Securing Linux Computer

- **Purpose**
- **Requirements**
  - Proper Allowance of Access and Use
  - Strong Passwords and/or SSH Keys on accounts or services running on the machine
  - Have the Firewall enabled and configured
    - Firewall Considerations
    - Make use of Fail2Ban
- **Rules of Thumb**
  - Disable what you aren’t using.
  - Restrict Access as much as possible
  - Keep the system updated
  - Double check your security after an Application Install
- **Check how exposed you are**
- **Special Cases**

**Purpose**

This article covers what should be considered mandatory concerns for Cybersecurity for Linux Based Computers

All users are responsible for the security of their computers per Campus and UC Network Policies and Procedures outlined by the following:

- Digital Millennium Copyright Act at UCSB
- University of California Electronic Communications Policy
- University of California’s Security Standard for Everyone and All Devices
- UCSB Network Citizenship

(These are outlined also at: UCSB Network Policy and Procedures)

**Requirements**

**Proper Allowance of Access and Use**

As outlined in the University of California Electronic Communications Policy:

- Access is to be restricted to University Users (As defined as University students, staff, faculty and affiliated with the University)
- Public (Non-University Users) may only have access to machines that have been authorized as Public Use/Access per sponsorship by the University.

This means that any and all access to machines hosted on the campus network should not have ‘open access’.

**Strong Passwords and/or SSH Keys on accounts or services running on the machine**

Regardless of what you are doing with the computer, all user accounts should have a Strong Password

The definition of a ‘Strong’ password is:

- Be at least 12 characters long (However, more is better)
- Case sensitive (Meaning should have UPPER and lower case letters)
- Contains a mixture of letters and numbers
- Contains symbols (Such as #, ! and so forth…)
- Does not use words found in any dictionary (Such as names or words)
- Does not use letters or numbers in sequence or in repeated fashion (Like 1111, 1234, abcd)
- Using a password that contains public knowledge information related to you (Such as your address and the like.)

(Reference: Password Management on UCSB Information Security)

If you have difficulties remembering a strong password, the alternative is to make use of SSH Keys to access the machine.

Just be aware that when using SSH keys, the SSH key should be unique to the computer trying to access the machine.

To make an SSH key, please refer to Setting up SSH Keys or Google it for the particular system you are using.

For services, it is highly recommended to change the password to a strong password.

Lastly, try to avoid using the same password on multiple services or accounts.
Have the Firewall enabled and configured

By default, Linux does not have its firewall configured to restrict access.

It is strongly encouraged to configure the system's firewall to restrict the access to the machine's resources to only what is necessary.

We can point you to IPTables - Basics to put up a basic firewall, but highly encourage doing proper fine tuning of your system's firewall for additional allowances.

Some flavors of Linux will have a GUI Firewall, which we highly recommend people to Google on how to use it and configure it locally.

While Ubuntu is not a supported operating system we do have some basic instructions due to the number of people asking for a UFW - Basics example

**Firewall Considerations**

Note, your computer will be on a Public IP address.

This means your computer is visible to the entire world.

Any services that are meant for research or testing should be restricted to the campus' network, which is 128.111.0.0/16 (128.111.0.0-128.111.254.254)

Any application or service that uses the Network is considered 'vulnerable' as some services like Hadoop, mysql and such are designed for network interaction beyond itself and often times not secured unless the user of the system proactively sets up security.

Always assume anything installed onto the system is not secure and you must secure it by all means possible.

Firewalls should be set to the Campus network for Allow and the default action for anything else to Drop or Reject to avoid ease of compromise.

**Make use of Fail2Ban**

In some cases, we recommend making use of Fail2Ban, a linux package that should be available for most Linux Flavors.

This works along with the linux firewall system with a specific purpose in mind...

For services you want it to watch and protect, it will note the number of attempts being made by an outside source.

If an IP has tried multiple times and failed, it will be put on a block list for a period of time, slowing down the intruder from accessing the system.

There are a few tutorials on how to set up fail2ban on Google, and we would recommend using this for at least protecting your SSH access to the machine.

**Rules of Thumb**

Disable what you aren't using.

Disable any services that isn't needed.

Avahi (mDNS or Bonjour) isn't necessary or should be running and often times shows up on OIT security scans.

SAMBA (File Sharing) isn't necessary unless you are planning on being a file share server.

RPCBIND (For NFS) isn't necessary unless there is going to be network file share links to be made.

Basically, look for what is running on the machine and disable what isn't necessary for what you need at this time.

Restrict Access as much as possible

As mentioned before, it is strongly encouraged to use the firewall, but even more so, restrict who can access to it.

By setting the firewall to only allow connections from campus, it requires people to make use of the campus network or the Campus VPN, which will require them to work harder to access the computer.

While this may seem to be an inconvenience for you access wise, it is much less of an inconvenience than to have your system compromised and cut off due to it being an issue or worse, requiring you to rebuild the system due to it being hijacked and encrypted.

Please refer to IPTables - Basics on setting up at least IPTables Firewall that is available for most Linux based OS systems.

Keep the system updated

Just like a Windows or Mac, Linux does have security updates that need to be taken care of from time to time.
Make sure your kernel is up to date and still supported.

Double check your security after an Application Install

Always check your system after a new application has been installed.

Some may open up ports to listen to that you did not have open before or set up a new account.

If this is the case, go through Security Checklist and make sure everything is secure.

If you have recently installed an network listening application, please be sure to update your firewall to restrict outside access appropriately and/or accounts related to it.

Check how exposed you are

There is a linux tool called nmap.

You can use this to check your machine for what ports are open.

nmap may require having sudo or root access at times for some of the functions.

You can also make use of http://nmap.online-domain-tools.com/ to test it from the internet side.

You should do this from time to time, especially after adding a new application to see what is visible.

Special Cases

Occasionally specific operating systems have some security concerns that are specific to said operating systems. For example users of Raspberry Pi's have to worry about disabling the default "Pi" user on older Raspberry Pi's, something that other operating systems do not have to worry about. Likewise Ubuntu users have to worry about turning on their firewall since it comes turned off by default, see UFW - Basics. While we do have specific pages for the most common issues, it is always good to check with the makers of each operating system for system specific security issues. Please note that Debian, Raspberry and Ubuntu are all non-supported operating systems, all help for them is "best effort". If you install these non-supported operating systems on your personal computer, you are essentially taking responsibility for your own security.

Centos - https://wiki.centos.org/HowTos/OS_Protection
Debian - https://www.debian.org/doc/user-manuals#securing

Related articles

- UFW - Basics
- Digital Piracy
- Securing Linux Computer
- I get 'Critical Security Alert' email from Google
- Security Checklist