**User Interfaces: How Users Communicate with the Operating System**

A computer's operating system (OS) serves as an intermediary between users and hardware, enabling task execution through **user interfaces (UIs)**. These interfaces allow users to control and interact with the OS efficiently.

The two main types of user interfaces are:

* **Graphical User Interface (GUI)** – Uses visual elements like icons and windows.
* **Command-Line Interface (CLI)** – Uses text-based commands to perform tasks.

**1. Graphical User Interface (GUI)**

A **GUI** is the most common way users interact with a computer. It provides a visual and intuitive experience with components such as:

* **Start menu** – Access programs and system settings.
* **Taskbar** – Launch and manage running applications.
* **Desktop icons** – Provide shortcuts to files and applications.

Using a GUI is like **ordering from a restaurant menu**—you select predefined options with minimal customization. Tasks are performed **one at a time**, making it user-friendly but sometimes less efficient for complex operations.

**2. Command-Line Interface (CLI)**

A **CLI** is a text-based interface where users enter commands to interact with the OS. Unlike a GUI, a CLI offers:

* **More flexibility and control** – Users can execute complex tasks quickly.
* **Automation and scripting** – Multiple operations can be completed simultaneously.
* **Efficient file management** – Tasks like moving specific file types can be done in seconds.

Using a CLI is like **cooking from scratch**—you have complete control over what you create. This makes it **powerful but requires technical knowledge**.

**3. Security Analysts and the CLI**

For security professionals, the **CLI is an essential tool** for tasks such as:

* **Log analysis** – Reviewing system activity for security threats.
* **User authentication and authorization** – Managing user access permissions.
* **System monitoring** – Checking processes and network activity.

While most users rely on a GUI, security analysts frequently use the CLI to **diagnose issues, automate tasks, and enhance security measures**.

**4. Learning to Use the CLI**

Most personal computers and mobile devices use a GUI, so many users are already familiar with this interface. However, security analysts need to master the **CLI, especially in Linux environments**. As you progress in your training, you will gain hands-on experience using the **command line for security-related tasks**.

A solid understanding of both interfaces ensures efficiency and adaptability when working with different systems.

# The command line in use

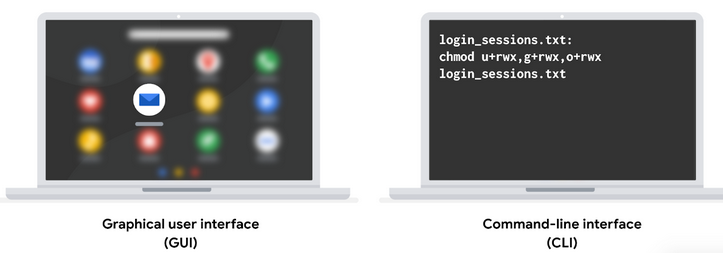
Previously, you explored graphical user interfaces (GUI) and command-line interfaces (CLI). In this reading, you’ll compare these two interfaces and learn more about how they’re used in cybersecurity.

## CLI vs. GUI

A **graphical user** **interface (GUI)** is a user interface that uses icons on the screen to manage different tasks on the computer. A **command-line interface (CLI)** is a text-based user interface that uses commands to interact with the computer.

### Display

One notable difference between these two interfaces is how they appear on the screen. A GUI has graphics and icons, such as the icons on your desktop or taskbar for launching programs. In contrast, a CLI only has text. It looks similar to lines of code.



### ****Function****

These two interfaces also differ in how they function. A GUI is an interface that only allows you to make one request at a time. However, a CLI allows you to make multiple requests at a time.

## Advantages of a CLI in cybersecurity

The choice between using a GUI or CLI is partly based on personal preference, but security analysts should be able to use both interfaces. Using a CLI can provide certain advantages.

### Efficiency

Some prefer the CLI because it can be used more quickly when you know how to manage this interface. For a new user, a GUI might be more efficient because they’re easier for beginners to navigate.

Because a CLI can accept multiple requests at one time, it’s more powerful when you need to perform multiple tasks efficiently. For example, if you had to create multiple new files in your system, you could quickly perform this task in a CLI. If you were using a GUI, this could take much longer, because you have to repeat the same steps for each new file.

### History file

For security analysts, using the Linux CLI is helpful because it records a history file of all the commands and actions in the CLI. If you were using a GUI, your actions are not necessarily saved in a history file.

For example, you might be in a situation where you’re responding to an incident using a playbook. The playbook’s instructions require you to run a series of different commands. If you used a CLI, you’d be able to go back to the history and ensure all of the commands were correctly used. This could be helpful if there were issues using the playbook and you had to review the steps you performed in the command line.

Additionally, if you suspect an attacker has compromised your system, you might be able to trace their actions using the history file.

## Key takeaways

GUIs and CLIs are two types of user interfaces that security analysts should be familiar with. There are multiple differences between a GUI and a CLI, including their displays and how they function. When working in cybersecurity, a CLI is often preferred over a GUI because it can handle multiple tasks simultaneously and it includes a history file.