
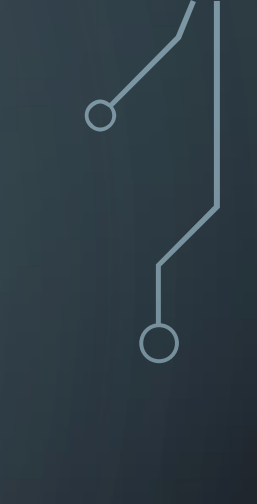
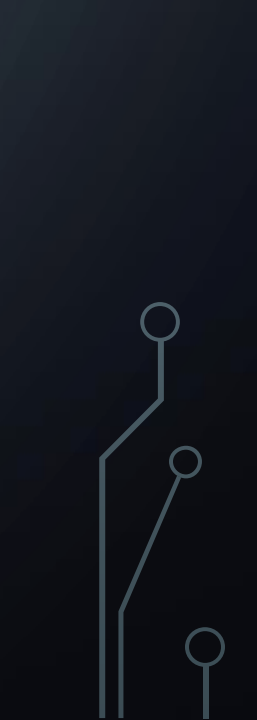




SELINUX



OBJECTIVES

- Describe what SELINUX is
 - Understand why we don't just disable it
 - Discuss how SELINUX provides Least Privilege
- 
- 
- 

PROBLEMS WITH DAC

- Administrators cannot control every user
- File permissions and ACLs cant protect against everything
- Processes can change permissions and other security properties
- Compromised software may have access to other parts of the system

SELINUX

- Stands for Security-Enhanced Linux
- Originally developed by the NSA to show the value of Mandatory Access Control
- Built into the Linux kernel as of kernel 2.6
- Primarily used in RedHat and related distributions – Fedora, CentOS, and Scientific Linux

SELINUX BREAKDOWN

- Deny by default
- Log everything
- Only allow exceptions one at a time

SELINUX MODES


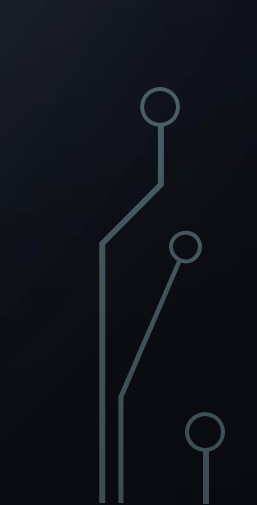
- Enforcing – Default mode which will enforce the SELinux security policy on the system
- Permissive – SELinux is enabled, but does not enforce. Also logs. Good for troubleshooting
- Disabled – SELinux is disabled. Never use this.

TYPES OF ENFORCEMENT

- Type Enforcement – Primary control which uses the “targeted” policy
- Role-Based Access Control – Enforcement based on a users role
- Multi-Level Security – Used in the “targeted” policy, but generally hidden and not often used
- Multi-Category Security – Extension of Multi-Level, but



FEATURES AND BENEFITS

- Policies are separate from enforcement
 - Great logging
 - Controls much of the OS such as files, processes, network, process execution
- 
- 

DOWNFALLS

- Can be time consuming to understand
- Complex
- While everything is logged, finding what may have been denied can be difficult
- If you make a change, you have to submit the new context

TYPICAL USAGE

- A web server might use SELinux to block a user from creating content within a directory
- Users might only be able to access certain files
- Secure systems might employ SELinux for least privilege across many areas

CONCLUSION

- SELinux provides powerful control over a system
- Use it if you want to have a very secure system
- Time and patience may be needed to configure it