Assignments:07

Module:- COSA(SELinux&Iptables) Name:- Prithviraj Nikam

Lab Assignment :-

3. SElinux

Security-Enhanced Linux (SELinux) is a security architecture for Linux® systems that allows administrators to have more control over who can access the system. It was originally developed by the United States National Security Agency (NSA) as a series of patches to

the Linux kernel using Linux Security Modules (LSM).SELinux was released to the open source community in 2000, and was integrated into the upstream Linux kernel in 2003.SELinux defines access controls for the applications, processes, and files on a system. It

uses security policies, which are a set of rules that tell SELinux what can or can't be accessed, to enforce the access allowed by a policy.When an application or process, known as a subject, makes a request to access an object,like a file, SELinux checks with an access vector cache (AVC), where permissions are cached for subjects and objects.

How to handle SELinux errors

When you get an error in SELinux there is something that needs to be addressed. It is likely 1 of these 4 common problems:

1. **The labels are wrong. If your labeling is incorrect you can use the tools to fix the labels.**
2. **A policy needs to be fixed. This could mean that you need to inform SELinux about a change you've made, or you might need to adjust a policy. You can fix it using booleans or policy modules.**
3. **There is a bug in the policy. It could be that a bug exists in the policy that needs to be addressed.**
4. **The system has been broken in to. Although SELinux can protect your systems in many scenarios, the possibility for a system to be compromised still exists. If you suspect that this is the case, take action immediately.**

4. Describe IPTABLES

Iptables is used to set up, maintain, and inspect the tables of IP packet filter rules in the Linux kernel. Several different tables may be defined. Each table contains a number of built-in chains and may also contain user-defined chains.Each chain is a list of rules which can match a set of packets. Each rule specifies what to do with a packet that matches. This is called a 'target', which may be a jump to a user-defined chain in the same table.