

# Cyber Security Lab – SE Linux

## Due

Thursday, March 27, 2008

## Goal

Exercise SELinux type enforcement and MCS policy to separate groups of users.

## Scenario

Bob Co is looking at using SELinux to separate groups of users instead of or in addition to their use of discretionary ACLs on Windows. As you recall from the Windows ACL exercise, Bob Co has three sets of employees:

- Engineers
- Financial folks
- System Administrators

Each set of folks would like a place on the file system where in general they have full control and other folks have read-only access. But each group of folks would like to have the following subareas with different access:

- A public area that gives all users read and write access.
- A private area that blocks everyone except for folks of the same set.

The lab machines have been populated with the following users

Alice – Currently an engineer, but she used to be a financial person and she still sometimes fulfills that role.

Bob – An engineer.

Carol and Dave are both Financial folks

Ellen and Gus are both sys admins

Bob, president of Bob Co, wants to know what a type enforcement policy to support this scenario would look like. He also wants to know if the MCS mechanism can support all of these requirements.

## Your tasks

You will work individually on your own linux VM. Use distinct VM names to avoid collisions with other students. Each machine has the following scripts installed in /root.

- Clone-local-vm.sh – Creates a clone of a VM on the machine. All the state for the virtual machines is stored in directories in /var/lib/vmware/Virtual Machines. To make a copy of sclass1-linux, invoke as root “/root/clone-local-vm.sh sclass1-linux sclass1-skh-linux”. After the script completes, you should be able to open the VM sclass1-skh-linux from within the vmware server (which you started as root).
- Clone-vm.sh – If the original machine you were working on is in use, you can copy a VM from one machine to another. On the original machine, tar and zip up the original directory, e.g. tar czf sclass1-skh-linux.tar.gz. Use scp to copy that tar.gz file to the /var/lib/vmware/Virtual Machines directory on the target system. Then on the target run (as root) “/root/clone-vm.sh sclass1-skh-linux.tar.gz sclass1-skh-linux sclass3-skh-linux”.

In both cases, you will need to rename the machine within the VM. This can be done by editing the /etc/sysconfig/network file.

You will need to perform the following tasks.

1. Use MCS to associate categories with users and files to enforce the required data separation.
  - a. Create a subdirectory to categorize and exercise the system requirements.
  - b. Determine whether all the requirements can be satisfied.
2. Use the Policy Generation tool to create the basics of user type enforcement policies to implement the required separation. The Policy Generation tool will create the appropriate user policies, but you will need to create the directory and file types and appropriate allow rules. Look at the “Configuring the SELinux Policy” (<http://www.nsa.gov/selinux/papers/policy2-abs.cfm>) distributed in class for details on the type enforcement language syntax and the standard rights sets and file type attributes. The Policy Generation tool will create a shell file that compiles and loads your policy. The SE Linux management tool can be used to associate users and delete modules if needed.
  - a. Create a subdirectory to set file labels and exercise the type enforcement policy.
  - b. Determine whether all the requirements can be satisfied.
  - c. Does your type enforcement policy work with unconfined users? Can you block users with the unconfined\_t type from reading or writing in the private area?
  - d. Use the Policy Analysis Tool (apol) to determine who has access to your new file types. Specifically, what access does unconfined\_t have to your file types?
  - e. You do not need to fix up the home directory labeling for the type enforcement users, but you may need to ssh in from the base system to test user access.

## Hand-in Items

Hand in via compass. Provide the following items:

- Use “zip” to compress and encrypt your virtual machine. In your writeup, indicate the physical machine you worked on, the location of your zip file, and the encryption password.
- Report on the the results of your MCS research. How did you configure the MCS policy? How well does MCS satisfy Bob Co's requirements. What if any requirements cannot be met? What experiments did you perform? This configuration should still be on your VM, so Bob can look it over.
  - Include a sample SE Linux access failure log entry from your MCS experiments. This can be retrieved from the SE Troubleshooter or directly from `/var/log/audit/audit.log`.
- Report on the results of your TE research. Where is your type enforcement policy? What if any requirement cannot be met? What experiments did you perform? This configuration should still be on your VM, so Bob can look it over.
  - Include a sample SE Linux access failure log entry from the TE case. This can be retrieved from the SE Troubleshooter or directly from `/var/log/audit/audit.log`.
  - Include the results of type analysis from `apol` to show what access `unconfined_t` has to one of the types you created for one of the group's files.
- How do both techniques compare to the ACL approach you saw in Windows? Which mechanism would you recommend to Bob Co and why?