AIR FORCE ASSOCIATION'S

CYBERPATRIOT

NATIONAL YOUTH CYBER EDUCATION PROGRAM

UNIT EIGHT

Ubuntu Security

www.uscyberpatriot.org

AIR FORCE ASSOCIATION'S

CYBERPATRIOT

NATIONAL YOUTH CYBER EDUCATION PROGRAM

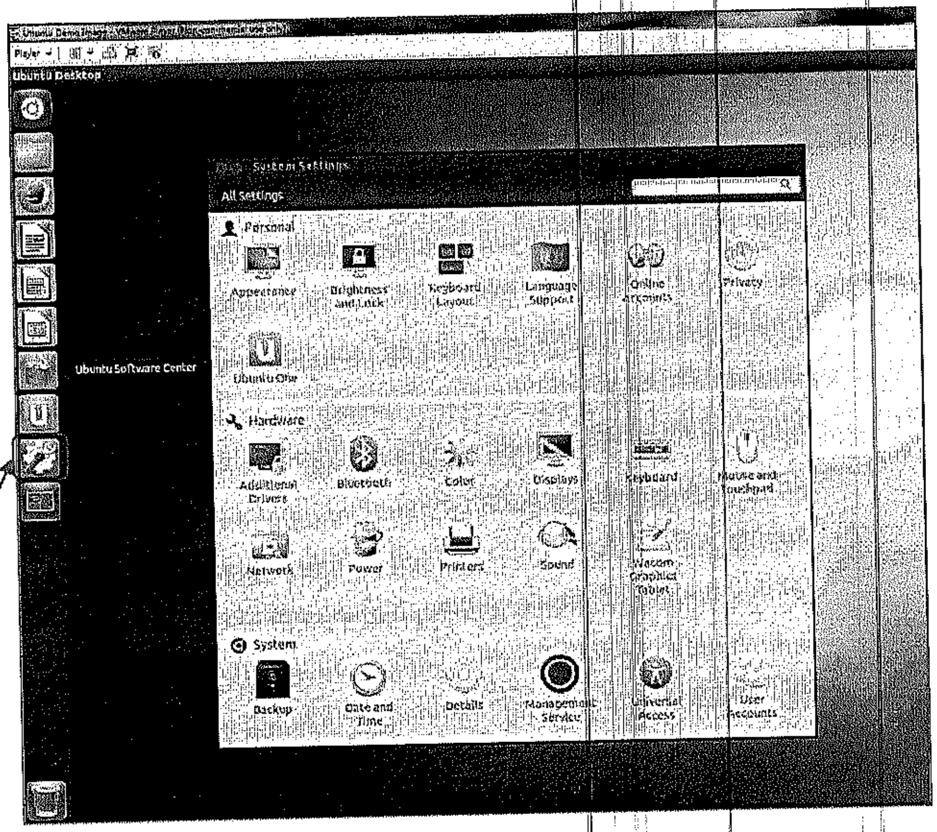
SECTION ONE

Basic GUI Security

www.uscyberpatriot.org

Basic Linux Security

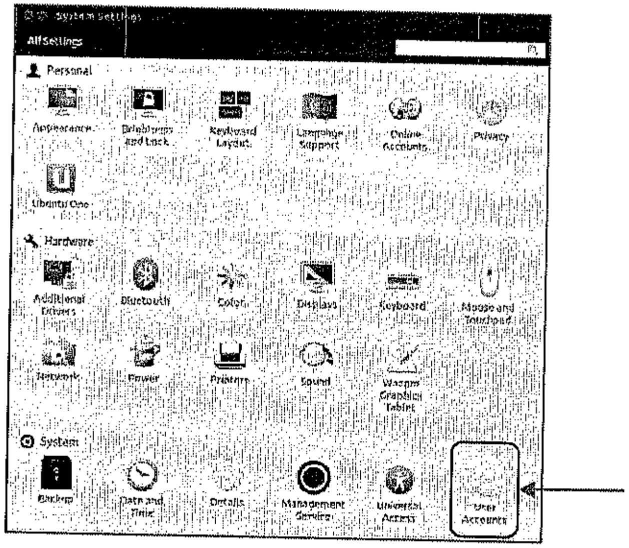
- This unit will show you how to make many of the same security settings you made in Unit 5
  - Linux has many of the same vulnerabilities, so the fixes are similar
- Linux does not have a Control Panel like in Windows
- The System Settings menu offers limited security tools
- Click the System Settings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



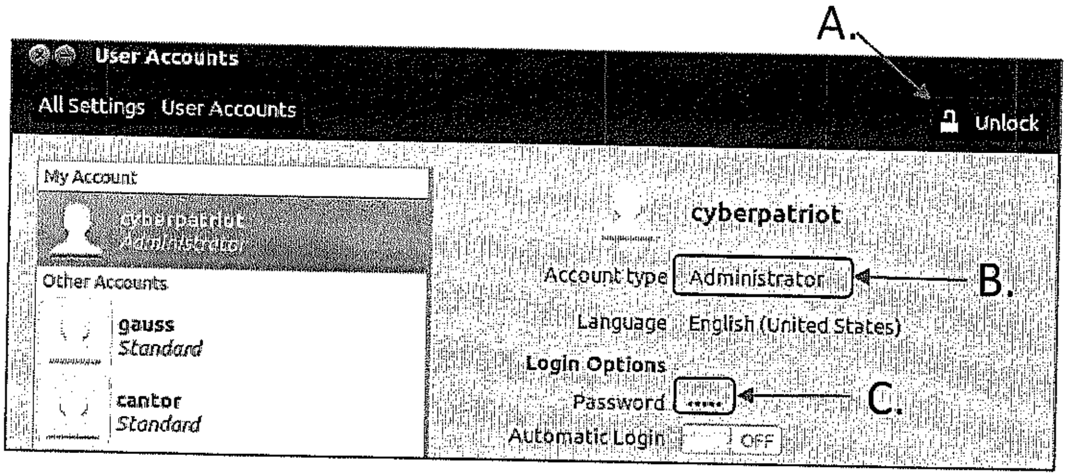
© Air Force Association

User Accounts

1.



2.



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

- 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

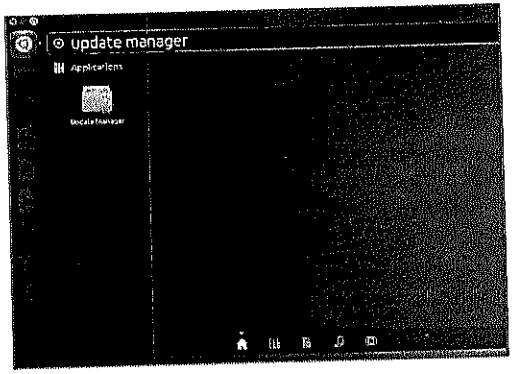
  C. Change passwords by clicking the asterisks next to the Password option

Installing and Automating Updates

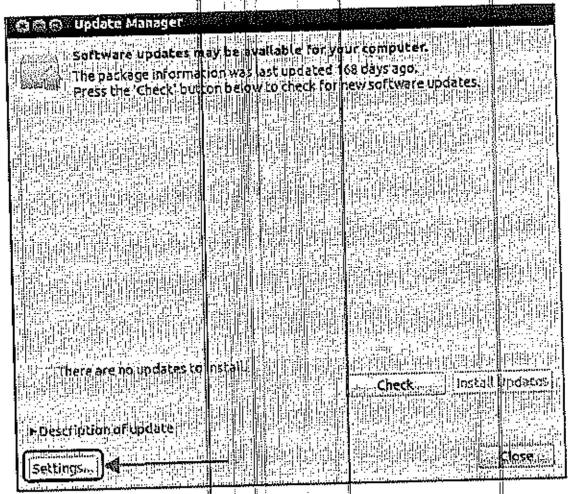
- The open-source community regularly develops improvements and patches for Ubuntu
- You should install these updates regularly

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.

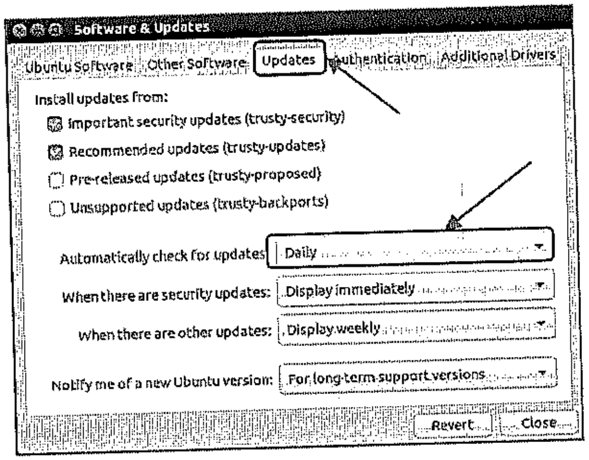


Update Manager

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.

3.



Software & Updates

Install updates from:

☒ Important security updates (trusty-security)
☒ Recommended updates (trusty-updates)
□ Pre-released updates (trusty-proposed)
□ Unsupported updates (trusty-backports)

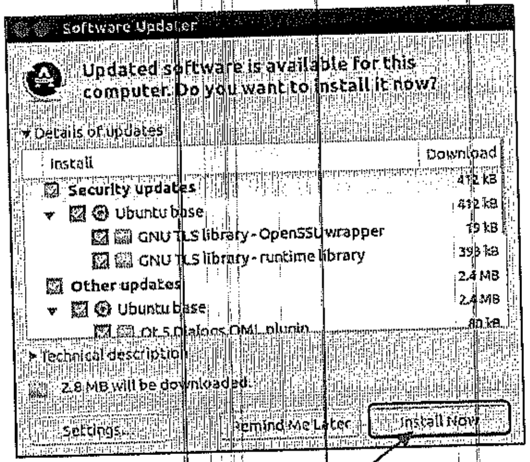
Automatically check for updates: Daily

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

4.



Software Updater

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

Details of updates

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

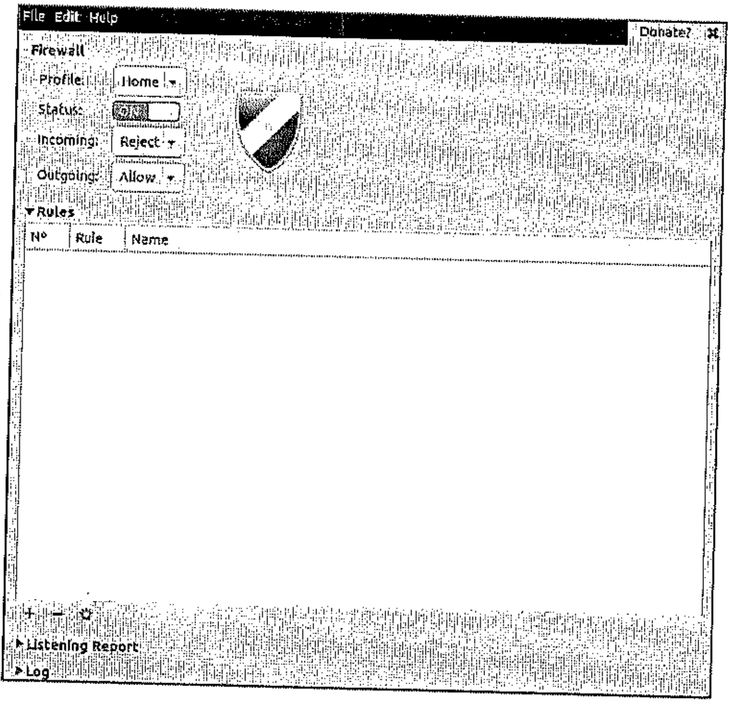
Technical description

2.8 MB will be downloaded.

© Air Force Association

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



Firewall

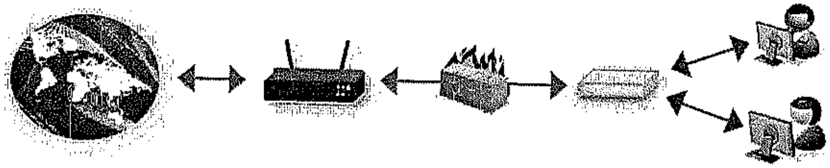
Profile: Home

Status: ON

Incoming: Reject

Outgoing: Allow

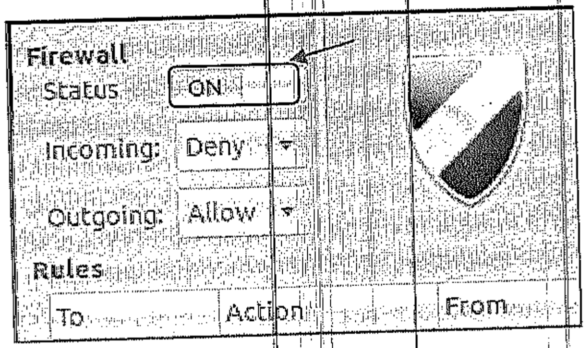
Nº	Rule	Name



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

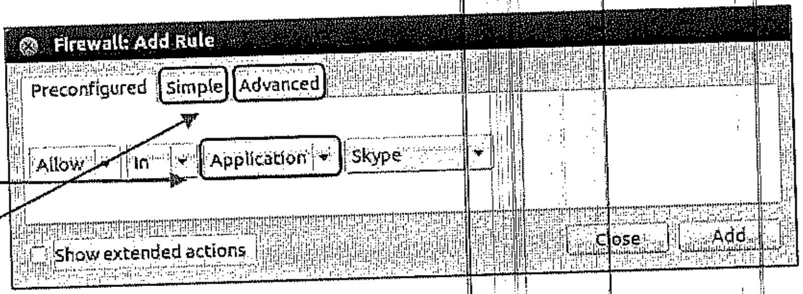
Using Gufw

- 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



Firewall
Status: ON
Incoming: Deny
Outgoing: Allow
Rules

To	Action	From



Firewall: Add Rule

Preconfigured | Simple | Advanced

Allow | In | Application | Skype

□ Show extended actions

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

AIR FORCE ASSOCIATION'S

CYBERPATRIOT

NATIONAL YOUTH CYBER EDUCATION PROGRAM

SECTION TWO

Basic Command Line Security

www.uscyberpatriot.org

The gedit Command

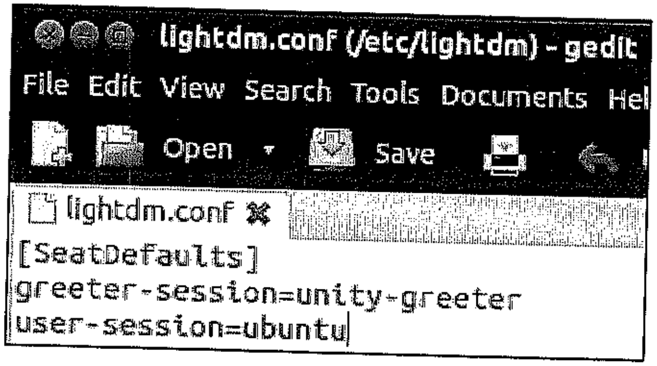
- Gedit is one of many text editor commands in Ubuntu
  - Syntax: gedit [filepath]
  - Unlike with other text editors, using gedit will cause a second window to pop-up where you can easily change the text of a file
  - This command will allow you to edit security policy files
- You need to enact root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


lightdm.conf (/etc/lightdm) - gedit
File Edit View Search Tools Documents Hel
Open
Save
lightdm.conf

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

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

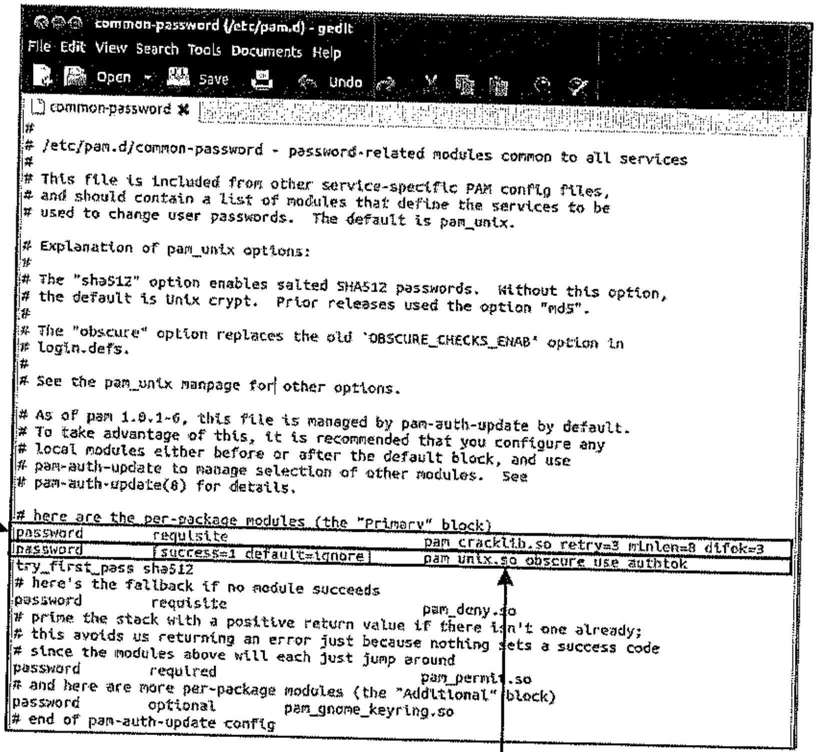
- Pluggable Authentication Modules (PAM) are used for logon and applications
- They simplify user authentication
  - They *do not* govern authorization (i.e. grant privileges to users)
- 4 types of PAM files:
  - Account – control account conditions (e.g. not expired, etc.)
  - Authentication – verify 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.



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
```

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.**

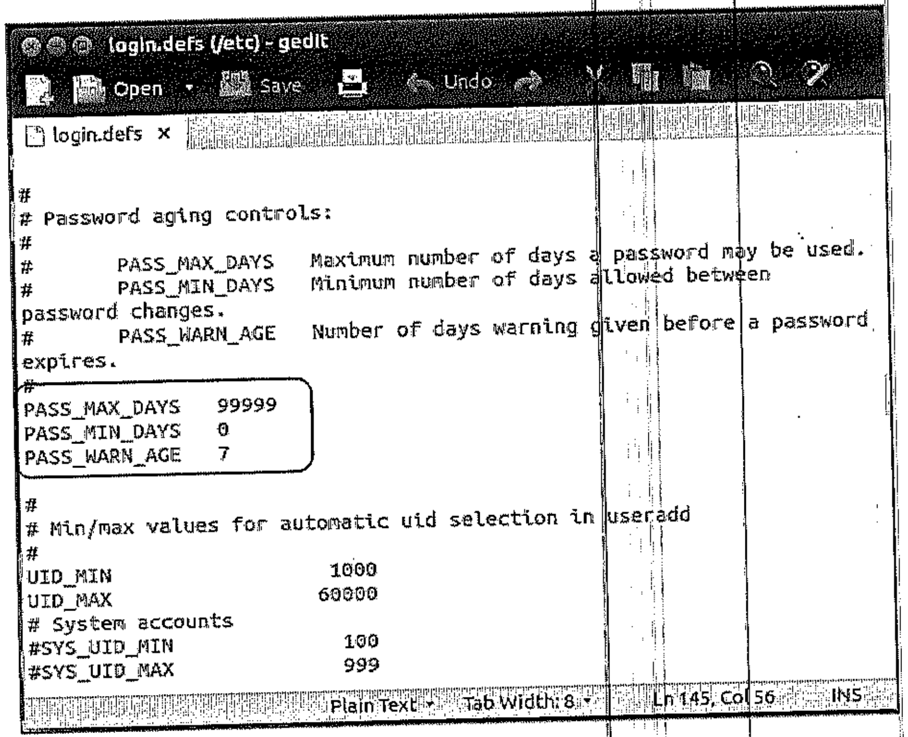
*ucredit = upper case, lcredit=lower case, dcredit = number and ocredit = symbol

**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



```
#
# 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
```

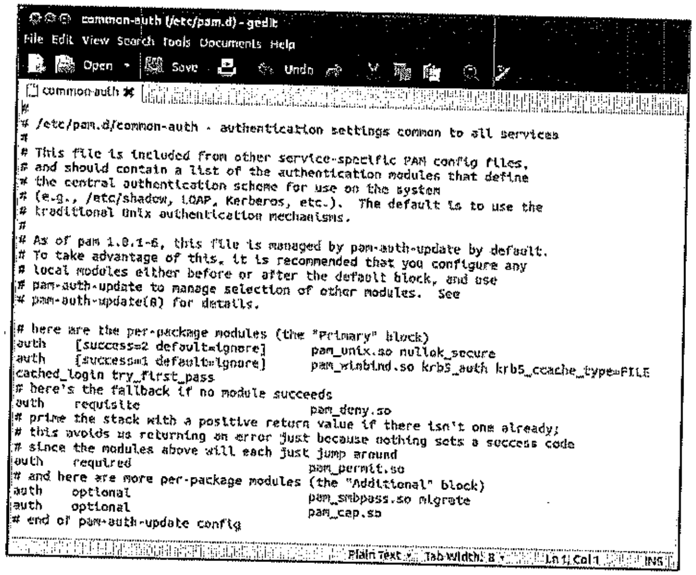
Sources: http://xmodulo.com/2013/12/set-password-policy-linux.html,

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
Open
Save
Undo
common-auth
Plain Text
Tab Width: 8
Ln 1, Col 1
INS

```
#
# /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
```

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

AIR FORCE ASSOCIATION'S

CYBERPATRIOT

NATIONAL YOUTH CYBER EDUCATION PROGRAM

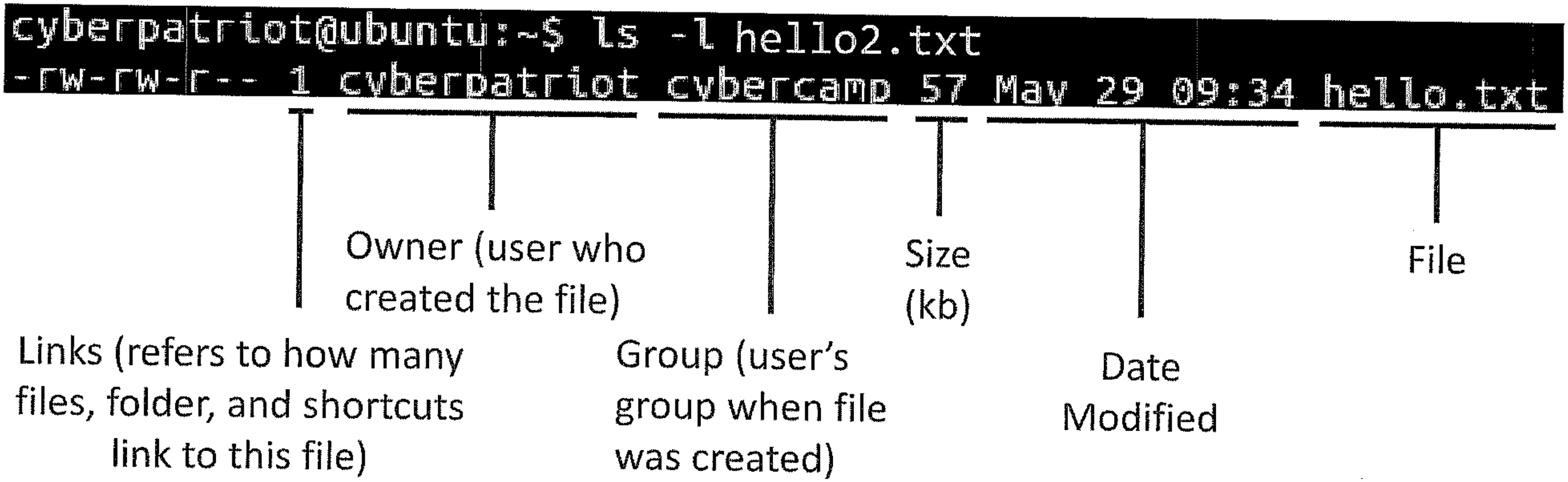
SECTION THREE

Advanced Ubuntu security

www.uscyberpatriot.org

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

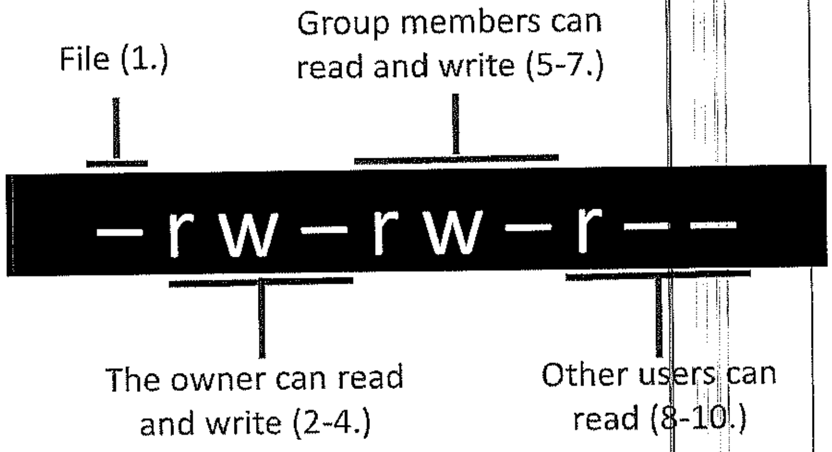
8-10. Other File Permissions

(Blank 2) Read - r

(Blank 3) Write/modify - w

(Blank 4) Execute – x

Example:



File (1.)

Group members can read and write (5-7.)

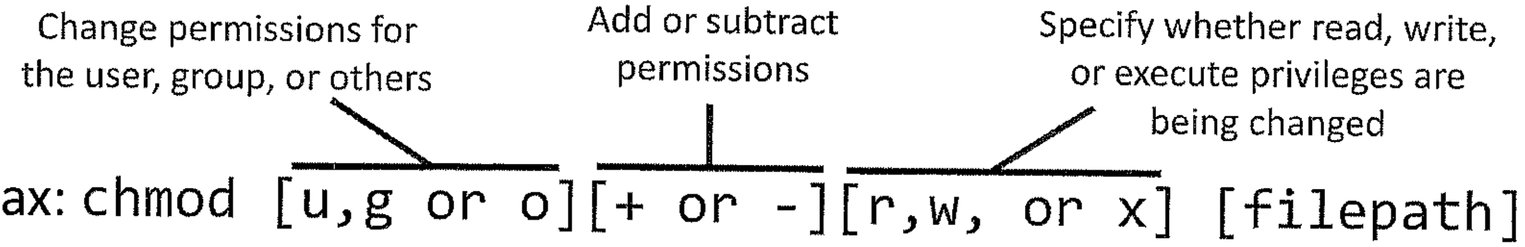
– r w – r w – r – –

The owner can read and write (2-4.)

Other users can read (8-10.)

The chmod Command

- Chmod allows you to change file permissions

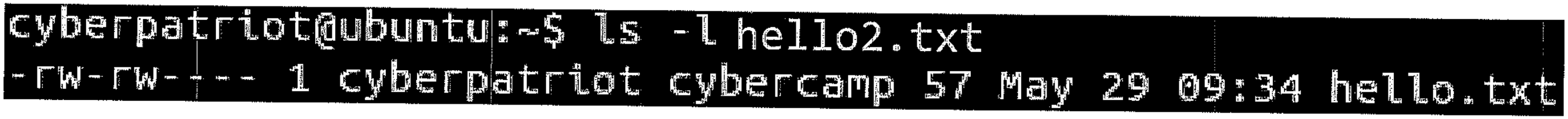


Change permissions for the user, group, or others

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

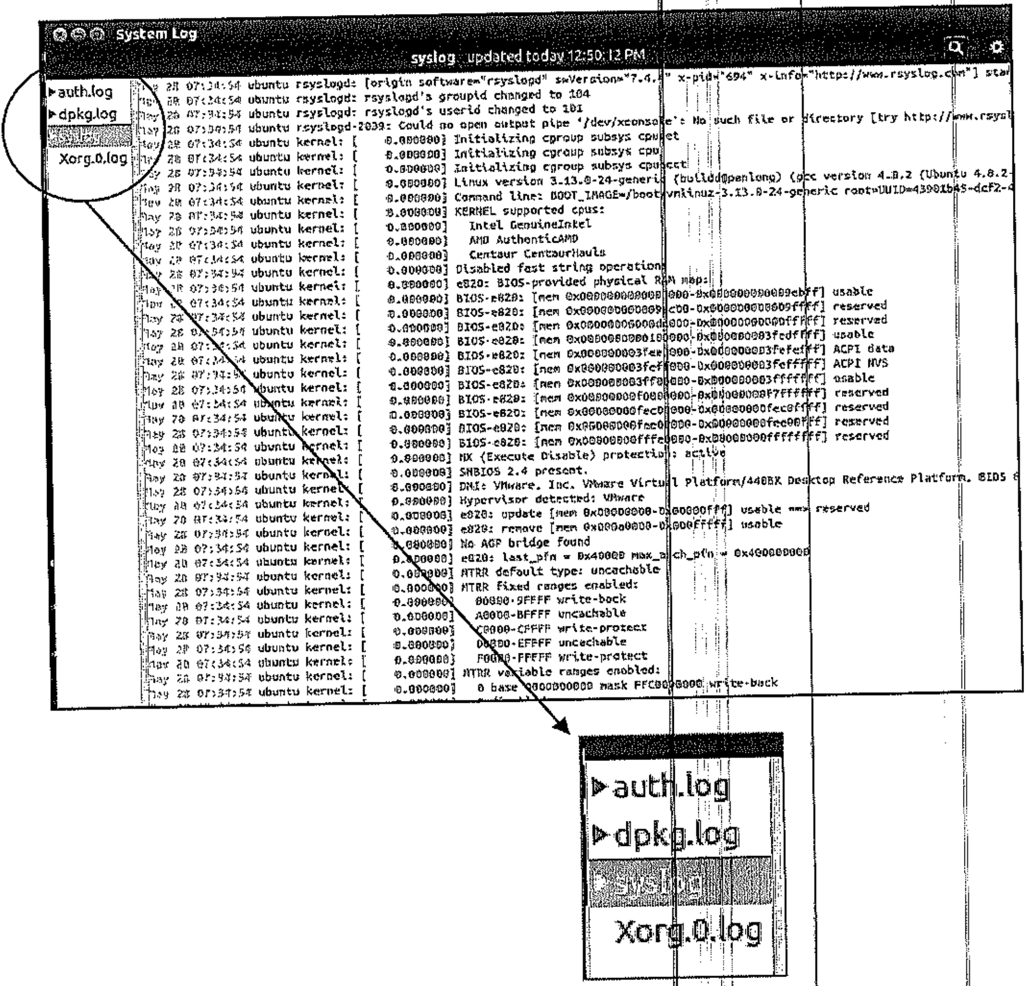


```
cyberpatriot@ubuntu:~$ ls -l hello2.txt
-rw-rw---- 1 cyberpatriot cybercamp 57 May 29 09:34 hello.txt
```

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

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



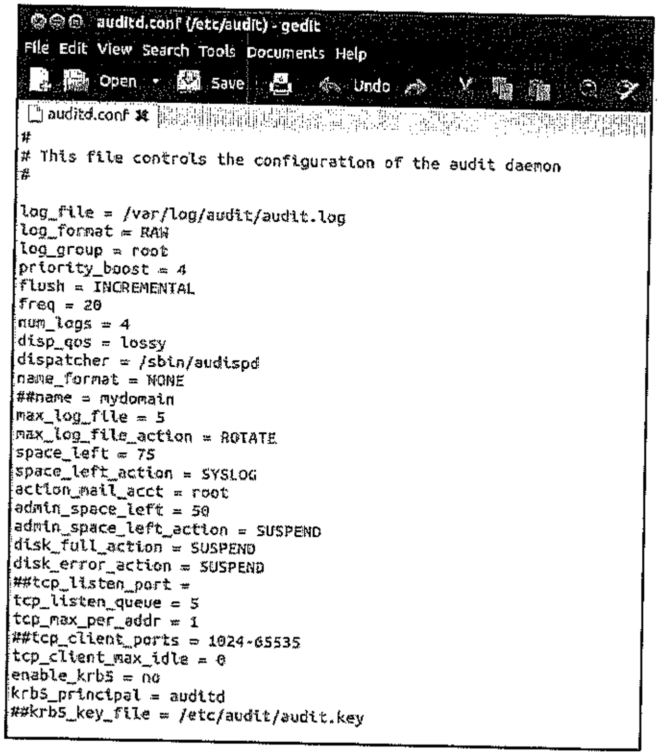
```
May 28 07:34:54 ubuntu rsyslogd: [origin software="rsyslogd" swVersion="7.4.4" x-pid="694" x-info="http://www.rsyslog.com"] sta
May 28 07:34:54 ubuntu rsyslogd: rsyslogd's groupid changed to 104
May 28 07:34:54 ubuntu rsyslogd: rsyslogd's userid changed to 101
May 28 07:34:54 ubuntu rsyslogd-2039: Could no open output pipe '/dev/xconsole': No such file or directory [try http://www.rsysl
May 28 07:34:54 ubuntu kernel: [    0.000000] Initializing cgroup subsys cpuset
May 28 07:34:54 ubuntu kernel: [    0.000000] Initializing cgroup subsys cpu
May 28 07:34:54 ubuntu kernel: [    0.000000] Initializing cgroup subsys cpuacct
May 28 07:34:54 ubuntu kernel: [    0.000000] Linux version 3.13.0-24-generic (buildd@panlong) (gcc version 4.8.2 (Ubuntu 4.8.2-
May 28 07:34:54 ubuntu kernel: [    0.000000] Command line: BOOT_IMAGE=/boot/vmlinuz-3.13.0-24-generic root=UUID=43901b45-dcf2-4
May 28 07:34:54 ubuntu kernel: [    0.000000] KERNEL supported cpus:
May 28 07:34:54 ubuntu kernel: [    0.000000]   Intel GenuineIntel
May 28 07:34:54 ubuntu kernel: [    0.000000]   AMD AuthenticAMD
May 28 07:34:54 ubuntu kernel: [    0.000000]   Centaur CentaurHauls
May 28 07:34:54 ubuntu kernel: [    0.000000] Disabled fast string operations
May 28 07:34:54 ubuntu kernel: [    0.000000] e820: BIOS-provided physical RAM map:
May 28 07:34:54 ubuntu kernel: [    0.000000] BIOS-e820: [mem 0x0000000000000000-0x000000000009ebff] usable
May 28 07:34:54 ubuntu kernel: [    0.000000] BIOS-e820: [mem 0x000000000009ec00-0x000000000009ffff] reserved
May 28 07:34:54 ubuntu kernel: [    0.000000] BIOS-e820: [mem 0x00000000000dc000-0x00000000000fffff] reserved
May 28 07:34:54 ubuntu kernel: [    0.000000] BIOS-e820: [mem 0x0000000000100000-0x000000003fedffff] usable
May 28 07:34:54 ubuntu kernel: [    0.000000] BIOS-e820: [mem 0x000000003fee0000-0x000000003fefefff] ACPI data
May 28 07:34:54 ubuntu kernel: [    0.000000] BIOS-e820: [mem 0x000000003feff000-0x000000003fefffff] ACPI NVS
May 28 07:34:54 ubuntu kernel: [    0.000000] BIOS-e820: [mem 0x000000003ff00000-0x000000003fffffff] usable
May 28 07:34:54 ubuntu kernel: [    0.000000] BIOS-e820: [mem 0x00000000f0000000-0x00000000f7ffffff] reserved
May 28 07:34:54 ubuntu kernel: [    0.000000] BIOS-e820: [mem 0x00000000fec00000-0x00000000fec0ffff] reserved
May 28 07:34:54 ubuntu kernel: [    0.000000] BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] reserved
May 28 07:34:54 ubuntu kernel: [    0.000000] BIOS-e820: [mem 0x00000000fffe0000-0x00000000ffffffff] reserved
May 28 07:34:54 ubuntu kernel: [    0.000000] NX (Execute Disable) protection: active
May 28 07:34:54 ubuntu kernel: [    0.000000] SMBIOS 2.4 present.
May 28 07:34:54 ubuntu kernel: [    0.000000] DMI: VMware, Inc. VMware Virtual Platform/440BX Desktop Reference Platform, BIOS 6
May 28 07:34:54 ubuntu kernel: [    0.000000] Hypervisor detected: VMware
May 28 07:34:54 ubuntu kernel: [    0.000000] e820: update [mem 0x00000000-0x00000fff] usable ==> reserved
May 28 07:34:54 ubuntu kernel: [    0.000000] e820: remove [mem 0x000a0000-0x000fffff] usable
May 28 07:34:54 ubuntu kernel: [    0.000000] No AGP bridge found
May 28 07:34:54 ubuntu kernel: [    0.000000] e820: last_pfn = 0x40000 max_arch_pfn = 0x400000000
May 28 07:34:54 ubuntu kernel: [    0.000000] MTRR default type: uncachable
May 28 07:34:54 ubuntu kernel: [    0.000000] MTRR fixed ranges enabled:
May 28 07:34:54 ubuntu kernel: [    0.000000]   00000-9FFFF write-back
May 28 07:34:54 ubuntu kernel: [    0.000000]   A0000-BFFFF uncachable
May 28 07:34:54 ubuntu kernel: [    0.000000]   C0000-CFFFF write-protect
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
```

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.

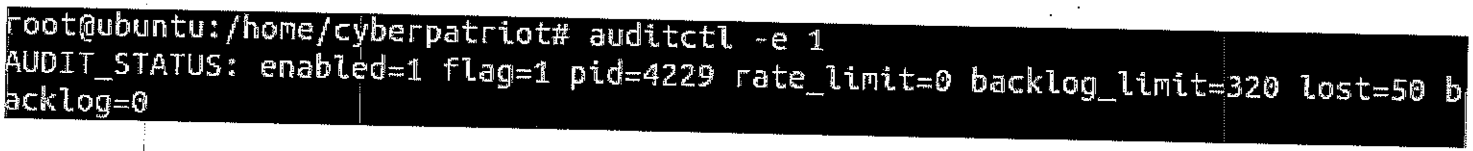


auditd.conf (/etc/audit) - gedit
File Edit View Search Tools Documents Help
Open
Save
Undo
auditd.conf

```
#
# 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
max_log_file_action = ROTATE
space_left = 75
space_left_action = SYSLOG
action_mail_acct = root
admin_space_left = 50
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
```

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: →

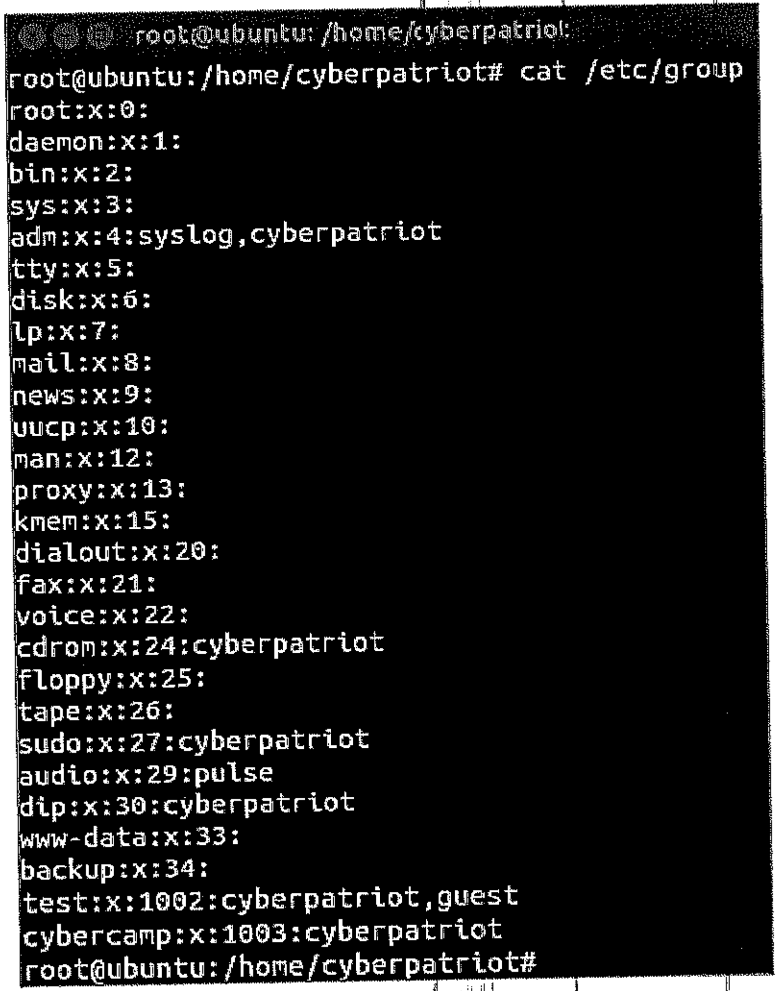
```
cat /etc/group
```

2. To add a group:

```
addgroup [groupname]
```

3. To add a user to a group:

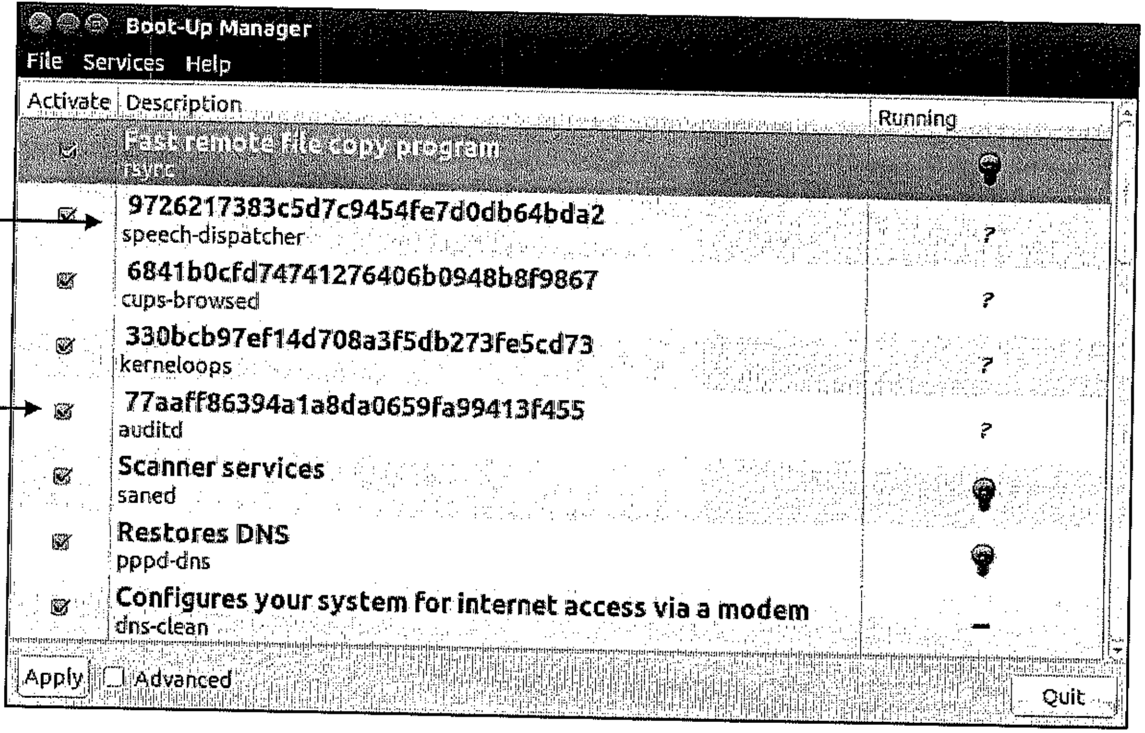
```
adduser [username] [groupname]
```



```
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



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	—

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.

Ubuntu Checklist

1. Read the readme

   Note down which ports/users are allowed.

2. **Do Forensics Questions**

   You may destroy the requisite information if you work on the checklist!

3. Secure root

   set `PermitRootLogin no` in `/etc/ssh/sshd_config`

4. Secure Users
   1. Disable the guest user.

      Go to `/etc/lightdm/lightdm.conf` and add the line

      ```
      allow-guest=false
      ```

      Then restart your session with `sudo restart lightdm`. This will log you out, so make sure you are not executing anything important.

   2. Open up `/etc/passwd` and check which users
      - Are uid 0
      - Can login
      - Are allowed in the readme
   3. Delete unauthorized users:

      ```
      sudo userdel -r $user
      ```

      ```
      sudo groupdel $user
      ```

   4. Check `/etc/sudoers.d` and make sure only members of group sudo can sudo.
   5. Check `/etc/group` and remove non-admins from sudo and admin groups.
   6. Check user directories.
      1. cd `/home`
      2. `sudo ls -Ra *`
      3. Look in any directories which show up for media files/tools and/or "hacking tools."
   7. Enforce Password Requirements.

      0. Add or change password expiration requirements to `/etc/login.defs`.

      1. `PASS_MIN_DAYS 7`

      2. `PASS_MAX_DAYS 90`

      3. `PASS_WARN_AGE 14`

      4. Add a minimum password length.

        1. Open `/etc/pam.d/common-password`.
        2. Add `minlen=8` to the end of the line that has `pam_unix.so` in it.
    5. Implement an account lockout policy.
        1. Open `/etc/pam.d/common-auth`.
        2. Add `deny=5 unlock_time=1800` to the end of the line with `pam_tally2.so` in it.
    6. Change all passwords to satisfy these requirements.

       `chpasswd` is very useful for this purpose.

5. Enable automatic updates

   In the GUI set Update Manager->Settings->Updates->Check for updates:->Daily.

6. Secure ports
    1. `sudo ss -ln`
    2. If a port has `127.0.0.1:$port` in its line, that means it's connected to loopback and isn't exposed. Otherwise, there should only be ports which are specified in the readme open (but there probably will be tons more).
    3. For each open port which should be closed:
        0. `sudo lsof -i :$port`
        1. Copy the program which is listening on the port. `whereis $program`
        2. Copy where the program is (if there is more than one location, just copy the first one). `dpkg -S $location`
        3. 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`
        4. Check to make sure you aren't accidentally removing critical packages before hitting "y".
        5. `sudo ss -l` to make sure the port actually closed.
7. Secure network
    1. Enable the firewall

       ```
       sudo ufw enable
       ```

    2. Enable syn cookie protection

       ```
       sysctl -n net.ipv4.tcp_syncookies
       ```

8. Install Updates

   Start this before half-way.

    - Do general updates.
        0. `sudo apt-get update.`
        1. `sudo apt-get upgrade.`

- Update services specified in readme.
    0. Google to find what the latest stable version is.
    1. Google "ubuntu install service version".
    2. Follow the instructions.
- Ensure that you have points for upgrading the kernel, each service specified in the readme, and bash if it is vulnerable to shellshock.

9. Configure services
    0. Check service configuration files for required services. Usually a wrong setting in a config file for sql, apache, etc. will be a point.
    1. Ensure all services are legitimate.

       ```
       service --status-all
       ```

10. Check the installed packages for "hacking tools," such as password crackers.
11. Run other (more comprehensive) checklists. This is checklist designed to get most of the common points, but it may not catch everything.

Tips

- Netcat is installed by default in ubuntu. You will most likely not get points for removing this version.
- Some services (such as `ssh`) may be required even if they are not mentioned in the readme. Others may be points even if they are explicitly mentioned in the readme

Linux Commands to help you!

nano commands

To open a file in nano type nano “filename” in command line
You can then edit the file from there.
ctrl+x to exit. Will prompt you to save.

gedit commands

To open a file in gedit type gedit “filename”
This will open up a gui text editor similar to notepad.

vi commands

To open a file in vi type vi “filename” in command line
Press i to edit the file.
Press ESC to stop editing the file
after pressing ESC type :w to save :wq to save and quit
you can use gedit instead of vi

sudo su m root

Linux CLI Commands

cd “foldername”	changes to the desired folder
cd ..	goes back a directory
cd ~	goes to current user home directory
cd /	goes to file system directory
ls	shows files
ls -a	shows hidden files
ls -al	shows hidden files and lists them with details
ps -aux or -ef	list all running processes
lsof	list open files
id “name”	tells you what group “name” is in
cat “filename”	shows the contents of a file
PWD	shows current directory

Create folder: mkdir “foldername”

To remove a file or folder : rm -r “file/foldername”

grep = find

PS

PS -ef | grep ( )

2. Add Security Repository and switch to daily updates

GUI Instructions:

Applications->System Tools->Administration->Update Manager
Settings -> Update Tab Check Important Security Updates
Set Automatically check for updates to Daily

CLI Instructions:

nano /etc/apt/sources.list
at the bottom add “deb http://security.ubuntu.com/ubuntu/ precise-security universe main multiverse restricted”
nano /etc/apt/apt.conf.d/10periodic (if that doesn’t work check that folder for the periodic file and put that in)
change APT::Periodic::Update-Package-Lists "0";
to APT::Periodic::Update-Package-Lists "1";

3. Update software

sudo apt-get -y update
sudo apt-get -y upgrade
sudo apt-get -y dist-upgrade
GUI Instructions see Page 3 Slide 4 of Ubuntu Security packet.

5. Search for Bad Files(Find a specific filename and Tree)

find “location” (options) “what you are looking for”

find / -name php	Finds all files named php in the computer

You can use wildcarding to find all files with php in it

find / -name *php	Finds all files that end with php
find / -name *php*	Finds all files that have php in it
find / -type d - perm 0777	Finds all world readable folders
find / -type d -perm 0777 -ls	Lists contents of all world readable folders

Options

-name	Looks for pattern
-type	Specify type of object d(directory) f(file).
-perm	Searches for permissions 0777 for world readable

This command will remove all files of a certain type

```
find / -name *.”file extension” -exec rm -f {} \;
```

Tree

To install tree: sudo apt-get install tree

tree -a	Show hidden files
tree -p	Show permissions

Files to search for

john ophcrack netcat nc nmap wireshark netbus
keylog web VNC Cryptcat crack
cat hydra

6. Securing Users and Groups

Remove Users

sudo cat /etc/shadow to see the users listed

deluser "username" to remove the user. This will also remove the user from any groups

Remember to also remove the users home folder if they have one

GUI Instructions see Page 2 Slide 3 of Ubuntu Security packet.

Disable autologin

CLI Instructions:

```
sudo vi /etc/gdm/custom.conf
```

Change AutomaticLoginEnable= true to AutomaticLoginEnable=false

Remove the line AutomaticLogin=

GUI Instructions:

Select the user name in upper right hand corner
Scroll down to User Accounts and select
Select unlock button in upper right hand corner of the window
Select the user you want on the left
Put the autologin button to off

Change User Password

CLI Instructions

```
sudo passwd "username"
```

It will then ask you to type the new password in two times

Ex. sudo passwd root To change root password

GUI Instructions

Select the user name in upper right hand corner
Scroll down to User Accounts and select
Select unlock button in upper right hand corner of the window
Select the user you want on the left
Select the password field in the box on the right
Type in the new password

List all Users and Groups

```
sudo cat /etc/group
```

This will show you all users in groups.

List All Groups a User is in

```
sudo groups “username”
```

Add Users to Groups

```
sudo adduser “username” “groupname”
```

Remove Users from Groups

```
deluser -G “username” “groupname”
```

Check user locations, before deleting or removing a user

7. Unistall Applications

Applications -> Ubuntu Software Center->Installed Software Section
Select application and click Remove

8. Disabling, Removing or Securing services

GUI

Open up Ubuntu Software Center. In the search bar type synaptic

Remove a service

```
sudo apt-get remove “service name”
                or
sudo dpkg --remove “service name”
apt-get autoremove
```

To secure SSH

sudo ~~nano~~ gedit /etc/ssh/sshd_config to open sshd_config in nano
Change LoginGraceTime 120 to LoginGraceTime 300
Change PermitRootLogin Yes to PermitRootLogin No
Add the following:

```
MaxAuthTries 3
Protocol 2
AllowUsers username1 username2 ….
ClientAliveInterval 600
ClientAliveCountMax 0
```

save

To secure Samba

sudo nano /etc/samba/smb.conf to open smb.conf
find all lines that say “guest ok = yes” change to “guest ok = no”
save

9. Open Ports and Processes

ps -ef or ps -aux (Show all processes currently running)
netstat -nap (Numeric, All, Program(showspid))
lsof -i (lists all files listening on the Internet)

10. Firewall

GUI Instructions see Page 3 Slide 5 of Ubuntu Security packet.

12. Password Policies

login.defs

sudo ~~nano~~ gedit /etc/login.defs to open login.defs
change UMASK 022 to UMASK 077
change PASS_MAX_DAYS 30
change PASS_MIN_DAYS 1
change LOGIN_RETRIES 3
change LOGIN_TIMEOUT 300
save
Also Page 7 Slide 12 of Ubuntu Security packet.

PAM Files

Page 6 Slide 11 and Page 7 slide 13 of Ubuntu Security packet.

13. Secure password policies (Not pam)

check current settings

sudo chage (option) username

Options:

--list

-E expiration date

-m waits days after password change to change again

-M force password change

-I disable account if not used in last 30 days

-W warn 14 days out of upcoming password change

```
sudo chage -E mm/dd/yyyy -m 5 -M 90 -I 30 -W 14 <username>
```

14. Securing Home Directories

```
sudo chmod 750 /home/username
```

15. Sudoers File

Type sudo gedit /etc/sudoers. Edit file to look like below.

16. Virus Scan

Follow instructions to download and run AVG
http://www.beginninglinux.com/home/applications/avg-free-antivirus-ubuntu-installation-from-command-line

```
sudo su
apt-get install clamav clamtk
freshclam
clamscan -ri --exclude-dir=^/sys\ | ^/proc\ | ^/dev /   (will exclude sys, proc, dev folders)
                or
clamscan -i -r “folder name”
```

Good Resources

http://www.computersecuritystudent.com
http://www.cyberciti.biz/
explainshell.com
askubuntu.com
https://www.digitalocean.com/community/tutorials/how-to-use-rkhunter-to-guard-against-rootkits-on-an-ubuntu-vps
http://ryanstutorials.net/linuxtutorial/

16. View Scheduled Tasks

```
ls -l /var/spool/cron/crontabs
```

17. Check Logs

/var/log/message :	General log messages
/var/log/boot:	System boot log
/var/log/debug:	Debugging log messages
/var/log/auth.log:	User login and authentication logs
/var/log/daemon.log:	Running services such as squid, ntpd and others log messages to this file
/var/log/kern.log:	Kernel Log File

Also check GNOME System Log Viewer

18. List all services

```
service --status-all
service “service name” status/start/stop/restart
```

21. Check Rootkits and System Analyzer

```
sudo su
apt-get install rkhunter chkrootkit
rkhunter --update
rkhunter --propupd
rkhunter --check
```

22. Syn Cookie protection

```
sudo su
apt-get install firestarter
start firestarter
```

Select Synaptic Package Manager and Install

Go to Desktop Search Bar and type in synaptic. Select Synaptic Package Manager. It will prompt you for sudo password.

In quick filter bar type in the package that you would like to remove

Once you have found the package right click on in and mark if for complete removal.

Once it is marked for removal press apply to remove the package.

CLI:

Make sure the README says to disable these services and you document the name of the service you are removing.

service --status-all This will tell you what services are running
You can pipe grep to have it highlight a service you are looking for.
I.E. service --status-all | grep inetd Inetd will come up in red so you can find the actual service name

If you don't have the correct service name you can use

dpkg --get-selections That will get all the packages installed
You can pipe grep to highlight a service just like before. This time only packages with that name will show up.

Disable a service

service stop "service name"
If that does not stop the service you can install bum (sudo apt-get install bum)
To run bum (sudo bum)
Right click on the service you want to deactivate and apply the service you want

Unusual Accounts

Look in /etc/passwd for new accounts in sorted list by UID:

```
# sort -nk3 -t: /etc/passwd | less
```

Normal accounts will be there, but look for new, unexpected accounts, especially with UID < 500.

Also, look for unexpected UID 0 accounts:

```
# egrep ':0+:' /etc/passwd
```

On systems that use multiple authentication methods:

```
# getent passwd | egrep ':0+:'
```

Look for orphaned files, which could be a sign of an attacker's temporary account that has been deleted.

```
# find / -nouser -print
```

Unusual Log Entries

Look through your system log files for suspicious events, including:

- "entered promiscuous mode"
- Large number of authentication or login failures from either local or remote access tools (e.g., telnetd, sshd, etc.)
- Remote Procedure Call (rpc) programs with a log entry that includes a large number (> 20) strange characters (such as ^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM)
- For systems running web servers: Larger than normal number of Apache logs saying "error"
- Reboots and/or application restarts

Other Unusual Items

Sluggish system performance:

```
$ uptime
```

– Look at "load average"

Excessive memory use: `$ free`

Sudden decreases in available disk space:

```
$ df
```

Additional Supporting Tools

The following tools are often not built into the Linux operating system, but can be used to analyze its security status in more detail. Each is available for free download at the listed web site.

DISCLAIMER: The SANS Institute is not responsible for creating, distributing, warranting, or supporting any of the following tools.

Chkrootkit looks for anomalies on systems introduced by user-mode and kernel-mode RootKits – www.chkrootkit.org

Tripwire looks for changes to critical system files – www.tripwire.org - free for Linux for non-commercial use

AIDE looks for changes to critical system files http://www.cs.tut.fi/~rammer/aide.html

The Center for Internet Security has released a Linux hardening guide for free at www.cisecurity.org.

The free Bastille Script provides automated security hardening for Linux systems, available at www.bastille-linux.org.

SANS INSTITUTE

Intrusion Discovery

Cheat Sheet v2.0

Linux

POCKET REFERENCE GUIDE

SANS Institute

www.sans.org and isc.sans.org

Download the latest version of this sheet from http://www.sans.org/resources/linsacheatsheet.pdf

Purpose

System Administrators are often on the front lines of computer security. This guide aims to support System Administrators in finding indications of a system compromise.

What to use this sheet for

On a periodic basis (daily, weekly, or each time you logon to a system you manage,) run through these quick steps to look for anomalous behavior that might be caused by a computer intrusion. Each of these commands runs locally on a system.

This sheet is split into these sections:

- Unusual Processes and Services
- Unusual Files
- Unusual Network Usage
- Unusual Scheduled Tasks
- Unusual Accounts
- Unusual Log Entries
- Other Unusual Items
- Additional Supporting Tools

If you spot anomalous behavior: **DO NOT PANIC!** Your system may or may not have come under attack. Please contact the Incident Handling Team immediately to report the activities and get further assistance.

Unusual Processes and Services

Look at all running processes:

```
      # ps -aux
```

Get familiar with "normal" processes for the machine. Look for unusual processes. Focus on processes with root (UID 0) privileges.

If you spot a process that is unfamiliar, investigate in more detail using:

```
      # lsof -p [pid]
```

This command shows all files and ports used by the running process.

If your machine has it installed, run chkconfig to see which services are enabled at various runlevels:

```
      # chkconfig --list
```

Unusual Files

Look for unusual SUID root files:

```
      # find / -uid 0 -perm -4000 -print
```

This requires knowledge of normal SUID files.

Look for unusual large files (greater than 10 MegaBytes):

```
      # find / -size +10000k -print
```

This requires knowledge of normal large files.

Look for files named with dots and spaces ("...", ".. ", ". ", and " ") used to camouflage files:

```
      # find / -name " " -print
      # find / -name ".. " -print
      # find / -name ". " -print
      # find / -name " " -print
```

Unusual Files Continued

Look for processes running out of or accessing files that have been unlinked (i.e., link count is zero). An attacker may be hiding data in or running a backdoor from such files:

```
      # lsof +L1
```

On a Linux machine with RPM installed (RedHat, Mandrake, etc.), run the RPM tool to verify packages:

```
      # rpm -Va | sort
```

This checks size, MD5 sum, permissions, type, owner, and group of each file with information from RPM database to look for changes. Output includes:

S – File size differs
M – Mode differs (permissions)
5 – MD5 sum differs
D – Device number mismatch
L – readLink path mismatch
U – user ownership differs
G – group ownership differs
T – modification time differs

Pay special attention to changes associated with items in /sbin, /bin, /usr/sbin, and /usr/bin.

In some versions of Linux, this analysis is automated by the built-in `check-packages` script.

Unusual Network Usage

Look for promiscuous mode, which might indicate a sniffer:

```
      # ip link | grep PROMISC
```

Note that the ifconfig doesn't work reliably for detecting promiscuous mode on Linux kernel 2.4, so please use "ip link" for detecting it.

Unusual Network Usage Continued

Look for unusual port listeners:

```
      # netstat -nap
```

Get more details about running processes listening on ports:

```
      # lsof -i
```

These commands require knowledge of which TCP and UDP ports are normally listening on your system. Look for deviations from the norm.

Look for unusual ARP entries, mapping IP address to MAC addresses that aren't correct for the LAN:

```
      # arp -a
```

This analysis requires detailed knowledge of which addresses are supposed to be on the LAN. On a small and/or specialized LAN (such as a DMZ), look for unexpected IP addresses.

Unusual Scheduled Tasks

Look for cron jobs scheduled by root and any other UID 0 accounts:

```
      # crontab -u root -l
```

Look for unusual system-wide cron jobs:

```
      # cat /etc/crontab
      # ls /etc/cron.*
```