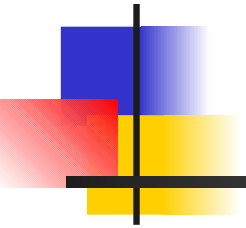
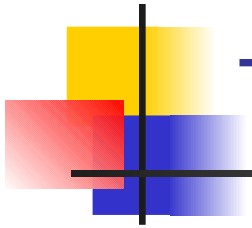


SEC520

System Hardening (part 2)



Today's Objectives

Rules of Least Privilege / Continued:

- AAA Protocol (Authorization)
  - ACLs
  - SELinux
  - Sudo
  - Cron Jobs

AAA Protocol (Authorization / Access)

ACLs are specialized permission sets for files and directories. They extend beyond the traditional user group method of limiting or permitting access to files and directories.

For example, when creating a group for members to share, you also have the ability to specify individual users and their permissions for that specific file or directory.

Setting group permissions with chmod blankets users that belong to same group (eg **read** only), but ACLs allow customized permissions for certain individuals (eg. **read** and **write**) for that same group.

You may be required to enable ACLs in the **/etc/fstab** file and modify the options for booting root "/"
(highlited in blue):

eg. errors=remount-ro**,acl**

AAA Protocol (Authorization / Access)

To set acl permissions for directories or files, you are required to issue the following command:

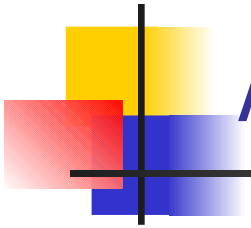
setfacl [options] g:groupname:permissions filepathname

Options: **R** – recursive
d – default (apply rules for newly-created files created in specific directory)
m – modify/change ACL rules

Permissions: **rwx** (or any combination to set)

To confirm ACLs, you use the command:

getfacl filepathname



AAA Protocol (Authorization / Access)

SELinux

Stands for **Security Enhanced Linux**

Contains a set of Kernel modifications that provide policies to make certain processes (user or system) are only running withing their limits.

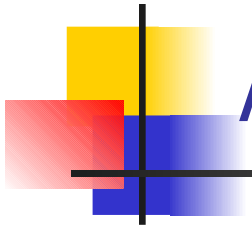
SELinux provides flexibility in setting policies.

There are basically **three modes** in SELinux:

- **Enforcing** (strictly enforces the policies)
- **Permissive** (prints warnings instead of enforcement)
- **Disabled** (Turn off SELinux)

The configuration file for SELinux is located in: **/etc/sysconfig/selinux** (pathnames may vary)

Can enforce SELinux in the configuration file, or issue the command: **setenforce <mode>**



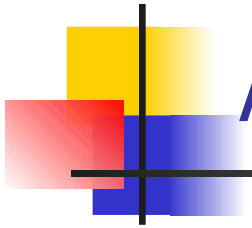
AAA Protocol (Authorization / Access)

Sudo

Stands for **Switch-User Do** (sometimes referred to as Super-User Do).

This allows the user that has root priviledge to issue Linux commands to perform administrative tasks, without opening a shell in root, thus preventing the possibility of making a mistake while logged in as root, or vulnerability to attack.

Example: Editing system configuration files,



AAA Protocol (Authorization / Access)

Sudoers File

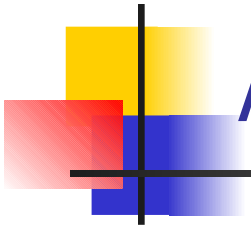
The configuration file for sudo.

The configuration file for sudo is located in the pathname: **/etc/sudoers**

Note: It is not recommended to edit this file directly in case there are errors in syntax in the **/etc/sudoers** file.

Instead, the administrator issues the command: **visudo**

This command pocesses the ability to check for syntax errors prior to taking effect on the system.



AAA Protocol (Authorization / Access)

Sudoers File

In this file, you will see the entry:

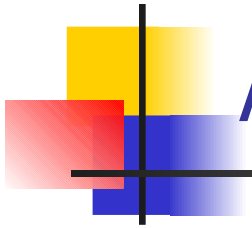
root ALL=(ALL) ALL

The first ALL indicates that root can run from any terminal. The second ALL indicates that root can run as any user. The Third ALL indicates that root can run any command.

If other **TRUSTED** users have been given elevated root priveleges, it is better to list the application(s) that the user has access to.

eg. (Add below the **root** entry):

username ALL=/usr/bin/vi # use absolute pathnames!
username ALL=ALL permits
full access via sudo command



AAA Protocol (Authorization / Access)

Crontab Utility

Cron is a scheduler for Unix and Linux operating systems. The name is the short for Cronograph which is an old expression for a watch or "time piece"

This scheduler can help Unix / Linux system administrators to run commands or shell scripts automatically at a desired date and time.

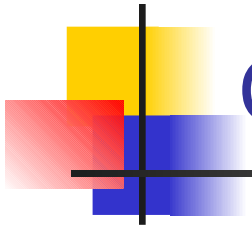
System administrators need to limit the number of users that run cron jobs for reducing the risk of system vulnerability. Poorly written shell scripts can all exploitation by hackers.

AAA Protocol (Authorization / Access)

How crontab file Works:

- The first entry is for scheduling:

```
.---------------- minute (0 - 59)
|   .------------- hour (0 - 23)
|   |   .---------- day of month (1 - 31)
|   |   |   .------- month (1 - 12) OR jan,feb,mar,apr ...
|   |   |   |   .---- day of week (0 - 6) (Sunday=0 or 7)  OR
|   |   |   |   |                  sun,mon,tue,wed,thu,fri,sat
|   |   |   |   |
*   *   *   *   *  command to be executed
```



Crontab Utility

How to use cron:

To create a crontab entry:

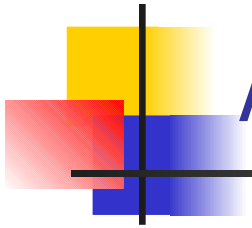
crontab -e (creates or edits crontab file)

Adminstrators should configure cron to not allow unpriviledged users from running cron jobs, and create exceptions for trusted users.

crontab -u username -e

The adminstrator can also permit or deny users from creating cron jobs by editing the files:

- **cron.allow**
- **cron.deny**



AAA Protocol (Authorization / Access)

Turning-off XWindows

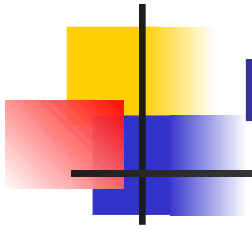
Hackers can exploit X-windows programs that are running on servers.

It may make sense to put your server into text-based mode (with networking) as opposed to graphical mode.

Older Linux systems use the init command (eg. **init 3**) , while newer Linux systems use the **systemctl** command.

You can refer to following notes:

http://zenit.senecac.on.ca/wiki/index.php/Init_vs_systemd



Lab Time

Perform:

Lab 7: Linux System Hardening (Part 2)