15.2.7 File Auditing Facts

File auditing involves looking for files that pose a security risk to the computer.

This lesson covers the following topics:

- File types that pose a risk
- Commands used to audit

File Types that Pose a Risk

File types that pose a security risk to a computer, include:

- Executable files owned by the root user that have the SUID (Set User ID) permission. With the SUID permission, executables will run with the owner permissions, not with the permissions of the user who runs them.
- Executable files owned by the root group that have the SGID (Set Group ID) permission. With the SGID permission, executables will run with the group permissions, not with the permissions of the user who runs them.
- Files that have the write and execute permissions for others (everyone on the Linux system who is not a user or group owner of the file). If the file is writable by others, anyone can replace the file with a malicious script to create a security risk.

There is a limited number of files on a Linux system owned by root or the root group that legitimately need the SUID or SGID permission set. Before changing permissions, first verify whether they actually have been set appropriately.

Commands Used to Audit

The following table lists several file auditing commands:

Command	Function	Examples
find / type f -perm	Audits for files that pose a security risk. Be aware of the following options: - **-o=x** audits for the execute permission for others. - **-o=w** audits for the write permission for others. - **-g=x** audits for the execute permissions for group owners. - **-g=s** audits for the SGID bit. - **-u=s** audits for the SUID bit. Include the **-ls** option to display the results with the long listing.	**find / -type f -perm -u=s -ls** **find / -type f -perm -g=s -ls** **find / -type f -perm -o=x -ls** **find / -type f -perm -g=x -ls** **find / -type f -perm -u=x,o=w -ls**
crontab -e	Schedules the auditing task to run on a regular basis.	