All things Operating System

- Introduction to Course 4
- Helpful resources and tips
- Welcome to week 1; Introduction to operating systems
- Kim: My journey into computing
- Compare operating systems
- Inside the operating system
- Requests to the operating system
- Resource allocation via the OS
- Virtualization technology
- GUI versus CLI
- The command line in use
- Ellen: My path into cybersecurity
- Wrap-up; Glossary terms from week 1

Introduction to Course 4

Hi! Welcome to this course on computing basics for security.
My name is Kim, and I work as a Technical Program Manager in security.
I grew up with computers and the internet but didn't really consider security as a career opportunity until I saw how it was interwoven into technology.

Before my first security job, I worked on a cloud application team and had to regularly interact with the security team.
It was my first experience working with security, but the idea of protecting information and working with others towards that goal was exciting to me.
As a result, I decided to work towards my CISSP, which led me to some new job opportunities at my company, and I was then able to move into security.

At this point, if you've been following along, you've already explored a variety of concepts useful to the security field, including security domains and networking.
I'm excited to join you during the next part of the program.
We'll take it slow so that you can understand these topics in practical ways.
The focus of this course is computing basics.
When you understand how the machines in an organization's system work, it helps you do your job as a security analyst more efficiently.

Part of your job as a security analyst is to keep systems protected from possible attacks.
You're one of the first levels of defense in protecting an organization's data.
To do this effectively, it's helpful to understand how the system you're protecting works.
In addition, you may need to investigate events to help correct errors in the system.
Being familiar with Linux operating system and its associated commands, and also being able to interact with
an organization's data through SQL, will help you with that.

In this course, you'll learn about operating systems and how they relate to applications and hardware.
Next, you'll explore the Linux operating system in more detail.
Then you'll use the Linux command line within a security context.
Finally, we'll discuss how you can use SQL to query databases while working as a security analyst.
I'm excited to explore all of these topics with you. Let's get started.

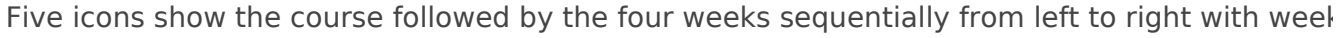
Course 4 content

because im legally not allowed to tell you the contents of the quizzes or its answers, the contents of the self review activities or interactive plugins. i wont be sharing that stuff but if you learn whats in this book you can probs do the quizzes pretty easly. however if you suck at writing idk maybe not so easly.

Each course of this certificate program is broken into weeks. You can complete courses at your own pace, but the weekly breakdowns are designed to help you finish the entire Google Cybersecurity Certificate in about six months.

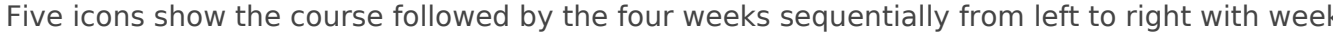
What’s to come? Here’s a quick overview of the skills you’ll learn in each week of this course.

Week 1: Introduction to operating systems



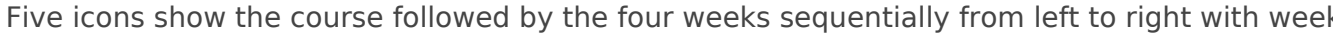
You will learn about the relationship between operating systems, hardware, and software, and become familiar with the primary functions of an operating system. You'll recognize common operating systems in use today and understand how the graphical user interface (GUI) and command-line interface (CLI) both allow users to interact with the operating system.

Week 2: The Linux operating system



You will be introduced to the Linux operating system and learn how it is commonly used in cybersecurity. You’ll also learn about Linux architecture and common Linux distributions. In addition, you'll be introduced to the Linux shell and learn how it allows you to communicate with the operating system.

Week 3: Linux commands in the Bash shell



You will be introduced to Linux commands as entered through the Bash shell. You'll use the Bash shell to navigate and manage the file system and to authorize and authenticate users. You'll also learn where to go for help when working with new Linux commands.

Week 4: Databases and SQL

Five icons show the course followed by the four weeks sequentially from left to right with week

You will practice using SQL to communicate with databases. You'll learn how to query a database and filter the results. You'll also learn how SQL can join multiple tables together in a query.

What to expect

Each course offers many types of learning opportunities:

- **Videos** led by Google instructors teach new concepts, introduce the use of relevant tools, offer career support, and provide inspirational personal stories.
- **Readings** build on the topics discussed in the videos, introduce related concepts, share useful resources, and describe case studies.
  - the following are available exclusively on Coursera
- **Discussion prompts** explore course topics for better understanding and allow you to chat and exchange ideas with other learners in the discussion forums
- **Self-review activities** and **labs** give you hands-on practice in applying the skills you are learning and allow you to assess your own work by comparing it to a completed example.
- **Interactive plug-ins** encourage you to practice specific tasks and help you integrate knowledge you have gained in the course.
- **In-video quizzes** help you check your comprehension as you progress through each video.
- **Practice quizzes** allow you to check your understanding of key concepts and provide valuable feedback.
- **Graded quizzes** demonstrate your understanding of the main concepts of a course. You must score 80% or higher on each graded quiz to obtain a certificate, and you can take a graded quiz multiple times to achieve a passing score.

because im legally not allowed to tell you the contents of the quizzes or its answers, the contents of the self review activities or interactive plugins. i wont be sharing that stuff but if you learn whats in this book you can probs do the quizzes pretty easily. however if you suck at writing idk maybe not so easily.

Tips for success

- It is strongly recommended that you go through the items in each lesson in the order they appear because new information and concepts build on previous knowledge.
- Participate in all learning opportunities to gain as much knowledge and experience as possible.
- If something is confusing, don't hesitate to replay a video, review a reading, or repeat a self-review activity.

- Use the additional resources that are referenced in this course. They are designed to support your learning. You can find all of these resources in the Resources
- tab.
- When you encounter useful links in this course, bookmark them so you can refer to the information later for study or review.
- Understand and follow the Coursera Code of Conduct

to ensure that the learning community remains a welcoming, friendly, and supportive place for all members.

Helpful resources and tips

As a learner, you can choose to complete one or multiple courses in this program. However, to obtain the Google Cybersecurity Certificate, you must complete all the courses. This reading describes what is required to obtain a certificate and best practices for you to have a good learning experience on Coursera.

Course completion to obtain a certificate

To submit graded assignments and be eligible to receive a Google Cybersecurity Certificate, you must:

- Pay the course certificate fee

or apply and be approved for a Coursera scholarship

- .
- Pass all graded quizzes in the eight courses with a score of at least 80%. Each graded quiz in a course is part of a cumulative grade for that course.

Healthy habits for course completion

Here is a list of best practices that will help you complete the courses in the program in a timely manner:

- **Plan your time:** Setting regular study times and following them each week can help you make learning a part of your routine. Use a calendar or timetable to create a schedule, and list what you plan to do each day in order to set achievable goals. Find a space that allows you to focus when you watch the videos, review the readings, and complete the activities.
- **Work at your own pace:** Everyone learns differently, so this program has been designed to let you work at your own pace. Although your personalized deadlines start when you enroll, feel free to move through the program at the speed that works best for you. There is no penalty for late assignments; to earn your certificate, all you have to do is complete all of the work. You can extend your deadlines at any time by going to **Overview** in the navigation panel and selecting **Switch Sessions**. If you have already missed previous deadlines, select **Reset my deadlines** instead.

- **Be curious:** If you find an idea that gets you excited, act on it! Ask questions, search for more details online, explore the links that interest you, and take notes on your discoveries. The steps you take to support your learning along the way will advance your knowledge, create more opportunities in this high-growth field, and help you qualify for jobs.
- **Take notes:** Notes will help you remember important information in the future, especially as you're preparing to enter a new job field. In addition, taking notes is an effective way to make connections between topics and gain a better understanding of those topics.
- **Review exemplars:** Exemplars are completed assignments that fully meet an activity's criteria. Many activities in this program have exemplars for you to validate your work or check for errors. Although there are often many ways to complete an assignment, exemplars offer guidance and inspiration about how to complete the activity.
- **Chat (responsibly) with other learners:** If you have a question, chances are, you're not alone. Use the discussion forums

to ask for help from other learners taking this program. You can also visit Coursera's Global Online Community. Other important things to know while learning with others can be found in the Coursera Honor Code and Code of Conduct

- .
- **Update your profile:** Consider updating your profile

- on Coursera to include your photo, career goals, and more. When other learners find you in the discussion forums, they can click on your name to access your profile and get to know you better.

Documents, spreadsheets, presentations, and labs for course activities

To complete certain activities in the program, you will need to use digital documents, spreadsheets, presentations, and/or labs. Security professionals use these software tools to collaborate within their teams and organizations. If you need more information about using a particular tool, refer to these resources:

- Microsoft Word: Help and learning
- : Microsoft Support page for Word
- Google Docs
- : Help Center page for Google Docs

- Microsoft Excel: Help and learning
- : Microsoft Support page for Excel
- Google Sheets
- : Help Center page for Google Sheets
- Microsoft PowerPoint: Help and learning
- : Microsoft Support page for PowerPoint
- How to use Google Slides
- : Help Center page for Google Slides
- Common problems with labs

- : Troubleshooting help for Qwiklabs activities

Weekly, course, and certificate glossaries

This program covers a lot of terms and concepts, some of which you may already know and some of which may be unfamiliar to you. To review terms and help you prepare for graded quizzes, refer to the following glossaries:

- **Weekly glossaries**: At the end of each week's content, you can review a glossary of terms from that week. Each week's glossary builds upon the terms from the previous weeks in that course. The weekly glossaries are not downloadable; however, all of the terms and definitions are included in the course and certificate glossaries, which are downloadable.
- **Course glossaries**: At the end of each course, you can access and download a glossary that covers all of the terms in that course.
- **Certificate glossary**: The certificate glossary includes all of the terms in the entire certificate program and is a helpful resource that you can reference throughout the program or at any time in the future.

You can access and download the certificate glossaries and save them on your computer. You can always find the course and certificate glossaries through the course's Resources

section. To access the **Cybersecurity Certificate glossary**, click the link below and select *Use Template*.

- Cybersecurity Certificate glossary

OR

- If you don’t have a Google account, you can download the glossary directly from the attachment below.

- click to donwload the doc

Course feedback

Providing feedback on videos, readings, and other materials is easy. With the resource open in your browser, you can find the thumbs-up and thumbs-down symbols.

- Click **thumbs-up** for materials that are helpful.
- Click **thumbs-down** for materials that are not helpful.

If you want to flag a specific issue with an item, click the flag icon, select a category, and enter an explanation in the text box. This feedback goes back to the course development team and isn’t visible to other learners. All feedback received helps to create even better certificate programs in the future.

For technical help, visit the Learner Help Center

.

Welcome to week 1; Introduction to operating systems

How many times a week do you use a computer?
For some of us, the answer might be "a lot"!
They are incredible machines that let us do everything from using specialized applications when completing a task at work to sending emails to loved ones in a distant place.
Have you ever thought about how computers can do all of this?
Well, that's where opperating systems come in.
In this section, we'll learn about common operating systems, and we'll explore the main functions of an operating system.
Then, we'll learn the relationship between operating systems, applications, and hardware.
Finally, we'll compare graphical user interfaces and command-line interfaces.
The command-line interface will be an essential part of your job as a security analyst.
Understanding operating systems is an important foundation for your career in security.
There's so much to explore. Let's begin.

Devices like computers, smartphones, and tablets all have operating systems.
If you've used a desktop or laptop computer, you may have used the Windows or MacOs operating systems. Smartphones and tablets run on mobile operating systems like Android and iOS.
Another popular operating system is Linux.
Linux is used in the security industry, and as a security professional, it's likely that you'll interact with the Linux OS.

So what exactly is an operating system?
It's the interface between the computer hardware and the user.
The operating system, or the OS as it's commonly called, is responsible for making the computer run as efficiently as possible while also making it easy to use.
Hardware may be another new term.
Hardware refers to the physical components of a computer.

The OS interface that we now rely on every day is something that early computers didn't have.
In the 1950s the biggest challenge with early computers was the amount of time it took to run a computer program. At the time, computers could not run multiple programs simultaneously.
Instead, people had to wait for a program to finish running, reset the computer, and load up the new program.
Imagine having to turn your computer on and off each time you had to open a new application!
It would take a long time to complete a simple task like sending an email.
Since then, operating systems have evolved, and we no longer have to worry about wasting time in this way.
Thanks to operating systems and their evolution, today's computers run efficiently.

They run multiple applications at once, and they also access external devices like printers, keyboards, and mice.

Another reason why operating systems are important is that they help humans and computers communicate with each other.
Computers communicate in a language called binary, which consists of 0s and 1s.
The OS provides an interface to bridge this communication gap between the user and the computer, allowing you to interact with the computer in complex ways.

Operating systems are critical for the use of computers. Likewise, OS security is also critical for the security of a computer.
This involves securing files, data access, and user authentication to help protect and prevent against threats such as viruses, worms, and malware.
Knowing how operating systems work is essential for completing different security related tasks.
For example, as a security analyst, you may be responsible for configuring and maintaining the security of a system by managing access.
You may also be responsible for managing and configuring firewalls, setting security policies, enabling virus protection, and performing auditing, accounting, and logging to detect unusual behavior.
All these tasks require a deep understanding of operating systems, and as we continue this course, we'll explore operating systems in greater detail.

Kim: My journey into computing

Hi, I'm Kim.
I'm a technical program manager at Google.
I'm currently working in the security, mergers, and acquisitions team.
Where I work with other companies that we purchase, and I help them integrate into the Google environment.
I've held multiple roles before getting into cybersecurity and even technology.
I first started working as a restaurant worker, and then I became an English Tutor for international students at my local college.
After doing multiple internships, and graduating from university, I had my first opportunity to work in technology, and that's where my interests in technology,
and eventually cybersecurity began.
I want to tell everyone with any type of background that you can get into cybersecurity.
If you're interested in protecting information, if you're interested in protecting people in the future, security is there for you.
There are so many different roles you can do, and all of the skills that you have now, and that you've gathered previously, can be applicable within security.
The skill that I use the most is connecting with people every day.
I can't get anything done unless I connect with them the right way.
So that's actually the biggest skill I lean on the most working in security.
A piece of advice I would give for someone new starting in the cybersecurity field is to keep an open mind.
I started out with a degree in business, so I didn't even feel like I was technical enough to be where I am today.
And before that, all of my experiences were either restaurant work, or marketing work, or just something that
felt like it was unrelated to technology.
But all of that helped me and motivated me to actually kind of get my feet more wet into technology, and then eventually security.
And before I knew it, that self-doubt was really replaced with more of a support from my peers and respect from other people that I've worked with.

Compare operating systems

You previously explored why operating systems are an important part of how a computer works. In this reading, you'll compare some popular operating systems used today. You'll also focus on the risks of using legacy operating systems.

Common operating systems

The following operating systems are useful to know in the security industry: Windows, macOS®, Linux, ChromeOS, Android, and iOS.

Windows and macOS

Windows and macOS are both common operating systems. The Windows operating system was introduced in 1985, and macOS was introduced in 1984. Both operating systems are used in personal and enterprise computers.

Windows is a closed-source operating system, which means the source code is not shared freely with the public. macOS is partially open source. It has some open-source components, such as macOS's kernel. macOS also has some closed-source components.

Linux

The first version of Linux was released in 1991, and other major releases followed in the early 1990s. Linux is a completely open-source operating system, which means that anyone can access Linux and its source code. The open-source nature of Linux allows developers in the Linux community to collaborate.

Linux is particularly important to the security industry. There are some distributions that are specifically designed for security. Later in this course, you'll learn about Linux and its importance to the security industry.

ChromeOS

ChromeOS launched in 2011. It's partially open source and is derived from Chromium OS, which is completely open source. ChromeOS is frequently used in the education field.

Android and iOS

Android and iOS are both mobile operating systems. Unlike the other operating systems mentioned, mobile operating systems are typically used in mobile devices, such as phones, tablets, and watches. Android was introduced for public use in 2008, and iOS was introduced in 2007. Android is open source, and iOS is partially open source.

Operating systems and vulnerabilities

Security issues are inevitable with all operating systems. An important part of protecting an operating system is keeping the system and all of its components up to date.

Legacy operating systems

A **legacy operating system** is an operating system that is outdated but still being used. Some organizations continue to use legacy operating systems because software they rely on is not compatible with newer operating systems. This can be more common in industries that use a lot of equipment that requires embedded software—software that's placed inside components of the equipment.

Legacy operating systems can be vulnerable to security issues because they're no longer supported or updated. This means that legacy operating systems might be vulnerable to new threats.

Other vulnerabilities

Even when operating systems are kept up to date, they can still become vulnerable to attack. Below are several resources that include information on operating systems and their vulnerabilities.

- Microsoft Security Response Center (MSRC)
  - A list of known vulnerabilities affecting Microsoft products and services
- Apple Security Updates
  - A list of security updates and information for Apple® operating systems, including macOS and iOS, and other products
- Common Vulnerabilities and Exposures (CVE) Report for Ubuntu
  - A list of known vulnerabilities affecting Ubuntu, which is a specific distribution of Linux
- Google Cloud Security Bulletin
  - A list of known vulnerabilities affecting Google Cloud products and services

Keeping an operating system up to date is one key way to help the system stay secure. Because it can be difficult to keep all systems updated at all times, it’s important for security analysts to be knowledgeable about legacy operating systems and the risks they can create.

Key takeaways

Windows, macOS, Linux, ChromeOS, Android, and iOS are all commonly used operating systems. Security analysts should be aware of vulnerabilities that affect operating systems. It’s especially important for security analysts to be familiar with legacy operating systems, which are systems that are outdated but still being used.

Inside the operating system

Previously, you learned about what operating systems are.
Now, let's discuss how they work.
In this video, you'll learn what happens with an operating system, or OS, when someone uses a computer for a task.

Think about when someone drives a car.
They push the gas pedal and the car moves forward.
They don't need to pay attention to all the mechanics that allow the car to move.
Just like a car can't work without its engine, a computer can't work without its operating system.

The job of an OS is to help other computer programs run efficiently.
The OS does this by taking care of all the messy details related to controlling, the computer's hardware, so you don't have to.

First, let's see what happens when you turn on the computer.
When you press the power button, you're interacting with the hardware.
This boosts the computer and brings up the operating system.
Booting the computer means that a special microchip called a BIOS is activated.
On many computers built after 2007, the chip was replaced by the UEFI.
Both BIOS and UEFI contain booting instructions that are responsible for loading a special program called the bootloader.
Then, the bootloader is responsible for starting the operating system.
Just like that, your computer is on.
As a security analyst, understanding these processes can be helpful for you.
Vulnerabilities can occur in something like a booting process.
Often, the BIOS is not scanned by the antivirus software, so it can be vulnerable to malware infection.
Now, that you learned how to boot the operating system, let's look at how you and all users communicate with the system to complete a task.

The process starts with you, the user.
And to complete tasks, you use applications on your computer.
An application is a program that performs a specific task.
When you do this, the application sends your request to the operating system.
From there, the operating system interprets this request and directs it to the appropriate component of the computer's hardware.

In the previous video, we learned that the hardware consists of all the physical components of the computer.
The hardware will also send information back to the operating system.
And this in turn is sent back to the application.

Let's give a simple overview of how this works when you want to use the calculator on your computer.
You use your mouse to click on the calculator application on your computer.
When you type in the number you want to calculate, the application communicates with the operating system.
Your operating system then sends a calculation to a component of the hardware, the central processing unit, or CPU.
Once the hardware does the work of determining the final number, it sends the answer back to your operating system.
Then, it can be displayed in your calculator application.

Understanding this process is helpful when investigating security events.
Security analysts should be able to trace back through this process flow to analyze where a security event could have occurred.

Just like a mechanic needs to understand the inner workings of a car more than an average driver, recognizing how operating systems work is important knowledge for a security analyst.

Requests to the operating system

Operating systems are a critical component of a computer. They make connections between applications and hardware to allow users to perform tasks. In this reading, you'll explore this complex process further and consider it using a new analogy and a new example.

Booting the computer

When you boot, or turn on, your computer, either a BIOS or UEFI microchip is activated. The **Basic Input/Output System (BIOS)** is a microchip that contains loading instructions for the computer and is prevalent in older systems. The **Unified Extensible Firmware Interface (UEFI)** is a microchip that contains loading instructions for the computer and replaces BIOS on more modern systems.

The BIOS and UEFI chips both perform the same function for booting the computer. BIOS was the standard chip until 2007, when UEFI chips increased in use. Now, most new computers include a UEFI chip. UEFI provides enhanced security features.

The BIOS or UEFI microchips contain a variety of loading instructions for the computer to follow. For example, one of the loading instructions is to verify the health of the computer's hardware.

The last instruction from the BIOS or UEFI activates the bootloader. The **bootloader** is a software program that boots the operating system. Once the operating system has finished booting, your computer is ready for use.

Completing a task

As previously discussed, operating systems help us use computers more efficiently. Once a computer has gone through the booting process, completing a task on a computer is a four-part process.

Shows a process that moves from user to application to operating systems and finally to hardv

User

The first part of the process is the user. The user initiates the process by having something they want to accomplish on the computer. Right now, you're a user! You've initiated the process of accessing this reading.

Application

The application is the software program that users interact with to complete a task. For example, if you want to calculate something, you would use the calculator application. If you want to write a report, you would use a word processing application. This is the second part of the process.

Operating system

The operating system receives the user's request from the application. It's the operating system's job to interpret the request and direct its flow. In order to complete the task, the operating system sends it on to applicable components of the hardware.

Hardware

The hardware is where all the processing is done to complete the tasks initiated by the user. For example, when a user wants to calculate a number, the CPU figures out the answer. As another example, when a user wants to save a file, another component of the hardware, the hard drive, handles this task.

After the work is done by the hardware, it sends the output back through the operating system to the application so that it can display the results to the user.

The OS at work behind the scenes

Consider once again how a computer is similar to a car. There are processes that someone won't directly observe when operating a car, but they do feel it move forward when they press the gas pedal. It's the same with a computer. Important work happens inside a computer that you don't experience directly. This work involves the operating system.

You can explore this through another analogy. The process of using an operating system is also similar to ordering at a restaurant. At a restaurant you place an order and get your food, but you don't see what's happening in the kitchen when the cooks prepare the food.

Ordering food is similar to using an application on a computer. When you order your food, you make a specific request like "a small soup, very hot." When you use an application, you also make specific requests like "print three double-sided copies of this document."

You can compare the food you receive to what happens when the hardware sends output. You receive the food that you ordered. You receive the document that you wanted to print.

Finally, the kitchen is like the OS. You don’t know what happens in the kitchen, but it’s critical in interpreting the request and ensuring you receive what you ordered. Similarly, though the work of the OS is not directly transparent to you, it’s critical in completing your tasks.

An example: Downloading a file from an internet browser

Previously, you explored how operating systems, applications, and hardware work together by examining a task involving a calculation. You can expand this understanding by exploring how the OS completes another task, downloading a file from an internet browser:

- First, the user decides they want to download a file that they found online, so they click on a download button near the file in the internet browser application.
- Then, the internet browser communicates this action to the OS.
- The OS sends the request to download the file to the appropriate hardware for processing.
- The hardware begins downloading the file, and the OS sends this information to the internet browser application. The internet browser then informs the user when the file has been downloaded.

Key takeaways

Although it operates in the background, the operating system is an essential part of the process of using a computer. The operating system connects applications and hardware to allow users to complete a task.

Resource allocation via the OS

Now we're ready to discuss a different aspect of your operating system.
Not only does the OS interact with other parts of your computer, but it's also responsible for managing the resources of the system.
This is a big task that requires a lot of balance to make sure all the resources of the computer are used efficiently.
Think of this like the concept of energy.
A person needs energy to complete different tasks.
Some tasks need more energy, while others require less.
For example, going for a run requires more energy than watching TV.
A computer's OS also needs to make sure that it has enough energy to function correctly for certain tasks.
Running an antivirus scan on your computer will use more energy than using the calculator application.

Imagine your computer is an orchestra.
Many different instruments like violins, drums, and trumpets are all part of the orchestra.
An orchestra also has a conductor to direct the flow of the music.
In a computer, the OS is the conductor.
The OS handles resource and memory management to ensure the limited capacity of the computer system is used where it's needed most.
A variety of programs, tasks, and processes are constantly competing for the resources of the central processing unit, or CPU.
They all have their own reasons why they need memory, storage, and input/output bandwidth.
The OS is responsible for ensuring that each program is allocating and de-allocating resources.
All this occurs in your computer at the same time so that your system functions efficiently.

Much of this is hidden from you as a user.
For example, your browser's task manager will list all of the tasks that are being processed, along with their memory and CPU usage.
As an analyst, it's helpful to know where a system's resources are used.
Understanding usage of resources can help you respond to an incident and troubleshoot applications in the system.
For example, if a computer is running slowly, an analyst might discover it's allocating resources to malware.
A basic understanding of how operating systems work will help you better understand the security skills you will learn later in this program.

Virtualization technology

You've explored a lot about operating systems. One more aspect to consider is that operating systems can run on virtual machines. In this reading, you'll learn about virtual machines and the general concept of virtualization. You'll explore how virtual machines work and the benefits of using them.

What is a virtual machine?

A **virtual machine (VM)** is a virtual version of a physical computer. Virtual machines are one example of virtualization. Virtualization is the process of using software to create virtual representations of various physical machines. The term "virtual" refers to machines that don't exist physically, but operate like they do because their software simulates physical hardware. Virtual systems don't use dedicated physical hardware. Instead, they use software-defined versions of the physical hardware. This means that a single virtual machine has a virtual CPU, virtual storage, and other virtual hardware. Virtual systems are just code.

You can run multiple virtual machines using the physical hardware of a single computer. This involves dividing the resources of the host computer to be shared across all physical and virtual components. For example, **Random Access Memory (RAM)** is a hardware component used for short-term memory. If a computer has 16GB of RAM, it can host three virtual machines so that the physical computer and virtual machines each have 4GB of RAM. Also, each of these virtual machines would have their own operating system and function similarly to a typical computer.

Benefits of virtual machines

Security professionals commonly use virtualization and virtual machines. Virtualization can increase security for many tasks and can also increase efficiency.

Security

One benefit is that virtualization can provide an isolated environment, or a sandbox, on the physical host machine. When a computer has multiple virtual machines, these virtual machines are "guests" of the computer. Specifically, they are isolated from the host computer and other guest virtual machines. This provides a layer of security, because virtual machines can be kept separate from the other systems. For example, if an individual virtual machine becomes infected with malware, it can be dealt with more securely because it's isolated from the other machines. A security professional could also intentionally place malware on a virtual machine to examine it in a more secure environment.

Note: Although using virtual machines is useful when investigating potentially infected machines or running malware in a constrained environment, there are still some risks. For example, a malicious program can escape virtualization and access the host machine. This is why you should never completely trust virtualized systems.

Efficiency

Using virtual machines can also be an efficient and convenient way to perform security tasks. You can open multiple virtual machines at once and switch easily between them. This allows you to streamline security tasks, such as testing and exploring various applications.

You can compare the efficiency of a virtual machine to a city bus. A single city bus has a lot of room and is an efficient way to transport many people simultaneously. If city buses didn’t exist, then everyone on the bus would have to drive their own cars. This uses more gas, cars, and other resources than riding the city bus.

Similar to how many people can ride one bus, many virtual machines can be hosted on the same physical machine. That way, separate physical machines aren't needed to perform certain tasks.

Managing virtual machines

Virtual machines can be managed with a software called a hypervisor. Hypervisors help users manage multiple virtual machines and connect the virtual and physical hardware. Hypervisors also help with allocating the shared resources of the physical host machine to one or more virtual machines.

One hypervisor that is useful for you to be familiar with is the Kernel-based Virtual Machine (KVM). KVM is an open-source hypervisor that is supported by most major Linux distributions. It is built into the Linux kernel, which means it can be used to create virtual machines on any machine running a Linux operating system without the need for additional software.

Other forms of virtualization

In addition to virtual machines, there are other forms of virtualization. Some of these virtualization technologies do not use operating systems. For example, multiple virtual servers can be created from a single physical server. Virtual networks can also be created to more efficiently use the hardware of a physical network.

Key takeaways

Virtual machines are virtual versions of physical computers and are one example of virtualization. Virtualization is a key technology in the security industry, and it’s important for security analysts to understand the basics. There are many benefits to using virtual machines, such as isolation of malware and other security risks. However, it’s important to remember there’s still a risk of malicious software escaping their virtualized environments.

GUI versus CLI

Now that you've learned the inner workings of computers, let's discuss how users and operating systems communicate with each other.
So far, you've learned that a computer has an operating system, hardware, and applications.
Remember, the operating system communicates with the hardware to execute tasks.
In this video, you'll learn how the user—that's you—interacts with the operating system in order to send tasks to the hardware.

The user communicates with the operating system via an interface.
A user interface is a program that allows a user to control the functions of the operating system.
Two user interfaces that we'll discuss are the graphical user interface, or GUI, and the command-line interface, or CLI.
Let's cover these interfaces in more detail.

A GUI is a user interface that uses icons on the screen to manage different tasks on the computer.
Most operating systems can be used with a graphical user interface.
If you've used a personal computer or a cell phone, you have experienced operating a GUI.
Most GUIs include these components:
a start menu with program groups, a task bar for launching programs, and a desktop with icons and shortcuts.
All these components help you communicate with the OS to execute tasks.
In addition to clicking on icons, when you use a GUI, you can also search for files or applications from the start menu.
You just have to remember the icon or name of the program to activate an application.

Now let's discuss the command-line interface.
In comparison, the command-line interface, or CLI, is a text-based user interface that uses commands to interact with the computer.
These commands communicate with the operating system and execute tasks like opening programs.
The command-line interface is a much different structure than the graphical user interface.
When you use the CLI, you'll immediately notice a difference.
There are no icons or graphics on the screen.
The command-line interface looks similar to lines of code using certain text languages.
A CLI is more flexible and more powerful than a GUI.
Think about using a CLI like creating whatever meal you'd like from ingredients bought at a grocery store.
This gives you a lot of control and customization about what you're going to eat.

In comparison, using a GUI is more like ordering food from a restaurant.
You can only order what's on the menu.
If you want both a noodle dish and pizza, but the first restaurant you go to only has pizza, you'll have to go to another restaurant

to order the noodles.
With a graphical user interface, you must do one task at a time.
But the command-line interface allows for customization, which lets you complete multiple tasks simultaneously.
For example, imagine you have a folder with hundreds of files of different file types, and you need to move only the JPEG files to a new folder.
Think about how slow and tedious this would be as you use a GUI to find each JPEG file in this folder and move it into the new one.
On the other hand, the CLI would allow you to streamline this process and move them all at once.

As you can see, there are very big differences in these two types of user interfaces.
As a security analyst, some of your work may involve the command-line interface.
When analyzing logs or authenticating and authorizing users, security analysts commonly use a CLI in their everyday work.
In this video, we discussed two types of user interfaces.
You learned that you already have experience using a graphical user interface, as most personal computers and cell phones use a GUI.
You were introduced to the command-line interface.
Later in the program, you'll learn how to use a CLI in Linux and how relevant it is to your daily work as a security analyst.
You'll get practical experience communicating through the command line. Pretty exciting, right?

The command line in use

Previously, you explored graphical user interfaces (GUI) and command-line user 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.

Side by side comparison of a graphical user interface with icons and a command line interface

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.

Ellen: My path into cybersecurity

My name is Ellen and I am a security engineering manager at Google focused in on how Google uses the cloud.
Cybersecurity wasn't a field when I got started in technology, something I came to later.
I got started in technology when I was working retail at a poster store.
And we needed to build a website and my feet hurt and I really needed to sit down.
And so I asked friends to teach me how to do HTML so I could sit down while working and I could let my blisters have a rest.
While I was at the poster store, one of our customers worked at a start up and used to get employee photos framed and they asked them for feedback on my website, and they ended up giving me an internship.
One of the specialties that I ended up having was API design or designing the interface by which a developer communicates with the machine.
As part of that, I got into a job where I was designing a miniature version of an operating system for security technology and started learning security from there.
Most of the people I know from cyber security, especially in the early days, do not have a degree at all.
Or if they do, they have a degree like I do in something like philosophy or poetry.
Almost everyone learned on their own by experimenting, by talking to people, by reading.
And so I would say no technical background is required.
And in fact, having a background where you're used to being out in the real world can sometimes make cybersecurity make more sense and help you make more balanced choices.
In almost all areas, there is a security community that you can find.
Figure out where they are, look for local conferences, start talking to people.
It's a lot more fun to learn that way than it is in a vacuum.
I've found that most people if you come to them and say, hey, you're really good at this thing, would you mind if I bought you a coffee and you showed me how to do it?
That they'll always pretty much say yes.
The advice I give to people who don't have technical backgrounds, the first one is, I wouldn't be afraid of the technology.
It can seem like only somebody with a computer science degree could ever understand things, but these concepts, these technologies are understandable by anyone.
And so never let the fact that you might not have a technical background get in the way, just pick an area that interests you and start diving in.
And as long as you're curious, and as long as you find it interesting, you'll, you'll learn the technology.

Wrap-up; Glossary terms from week 1

We did it!
What a great section of learning!
The best thing is that we did this together and covered some very useful topics.
Let's recap this section's lessons.
As a security analyst, it's important that you understand the systems that you're working with.
Understanding computer basics will help you do your job more effectively and efficiently.
In this section, we covered common operating systems.
We also discussed the main functions of an operating system.
Importantly, you learned about the relationship between operating systems, applications, and hardware.
It was nice to learn how they flow together like an orchestra.
In addition, you learned about the differences between the graphical user interface and the command-line interface.
Understanding the command-line interface will be very important for your work.

I enjoyed exploring the world of operating systems with you.
Knowing how operating systems work is an important step in preparing for a position as a security analyst.
You're doing great!
Let's keep moving forward with this program.
In the next section, we'll focus specifically on the Linux operating system.

Terms and definitions from Course 4, Week 1

Application: A program that performs a specific task

Basic Input/Output System (BIOS): A microchip that contains loading instructions for the computer and is prevalent in older systems

Bootloader: A software program that boots the operating system

Command-line interface (CLI): A text-based user interface that uses commands to interact with the computer

Graphical user interface (GUI): A user interface that uses icons on the screen to manage different tasks on the computer

Hardware: The physical components of a computer

Legacy operating system: An operating system that is outdated but still being used

Operating system (OS): The interface between computer hardware and the user

Random Access Memory (RAM): A hardware component used for short-term memory

Unified Extensible Firmware Interface (UEFI): A microchip that contains loading instructions for the computer and replaces BIOS on more modern systems

User interface: A program that allows the user to control the functions of the operating system

Virtual machine (VM): A virtual version of a physical computer