Lab 10
Sandboxing
Due Wednesday November 28, 2018
Jennifer Garcia, Michael Gonzalez, Rachid Afaf, Yevgeniya Martynyuk

Lab Break Down	
Jennifer Garcia	
Michael Gonzalez	4.1.2 Systrace, 4.2 Network Interference Analysis, Word Problems
Rachid Afaf	4.1.1 AppArmor, Word Problems
Yevgeniya Martynyuk	

Introduction:

This lab handles the limiting of common exploits via the introduction of sandboxing. Sandboxing would contain these exploits, any modifications/tampering in practice should not affect the host system in any way.

4.1.1 AppArmor:

After installing the apparmor packages, then I loaded it, and make it in learning mode. After that that I created new profile that violate the pemitted logging, and then I enforced profile policy as well as loggig the violation. And that was done by following the following steps;

- apparmor_status is used to view the current status of AppArmor profiles.

```
sudo apparmor_status
```

- aa-complain places a profile into complain mode.

```
sudo aa-complain /path/to/bin
```

- aa-enforce places a profile into enforce mode.

```
sudo aa-enforce /path/to/bin
```

- The /etc/apparmor.d directory is where the AppArmor profiles are located. It can be used to manipulate the mode of all profiles.
- Enter the following to place all profiles into complain mode:

```
sudo aa-complain /etc/apparmor.d/*
```

- To place all profiles in enforce mode:

  ```
  sudo aa-enforce /etc/apparmor.d/*
  ```

- apparmor_parser is used to load a profile into the kernel. It can also be used to reload a currently loaded profile using the -r option. To load a profile:

  ```
  cat /etc/apparmor.d/profile.name | sudo apparmor_parser -a
  ```

- To reload a profile:

  ```
  cat /etc/apparmor.d/profile.name | sudo apparmor_parser -r
  ```

- systemctl can be used to reload all profiles:

  ```
  sudo systemctl reload apparmor.service
  ```

- The /etc/apparmor.d/disable directory can be used along with the apparmor_parser -R option to disable a profile.

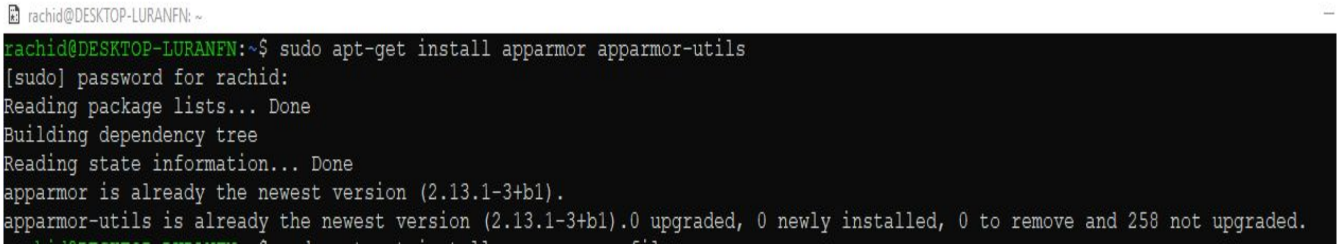
  ```
  sudo ln -s /etc/apparmor.d/profile.name /etc/apparmor.d/disable/
  sudo apparmor_parser -R /etc/apparmor.d/profile.name
  ```

- To re-enable a disabled profile remove the symbolic link to the profile in /etc/apparmor.d/disable/. Then load the profile using the -a option.

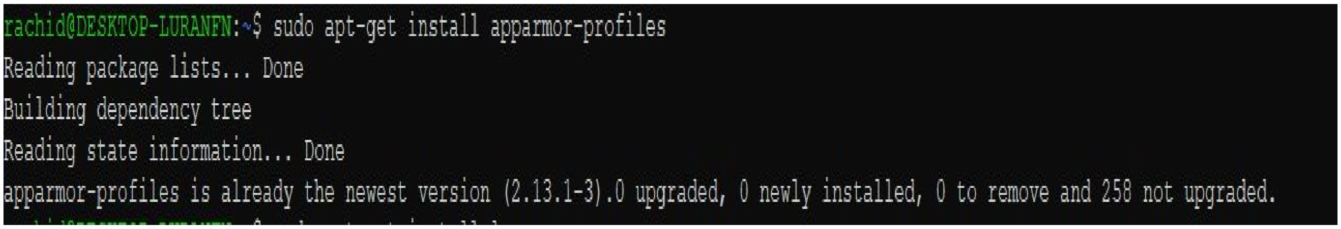
  ```
  sudo rm /etc/apparmor.d/disable/profile.name
  cat /etc/apparmor.d/profile.name | sudo apparmor_parser -a
  ```

- AppArmor can be disabled, and the kernel module unloaded by entering the following:
  ```
  sudo systemctl stop apparmor.service
  sudo update-rc.d -f apparmor remove
  ```
- To re-enable AppArmor enter:

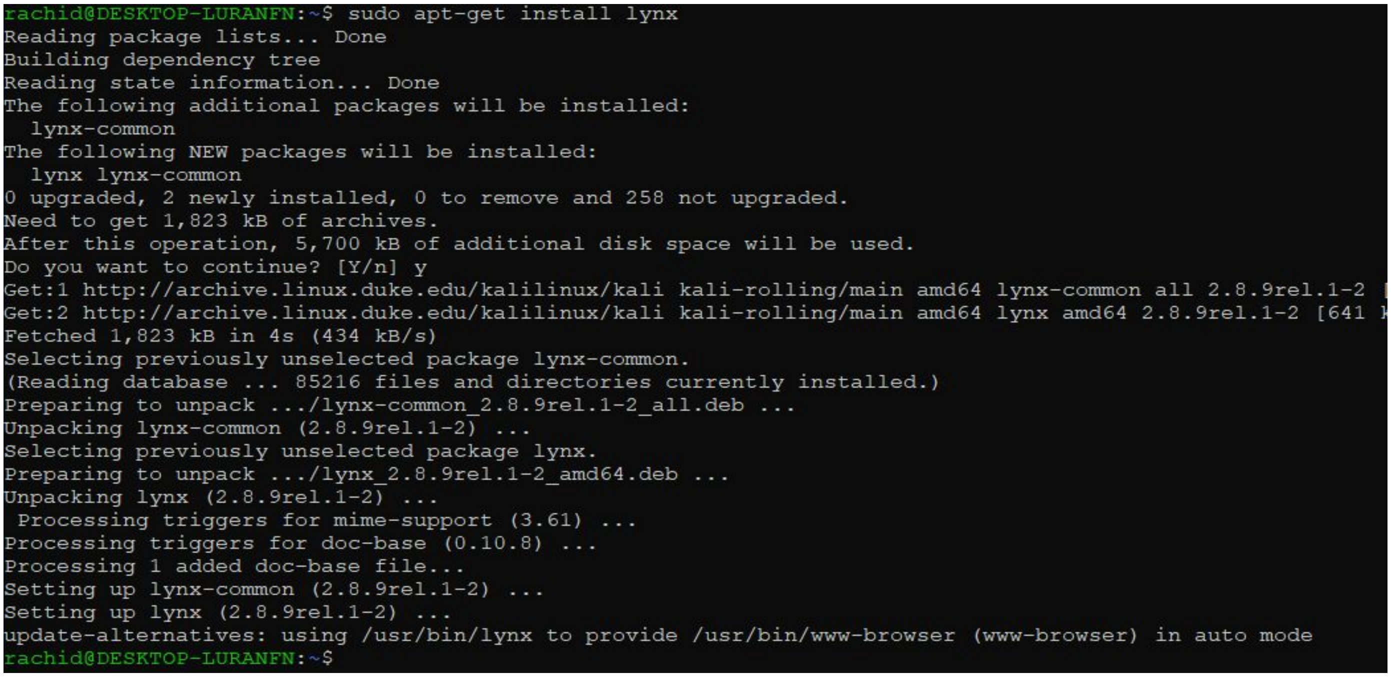
  ```
  sudo systemctl start apparmor.service
  sudo update-rc.d apparmor defaults
  ```



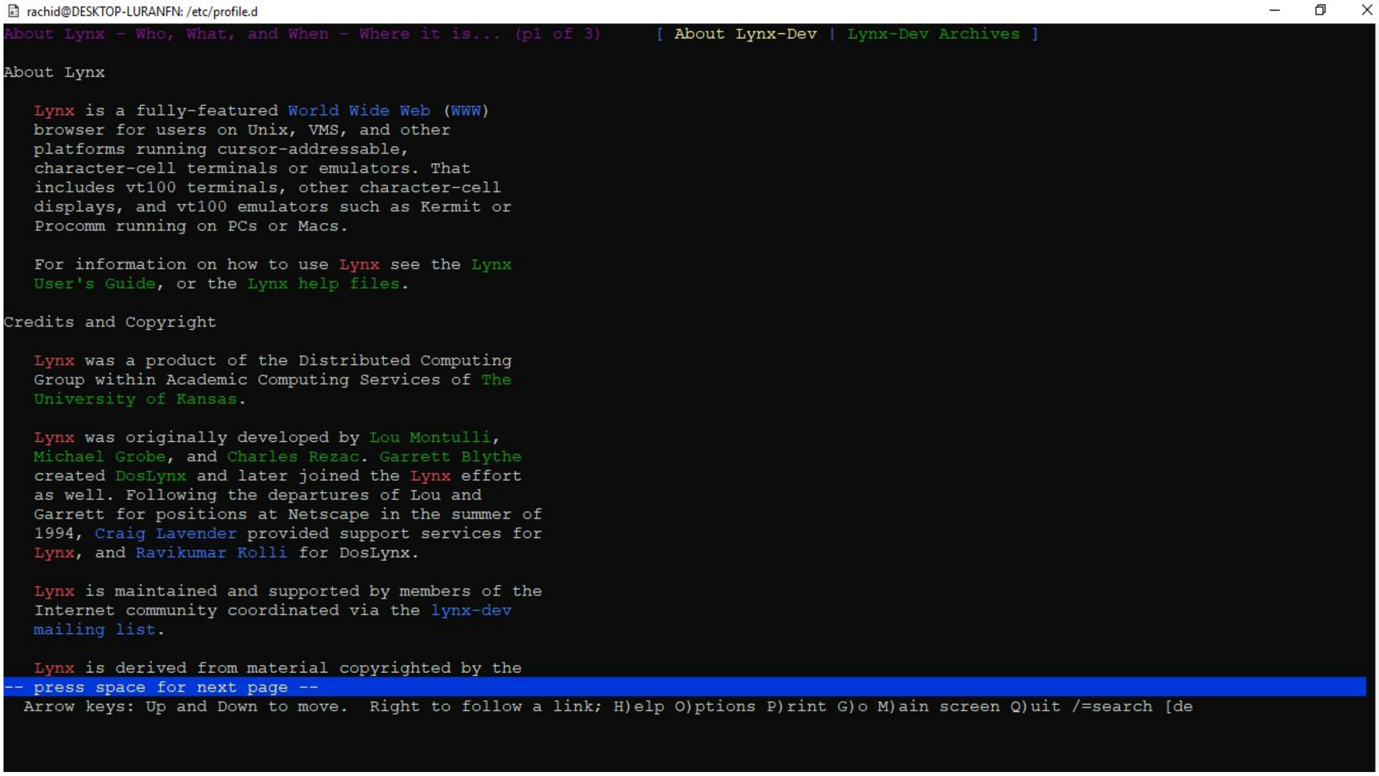
```
rachid@DESKTOP-LURANFN:~$ sudo apt-get install apparmor apparmor-utils
[sudo] password for rachid:
Reading package lists... Done
Building dependency tree
Reading state information... Done
apparmor is already the newest version (2.13.1-3+b1).
apparmor-utils is already the newest version (2.13.1-3+b1).0 upgraded, 0 newly installed, 0 to remove and 258 not upgraded.
```



```
rachid@DESKTOP-LURANFN:~$ sudo apt-get install apparmor-profiles
Reading package lists... Done
Building dependency tree
Reading state information... Done
apparmor-profiles is already the newest version (2.13.1-3).0 upgraded, 0 newly installed, 0 to remove and 258 not upgraded.
```

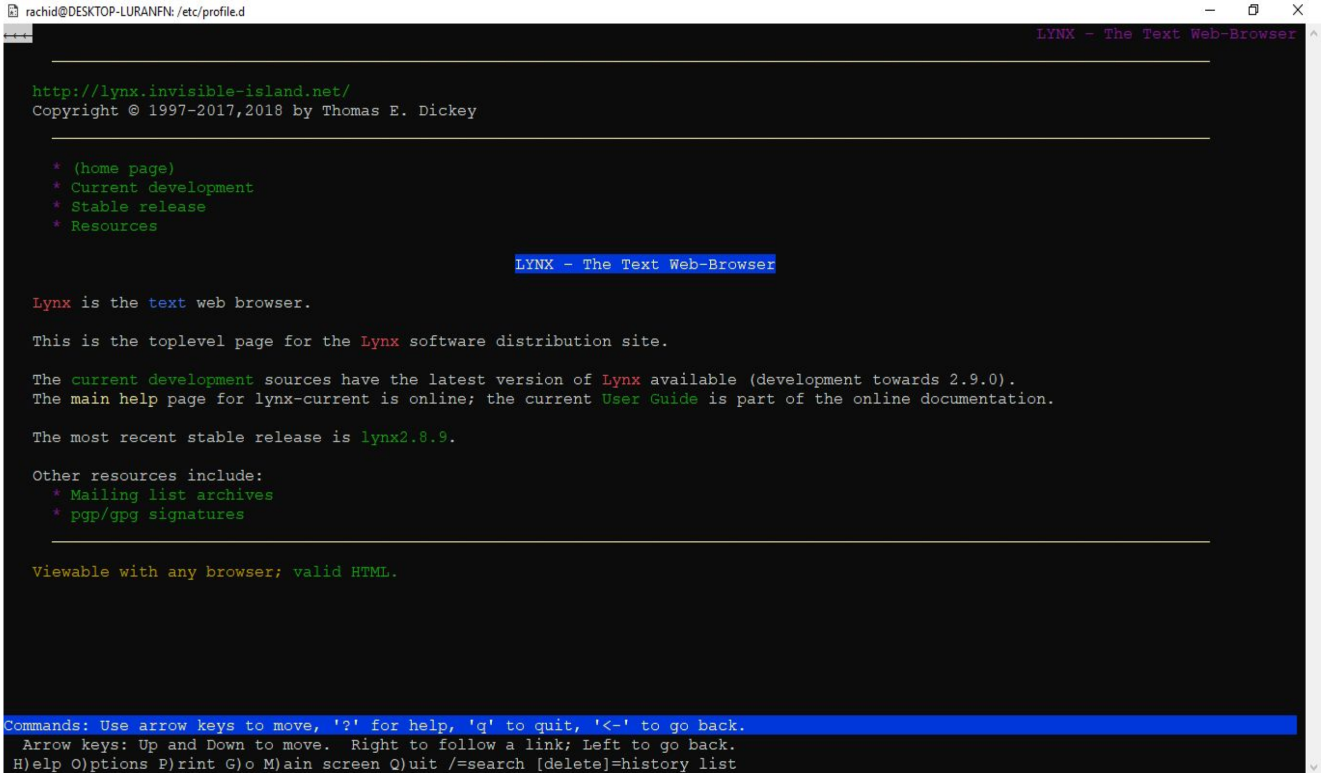


```
rachid@DESKTOP-LURANFN:~$ sudo apt-get install lynx
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  lynx-common
The following NEW packages will be installed:
  lynx lynx-common
0 upgraded, 2 newly installed, 0 to remove and 258 not upgraded.
Need to get 1,823 kB of archives.
After this operation, 5,700 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://archive.linux.duke.edu/kalilinux/kali kali-rolling/main amd64 lynx-common all 2.8.9rel.1-2 [
Get:2 http://archive.linux.duke.edu/kalilinux/kali kali-rolling/main amd64 lynx amd64 2.8.9rel.1-2 [641 k
Fetched 1,823 kB in 4s (434 kB/s)
Selecting previously unselected package lynx-common.
(Reading database ... 85216 files and directories currently installed.)
Preparing to unpack .../lynx-common_2.8.9rel.1-2_all.deb ...
Unpacking lynx-common (2.8.9rel.1-2) ...
Selecting previously unselected package lynx.
Preparing to unpack .../lynx_2.8.9rel.1-2_amd64.deb ...
Unpacking lynx (2.8.9rel.1-2) ...
 Processing triggers for mime-support (3.61) ...
Processing triggers for doc-base (0.10.8) ...
Processing 1 added doc-base file...
Setting up lynx-common (2.8.9rel.1-2) ...
Setting up lynx (2.8.9rel.1-2) ...
update-alternatives: using /usr/bin/lynx to provide /usr/bin/www-browser (www-browser) in auto mode
rachid@DESKTOP-LURANFN:~$
```

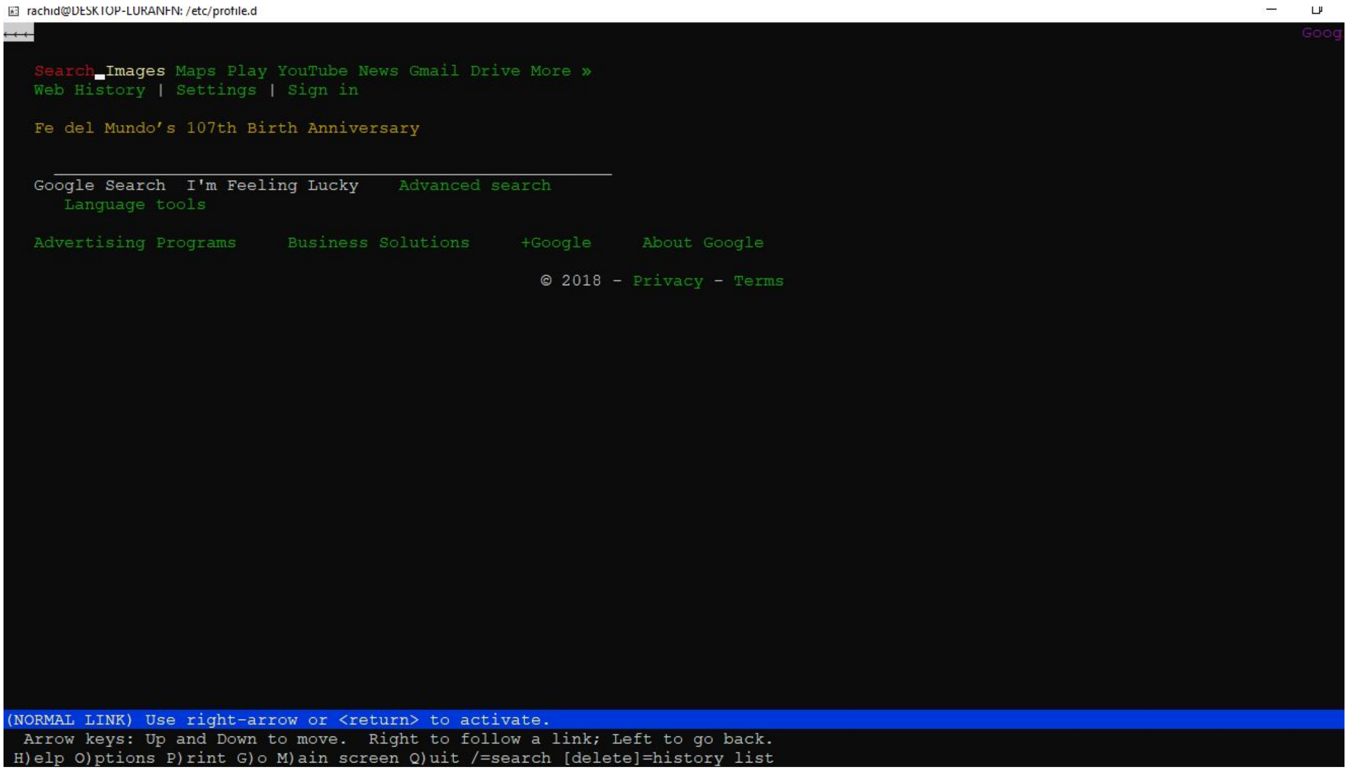


rachid@DESKTOP-LURANFN: /etc/profile.d

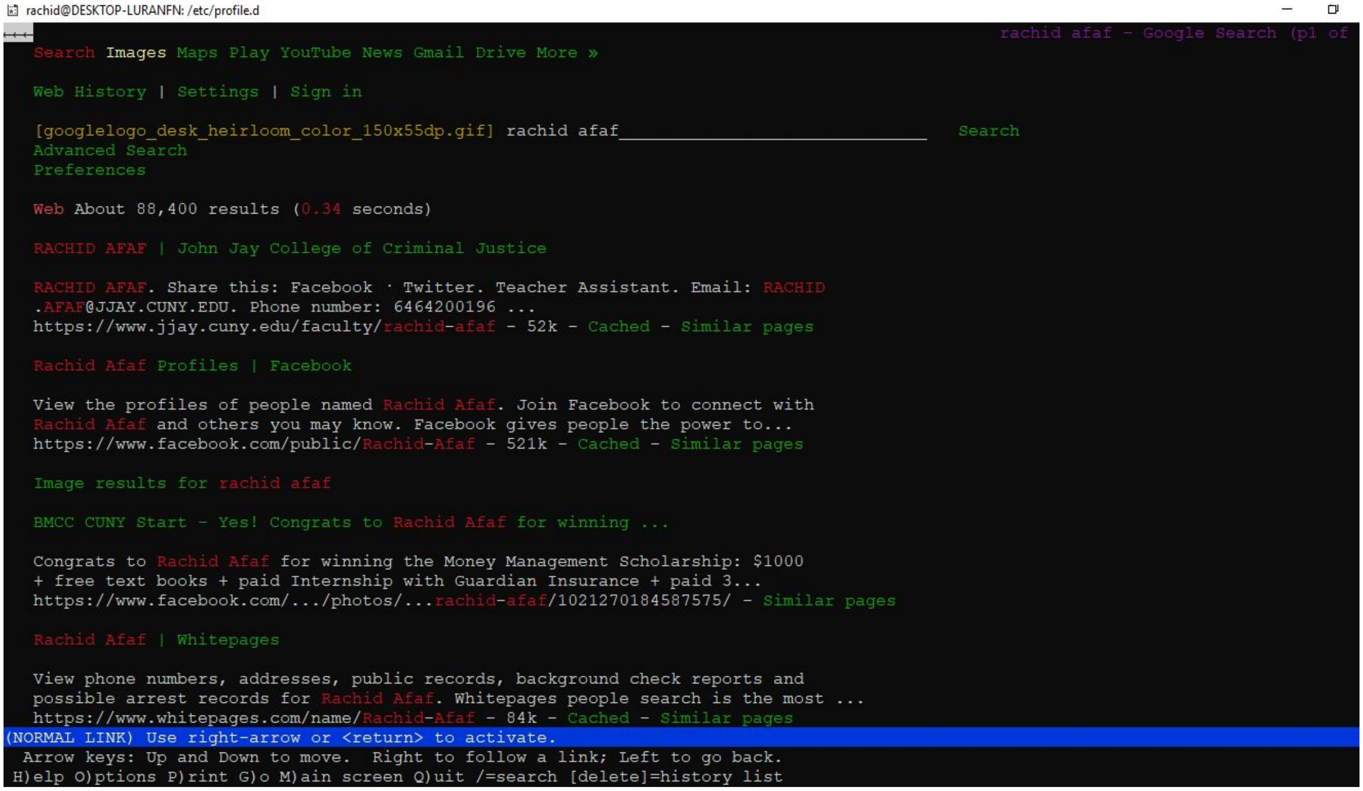
```
About Lynx - Who, What, and When - Where it is... (p1 of 3)      [ About Lynx-Dev | Lynx-Dev Archives ]

About Lynx

   Lynx is a fully-featured World Wide Web (WWW)
   browser for users on Unix, VMS, and other
   platforms running cursor-addressable,
   character-cell terminals or emulators. That
   includes vt100 terminals, other character-cell
   displays, and vt100 emulators such as Kermit or
   Procomm running on PCs or Macs.

   For information on how to use Lynx see the Lynx
   User's Guide, or the Lynx help files.

Credits and Copyright

   Lynx was a product of the Distributed Computing
   Group within Academic Computing Services of The
   University of Kansas.

   Lynx was originally developed by Lou Montulli,
   Michael Grobe, and Charles Rezac. Garrett Blythe
   created DosLynx and later joined the Lynx effort
   as well. Following the departures of Lou and
   Garrett for positions at Netscape in the summer of
   1994, Craig Lavender provided support services for
   Lynx, and Ravikumar Kolli for DosLynx.

   Lynx is maintained and supported by members of the
   Internet community coordinated via the lynx-dev
   mailing list.

   Lynx is derived from material copyrighted by the
-- press space for next page --
  Arrow keys: Up and Down to move.  Right to follow a link; H)elp O)ptions P)rint G)o M)ain screen Q)uit /=search [de
```



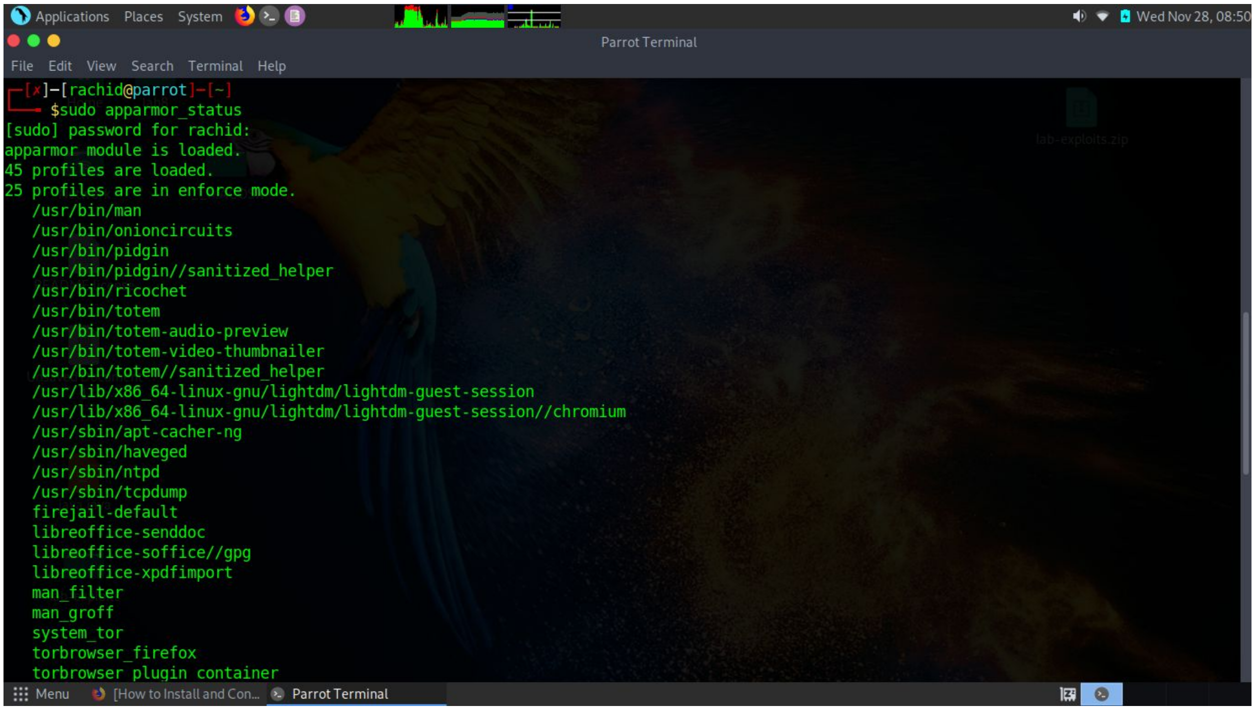
```
                                                                                         LYNX – The Text Web-Browser
     ____________________________________________________________________________________________

   http://lynx.invisible-island.net/
   Copyright © 1997-2017,2018 by Thomas E. Dickey
     ____________________________________________________________________________________________

     * (home page)
     * Current development
     * Stable release
     * Resources

                                                     LYNX – The Text Web-Browser

   Lynx is the text web browser.

   This is the toplevel page for the Lynx software distribution site.

   The current development sources have the latest version of Lynx available (development towards 2.9.0).
   The main help page for lynx-current is online; the current User Guide is part of the online documentation.

   The most recent stable release is lynx2.8.9.

   Other resources include:
     * Mailing list archives
     * pgp/gpg signatures
     ____________________________________________________________________________________________

   Viewable with any browser; valid HTML.




Commands: Use arrow keys to move, '?' for help, 'q' to quit, '<-' to go back.
  Arrow keys: Up and Down to move.  Right to follow a link; Left to go back.
 H)elp O)ptions P)rint G)o M)ain screen Q)uit /=search [delete]=history list
```



```
                                                                                                          Goog

   Search_Images Maps Play YouTube News Gmail Drive More »
   Web History | Settings | Sign in

   Fe del Mundo's 107th Birth Anniversary

     __________________________________________
   Google Search  I'm Feeling Lucky    Advanced search
      Language tools

   Advertising Programs     Business Solutions     +Google     About Google

                                                        © 2018 - Privacy - Terms




(NORMAL LINK) Use right-arrow or <return> to activate.
  Arrow keys: Up and Down to move.  Right to follow a link; Left to go back.
 H)elp O)ptions P)rint G)o M)ain screen Q)uit /=search [delete]=history list
```

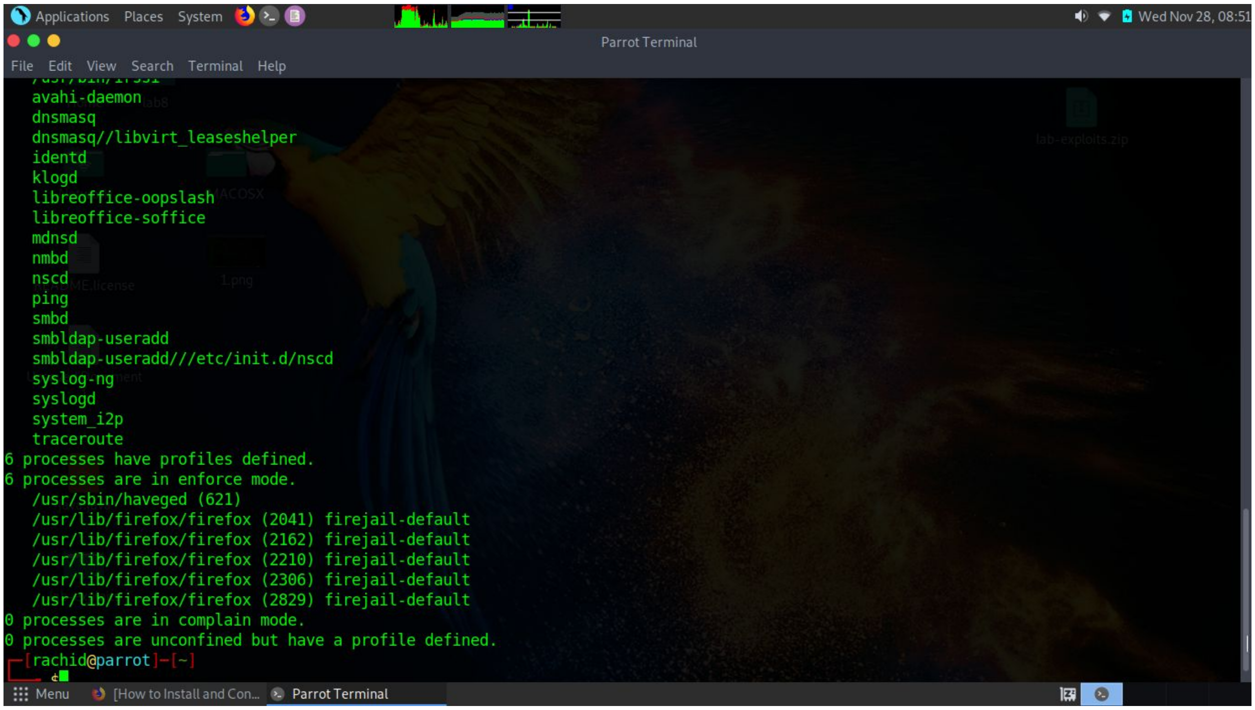


```
                                                                   rachid afaf - Google Search (p1 of
  Search Images Maps Play YouTube News Gmail Drive More »

  Web History | Settings | Sign in

  [googlelogo_desk_heirloom_color_150x55dp.gif] rachid afaf______________________________   Search
  Advanced Search
  Preferences

  Web About 88,400 results (0.34 seconds)

  RACHID AFAF | John Jay College of Criminal Justice

  RACHID AFAF. Share this: Facebook · Twitter. Teacher Assistant. Email: RACHID
  .AFAF@JJAY.CUNY.EDU. Phone number: 6464200196 ...
  https://www.jjay.cuny.edu/faculty/rachid-afaf - 52k - Cached - Similar pages

  Rachid Afaf Profiles | Facebook

  View the profiles of people named Rachid Afaf. Join Facebook to connect with
  Rachid Afaf and others you may know. Facebook gives people the power to...
  https://www.facebook.com/public/Rachid-Afaf - 521k - Cached - Similar pages

  Image results for rachid afaf

  BMCC CUNY Start - Yes! Congrats to Rachid Afaf for winning ...

  Congrats to Rachid Afaf for winning the Money Management Scholarship: $1000
  + free text books + paid Internship with Guardian Insurance + paid 3...
  https://www.facebook.com/.../photos/...rachid-afaf/1021270184587575/ - Similar pages

  Rachid Afaf | Whitepages

  View phone numbers, addresses, public records, background check reports and
  possible arrest records for Rachid Afaf. Whitepages people search is the most ...
  https://www.whitepages.com/name/Rachid-Afaf - 84k - Cached - Similar pages
(NORMAL LINK) Use right-arrow or <return> to activate.
  Arrow keys: Up and Down to move.  Right to follow a link; Left to go back.
 H)elp O)ptions P)rint G)o M)ain screen Q)uit /=search [delete]=history list
```



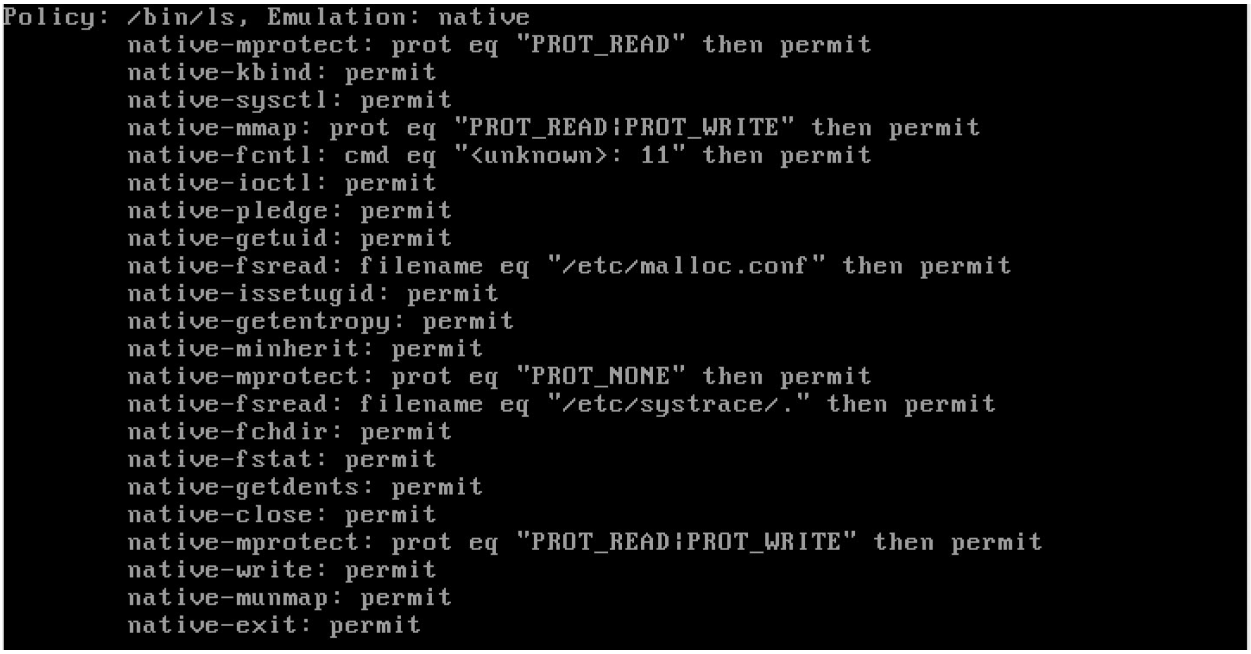
Applications Places System
Wed Nov 28, 08:50
Parrot Terminal
File Edit View Search Terminal Help
lab-exploits.zip
Menu
[How to Install and Con...
Parrot Terminal

```
┌─[✗]─[rachid@parrot]─[~]
└──╼ $sudo apparmor_status
[sudo] password for rachid:
apparmor module is loaded.
45 profiles are loaded.
25 profiles are in enforce mode.
   /usr/bin/man
   /usr/bin/onioncircuits
   /usr/bin/pidgin
   /usr/bin/pidgin//sanitized_helper
   /usr/bin/ricochet
   /usr/bin/totem
   /usr/bin/totem-audio-preview
   /usr/bin/totem-video-thumbnailer
   /usr/bin/totem//sanitized_helper
   /usr/lib/x86_64-linux-gnu/lightdm/lightdm-guest-session
   /usr/lib/x86_64-linux-gnu/lightdm/lightdm-guest-session//chromium
   /usr/sbin/apt-cacher-ng
   /usr/sbin/haveged
   /usr/sbin/ntpd
   /usr/sbin/tcpdump
   firejail-default
   libreoffice-senddoc
   libreoffice-soffice//gpg
   libreoffice-xpdfimport
   man_filter
   man_groff
   system_tor
   torbrowser_firefox
   torbrowser_plugin_container
```

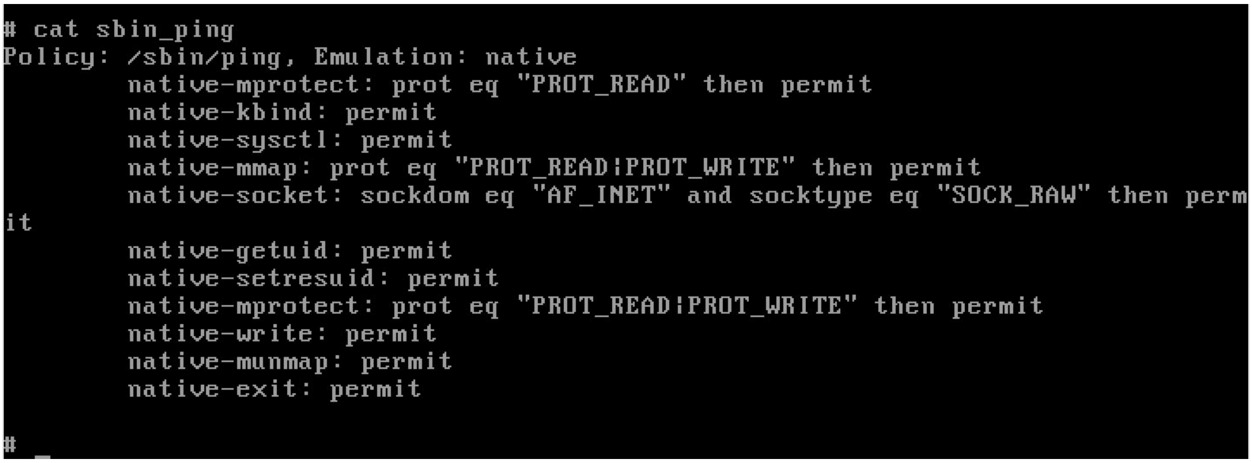


```
   /usr/bin/irssi
   avahi-daemon
   dnsmasq
   dnsmasq//libvirt_leaseshelper
   identd
   klogd
   libreoffice-oopslash
   libreoffice-soffice
   mdnsd
   nmbd
   nscd
   ping
   smbd
   smbldap-useradd
   smbldap-useradd///etc/init.d/nscd
   syslog-ng
   syslogd
   system_i2p
   traceroute
6 processes have profiles defined.
6 processes are in enforce mode.
   /usr/sbin/haveged (621)
   /usr/lib/firefox/firefox (2041) firejail-default
   /usr/lib/firefox/firefox (2162) firejail-default
   /usr/lib/firefox/firefox (2210) firejail-default
   /usr/lib/firefox/firefox (2306) firejail-default
   /usr/lib/firefox/firefox (2829) firejail-default
0 processes are in complain mode.
0 processes are unconfined but have a profile defined.
┌─[rachid@parrot]─[~]
└──╼ $
```

4.1.2 Systrace:



```
Policy: /bin/ls, Emulation: native
        native-mprotect: prot eq "PROT_READ" then permit
        native-kbind: permit
        native-sysctl: permit
        native-mmap: prot eq "PROT_READ|PROT_WRITE" then permit
        native-fcntl: cmd eq "<unknown>: 11" then permit
        native-ioctl: permit
        native-pledge: permit
        native-getuid: permit
        native-fsread: filename eq "/etc/malloc.conf" then permit
        native-issetugid: permit
        native-getentropy: permit
        native-minherit: permit
        native-mprotect: prot eq "PROT_NONE" then permit
        native-fsread: filename eq "/etc/systrace/." then permit
        native-fchdir: permit
        native-fstat: permit
        native-getdents: permit
        native-close: permit
        native-mprotect: prot eq "PROT_READ|PROT_WRITE" then permit
        native-write: permit
        native-munmap: permit
        native-exit: permit
```



```
# cat sbin_ping
Policy: /sbin/ping, Emulation: native
        native-mprotect: prot eq "PROT_READ" then permit
        native-kbind: permit
        native-sysctl: permit
        native-mmap: prot eq "PROT_READ|PROT_WRITE" then permit
        native-socket: sockdom eq "AF_INET" and socktype eq "SOCK_RAW" then perm
it
        native-getuid: permit
        native-setresuid: permit
        native-mprotect: prot eq "PROT_READ|PROT_WRITE" then permit
        native-write: permit
        native-munmap: permit
        native-exit: permit

# _
```

fhttpd systrace sketch:

- Inside of the zip folder titled “fhttpdpolicy.txt”

4.2 Network Interference Analysis:

- John Jay Network scan using Netalyzr:

The first scan performed using the NetAlyzr tool online was within the John Jay network. Within the network some red flags included, DNS lookups of popular domain names, specifically mail.live.com; where possible DNS misconfiguration is possible or even an ISP DNS MITM is occuring:

Note! The session content is potentially harmful to your computer when viewed in a browser, so use caution when examining it.

Name	IP Address	Reverse Name/SOA
mail.live.com	204.79.197.212	a-0010.a-msedge.net

Another red flag occurred with network connectivity issues as reported here:

Background measurement of network health (?): 1 transient outages, longest: 36.2 seconds–

During most of Netalyzr's execution, the client continuously measures the state of the network in the background, looking for short outages. During testing, the client observed 1 such outages. The longest outage lasted for 36.2 seconds. This suggests a general problem with the network where connectivity is intermittent. This loss might also cause some of Netalyzr's other tests to produce incorrect results.

Additionally, quite a few ports were blocked presumably to preserve bandwidth in some cases, in others simply because the associated services were unneeded and would create a larger attack surface that would be easily avoidable by preventing access.

Attached within the project zip file, you will find the text file for the client and the browser .htm file of the website. For full functionality please click the permalink option on the top right.

5 Word Problems:

1. Compare SELinux, systrace, and AppArmor in their approach to protect the operating system from attacks.
    - These tools are used to provide secure environments for applications/services to run in.

    - SELinux attempts to control the processes using strict access control policies, in general these rules are far more complex than the access control options in standard Linux. SELinux serves as a hardened option, which modifies the kernel, ideally running the profile kernel_t until the user is logged in. The user will then have been swapped by context switching to either uncofined_t or user_t.
    Profiles referenced from: https://fedoraproject.org/wiki/SELinux/EnforcePolicy

    - SysTrace is a tool which comes installed within OpenBSD which utilizes the system structure in hopes to monitor, intercept, or restrict system calls within OpenBSD. This leads to policy enforcement and can minimize the attacks resulting from many forms of security vulnerabilities, overflows, control flow hijacks, etc. The idea is that you enact policies for each subsystem that the user will protected in unknown environments/paths, within the policy set to protect against new paths being executed.
    OpenBSD Systrace Referenced from:
    http://www.informit.com/articles/article.aspx?p=363731

    - Lastly, AppArmor uses profiles generated in order to provide restricted access to applications/services. It enacts logging of policy violations, and allows for dual mode usage where AppArmor can monitor logs and learn restricted behavior or enforcing mode which enforces installed/generated profiles on the system in order to protect system access, and enforce the user space.

2. What is your base trust as you connect to remote servers, i.e. what (counter)measures do you need to ascertain the integrity of the network data (e.g. web pages, images, streams, correct destination) sent by you and to you?
    - A simple baseline would be a firewall and antivirus installation on all equipment used within the corporation. Limit or avoid the use of flash drives to prevent the spread of malware and lost or theft of data. The systems should be checked regularly for any possible hidden or visible malware.