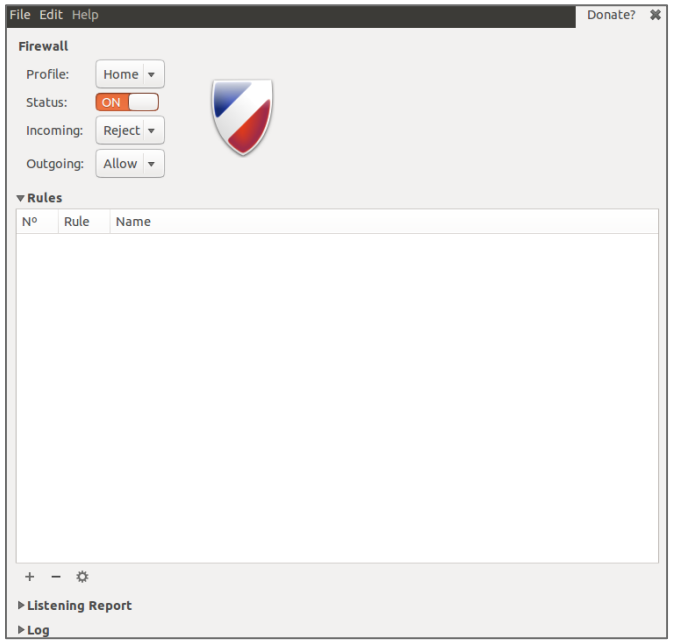


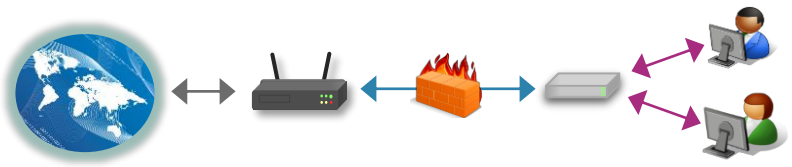
4.



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

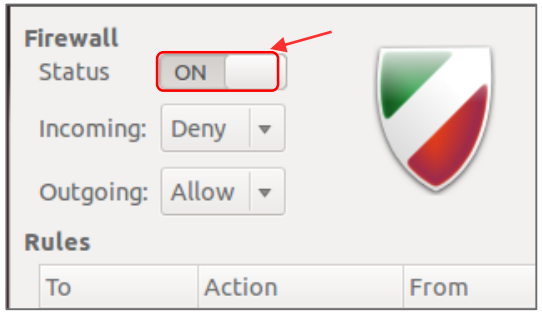




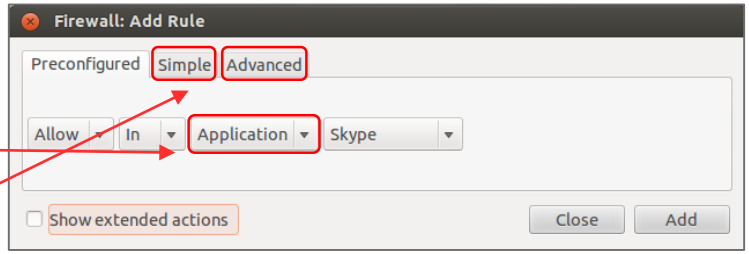
Source: https://help.ubuntu.com/community/UFW

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

SECTION TWO

Basic Command Line Security

The gedit Command

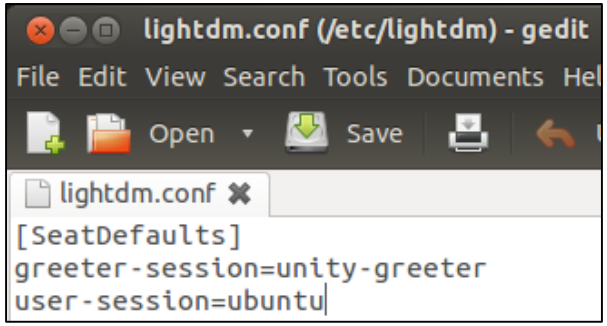
- Gedit is one of many text editor commands in Ubuntu
  - Syntax: gedit [filepath]
  - Unlike with other text editors, using gedit will cause a second window to pop-up where you can easily change the text of a file
  - This command will allow you to edit security policy files
- You need to enact root 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

PAM Files

- Pluggable Authentication Modules (PAM) are used for logon and applications
- They simplify user authentication
  - They *do not* govern authorization (i.e. grant privileges to users)
- 4 types of PAM files:
  - Account – control account conditions (e.g. not expired, etc.)
  - Authentication – verify user identities
  - Password – control some password policies
  - Session – define actions performed at the beginning and end of user sessions.

Source: http://i.walmartimages.com/i/p/00/06/41/44/03/0006414403031_500X500.jpg

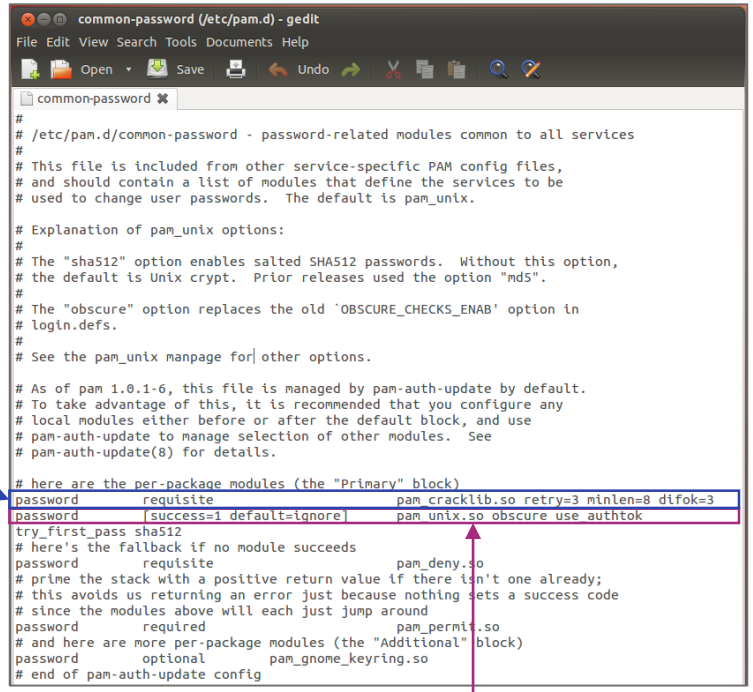
Source: http://www.linux-mag.com/id/7887/

Editing the PAM Password File

- Type `gedit /etc/pam.d/common-password`
- Lines in the file starting with "#" are comments to help the user understand the file. They do not enforce any policies.
- After making changes, save the file and close it.

1. To enforce password history of 5 :
Add "`remember=5`" to the end of the line that has "pam_unix.so" in it.

2. To enforce Password length of 8:
Add "`minlen=8`" to the end of the line that has "pam_unix.so" in it



3. To enforce password complexity with one of each type of character:*
Add "`ucredit=-1 lcredit=-1 dcredit=-1 ocredit=-1`" to the end of the line with "pam_cracklib.so" in it.**

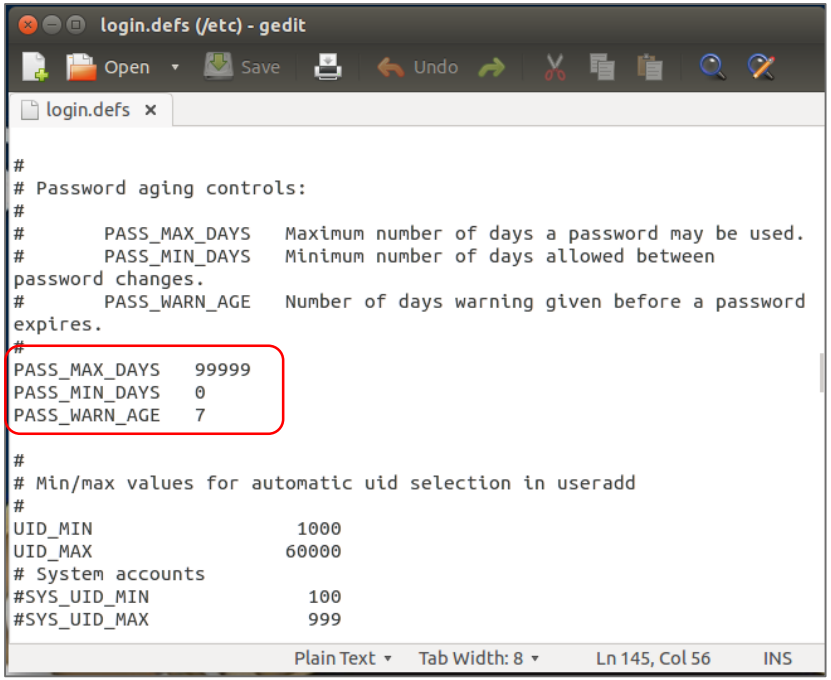
*ucredit = upper case, lcredit=lower case, dcredit = number and ocredit = symbol

**cracklib may need to be installed before enforcing password complexity

Source: http://www.deer-run.com/~hal/sysadmin/pam_cracklib.html

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



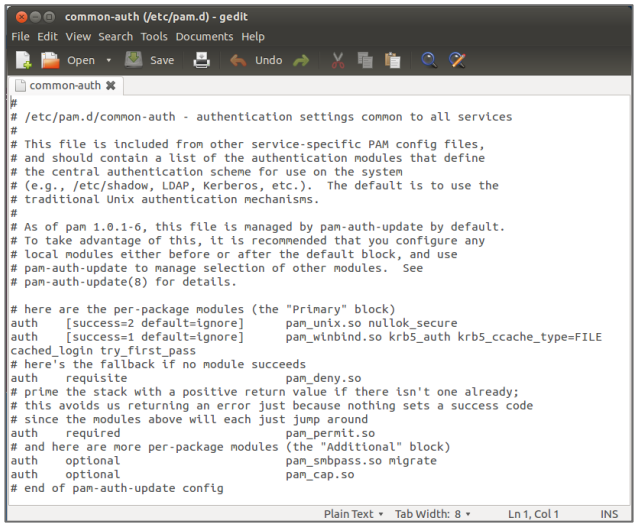
Sources: http://xmodulo.com/2013/12/set-password-policy-linux.html,

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



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

SECTION THREE

Advanced Ubuntu security

The `ls` Command

- The `ls` command (lower case "L") lists the contents and properties of a file or directory
- Syntax: `ls [option] [filepath]`
  - `-l` is a common option (lower case "L"), which provides the user with more details about the file or directory
- Example: `ls -l hello2.txt` will yield a description similar to the one below (exact details may differ)

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

Links (refers to how many files, folder, and shortcuts link to this file)

Owner (user who created the file)

Group (user's group when file was created)

Size (kb)

Date Modified

File

Viewing File Permissions with the `ls` Command

- File permissions are the first items noted when using the `ls` command with the `-l` option
- File permissions are split into the 10 fields outlined below
- If any fields are blank, the users in that section cannot do that action with the file

1. Type: if this says "d," the item in question is a directory. A blank means it is a file.

2-4. Owner File Permissions: what the user can do with the file or directory

(Blank 2) Read - r

(Blank 3) Write/modify - w

(Blank 4) Execute – x

5-7. Group File Permissions

(Blank 2) Read - r

(Blank 3) Write/modify - w

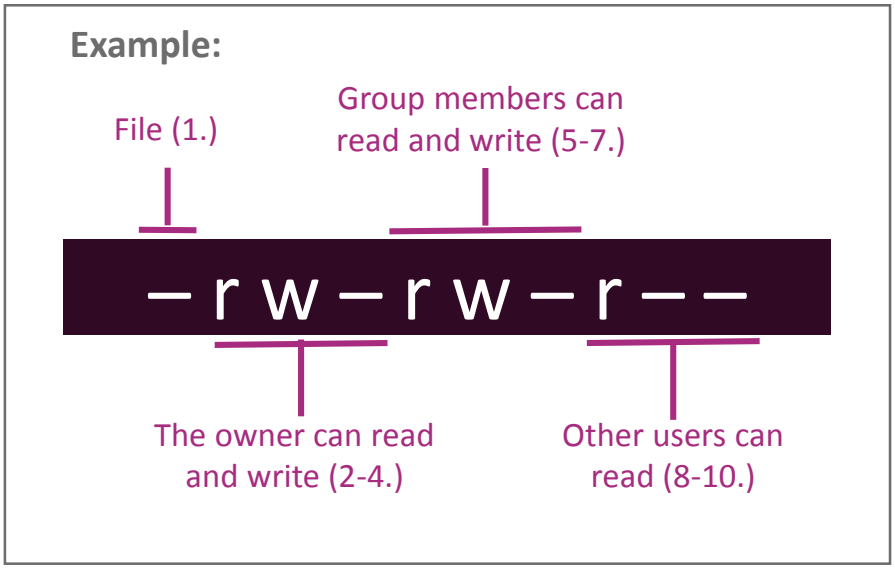
(Blank 4) Execute – x

8-10. Other File Permissions

(Blank 2) Read - r

(Blank 3) Write/modify - w

(Blank 4) Execute – x



The chmod Command

- Chmod allows you to change file permissions

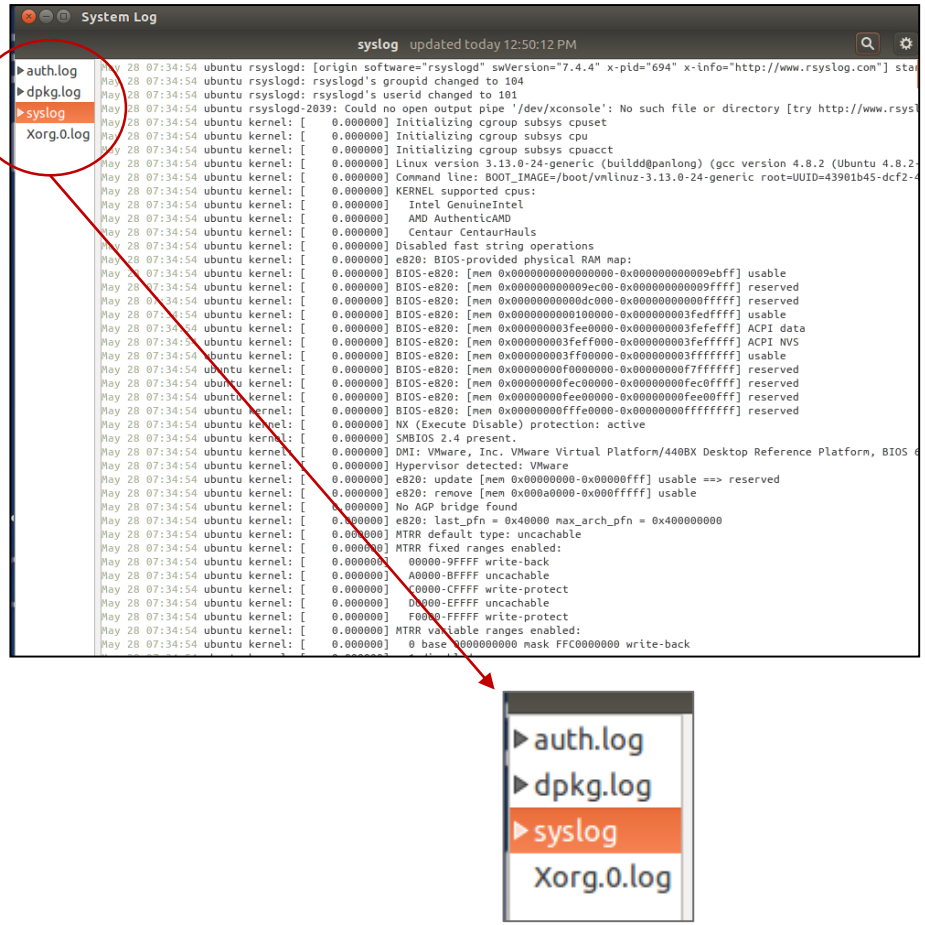
- Syntax: `chmod [u,g or o][+ or -][r,w, or x] [filepath]`
  - Do not put spaces between the three fields after "chmod"
- Example:
  1. Type `chmod o-r hello2.txt`
  2. Type `ls –l hello2.txt`
  3. If your permissions originally matched those on the last slide, you should see hello2.txt's new file permissions 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

System Logs

- Similar to Windows Event Viewer
- From the Search field in the Ubuntu menu on the left of the desktop, type System Log to view available logs
- Four types of logs
  - **auth.log**: Tracks authentication events that prompt for user passwords (e.g., uses of PAM files and sudo)
  - **dpkg.log:** Tracks software events (e.g., installations and updates)
  - **syslog**: Tracks operating system events (e.g. error messages)
  - **Xorg.0.log:** Tracks desktop events (e.g., service changes and graphic card errors.
- Can add different types of logs

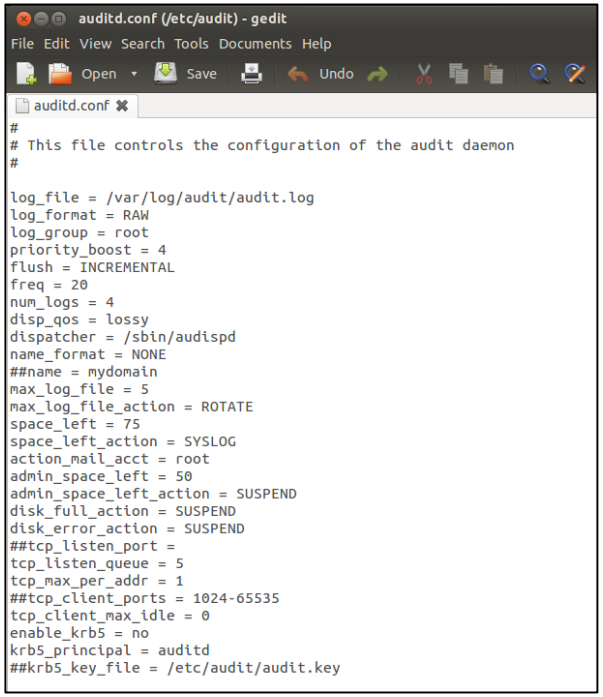


Sources: http://debian-handbook.info/browse/stable/sect.manipulating-packages-with-dpkg.html, http://ubuntuforums.org/showthread.php?t=900245

Setting Audit Policies

- Unlike Windows, auditing is not set up by default in Ubuntu
- Three step process to setting up audits:
  1. Install the auditing program by typing `apt-get install auditd`
  2. Enable audits by typing `auditctl -e 1`
  3. View and modify policies by typing `gedit /etc/audit/auditd.conf`

3.



2.

```
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
```

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:

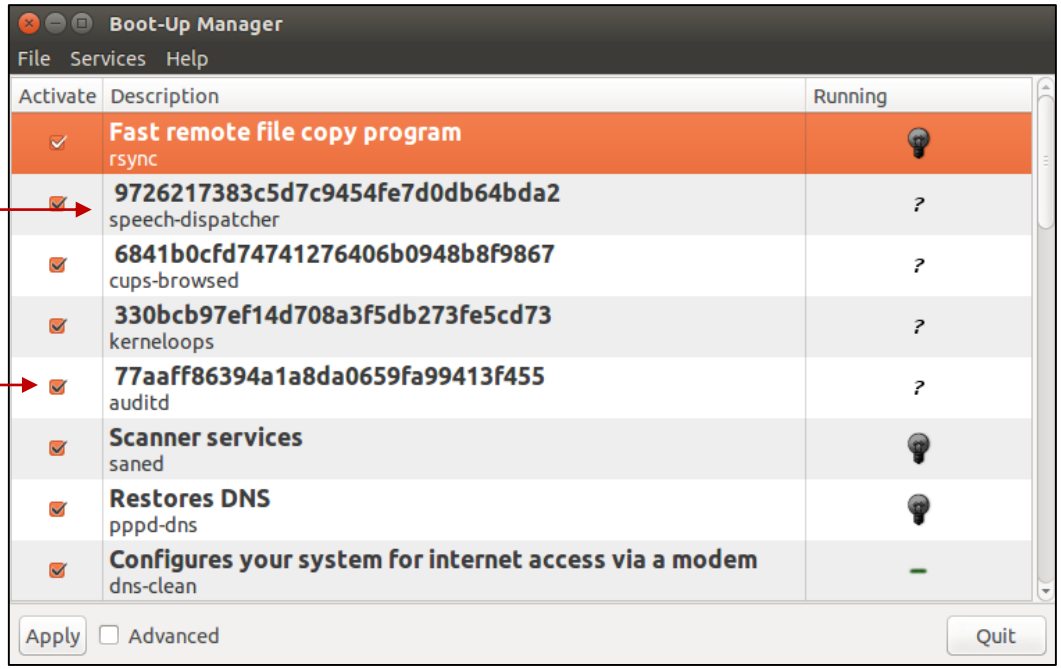
     `adduser [username] [groupname]`

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.