

Cyber Security Lab2 - Comments

Most everyone got the basic corporate policy working eventually. The biggest difficulty was getting the policy to load and getting audit messages to show up. Unfortunately, we seemed to have encountered more problems this year than last year. Perhaps because I had tried to introduce MLS policy and so increased the number of versions of policies that could collide. Also, I think SE Linux itself is going through many transitions this year, and so it is in a more fragile state than it has been in the past.

This war of attrition with getting things to work is fairly standard in working with complex systems, but I am afraid that the SE Linux exercise this year was worse than normal. This is an excellent example of why people administering real world systems will try out the new versions in a lab environment first before committing upgrades to their installed base.

Auditing successful transitions

Fillipo was the only person to get the auditallow to work to track role transitions. Since we are looking at auditing transitions, we are actually looking at executing another program to enable the transition. So you need to have two audit allow statements.

I've decided to score the successful auditing as an extra credit. As long as you made a reasonable attempt at using auditallow you will get the base credit.

```
auditallow user_t newrole_t:process transition;  
auditallow newrole_t corporate_t:process transition;
```

Then someone reviewing the log would need to note two audit logs to have proof that someone made the transition from user_t to corporate_t domains.

Policy Discussion

Some of the discussion of what policy was preventing and allowing access was a bit unclear. Several folks said that sysadmin_t was like root in standard Unix and had special exemption from privilege. This is not the case. In the strict policy, sysadmin_t is a very privileged domain and has many "allow" statements that enable it to access most if not all types. But that is just how this policy is put together not something intrinsic to the SE Linux type enforcement model.

Some others made statements that domains cannot access types in other domains. For the standard user domains like user_t and corporate_t this is mostly true for this policy. Although standard user domains are able to execute files in system domains like newrole_t. The more basic statement that I was looking for was that there was no rule allowing the access between the domains and so the SE Linux model of default deny would block the access.