Core commands for navigation and reading files

Welcome back. I hope you're learning a lot about how to communicate with the Linux OS.
As we continue our journey into utilizing the Linux command line, we'll focus on how to navigate the Linux file system.

Now, I want you to imagine a tree.
What did you notice first about the tree?
Would you say the trunk or the branches?
These might definitely get your attention, but what about its roots?
Everything about a tree starts in the roots.
Something similar happens when we think about the Linux file system.

Previously, we learned about the components of the Linux architecture.
The Filesystem Hierarchy Standard, or FHS, is the component of the Linux OS that organizes data.
This file system is a very important part of Linux because everything we do in Linux is considered a file somewhere in the system's directory.
The FHS is a hierarchical system, and just like with a tree, everything grows and branches out from the root.
The root directory is the highest-level directory in Linux.
It's designated by a single slash.
Subdirectories branch off from the root directory.
The subdirectories branch out further and further away from the root directory.
When describing the directory structure in Linux, slashes are used when tracing back through these branches to the root.
For example, here, the first slash indicates the root directory.
Then it branches out a level into the home subdirectory.
Another slash indicates it is branching out again.
This time it's to the analyst subdirectory that is located within home.
When working in security, it is essential that you learn to navigate a file system to locate and analyze logs, such as log files.
You'll analyze these log files for application usage and authentication.

With that background, we're now ready to learn the commands commonly used for navigating the file system.
First, pwd prints the working directory onto the screen.
When you use this command, the output tells you which directory you're currently in.
Next, ls displays the names of files and directories in the current working directory. And finally, cd navigates between directories.
This is the command you'll use when you want to change directories.

Let's use these commands in Bash.
First, we'll type the command pwd to display the current location and then press enter.
The output is the path to the analyst directory where we're currently working.
Next, let's input ls to display the files and directories within the analyst directory.
The output is the name of four directories: logs, oldreports, projects, and reports, and one file named updates.txt.
So let's say we now want to go into the logs directory to check for unauthorized access.
We'll input: cd logs to change directories.
We won't get any output on the screen from the cd command, but if we enter pwd again, its output indicates that the working directory is logs.
Logs is a subdirectory of the analyst directory.

As a security analyst, you'll also need to know how to read file content in Linux.
For example, you may need to read files that contain configuration settings to identify potential vulnerabilities.
Or, you might look at user access reports while investigating unauthorized access.
When reading file content, there are some commands that will help you.
First, cat displays the content of a file.
This is useful, but sometimes you won't want the full contents of a large file.
In these cases, you can use the head command.
It displays just the beginning of a file, by default ten lines.

Let's try out these commands.
Imagine that we want to read the contents of access.txt, and we're already in the working directory where it's located.
First, we input the cat command and then follow it with the name of the file, access.txt.
And Bash returns the full contents of this file.
Let's compare that to the head command.
When we input the head command followed by our file name, only the first 10 lines of this file are displayed.

Wow, this section had lots of action, and it's just the beginning!
I'm glad you learned how security analysts can use essential commands to navigate the system.
Next, we'll explore how to manage the system.

Revision #1
Created 2023-07-05 11:28:41 UTC by naruzkurai
Updated 2023-07-05 11:37:17 UTC by naruzkurai