Cybersecurity

Operations and Incident Response

4.1.2 File Manipulation Tools

What are 6 tools used to interact with files from the command line?

Overview
Given a scenario, the student will use the appropriate tool to assess organizational security.

Grade Level(s)
10, 11, 12

Cyber Connections

- Threats & Vulnerabilities
- Networks & Internet
- Hardware & Software

This content is based upon work supported by the US Department of Homeland Security's Cybersecurity & Infrastructure Security Agency under the Cybersecurity Education Training and Assistance Program (CETAP).

Teacher Notes:

CompTIA SY0-601 Security+ Objectives

Objective 4.1

- Given a scenario, use the appropriate tool to assess organizational security.
    - File manipulation
        - head
        - tail
        - cat
        - grep
        - chmod
        - logger

File Manipulation Tools

There are many tools that allow users to interact with files from the command line; one of the first command line tools that someone would use is the cat command. The `cat` command can be used in a couple of ways, either combining (or concatenating) files or printing their output to the Terminal. Simply using cat with a file name, like `cat constitution.txt`, would display the contents of the file in the Terminal. This can be handy if the user wants to read what is in a file without having to open that file. Cat can also be used to combine files in different ways. One popular method is by adding text to another file. For example, `cat bill1754.txt > constitution.txt` is a command that would add the contents of bill1754.txt to the end of constitution.txt.

The `cat` command is a great command to quickly read the contents of a file, but what happens if that file is super long, like if it was an entire novel? The `head` command will show the first few lines of a file if a user only wants to see a certain number of lines. For example, `head TaleOfTwoCities.txt` would only show the first 10 lines of the document TaleOfTwoCities.txt (10 is the default number of lines). If the user wanted to show the first 20 lines, they could use the command head `-n 20 TaleOfTwoCities.txt`. Similarly, if a user wanted to show the last lines of a file, they could use the tail command. `tail -n 20 TaleOfTwoCities` would show the last 20 lines of the document TaleOfTwoCities.txt.

What if a user wants to search for a certain word or phrase in a file? This can be done with the `grep` command. `grep` technically searches for patterns within a file and is a very powerful tool. A simple `grep` command can

Teacher Notes:

look like `grep 'Watson' sherlock.txt`; this would search a file called sherlock.txt for the phrase (or word in this case) "Watson" and display all the lines that contain it. There are options to ignore case (make it case insensitive), not display the lines but rather how many lines contain the phrase, plus many more options for the `grep` command.

Every file can have three different permissions for all the users on the system. Each user can have any form of the following three permissions: they can have the ability to execute the file, or run the file, they can read the file, view what is inside the file, and/or they can write the file or edit it. The `chmod` (Change Mode) command controls the permissions that each user has. This can be done numerically or with letters. This is done numerically by adding up from the following: execute = 1, write = 2, and read = 4. Thus, if a user has the number 3 for a file, they have the permissions to execute and write the file since 2+1=3. If they have a 7, then they have the ability to read, write, and execute the file. A 0 means they have no permission on the file. Another form is through letters where r = read, w = write, and x = execute. If they have wx, then the user has the permissions to write and execute the file.

The last command is the `logger` command. This command allows a user to enter messages into the system log. By default, the commands are stored in the `/var/log/syslog` file. This allows all users on the system to keep up to date by reading the syslog to see what everyone has done on the system.