UNIT EIGHT

Ubuntu Security
SECTION ONE

Basic GUI 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. Click User Accounts in the System Settings window
2. 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
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`
  - 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,
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://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](http://www.deer-run.com/~hal/sysadmin/pam_cracklib.html)
• 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](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](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 hello2.txt
```

<table>
<thead>
<tr>
<th>Owner (user who created the file)</th>
<th>Group (user’s group when file was created)</th>
<th>Size (kb)</th>
<th>Date Modified</th>
<th>File Links (refers to how many files, folder, and shortcuts link to this file)</th>
</tr>
</thead>
<tbody>
<tr>
<td>cyberpatriot</td>
<td>cybercamp</td>
<td>57</td>
<td>May 29 09:34</td>
<td>1</td>
</tr>
</tbody>
</table>
• 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

---

**Example:**

```
- r w - r w - r --
```

- The owner can read and write (2-4.)
- Group members can read and write (5-7.)
- Other users can read (8-10.)
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 hello2.txt
```

Sources: [http://condor.depaul.edu/dpowebpg/support/chmod.html](http://condor.depaul.edu/dpowebpg/support/chmod.html), [https://help.ubuntu.com/community/FilePermissions](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

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`
Groups

• Work very similarly to Windows
  - Root permissions are required
1. To list all groups:  
  \( \text{cat} \ 	ext{/etc/group} \)
2. To add a group:  
  \( \text{addgroup} \ [\text{groupname}] \)
3. To add a user to a group:  
  \( \text{adduser} \ [\text{username}] \ [\text{groupname}] \)
- 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.