SE Linux

Security Design

System Examination

System Configuration

Firewalls and Filters

Hardening Software

Backups and Change Management

Access Control and Authentication

Virtual Private Networking

Logging and Monitoring

Security Policy and Management Support

SELinux

Linux Systems Security

SELinux Concepts

- SELinux is a set of tools, libraries, and kernel components which add Mandatory Access Control (MAC) features to Linux using a least-privilege model
- It defines labels for SELinux users (distinct from Linux users), SELinux roles, SELinux types, and SELinux categories
- File and network connection resources are labeled
- Linux users are assigned SELinux labels, typical systems just lump all Linux users together as a single SELinux user for MAC purposes
- Linux processes are assigned SELinux labels
- Attempted uses of resources must not only be permitted by the Discretionary Access Control permissions, but also be allowed by the MAC policy rules

SELinux Modes

- SELinux can be set to 3 different operating modes
- Disabled means SELinux may be configured but is ignored
- Permissive means SELinux is configured and logs policy violations, but does not interfere with any use of any resources
- Enforcing means SELinux is configured and prevents any resource uses which are not permitted by policy rules, logging those violations in /var/log/audit/audit.log

SELinux Operation

- The permissive or enforcing modes may be set as Strict, Targeted, or MLS
- Strict means all resources and processes are labeled and affected by SELinux
- Targeted means only specific processes are affected by SELinux, they run in a confined domain, everything else runs in an unconfined domain
- MLS/MCS allows for more complex multilevel labeling of entities using a sensitivity value and a category value which can then be used in dominance rules and is not typically implemented

SELinux Type Enforcement

- Type enforcement is the primary method of providing MAC in SELinux, as opposed to RBAC (using SELinux users and roles) and MLS/MCS (Using sensitivity and category along with dominance rules)
- TE means that each file and network connection has a context label, running processes also have a context label
- Since the default targeted policy more or less obviates users, roles, and dominance, TE means that access is granted or denied based on whether the process context has access to the resource context in the installed policy
- The configured SELinux mode and enforcement mechanism is found in /etc/selinux/config

SELinux Status

- The sestatus command will show the current state of SELinux on your system - you may have to install policycoreutils to get this utility
- The seinfo -t command will show the currently configured contexts on your system - you may have to install setools to get this utility
- The semanage user -l command will show the configured SELinux users and their sensitivities, categories, and roles - you may have to install policycoreutils-python-utils to get this utility
- The semanage login -l command will show the configured SELinux to Linux user mappings
- The semanage port -l command will show the configured SELinux network port contexts

SELinux Labeling

- To see if a file has an SELinux label, look for the . at the end of the permission bits
- To see the label on a file, use ls -Z
- To see the label on a process use ps -Z
- To change the label on a file, use chcon
- To automatically label an entire filesystem, create an empty .autorelabel file at the top of the filesystem and reboot

SELinux Logging

- SELinux writes log entries to /var/log/audit/audit.log unless auditd is not running, in which case they go to /var/log/messages
- The entries can be found by looking for lines with AVC in them
- There is a GUI tool for reviewing them in the setroubleshoot package
- The audit2allow command can take log entries as input and produce a policy rules file you can import to update your policy to allow things which your current policy denies and logs

SELinux Resources

- https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/SELinux_Users_and_Administrators_Guide/
- https://wiki.centos.org/HowTos/SELinux
- https://wiki.gentoo.org/wiki/SELinux/Tutorials
- http://www.fosteringlinux.com/category/articles/selinux/
- SELinux internals - https://www.imperialviolet.org/2009/07/14/selinux.html