**Module 1: Introduction to operating systems – Giới thiệu về hệ điều hành**

|  |
| --- |
| 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. |

Bạn sẽ tìm hiểu về mối quan hệ giữa hệ điều hành, phần cứng và phần mềm và làm quen với các chức năng chính của hệ điều hành. Bạn sẽ nhận ra các hệ điều hành phổ biến được sử dụng ngày nay và hiểu cách cả giao diện đồ họa người dùng (GUI) và giao diện dòng lệnh (CLI) đều cho phép người dùng tương tác với hệ điều hành.

|  |
| --- |
| **Learning Objectives**   * Describe the main functions of an operating system. * Recognize the most common operating systems in use. * Explain the relationship between operating systems, applications, and hardware. * Compare a graphical user interface to a command line interface. |

**Mục tiêu học tập**

* Trình bày các chức năng chính của hệ điều hành.
* Nhận biết các hệ điều hành phổ biến nhất được sử dụng.
* Giải thích mối quan hệ giữa hệ điều hành, ứng dụng và phần cứng.
* So sánh giao diện người dùng đồ họa với giao diện dòng lệnh.

**1. Get started with the course – Bắt đầu với khóa học**

***1.1. Introduction to Course 4 – Giới thiệu khóa học 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. |

CHÀO! Chào mừng đến với khóa học nàyvề vấn đề cơ bản về tính toán để bảo mật.Tên tôi là Kim, tôi làm việc ởNgười quản lý chương trình kỹ thuật về bảo mật.Tôi lớn lên với máy tính và internetnhưng không thực sự coi vấn đề bảo mật làmột cơ hội nghề nghiệp cho đến khi tôi nhìn thấynó được đan xen vào công nghệ như thế nào.

|  |
| --- |
| 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. |

Trước công việc an ninh đầu tiên của tôi,Tôi đã làm việc trong nhóm ứng dụng đám mâyvà phải thường xuyên tương tác với đội an ninh.Đó là trải nghiệm đầu tiên của tôi khi làm việc với lĩnh vực bảo mật,nhưng ý tưởng bảo vệ thông tin và làm việccùng với những người khác hướng tới mục tiêu đó là điều thú vị đối với tôi.Kết quả là tôi quyết định hướng tới CISSP của mình,điều đó dẫn tôi đến một số công việc mớicơ hội tại công ty của tôi,và sau đó tôi có thể chuyển sang bảo mật.

|  |
| --- |
| 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. |

Tại thời điểm này, nếu bạn đã theo dõi,bạn đã khám phá nhiều loạicác khái niệm hữu ích cho lĩnh vực an ninh,bao gồm các lĩnh vực bảo mật và mạng.Tôi rất vui được tham gia cùng bạntrong phần tiếp theo của chương trình.Chúng tôi sẽ làm chậm lại để bạn có thểhiểu những chủ đề này theo những cách thực tế.Trọng tâm của khóa học này là những điều cơ bản về máy tính.Khi bạn hiểu làm thế nàocác máy móc trong hệ thống của tổ chức hoạt động,nó giúp bạn thực hiện công việc của mình nhưmột nhà phân tích bảo mật hiệu quả hơn.

|  |
| --- |
| 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. |

Một phần công việc của bạn với tư cách là nhà phân tích bảo mật làgiữ cho hệ thống được bảo vệ khỏi các cuộc tấn công có thể xảy ra.Bạn là một trong những cấp độ đầu tiên củaphòng thủ trong việc bảo vệ dữ liệu của một tổ chức.Để làm được điều này một cách hiệu quả,thật hữu ích để hiểu làm thế nàohệ thống bạn đang bảo vệ đang hoạt động.Ngoài ra, bạn có thể cần phảiđiều tra các sự kiện để giúp sửa lỗi trong hệ thống.Làm quen với hệ điều hành Linuxvà các lệnh liên quan của nó,và còn có thể tương tác vớidữ liệu của một tổ chức thông quaSQL sẽ giúp bạn điều đó.

|  |
| --- |
| 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. |

Trong khóa học này, bạn sẽ tìm hiểu vềhệ điều hành và cách chúngliên quan đến ứng dụng và phần cứng.Tiếp theo, bạn sẽ khám pháhệ điều hành Linux một cách chi tiết hơn.Sau đó, bạn sẽ sử dụng dòng lệnh Linuxtrong bối cảnh bảo mật.Cuối cùng, chúng ta sẽ thảo luận cách bạn có thể sử dụng SQL để truy vấncơ sở dữ liệu trong khi làm việc như một nhà phân tích bảo mật.Tôi háo hức khám phá tất cảnhững chủ đề này với bạn. Bắt đầu nào.

***1.2. Course 4 overview – Tổng quan về khóa 4***

|  |
| --- |
| **Course 4 overview** |

**Tổng quan về khóa 4**



|  |
| --- |
| Hello, and welcome to **Tools of the Trade: Linux and SQL**, the fourth course in the Google Cybersecurity Certificate. You're on an exciting journey! |

Xin chào và chào mừng bạn đến với **Công cụ thương mại: Linux và SQL** , khóa học thứ tư trong Chứng chỉ an ninh mạng của Google. Bạn đang trên một hành trình thú vị!

|  |
| --- |
| By the end of this course, you will develop a greater understanding of the basics of computing that will support your work as a security analyst. You will learn foundational concepts related to understanding operating systems, communicating with the Linux operating system through commands, and querying databases with Structured Query Language (SQL). These are key concepts in the cybersecurity field and understanding them will help you keep organizations secure. |

Khi kết thúc khóa học này, bạn sẽ hiểu rõ hơn về những kiến ​​thức cơ bản về điện toán để hỗ trợ công việc của bạn với tư cách là nhà phân tích bảo mật. Bạn sẽ học các khái niệm nền tảng liên quan đến việc hiểu hệ điều hành, giao tiếp với hệ điều hành Linux thông qua các lệnh và truy vấn cơ sở dữ liệu bằng Ngôn ngữ truy vấn có cấu trúc (SQL). Đây là những khái niệm quan trọng trong lĩnh vực an ninh mạng và việc hiểu chúng sẽ giúp bạn đảm bảo an toàn cho tổ chức.

|  |
| --- |
| **Certificate program progress** |

**Tiến độ chương trình chứng chỉ**

|  |
| --- |
| The Google Cybersecurity Certificate program has eight courses. **Tools of the Trade: Linux and SQL** is the fourth course. |

Chương trình Chứng chỉ An ninh mạng của Google có tám khóa học. **Công cụ giao dịch: Linux và SQL** là khóa học thứ tư.

|  |
| --- |
| 1. [**Foundations of Cybersecurity**](https://www.coursera.org/learn/foundations-of-cybersecurity/home/week/1)— Explore the cybersecurity profession, including significant events that led to the development of the cybersecurity field and its continued importance to organizational operations. Learn about entry-level cybersecurity roles and responsibilities. 2. [**Play It Safe: Manage Security Risks**](https://www.coursera.org/learn/manage-security-risks/home/week/1)— Identify how cybersecurity professionals use frameworks and controls to protect business operations, and explore common cybersecurity tools. 3. [**Connect and Protect: Networks and Network Security**](https://www.coursera.org/learn/networks-and-network-security/home/week/1)— Gain an understanding of network-level vulnerabilities and how to secure networks. 4. [**Tools of the Trade: Linux and SQL**](https://www.coursera.org/learn/linux-and-sql/home/week/1)— *(current course)* Explore foundational computing skills, including communicating with the Linux operating system through the command line and querying databases with SQL. 5. [**Assets, Threats, and Vulnerabilities**](https://www.coursera.org/learn/assets-threats-and-vulnerabilities/home/week/1)— Learn about the importance of security controls and developing a threat actor mindset to protect and defend an organization’s assets from various threats, risks, and vulnerabilities. 6. [**Sound the Alarm: Detection and Response**](https://www.coursera.org/learn/detection-and-response/home/week/1)— Understand the incident response lifecycle and practice using tools to detect and respond to cybersecurity incidents. 7. [**Automate Cybersecurity Tasks with Python**](https://www.coursera.org/learn/automate-cybersecurity-tasks-with-python/home/week/1)— Explore the Python programming language and write code to automate cybersecurity tasks. 8. [**Put It to Work: Prepare for Cybersecurity Jobs**](https://www.coursera.org/learn/prepare-for-cybersecurity-jobs/home/week/1)— Learn about incident classification, escalation, and ways to communicate with stakeholders. This course closes out the program with tips on how to engage with the cybersecurity community and prepare for your job search. |

1. [**Nền tảng của an ninh mạng**](https://www.coursera.org/learn/foundations-of-cybersecurity/home/week/1)— Khám phá nghề an ninh mạng, bao gồm các sự kiện quan trọng dẫn đến sự phát triển của lĩnh vực an ninh mạng và tầm quan trọng liên tục của nó đối với hoạt động của tổ chức. Tìm hiểu về vai trò và trách nhiệm an ninh mạng cấp cơ bản.
2. [**Chơi an toàn: Quản lý rủi ro bảo mật**](https://www.coursera.org/learn/manage-security-risks/home/week/1)— Xác định cách các chuyên gia an ninh mạng sử dụng khuôn khổ và biện pháp kiểm soát để bảo vệ hoạt động kinh doanh cũng như khám phá các công cụ an ninh mạng phổ biến.
3. [**Kết nối và bảo vệ: Mạng và an ninh mạng**](https://www.coursera.org/learn/networks-and-network-security/home/week/1)- Hiểu biết về các lỗ hổng ở cấp độ mạng và cách bảo mật mạng.
4. [**Công cụ giao dịch: Linux và SQL**](https://www.coursera.org/learn/linux-and-sql/home/week/1)- *(khóa học hiện tại)* Khám phá các kỹ năng tính toán cơ bản, bao gồm giao tiếp với hệ điều hành Linux thông qua dòng lệnh và truy vấn cơ sở dữ liệu bằng SQL.
5. [**Tài sản, mối đe dọa và lỗ hổng**](https://www.coursera.org/learn/assets-threats-and-vulnerabilities/home/week/1)— Tìm hiểu về tầm quan trọng của kiểm soát bảo mật và phát triển tư duy của tác nhân đe dọa để bảo vệ và bảo vệ tài sản của tổ chức khỏi các mối đe dọa, rủi ro và lỗ hổng khác nhau.
6. [**Phát âm thanh báo động: Phát hiện và phản hồi**](https://www.coursera.org/learn/detection-and-response/home/week/1)— Hiểu vòng đời ứng phó sự cố và thực hành sử dụng các công cụ để phát hiện và ứng phó sự cố an ninh mạng.
7. [**Tự động hóa các tác vụ an ninh mạng với Python**](https://www.coursera.org/learn/automate-cybersecurity-tasks-with-python/home/week/1)— Khám phá ngôn ngữ lập trình Python và viết mã để tự động hóa các tác vụ an ninh mạng.
8. [**Đưa nó vào hoạt động: Chuẩn bị cho công việc an ninh mạng**](https://www.coursera.org/learn/prepare-for-cybersecurity-jobs/home/week/1)— Tìm hiểu về phân loại sự cố, trình báo và cách liên lạc với các bên liên quan. Khóa học này kết thúc chương trình với các mẹo về cách tương tác với cộng đồng an ninh mạng và chuẩn bị cho quá trình tìm kiếm việc làm của bạn.

|  |
| --- |
| **Course 4 content** |

**Nội dung khóa 4**

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

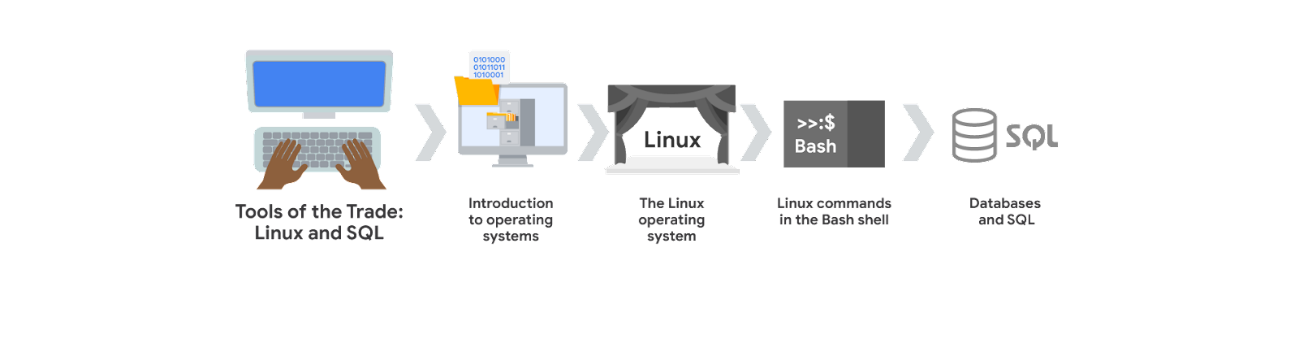
Mỗi khóa học của chương trình chứng chỉ này được chia thành các mô-đun. Bạn có thể hoàn thành các khóa học theo tốc độ của riêng mình nhưng phần phân tích mô-đun được thiết kế để giúp bạn hoàn thành toàn bộ Chứng chỉ an ninh mạng của Google trong khoảng sáu tháng.

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

Điều gì sẽ đến? Dưới đây là tổng quan nhanh về các kỹ năng bạn sẽ học trong mỗi mô-đun của khóa học này.

|  |
| --- |
| **Module 1: Introduction to operating systems** |

**Mô-đun 1: Giới thiệu về hệ điều hành**

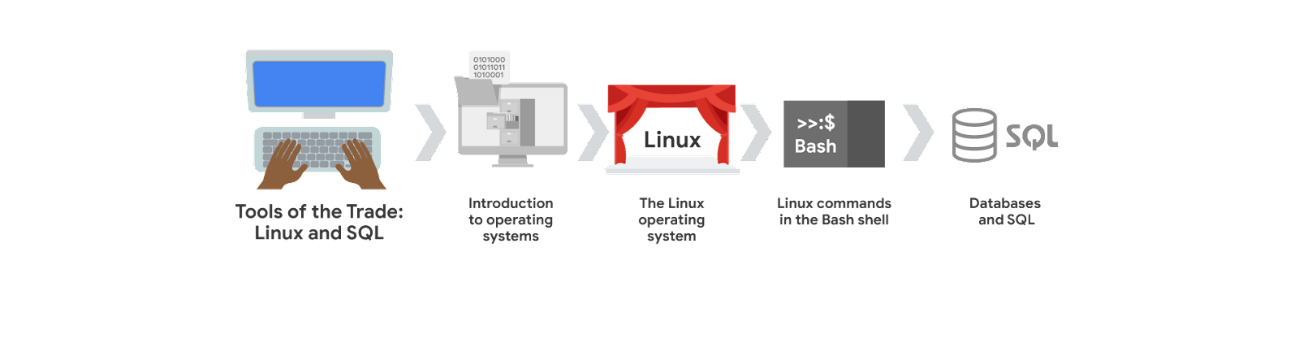


|  |
| --- |
| You will learn about the relationship between operating systems, hardware, and software, and become familiar with the primary functions of an operating system. You'll recognize common operating systems in use today and understand how the graphical user interface (GUI) and command-line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

Bạn sẽ tìm hiểu về mối quan hệ giữa hệ điều hành, phần cứng và phần mềm và làm quen với các chức năng chính của hệ điều hành. Bạn sẽ nhận ra các hệ điều hành phổ biến được sử dụng ngày nay và hiểu cách cả giao diện đồ họa người dùng (GUI) và giao diện dòng lệnh (CLI) đều cho phép người dùng tương tác với hệ điều hành.

|  |
| --- |
| **Module 2:  The Linux operating system** |

**Mô-đun 2: Hệ điều hành Linux**

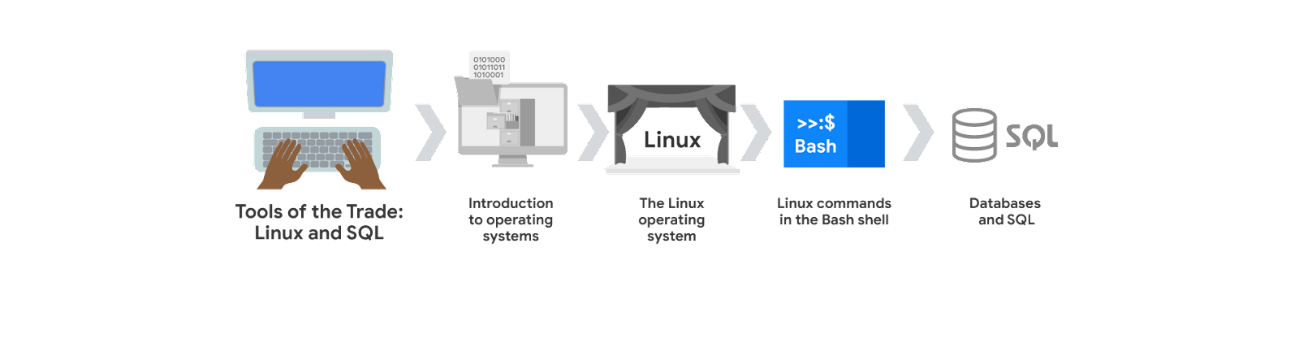


|  |
| --- |
| You will be introduced to the Linux operating system and learn how it is commonly used in cybersecurity. You’ll also learn about Linux architecture and common Linux distributions. In addition, you'll be introduced to the Linux shell and learn how it allows you to communicate with the operating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

Bạn sẽ được giới thiệu về hệ điều hành Linux và tìm hiểu cách nó được sử dụng phổ biến trong an ninh mạng. Bạn cũng sẽ tìm hiểu về kiến ​​trúc Linux và các bản phân phối Linux phổ biến. Ngoài ra, bạn sẽ được giới thiệu về Linux shell và tìm hiểu cách nó cho phép bạn giao tiếp với hệ điều hành.

|  |
| --- |
| **Module 3: Linux commands in the Bash shell** |

**Mô-đun 3: Các lệnh Linux trong shell Bash**

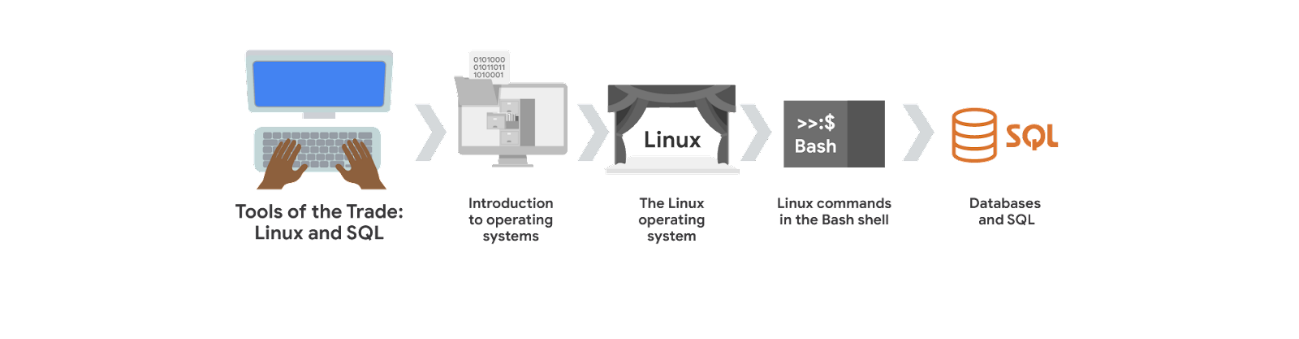


|  |
| --- |
| You will be introduced to Linux commands as entered through the Bash shell. You'll use the Bash shell to navigate and manage the file system and to authorize and authenticate users. You'll also learn where to go for help when working with new Linux commands. |

Bạn sẽ được giới thiệu các lệnh Linux được nhập thông qua shell Bash. Bạn sẽ sử dụng shell Bash để điều hướng và quản lý hệ thống tệp cũng như ủy quyền và xác thực người dùng. Bạn cũng sẽ biết nơi cần trợ giúp khi làm việc với các lệnh Linux mới.

|  |
| --- |
| **Module 4: Databases and SQL** |

**Mô-đun 4: Cơ sở dữ liệu và SQL**



|  |
| --- |
| 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. |

Bạn sẽ thực hành sử dụng SQL để giao tiếp với cơ sở dữ liệu. Bạn sẽ tìm hiểu cách truy vấn cơ sở dữ liệu và lọc kết quả. Bạn cũng sẽ tìm hiểu cách SQL có thể nối nhiều bảng lại với nhau trong một truy vấn.

|  |
| --- |
| **What to expect** |

**Những gì mong đợi**

|  |
| --- |
| 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. * **Discussion prompts** explore course topics for better understanding and allow you to chat and exchange ideas with other learners in the [discussion forums](https://www.coursera.org/learn/linux-and-sql/discussions). * **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. |

Mỗi khóa học cung cấp nhiều loại cơ hội học tập:

* **Các video** do người hướng dẫn của Google dẫn dắt sẽ dạy các khái niệm mới, giới thiệu cách sử dụng các công cụ có liên quan, cung cấp hỗ trợ nghề nghiệp và cung cấp những câu chuyện cá nhân đầy cảm hứng.
* **Các bài đọc** được xây dựng dựa trên các chủ đề được thảo luận trong video, giới thiệu các khái niệm liên quan, chia sẻ các tài nguyên hữu ích và mô tả các nghiên cứu điển hình.
* **Lời nhắc thảo luận** khám phá các chủ đề khóa học để hiểu rõ hơn và cho phép bạn trò chuyện cũng như trao đổi ý tưởng với những người học khác trong khóa học.[diễn đàn thảo luận](https://www.coursera.org/learn/linux-and-sql/discussions).
* **Các hoạt động tự đánh giá** và **phòng thí nghiệm** giúp bạn thực hành thực hành trong việc áp dụng các kỹ năng bạn đang học và cho phép bạn đánh giá bài làm của chính mình bằng cách so sánh nó với một ví dụ hoàn chỉnh.
* **Các plug-in tương tác** khuyến khích bạn thực hành các nhiệm vụ cụ thể và giúp bạn tích hợp kiến ​​thức bạn đã thu được trong khóa học.
* **Các câu đố trong video** giúp bạn kiểm tra mức độ hiểu của mình khi bạn xem qua từng video.
* **Các câu hỏi thực hành** cho phép bạn kiểm tra sự hiểu biết của mình về các khái niệm chính và cung cấp phản hồi có giá trị.
* **Các câu hỏi được chấm điểm** thể hiện sự hiểu biết của bạn về các khái niệm chính của khóa học. Bạn phải đạt 80% điểm trở lên trong mỗi bài kiểm tra được xếp loại để nhận được chứng chỉ và bạn có thể làm bài kiểm tra được xếp loại nhiều lần để đạt được điểm đậu.

|  |
| --- |
| **Tips for success** |

**Lời khuyên để thành công**

|  |
| --- |
| * 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](https://www.coursera.org/learn/linux-and-sql/resources/y7Px8) 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](https://www.coursera.support/s/article/208280036-Coursera-Code-of-Conduct?) to ensure that the learning community remains a welcoming, friendly, and supportive place for all members. |

* Chúng tôi đặc biệt khuyên bạn nên xem qua các mục trong mỗi bài học theo thứ tự chúng xuất hiện vì thông tin và khái niệm mới được xây dựng dựa trên kiến ​​thức trước đó.
* Tham gia vào tất cả các cơ hội học tập để có được càng nhiều kiến ​​thức và kinh nghiệm càng tốt.
* Nếu có điều gì đó khó hiểu, đừng ngần ngại phát lại video, xem lại bài đọc hoặc lặp lại hoạt động tự xem xét.
* Sử dụng các tài nguyên bổ sung được tham chiếu trong khóa học này. Chúng được thiết kế để hỗ trợ việc học của bạn. Bạn có thể tìm thấy tất cả các tài nguyên này trong[Tài nguyên](https://www.coursera.org/learn/linux-and-sql/resources/y7Px8)chuyển hướng.
* Khi bạn gặp các liên kết hữu ích trong khóa học này, hãy đánh dấu chúng để bạn có thể tham khảo thông tin sau này để nghiên cứu hoặc ôn tập.
* Hãy hiểu và làm theo[Quy tắc ứng xử của Coursera](https://www.coursera.support/s/article/208280036-Coursera-Code-of-Conduct?)để đảm bảo rằng cộng đồng học tập vẫn là một nơi thân thiện, thân thiện và hỗ trợ cho tất cả các thành viên.

***1.3. Helpful resources and tips – Tài nguyên và lời khuyên hữu ích***

|  |
| --- |
| **Helpful resources and tips** |

**Tài nguyên và lời khuyên hữu ích**

|  |
| --- |
| 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. |

Là người học, bạn có thể chọn hoàn thành một hoặc nhiều khóa học trong chương trình này. Tuy nhiên, để có được Chứng chỉ an ninh mạng của Google, bạn phải hoàn thành tất cả các khóa học. Bài đọc này mô tả những gì cần thiết để có được chứng chỉ và các phương pháp hay nhất để bạn có trải nghiệm học tập tốt trên Coursera.

|  |
| --- |
| **Course completion to obtain a certificate** |

**Hoàn thành khóa học để được cấp chứng chỉ**

|  |
| --- |
| To submit graded assignments and be eligible to receive a Google Cybersecurity Certificate, you must:   * Pay the [course certificate fee](https://www.coursera.support/s/article/209818963-Payments-on-Coursera?language=en_US) or apply and be approved for a Coursera [scholarship](https://www.coursera.support/s/article/209819033-Apply-for-Financial-Aid-or-a-Scholarship?language=en_US). * 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. |

Để gửi bài tập đã chấm điểm và đủ điều kiện nhận Chứng chỉ an ninh mạng của Google, bạn phải:

* Tra[lệ phí cấp chứng chỉ khóa học](https://www.coursera.support/s/article/209818963-Payments-on-Coursera?language=en_US)hoặc đăng ký và được chấp thuận tham gia Coursera[học bổng](https://www.coursera.support/s/article/209819033-Apply-for-Financial-Aid-or-a-Scholarship?language=en_US).
* Vượt qua tất cả các câu hỏi được chấm điểm trong tám khóa học với số điểm ít nhất là 80%. Mỗi bài kiểm tra được chấm điểm trong một khóa học là một phần của điểm tích lũy cho khóa học đó.

|  |
| --- |
| **Healthy habits for course completion** |

**Thói quen lành mạnh khi hoàn thành khóa học**

|  |
| --- |
| 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](https://www.coursera.org/learn/linux-and-sql/discussions) to ask for help from other learners taking this program. You can also visit Coursera’s [Global Online Community](https://coursera.community/). Other important things to know while learning with others can be found in the [Coursera Honor Code](https://learner.coursera.help/hc/en-us/articles/209818863-Coursera-Honor-Code) and [Code of Conduct](https://learner.coursera.help/hc/en-us/articles/208280036-Coursera-Code-of-Conduct). * **Update your profile:** Consider [updating your profile](https://www.coursera.org/account/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. |

Dưới đây là danh sách các phương pháp hay nhất sẽ giúp bạn hoàn thành các khóa học trong chương trình một cách kịp thời:

* **Lập kế hoạch thời gian của bạn:** Đặt thời gian học tập thường xuyên và tuân theo chúng mỗi tuần có thể giúp bạn biến việc học trở thành một phần thói quen của mình. Sử dụng lịch hoặc thời gian biểu để tạo lịch trình và liệt kê những việc bạn dự định làm mỗi ngày để đặt ra các mục tiêu có thể đạt được. Tìm một không gian cho phép bạn tập trung khi xem video, xem lại bài đọc và hoàn thành các hoạt động.
* **Làm việc theo tốc độ của riêng bạn:** Mọi người học theo cách khác nhau, vì vậy chương trình này được thiết kế để giúp bạn làm việc theo tốc độ của riêng mình. Mặc dù thời hạn được cá nhân hóa của bạn bắt đầu khi bạn đăng ký, nhưng hãy thoải mái chuyển qua chương trình với tốc độ phù hợp nhất với bạn. Không có hình phạt cho bài tập muộn; để có được chứng chỉ, tất cả những gì bạn phải làm là hoàn thành tất cả công việc. Bạn có thể gia hạn thời hạn của mình bất kỳ lúc nào bằng cách đi tới **Tổng quan** trong bảng điều hướng và chọn **Chuyển đổi phiên** . Nếu bạn đã bỏ lỡ thời hạn trước đó, hãy chọn **Đặt lại thời hạn của tôi** .
* **Hãy tò mò:** Nếu bạn tìm thấy một ý tưởng khiến bạn hứng thú, hãy hành động theo nó! Đặt câu hỏi, tìm kiếm thêm chi tiết trực tuyến, khám phá các liên kết mà bạn quan tâm và ghi chú những khám phá của bạn. Các bước bạn thực hiện để hỗ trợ quá trình học tập của mình sẽ nâng cao kiến ​​thức của bạn, tạo ra nhiều cơ hội hơn trong lĩnh vực có tốc độ tăng trưởng cao này và giúp bạn đủ điều kiện tìm việc làm.
* **Ghi chú:** Ghi chú sẽ giúp bạn ghi nhớ những thông tin quan trọng trong tương lai, đặc biệt khi bạn đang chuẩn bị bước vào một lĩnh vực công việc mới. Ngoài ra, ghi chép là một cách hiệu quả để tạo sự kết nối giữa các chủ đề và hiểu rõ hơn về các chủ đề đó.
* **Xem lại các mẫu:** Các mẫu là các bài tập đã hoàn thành đáp ứng đầy đủ các tiêu chí của hoạt động. Nhiều hoạt động trong chương trình này có mẫu để bạn xác thực công việc của mình hoặc kiểm tra lỗi. Mặc dù thường có nhiều cách để hoàn thành bài tập nhưng các ví dụ mẫu sẽ đưa ra hướng dẫn và nguồn cảm hứng về cách hoàn thành hoạt động.
* **Trò chuyện (có trách nhiệm) với những người học khác:** Nếu bạn có câu hỏi, rất có thể bạn không đơn độc. Sử dụng[diễn đàn thảo luận](https://www.coursera.org/learn/linux-and-sql/discussions)để yêu cầu sự giúp đỡ từ những người học khác tham gia chương trình này. Bạn cũng có thể ghé thăm Coursera's[Cộng đồng trực tuyến toàn cầu](https://coursera.community/). Những điều quan trọng khác cần biết khi học cùng người khác có thể được tìm thấy trong[Mã danh dự Coursera](https://learner.coursera.help/hc/en-us/articles/209818863-Coursera-Honor-Code)Và[Quy tắc ứng xử](https://learner.coursera.help/hc/en-us/articles/208280036-Coursera-Code-of-Conduct).
* **Cập nhật hồ sơ của bạn:** Hãy xem xét[cập nhật hồ sơ của bạn](https://www.coursera.org/account/profile)trên Coursera để đưa ảnh của bạn, mục tiêu nghề nghiệp, v.v. Khi những người học khác tìm thấy bạn trong các diễn đàn thảo luận, họ có thể nhấp vào tên của bạn để truy cập hồ sơ của bạn và hiểu rõ hơn về bạn.

|  |
| --- |
| **Documents, spreadsheets, presentations, and labs for course activities** |

**Tài liệu, bảng tính, bài thuyết trình và phòng thí nghiệm cho các hoạt động của khóa học**

|  |
| --- |
| 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](https://support.microsoft.com/en-us/word): Microsoft Support page for Word * [Google Docs](https://support.google.com/docs/topic/9046002?hl=en&ref_topic=1382883): Help Center page for Google Docs * [Microsoft Excel: Help and learning](https://support.microsoft.com/en-us/excel): Microsoft Support page for Excel * [Google Sheets](https://support.google.com/docs/topic/9054603?hl=en&ref_topic=1382883): Help Center page for Google Sheets * [Microsoft PowerPoint: Help and learning](https://support.microsoft.com/en-us/powerpoint): Microsoft Support page for PowerPoint * [How to use Google Slides](https://support.google.com/docs/answer/2763168?hl=en&co=GENIE.Platform%3DDesktop): Help Center page for Google Slides * [Common problems with labs](https://support.google.com/qwiklabs/answer/9133560?hl=en&ref_topic=9134804): Troubleshooting help for Qwiklabs activities |

Để hoàn thành một số hoạt động nhất định trong chương trình, bạn sẽ cần sử dụng tài liệu kỹ thuật số, bảng tính, bản trình bày và/hoặc phòng thí nghiệm. Các chuyên gia bảo mật sử dụng các công cụ phần mềm này để cộng tác trong nhóm và tổ chức của họ. Nếu bạn cần thêm thông tin về cách sử dụng một công cụ cụ thể, hãy tham khảo các tài nguyên sau:

* [Microsoft Word: Trợ giúp và học tập](https://support.microsoft.com/en-us/word): Trang hỗ trợ của Microsoft dành cho Word
* [Google Tài liệu](https://support.google.com/docs/topic/9046002?hl=en&ref_topic=1382883): Trang Trung tâm trợ giúp dành cho Google Documents
* [Microsoft Excel: Trợ giúp và học tập](https://support.microsoft.com/en-us/excel): Trang hỗ trợ của Microsoft dành cho Excel
* [Google Trang tính](https://support.google.com/docs/topic/9054603?hl=en&ref_topic=1382883): Trang Trung tâm trợ giúp dành cho Google Trang tính
* [Microsoft PowerPoint: Trợ giúp và học tập](https://support.microsoft.com/en-us/powerpoint): Trang hỗ trợ của Microsoft dành cho PowerPoint
* [Cách sử dụng Google Trang trình bày](https://support.google.com/docs/answer/2763168?hl=en&co=GENIE.Platform%3DDesktop): Trang Trung tâm trợ giúp dành cho Google Trang trình bày
* [Các vấn đề thường gặp với phòng thí nghiệm](https://support.google.com/qwiklabs/answer/9133560?hl=en&ref_topic=9134804): Trợ giúp khắc phục sự cố cho các hoạt động của Qwiklabs

|  |
| --- |
| **Module, course, and certificate glossaries** |

**Bảng thuật ngữ mô-đun, khóa học và chứng chỉ**

|  |
| --- |
| 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:   * **Module glossaries**: At the end of each module’s content, you can review a glossary of terms from that module. Each module’s glossary builds upon the terms from the previous modules in that course. The module 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. |

Chương trình này bao gồm rất nhiều thuật ngữ và khái niệm, một số trong đó bạn có thể đã biết và một số có thể xa lạ với bạn. Để xem lại các thuật ngữ và giúp bạn chuẩn bị cho các bài kiểm tra được chấm điểm, hãy tham khảo các bảng thuật ngữ sau:

* **Bảng thuật ngữ mô-đun** : Ở cuối nội dung của mỗi mô-đun, bạn có thể xem lại bảng chú giải thuật ngữ của mô-đun đó. Bảng thuật ngữ của mỗi mô-đun được xây dựng dựa trên các thuật ngữ từ các mô-đun trước đó trong khóa học đó. Bảng thuật ngữ mô-đun không thể tải xuống được; tuy nhiên, tất cả các thuật ngữ và định nghĩa đều có trong bảng thuật ngữ khóa học và chứng chỉ, có thể tải xuống được.
* **Bảng thuật ngữ khóa học** : Vào cuối mỗi khóa học, bạn có thể truy cập và tải xuống bảng chú giải thuật ngữ bao gồm tất cả các thuật ngữ trong khóa học đó.
* **Bảng chú giải thuật ngữ chứng chỉ** : Bảng chú giải chứng chỉ bao gồm tất cả các thuật ngữ trong toàn bộ chương trình chứng chỉ và là nguồn tài nguyên hữu ích mà bạn có thể tham khảo trong suốt chương trình hoặc bất kỳ lúc nào trong tương lai.

|  |
| --- |
| 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](https://www.coursera.org/learn/linux-and-sql/resources/FUN4o) section. To access the **Cybersecurity Certificate glossary**, click the link below and select *Use Template*.   * [Cybersecurity Certificate glossary](https://docs.google.com/document/d/1Feb8pHRY-blnpaLOohds2esd6IWdCIp-ikG7G_omSj4/template/preview?usp=sharing&resourcekey=0-YHcAISkCiqGDq5KwO6yNeQ) |

Bạn có thể truy cập và tải xuống bảng chú giải chứng chỉ và lưu chúng trên máy tính của mình. Bạn luôn có thể tìm thấy bảng chú giải thuật ngữ về khóa học và chứng chỉ thông qua trang của khóa học.[Tài nguyên](https://www.coursera.org/learn/linux-and-sql/resources/FUN4o)phần. Để truy cập **bảng chú giải Chứng chỉ An ninh mạng** , hãy nhấp vào liên kết bên dưới và chọn *Sử dụng Mẫu* .

* [Thuật ngữ chứng chỉ an ninh mạng](https://docs.google.com/document/d/1Feb8pHRY-blnpaLOohds2esd6IWdCIp-ikG7G_omSj4/template/preview?usp=sharing&resourcekey=0-YHcAISkCiqGDq5KwO6yNeQ)

|  |
| --- |
| **Course feedback** |

**Phản hồi khóa học**

|  |
| --- |
| 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. |

Việc cung cấp phản hồi về video, bài đọc và các tài liệu khác thật dễ dàng. Khi tài nguyên mở trong trình duyệt của bạn, bạn có thể tìm thấy các biểu tượng không thích và không thích.

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

* Hãy bấm **nút thích** để xem những tài liệu hữu ích.
* Hãy **nhấp vào nút không thích** đối với những tài liệu không hữu ích.

|  |
| --- |
| 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. |

Nếu bạn muốn gắn cờ một vấn đề cụ thể cho một mục, hãy nhấp vào biểu tượng lá cờ, chọn một danh mục và nhập lời giải thích vào hộp văn bản. Phản hồi này sẽ được chuyển lại cho nhóm phát triển khóa học và những người học khác sẽ không nhìn thấy được. Tất cả phản hồi nhận được sẽ giúp tạo ra các chương trình chứng chỉ tốt hơn nữa trong tương lai.

|  |
| --- |
| For technical help, visit the [Learner Help Center](https://learner.coursera.help/hc/en-us). |

Để được trợ giúp kỹ thuật, hãy truy cập[Trung tâm trợ giúp người học](https://learner.coursera.help/hc/en-us).

***1.4. Connect with your classmates – Kết nối với các bạn cùng lớp của bạn***

**2. The wonderful world of operating systems – Thế giới tuyệt vời của hệ điều hành**

***2.1. Welcome to module 1 – Chào mừng đến với mô-đun 1***

|  |
| --- |
| 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 operating systems come in. |

Bạn sử dụng máy tính bao nhiêu lần một tuần?Đối với một số người trong chúng ta, câu trả lời có thể là "rất nhiều"!Chúng là những cỗ máy đáng kinh ngạchãy để chúng tôi làm mọi thứ từ việc sử dụngứng dụng chuyên dụng khi hoàn thành nhiệm vụ trong công việcđể gửi email cho những người thân yêu ở một nơi xa.Bạn đã bao giờ nghĩ về cách máy tínhcó thể làm được tất cả những điều này?Vâng, đó là nơi hệ điều hành xuất hiện.

|  |
| --- |
| 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. |

Trong phần này chúng ta sẽ tìm hiểu vềcác hệ điều hành phổ biến và chúng ta sẽ khám pháchức năng chính của một hệ điều hành.Sau đó chúng ta sẽ tìm hiểu mối quan hệ giữahệ điều hành, ứng dụng và phần cứng.Cuối cùng, chúng ta sẽ so sánhgiao diện người dùng đồ họa và giao diện dòng lệnh.Giao diện dòng lệnh sẽ làmột phần thiết yếu trong công việc của bạn với tư cách là nhà phân tích bảo mật.Tìm hiểu hệ điều hành lànền tảng quan trọng cho sự nghiệp bảo mật của bạn.Có quá nhiều thứ để khám phá. Hãy bắt đầu nào.

***2.2. Kim: My journey into computing – Kim: Hành trình đến với máy tính của tôi***

|  |
| --- |
| 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. |

Xin chào, tôi là Kim.Tôi là người quản lý chương trình kỹ thuật tại Google.Tôi hiện đang làm việc tạinhóm an ninh, sáp nhập và mua lại.Nơi tôi làm việc với các công ty khác mà chúng tôi mua,và tôi giúp họ hòa nhập vào môi trường Google.Tôi đã đảm nhiệm nhiều vai trò trước khi tham giaan ninh mạng và thậm chí cả công nghệ.Lần đầu tiên tôi bắt đầu làm nhân viên nhà hàng,và sau đó tôi trở thành Gia sư tiếng Anhcho sinh viên quốc tế tại trường đại học địa phương của tôi.Sau nhiều lần thực tập,và tốt nghiệp đại học,Tôi có cơ hội đầu tiên làm việc trong lĩnh vực công nghệ,và đó là nơi tôi quan tâm đến công nghệ,và cuối cùng an ninh mạng đã bắt đầu.Tôi muốn nói với mọi người về bất kỳ loạinền tảng mà bạn có thể tham gia vào an ninh mạng.Nếu bạn quan tâm đến việc bảo vệ thông tin,nếu bạn quan tâm đến việc bảo vệ con người trong tương lai,an ninh ở đó dành cho bạn.Có rất nhiều vai trò khác nhau mà bạn có thể làm,và tất cả những kỹ năng bạn có hiện tại,và bạn đã thu thập trước đó,có thể được áp dụng trong phạm vi bảo mật.Kỹ năng mà tôi sử dụng nhiều nhất làkết nối với mọi người mỗi ngày.Tôi không thể làm được việc gìtrừ khi tôi kết nối với họ đúng cách.Đó thực sự là kỹ năng lớn nhất mà tôidựa vào những người làm việc tốt nhất trong lĩnh vực bảo mật.Một lời khuyên tôi sẽ đưa radành cho người mới bắt đầulĩnh vực an ninh mạng là giữ một tâm trí cởi mở.Tôi bắt đầu với tấm bằng kinh doanh,nên tôi thậm chí còn không cảm thấy như mìnhđủ kỹ thuật để có được vị trí như ngày hôm nay.Và trước đó, tất cả kinh nghiệm của tôihoặc là làm việc ở nhà hàng,hoặc công việc tiếp thị, hoặc chỉ một cái gì đócảm giác như nó không liên quan đến công nghệ.Nhưng tất cả những điều đó đã giúp ích và động viên tôithực sự là tôi bắt đầu làm quen với công nghệ nhiều hơn,và cuối cùng là bảo mật.Và trước khi tôi biết điều đó,sự nghi ngờ bản thân đó thực sự làđược thay thế bằng nhiều sự hỗ trợ hơntừ các đồng nghiệp của tôi vàsự tôn trọng từ những người khác mà tôi đã làm việc cùng.

***2.3. Introduction to operating systems – Giới thiệu về hệ điều hành***

|  |
| --- |
| 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. |

Các thiết bị như máy tính, điện thoại thông minh và máy tính bảng đều có hệ điều hành.Nếu bạn đã sử dụng máy tính để bàn hoặc máy tính xách tay,bạn có thể đã sử dụng hệ điều hành Windows hoặc MacOs. Điện thoại thông minh vàmáy tính bảng chạy trên hệ điều hành di động như Android và iOS.Một hệ điều hành phổ biến khác là Linux.Linux được sử dụng trong ngành bảo mật,và là một chuyên gia bảo mật, rất có thể bạn sẽ tương tác với HĐH Linux.

|  |
| --- |
| 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. |

Vậy chính xác hệ điều hành là gì?Đó là giao diện giữa phần cứng máy tính và người dùng.Hệ điều hành, hay hệ điều hành như nó thường được gọi, chịu trách nhiệm vềlàm cho máy tính chạy hiệu quả nhất có thể đồng thời làm cho nó dễ sử dụng.Phần cứng có thể là một thuật ngữ mới.Phần cứng đề cập đến các thành phần vật lý của máy tính.

|  |
| --- |
| 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. |

Giao diện hệ điều hành mà chúng ta hiện đang sử dụng hàng ngày là một thứ còn quá sớmmáy tính không có.Vào những năm 1950, thách thức lớn nhất đối với những chiếc máy tính đời đầu là lượng thời giancần phải chạy một chương trình máy tính. Vào thời điểm đó, máy tính không thể chạy nhiềucác chương trình cùng một lúc.Thay vào đó, mọi người phải đợi chương trình chạy xong,khởi động lại máy tính và tải chương trình mới lên.Hãy tưởng tượng bạn phải bật máy tính lên vàtắt mỗi khi bạn phải mở một ứng dụng mới!Sẽ mất nhiều thời gian để hoàn thành một nhiệm vụ đơn giản như gửi email.Kể từ đó, các hệ điều hành đã phát triển vàchúng ta không còn phải lo lắng về việc lãng phí thời gian theo cách này nữa.Nhờ hệ điều hành và sự phát triển của chúng,máy tính ngày nay chạy hiệu quả.Họ chạy nhiều ứng dụng cùng một lúc vàhọ cũng truy cập các thiết bị bên ngoài như máy in, bàn phím và chuột.

|  |
| --- |
| 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. |

Một lý do khác tại sao hệ điều hành lại quan trọng là chúng giúp con người vàcác máy tính giao tiếp với nhau.Máy tính giao tiếp bằng ngôn ngữ gọi là nhị phân, bao gồm 0 và 1.Hệ điều hành cung cấp một giao diện để thu hẹp khoảng cách giao tiếp giữa người dùngvà máy tính, cho phép bạn tương tác với máy tính theo những cách phức tạp.

|  |
| --- |
| 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. |

Hệ điều hành rất quan trọng đối với việc sử dụng máy tính. Tương tự như vậy,Bảo mật hệ điều hành cũng rất quan trọng đối với bảo mật của máy tính.Điều này liên quan đến việc bảo mật các tập tin, quyền truy cập dữ liệu và xác thực người dùng đểgiúp bảo vệ và ngăn chặn các mối đe dọa như vi-rút, sâu và phần mềm độc hại.Biết hệ điều hành hoạt động như thế nào là điều cần thiết chohoàn thành các nhiệm vụ liên quan đến bảo mật khác nhau.Ví dụ: với tư cách là nhà phân tích bảo mật, bạn có thể chịu trách nhiệm định cấu hình vàduy trì tính bảo mật của hệ thống bằng cách quản lý quyền truy cập.Bạn cũng có thể chịu trách nhiệm quản lý và định cấu hình tường lửa,thiết lập các chính sách bảo mật, cho phép bảo vệ chống vi-rút vàthực hiện kiểm toán, kế toán và ghi nhật ký để phát hiện hành vi bất thường.Tất cả những nhiệm vụ này đòi hỏi sự hiểu biết sâu sắc về hệ điều hành vàKhi tiếp tục khóa học này, chúng ta sẽ khám phá hệ điều hành một cách chi tiết hơn.

***2.4. Compare operating systems – So sánh hệ điều hành***

|  |
| --- |
| **Compare operating systems** |

**So sánh hệ điều hành**

|  |
| --- |
| 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. |

Trước đây bạn đã khám phá lý do tại sao hệ điều hành là một phần quan trọng trong cách thức hoạt động của máy tính. Trong bài đọc này, bạn sẽ so sánh một số hệ điều hành phổ biến được sử dụng ngày nay. Bạn cũng sẽ tập trung vào những rủi ro khi sử dụng hệ điều hành cũ.

|  |
| --- |
| **Common operating systems** |

**Hệ điều hành phổ biến**

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

Các hệ điều hành sau đây rất hữu ích cần biết trong ngành bảo mật: Windows, macOS®, Linux, ChromeOS, Android và iOS.

|  |
| --- |
| **Windows and macOS** |

**Windows và 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 và macOS đều là những hệ điều hành phổ biến. Hệ điều hành Windows được giới thiệu vào năm 1985 và macOS được giới thiệu vào năm 1984. Cả hai hệ điều hành đều được sử dụng trong máy tính cá nhân và doanh nghiệp.

|  |
| --- |
| 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. |

Windows là một hệ điều hành nguồn đóng, có nghĩa là mã nguồn không được chia sẻ rộng rãi với công chúng. macOS là nguồn mở một phần. Nó có một số thành phần nguồn mở, chẳng hạn như kernel của macOS. macOS cũng có một số thành phần nguồn đóng.

|  |
| --- |
| **Linux** |

**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. |

Phiên bản đầu tiên của Linux được phát hành vào năm 1991 và các phiên bản chính khác tiếp theo vào đầu những năm 1990. Linux là một hệ điều hành hoàn toàn mã nguồn mở, có nghĩa là bất kỳ ai cũng có thể truy cập Linux và mã nguồn của nó. Bản chất nguồn mở của Linux cho phép các nhà phát triển trong cộng đồng Linux cộng tác.

|  |
| --- |
| 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. |

Linux đặc biệt quan trọng đối với ngành bảo mật. Có một số bản phân phối được thiết kế đặc biệt để bảo mật. Ở phần sau của khóa học này, bạn sẽ tìm hiểu về Linux và tầm quan trọng của nó đối với ngành bảo mật.

|  |
| --- |
| **ChromeOS** |

**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. |

ChromeOS ra mắt vào năm 2011. Nó là nguồn mở một phần và có nguồn gốc từ Chrome OS, đây là nguồn mở hoàn toàn. ChromeOS thường xuyên được sử dụng trong lĩnh vực giáo dục.

|  |
| --- |
| **Android and iOS** |

**Android và 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. |

Android và iOS đều là hệ điều hành di động. Không giống như các hệ điều hành khác được đề cập, hệ điều hành di động thường được sử dụng trong các thiết bị di động, chẳng hạn như điện thoại, máy tính bảng và đồng hồ. Android được giới thiệu để sử dụng rộng rãi vào năm 2008 và iOS được giới thiệu vào năm 2007. Android là nguồn mở và iOS là nguồn mở một phần.

|  |
| --- |
| **Operating systems and vulnerabilities** |

**Hệ điều hành và lỗ hổng**

|  |
| --- |
| 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. |

Vấn đề bảo mật là điều không thể tránh khỏi với mọi hệ điều hành. Một phần quan trọng trong việc bảo vệ hệ điều hành là luôn cập nhật hệ thống và tất cả các thành phần của nó.

|  |
| --- |
| **Legacy operating systems** |

**Hệ điều cũ**

|  |
| --- |
| 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. |

Hệ **điều hành cũ** là hệ điều hành đã lỗi thời nhưng vẫn được sử dụng. Một số tổ chức tiếp tục sử dụng hệ điều hành cũ vì phần mềm mà họ dựa vào không tương thích với hệ điều hành mới hơn. Điều này có thể phổ biến hơn trong các ngành sử dụng nhiều thiết bị yêu cầu phần mềm nhúng—phần mềm được đặt bên trong các bộ phận của thiết bị.

|  |
| --- |
| 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. |

Các hệ điều hành cũ có thể dễ gặp phải các vấn đề bảo mật vì chúng không còn được hỗ trợ hoặc cập nhật nữa. Điều này có nghĩa là các hệ điều hành cũ có thể dễ bị tổn thương trước các mối đe dọa mới.

|  |
| --- |
| **Other vulnerabilities** |

**Các lỗ hổng khác**

|  |
| --- |
| 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. |

Ngay cả khi hệ điều hành được cập nhật, chúng vẫn có thể dễ bị tấn công. Dưới đây là một số tài nguyên bao gồm thông tin về hệ điều hành và các lỗ hổng của chúng.

|  |
| --- |
| * [Microsoft Security Response Center (MSRC)](https://msrc.microsoft.com/update-guide/vulnerability): A list of known vulnerabilities affecting Microsoft products and services * [Apple Security Updates](https://support.apple.com/en-us/HT201222): 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](https://ubuntu.com/security/cves): A list of known vulnerabilities affecting Ubuntu, which is a specific distribution of Linux * [Google Cloud Security Bulletin](https://cloud.google.com/support/bulletins): A list of known vulnerabilities affecting Google Cloud products and services |

* [Trung tâm phản hồi bảo mật của Microsoft (MSRC)](https://msrc.microsoft.com/update-guide/vulnerability): Danh sách các lỗ hổng đã biết ảnh hưởng đến các sản phẩm và dịch vụ của Microsoft
* [Cập nhật bảo mật của Apple](https://support.apple.com/en-us/HT201222): Danh sách các bản cập nhật bảo mật và thông tin dành cho hệ điều hành Apple®, bao gồm macOS và iOS cũng như các sản phẩm khác
* [Báo cáo về các lỗ hổng và nguy cơ phơi nhiễm phổ biến (CVE) cho Ubuntu](https://ubuntu.com/security/cves): Danh sách các lỗ hổng đã biết ảnh hưởng đến Ubuntu, một bản phân phối cụ thể của Linux
* [Bản tin bảo mật đám mây của Google](https://cloud.google.com/support/bulletins): Danh sách các lỗ hổng đã biết ảnh hưởng đến các sản phẩm và dịch vụ của Google Cloud

|  |
| --- |
| 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. |

Luôn cập nhật hệ điều hành là một cách quan trọng để giúp hệ thống luôn an toàn. Vì khó có thể luôn cập nhật tất cả các hệ thống nên điều quan trọng là các nhà phân tích bảo mật phải có kiến ​​thức về các hệ điều hành cũ và những rủi ro mà chúng có thể tạo ra.

|  |
| --- |
| **Key takeaways** |

**Bài học chính**

|  |
| --- |
| 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. |

Windows, macOS, Linux, ChromeOS, Android và iOS đều là những hệ điều hành được sử dụng phổ biến. Các nhà phân tích bảo mật nên nhận thức được các lỗ hổng ảnh hưởng đến hệ điều hành. Điều đặc biệt quan trọng đối với các nhà phân tích bảo mật là phải làm quen với các hệ điều hành cũ, đó là những hệ thống đã lỗi thời nhưng vẫn đang được sử dụng.

***2.5. Your background in operating systems – Nền tảng của bạn về hệ điều hành***

***2.6. Test your knowledge: The wonderful world of operating systems – Kiểm tra kiến ​​thức của bạn: Thế giới tuyệt vời của hệ điều hành***

**3. The operating system at work – Hệ điều hành đang hoạt động**

***3.1. Inside the operating system – Bên trong hệ điều hành***

|  |
| --- |
| 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. |

Trước đây các bạn đã biết hệ điều hành là gì.Bây giờ, hãy thảo luận về cách chúng hoạt động.Trong video này, bạn sẽ tìm hiểu điều gì xảy ra vớimột hệ điều hành hoặc hệ điều hành,khi ai đó sử dụng máy tính cho một công việc.

|  |
| --- |
| 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. |

Hãy nghĩ về khi ai đó lái xe ô tô.Họ nhấn bàn đạp ga và chiếc xe di chuyển về phía trước.Họ không cần phải chú ý tớitất cả các cơ chế cho phép ô tô chuyển động.Giống như một chiếc ô tô không thể hoạt động nếu không có động cơ,một máy tính không thể hoạt động nếu không có hệ điều hành.

|  |
| --- |
| 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. |

Công việc của hệ điều hành là giúp đỡcác chương trình máy tính khác chạy hiệu quả.Hệ điều hành thực hiện điều này bằng cách chăm sóctất cả những chi tiết lộn xộn liên quan đến việc kiểm soát,phần cứng của máy tính nên bạn không cần phải làm vậy.

|  |
| --- |
| 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 boots 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. |

Đầu tiên, chúng ta hãy xem những gìxảy ra khi bạn bật máy tính.Khi bạn nhấn nút nguồn,bạn đang tương tác với phần cứng.Thao tác này khởi động máy tính vàhệ điều hành xuất hiện.Khởi động máy tính có nghĩa làmột vi mạch đặc biệt gọi là BIOS được kích hoạt.Trên nhiều máy tính được sản xuất sau năm 2007,con chip đã được thay thế bằng UEFI.Cả BIOS và UEFI đều chứa các hướng dẫn khởi độngchịu trách nhiệm tải một chương trình đặc biệtđược gọi là bộ nạp khởi động.Sau đó, bộ nạp khởi động làchịu trách nhiệm khởi động hệ điều hành.Cứ như vậy, máy tính của bạn đã được bật.

|  |
| --- |
| 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. |

Là một nhà phân tích chứng khoán,hiểu các quy trình này có thể hữu ích cho bạn.Các lỗ hổng có thể xảy ra ởmột cái gì đó giống như một quá trình khởi động.Thông thường, BIOS khôngđược quét bằng phần mềm diệt virus,vì vậy nó có thể dễ bị nhiễm phần mềm độc hại.Bây giờ, bạn đã học cách khởi động hệ điều hành,hãy xem cách bạn và tất cả người dùnggiao tiếp với hệ thống để hoàn thành nhiệm vụ.

|  |
| --- |
| 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. |

Quá trình bắt đầu với bạn, người dùng.Và để hoàn thành nhiệm vụ, bạn sử dụng các ứng dụng trên máy tính.Ứng dụng là một chương trìnhđó thực hiện một nhiệm vụ cụ thể.Khi bạn làm điều này, ứng dụnggửi yêu cầu của bạn đến hệ điều hành.Từ đó, hệ điều hành diễn giải yêu cầu nàyvà hướng nó đến thành phần thích hợpcủa phần cứng của máy tính.

|  |
| --- |
| 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. |

Trong video trước,chúng tôi đã biết rằng phần cứng bao gồmtất cả các thành phần vật lý của máy tính.Phần cứng cũng sẽ gửithông tin trở lại hệ điều hành.Và điều này lần lượt được gửi trở lại ứng dụng.

|  |
| --- |
| 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. |

Hãy đưa ra một cái nhìn tổng quan đơn giản về cách thức hoạt động của nókhi bạn muốn sử dụng máy tính trên máy tính của mình.Bạn dùng chuột click vàoứng dụng máy tính trên máy tính của bạn.Khi bạn gõ số bạn muốn tính toán,ứng dụng giao tiếp với hệ điều hành.Hệ điều hành của bạn sau đó sẽ gửitính toán cho một thành phần của phần cứng,bộ xử lý trung tâm hay CPU.Một khi phần cứng đã hoạt độngxác định số cuối cùng,nó sẽ gửi câu trả lời trở lại hệ điều hành của bạn.Sau đó, nó có thể được hiển thị trong ứng dụng máy tính của bạn.

|  |
| --- |
| 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. |

Hiểu được quá trình này làhữu ích khi điều tra các sự kiện bảo mật.Các nhà phân tích bảo mật sẽ có thểtheo dõi lại quá trình nàyđể phân tích nơi một sự kiện bảo mật có thể xảy ra.

|  |
| --- |
| 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. |

Giống như một người thợ cơ khí cầnhiểu hoạt động bên trong của ô tôhơn một người lái xe bình thường,nhận biết hệ điều hành như thế nàocông việc là kiến ​​thức quan trọng đối với một nhà phân tích chứng khoán.

***3.2. Requests to the operating system – Yêu cầu đối với hệ điều hành***

|  |
| --- |
| **Requests to the operating system** |

**Yêu cầu đối với hệ điều hành**

|  |
| --- |
| 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. |

Hệ điều hành là một thành phần quan trọng của máy tính. Chúng tạo kết nối giữa các ứng dụng và phần cứng để cho phép người dùng thực hiện các tác vụ. Trong bài đọc này, bạn sẽ khám phá sâu hơn về quá trình phức tạp này và xem xét nó bằng cách sử dụng một phép loại suy mới và một ví dụ mới.

|  |
| --- |
| **Booting the computer** |

**Khởi động máy tính**

|  |
| --- |
| 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. |

Khi bạn khởi động hoặc bật máy tính, vi mạch BIOS hoặc UEFI sẽ được kích hoạt. Hệ **thống đầu vào/đầu ra cơ bản (BIOS)** là một vi mạch chứa các hướng dẫn tải cho máy tính và phổ biến trong các hệ thống cũ. Giao **diện phần mềm mở rộng hợp nhất (UEFI)** là một vi mạch chứa các hướng dẫn tải cho máy tính và thay thế BIOS trên các hệ thống hiện đại hơn.

|  |
| --- |
| 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. |

Các chip BIOS và UEFI đều thực hiện cùng chức năng khởi động máy tính. BIOS là chip tiêu chuẩn cho đến năm 2007, khi chip UEFI được sử dụng ngày càng nhiều. Hiện nay, hầu hết các máy tính mới đều có chip UEFI. UEFI cung cấp các tính năng bảo mật nâng cao.

|  |
| --- |
| 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. |

Các vi mạch BIOS hoặc UEFI chứa nhiều hướng dẫn tải khác nhau để máy tính tuân theo. Ví dụ: một trong những hướng dẫn tải là xác minh tình trạng phần cứng của máy tính.

|  |
| --- |
| 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. |

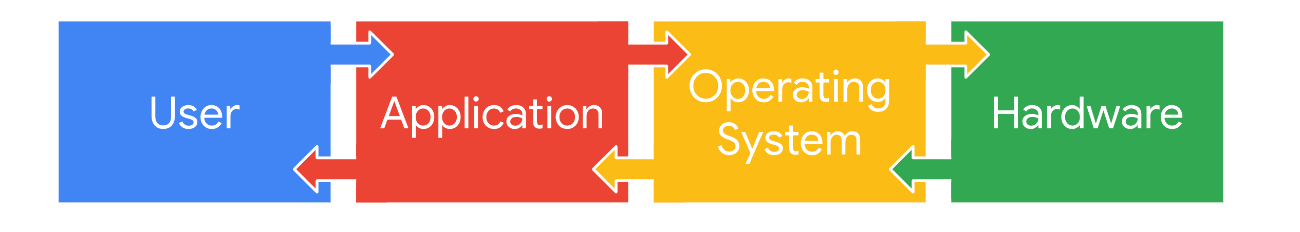
Lệnh cuối cùng từ BIOS hoặc UEFI sẽ kích hoạt bộ nạp khởi động. **Bootloader** là một chương trình phần mềm khởi động hệ điều hành. Sau khi hệ điều hành khởi động xong, máy tính của bạn đã sẵn sàng để sử dụng.

|  |
| --- |
| **Completing a task** |

**Hoàn thành một nhiệm vụ**

|  |
| --- |
| 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. |

Như đã thảo luận trước đây, hệ điều hành giúp chúng ta sử dụng máy tính hiệu quả hơn. Khi máy tính đã trải qua quá trình khởi động, việc hoàn thành tác vụ trên máy tính là một quá trình gồm bốn phần.



|  |
| --- |
| **User** |

**Người dùng**

|  |
| --- |
| 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. |

Phần đầu tiên của quá trình này là người dùng. Người dùng bắt đầu quá trình bằng cách thực hiện điều gì đó họ muốn thực hiện trên máy tính. Ngay bây giờ, bạn là người dùng! Bạn đã bắt đầu quá trình truy cập bài đọc này.

|  |
| --- |
| **Application** |

**Ứng dụng**

|  |
| --- |
| 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. |

Ứng dụng là chương trình phần mềm mà người dùng tương tác để hoàn thành một tác vụ. Ví dụ: nếu bạn muốn tính toán một cái gì đó, bạn sẽ sử dụng ứng dụng máy tính. Nếu bạn muốn viết báo cáo, bạn sẽ sử dụng một ứng dụng xử lý văn bản. Đây là phần thứ hai của quá trình.

|  |
| --- |
| **Operating system** |

**Hệ điều hành**

|  |
| --- |
| 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. |

Hệ điều hành nhận được yêu cầu của người dùng từ ứng dụng. Nhiệm vụ của hệ điều hành là diễn giải yêu cầu và điều khiển luồng của nó. Để hoàn thành nhiệm vụ, hệ điều hành sẽ gửi nó tới các thành phần có thể áp dụng của phần cứng.

|  |
| --- |
| **Hardware** |

**Phần cứng**

|  |
| --- |
| 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. |

Phần cứng là nơi thực hiện tất cả quá trình xử lý để hoàn thành các tác vụ do người dùng khởi tạo. Ví dụ: khi người dùng muốn tính một số, CPU sẽ tìm ra câu trả lời. Một ví dụ khác, khi người dùng muốn lưu một tập tin, một thành phần khác của phần cứng, ổ cứng, sẽ xử lý tác vụ này.

|  |
| --- |
| 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. |

Sau khi phần cứng hoàn thành công việc, nó sẽ gửi kết quả đầu ra qua hệ điều hành đến ứng dụng để có thể hiển thị kết quả cho người dùng.

|  |
| --- |
| **The OS at work behind the scenes** |

**Hệ điều hành đang hoạt động ở hậu trường**

|  |
| --- |
| 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. |

Hãy xem xét một lần nữa máy tính giống với ô tô như thế nào. Có những quá trình mà ai đó sẽ không trực tiếp quan sát được khi điều khiển ô tô, nhưng họ sẽ cảm thấy nó di chuyển về phía trước khi nhấn bàn đạp ga. Máy tính cũng vậy. Công việc quan trọng diễn ra bên trong máy tính mà bạn không trực tiếp trải nghiệm. Công việc này liên quan đến hệ điều hành.

|  |
| --- |
| 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. |

Bạn có thể khám phá điều này thông qua một sự tương tự khác. Quá trình sử dụng hệ điều hành cũng tương tự như việc gọi món ở nhà hàng. Tại một nhà hàng, bạn đặt hàng và nhận đồ ăn, nhưng bạn không thấy điều gì đang xảy ra trong bếp khi đầu bếp chuẩn bị đồ ăn.

|  |
| --- |
| 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.” |

Việc gọi món cũng tương tự như việc sử dụng một ứng dụng trên máy tính. Khi gọi đồ ăn, bạn đưa ra một yêu cầu cụ thể như “một món súp nhỏ, thật nóng”. Khi sử dụng một ứng dụng, bạn cũng đưa ra các yêu cầu cụ thể như “in ba bản sao hai mặt của tài liệu này”.

|  |
| --- |
| 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. |

Bạn có thể so sánh thực phẩm bạn nhận được với những gì xảy ra khi phần cứng gửi đầu ra. Bạn nhận được món ăn mà bạn đã đặt hàng. Bạn nhận được tài liệu mà bạn muốn in.

|  |
| --- |
| 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. |

Cuối cùng, nhà bếp giống như hệ điều hành. Bạn không biết điều gì xảy ra trong nhà bếp, nhưng điều quan trọng là phải hiểu được yêu cầu và đảm bảo bạn nhận được món mình đã gọi. Tương tự, mặc dù công việc của HĐH không trực tiếp rõ ràng đối với bạn nhưng nó rất quan trọng trong việc hoàn thành nhiệm vụ của bạn.

|  |
| --- |
| **An example: Downloading a file from an internet browser** |

**Ví dụ: Tải xuống tệp từ trình duyệt internet**

|  |
| --- |
| 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: |

Trước đây, bạn đã khám phá cách hệ điều hành, ứng dụng và phần cứng phối hợp với nhau bằng cách kiểm tra một tác vụ liên quan đến phép tính. Bạn có thể mở rộng hiểu biết này bằng cách khám phá cách HĐH hoàn thành một tác vụ khác, tải xuống tệp từ trình duyệt internet:

|  |
| --- |
| * 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. |

* Đầu tiên, người dùng quyết định muốn tải xuống một tệp mà họ tìm thấy trên mạng, vì vậy họ nhấp vào nút tải xuống gần tệp đó trong ứng dụng trình duyệt internet.
* Sau đó, trình duyệt internet sẽ thông báo hành động này tới HĐH.
* Hệ điều hành gửi yêu cầu tải file xuống phần cứng thích hợp để xử lý.
* Phần cứng bắt đầu tải tệp xuống và hệ điều hành sẽ gửi thông tin này đến ứng dụng trình duyệt internet. Trình duyệt internet sau đó sẽ thông báo cho người dùng khi tệp đã được tải xuống.

|  |
| --- |
| **Key takeaways** |

**Bài học chính**

|  |
| --- |
| 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. |

Mặc dù hoạt động ở chế độ nền nhưng hệ điều hành là một phần thiết yếu trong quá trình sử dụng máy tính. Hệ điều hành kết nối các ứng dụng và phần cứng để cho phép người dùng hoàn thành một tác vụ.

***3.3. Practice: Order of operations in the OS – Thực hành: Thứ tự thao tác trong hệ điều hành***

|  |
| --- |
| Order the steps involved in booting a computer |
| **Step 1**  The user powers on the computer. |
| **Step 2**  BIOS or UEFI loads the bootloader. |
| **Step 3**  The bootloader program loads the OS. |

|  |
| --- |
| Thứ tự các bước tiến hành khởi động máy tính |
| **Step 1**  Người dùng cấp quyền trên máy tính. |
| **Step 2**  BIOS hoặc UEFI tải bộ nạp khởi động. |
| **Step 3**  Chương trình bootloader tải hệ điều hành. |

|  |
| --- |
| Order the steps involved in saving a file |
| **Step 1**  User opens a word processing application and types a document. |
| **Step 2**  When the user saves the document, the application communicates with the OS. |
| **Step 3**  OS saves the file to a hardware component called the hard drive. |
| **Step 4**  Hard drive confirms file was saved, communicates this to OS. OS indicates this within the application. |

|  |
| --- |
| Thứ tự các bước liên quan đến việc lưu một tập tin |
| **Step 1**  Người dùng mở một ứng dụng xử lý văn bản và gõ một tài liệu. |
| **Step 2**  Khi người dùng lưu tài liệu, ứng dụng sẽ liên lạc với OS. |
| **Step 3**  Hệ điều hành lưu tệp vào một thành phần phần cứng được gọi là ổ cứng. |
| **Step 4**  Ổ cứng xác nhận tệp đã được lưu, truyền thông tin này tới HĐH. Hệ điều hành chỉ ra điều này trong ứng dụng. |

***3.4. Resource allocation via the OS – Phân bổ tài nguyên thông qua hệ điều hành***

|  |
| --- |
| 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. |

Bây giờ chúng ta đã sẵn sàng thảo luậnmột khía cạnh khác của hệ điều hành của bạn.Hệ điều hành không chỉtương tác với các bộ phận khác của máy tính,nhưng nó cũng chịu trách nhiệm vềquản lý tài nguyên của hệ thống.Đây là một nhiệm vụ lớn đòi hỏi rất nhiều sự cân bằng để thực hiệnchắc chắn tất cả các nguồn lực củamáy tính được sử dụng hiệu quả.Hãy nghĩ về điều này giống như khái niệm năng lượng.Một người cần năng lượng để hoàn thành các nhiệm vụ khác nhau.Một số nhiệm vụ cần nhiều năng lượng hơn,trong khi những người khác yêu cầu ít hơn.Ví dụ như chạy bộđòi hỏi nhiều năng lượng hơn là xem TV.Hệ điều hành của máy tính cũng cần đảm bảo rằng nócó đủ năng lượng đểhoạt động chính xác cho một số nhiệm vụ nhất định.Việc quét vi-rút trên máy tính của bạn sẽ sử dụngtốn nhiều năng lượng hơn so với việc sử dụng ứng dụng máy tính.

|  |
| --- |
| 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. |

Hãy tưởng tượng máy tính của bạn là một dàn nhạc.Nhiều nhạc cụ khác nhau như violin,trống và kèn đều là một phần của dàn nhạc.Một dàn nhạc cũng cómột nhạc trưởng để điều khiển dòng nhạc.Trong máy tính, hệ điều hành là dây dẫn.Hệ điều hành xử lý việc quản lý tài nguyên và bộ nhớ để đảm bảonăng lực hạn chế củahệ thống máy tính được sử dụng ở nơi cần thiết nhất.Chương trình, nhiệm vụ đa dạngvà các quy trình liên tục cạnh tranh để giành đượctài nguyên của bộ xử lý trung tâm hoặc CPU.Tất cả họ đều có lý do riêng tại sao họ cần trí nhớ,lưu trữ và băng thông đầu vào/đầu ra.Hệ điều hành có trách nhiệm đảm bảo rằngmỗi chương trình đang phân bổ và hủy phân bổ tài nguyên.Tất cả điều này xảy ra trong máy tính của bạn tạicùng lúc để hệ thống của bạn hoạt động hiệu quả.

|  |
| --- |
| Much of this is hidden from you as a user. |

Phần lớn điều này được ẩn khỏi bạn với tư cách là người dùng.

|  |
| --- |
| But, your task manager will list all of the tasks that are being processed, |

Tuy nhiên, trình quản lý tác vụ của bạnsẽ liệt kê tất cảcác tác vụ đang được xử lý,

|  |
| --- |
| along with their memory and CPU usage. |

cùng với việc sử dụng bộ nhớ và CPU của họ.

|  |
| --- |
| 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. |

Là một nhà phân tích, thật hữu ích khi biếtnơi tài nguyên của hệ thống được sử dụng.Hiểu cách sử dụng tài nguyên có thể giúp bạn phản hồitới một sự cố và khắc phục sự cốcác ứng dụng trong hệ thống.

|  |
| --- |
| 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. |

Ví dụ: nếu máy tính chạy chậm,một nhà phân tích có thể khám phánó đang phân bổ tài nguyên cho phần mềm độc hại.Sự hiểu biết cơ bản về cáchhệ điều hành hoạt động sẽ giúp bạnhiểu rõ hơn về kỹ năng bảo mậtbạn sẽ học sau trong chương trình này.

***3.5. Virtualization technology – Công nghệ ảo hóa***

|  |
| --- |
| **Virtualization technology** |

**Công nghệ ảo hóa**

|  |
| --- |
| 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. |

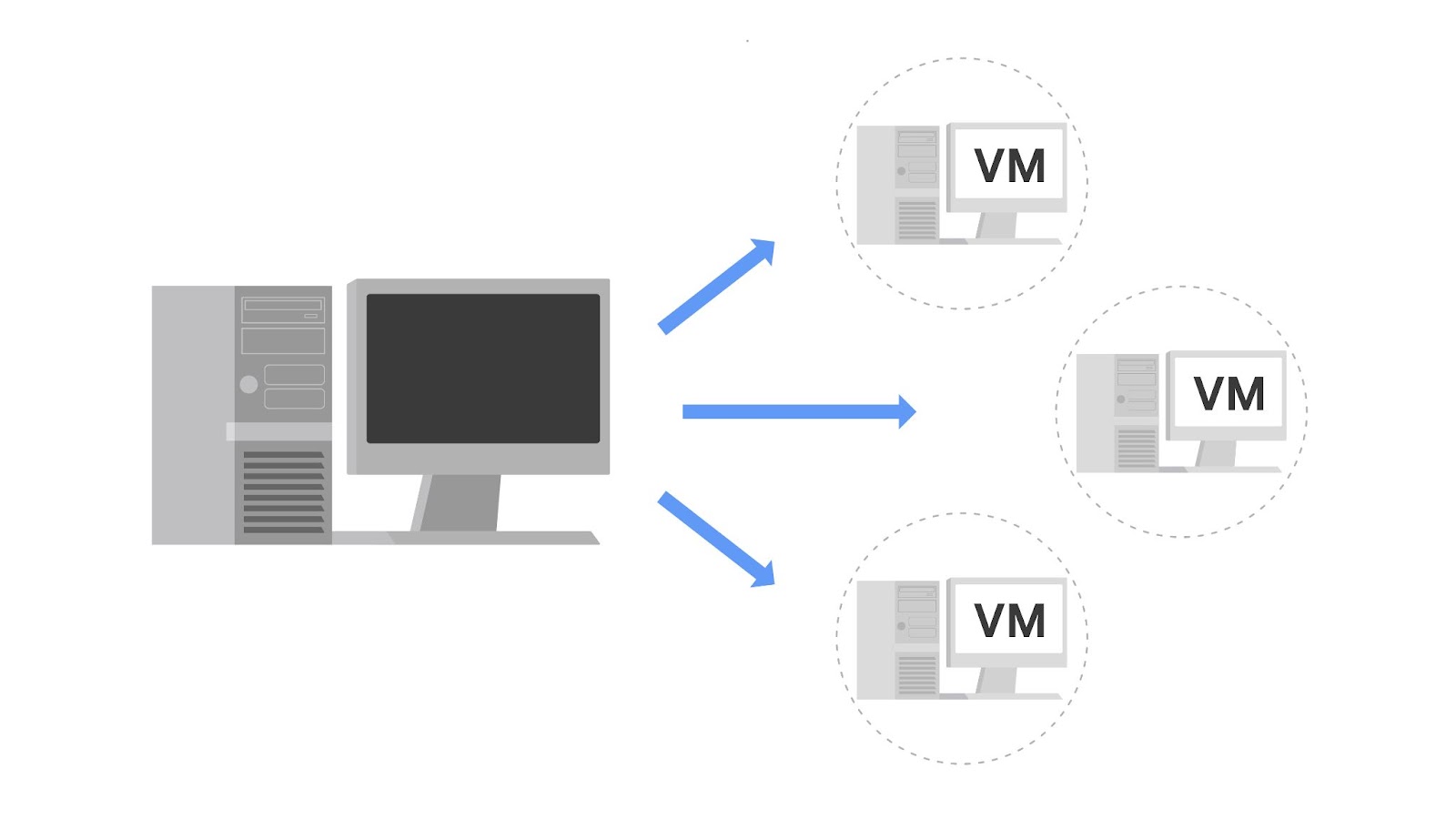
Bạn đã khám phá rất nhiều về hệ điều hành. Một khía cạnh nữa cần xem xét là hệ điều hành có thể chạy trên máy ảo. Trong bài đọc này, bạn sẽ tìm hiểu về máy ảo và khái niệm chung về ảo hóa. Bạn sẽ khám phá cách hoạt động của máy ảo và lợi ích của việc sử dụng chúng.

|  |
| --- |
| **What is a virtual machine?** |

**Máy ảo là gì?**

|  |
| --- |
| 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. |

Máy **ảo (VM)** là phiên bản ảo của máy tính vật lý. Máy ảo là một ví dụ về ảo hóa. Ảo hóa là quá trình sử dụng phần mềm để tạo ra các biểu diễn ảo của các máy vật lý khác nhau. Thuật ngữ “ảo” dùng để chỉ các máy không tồn tại về mặt vật lý nhưng hoạt động giống như vậy vì phần mềm của chúng mô phỏng phần cứng vật lý. Hệ thống ảo không sử dụng phần cứng vật lý chuyên dụng. Thay vào đó, họ sử dụng các phiên bản phần cứng vật lý được xác định bằng phần mềm. Điều này có nghĩa là một máy ảo có CPU ảo, bộ lưu trữ ảo và phần cứng ảo khác. Hệ thống ảo chỉ là mã.



|  |
| --- |
| 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. |

Bạn có thể chạy nhiều máy ảo bằng phần cứng vật lý của một máy tính. Điều này liên quan đến việc phân chia tài nguyên của máy chủ để chia sẻ trên tất cả các thành phần vật lý và ảo. Ví dụ: **Bộ nhớ truy cập ngẫu nhiên (RAM)** là thành phần phần cứng được sử dụng cho bộ nhớ ngắn hạn. Nếu một máy tính có RAM 16GB, nó có thể lưu trữ ba máy ảo để mỗi máy tính vật lý và máy ảo có 4GB RAM. Ngoài ra, mỗi máy ảo này sẽ có hệ điều hành riêng và hoạt động tương tự như một máy tính thông thường.

|  |
| --- |
| **Benefits of virtual machines** |

**Lợi ích của máy ảo**

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

Các chuyên gia bảo mật thường sử dụng ảo hóa và máy ảo. Ảo hóa có thể tăng tính bảo mật cho nhiều tác vụ và cũng có thể tăng hiệu quả.

|  |
| --- |
| **Security** |

**Bảo vệ**

|  |
| --- |
| 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. |

Một lợi ích là ảo hóa có thể cung cấp một môi trường biệt lập hoặc hộp cát trên máy chủ vật lý. Khi một máy tính có nhiều máy ảo thì những máy ảo này là “khách” của máy tính. Cụ thể, chúng được cách ly khỏi máy chủ và các máy ảo khách khác. Điều này cung cấp một lớp bảo mật vì máy ảo có thể được tách biệt khỏi các hệ thống khác. Ví dụ: nếu một máy ảo riêng lẻ bị nhiễm phần mềm độc hại, nó có thể được xử lý an toàn hơn vì nó được cách ly với các máy khác. Chuyên gia bảo mật cũng có thể cố tình đặt phần mềm độc hại vào máy ảo để kiểm tra nó trong môi trường an toàn hơn.

|  |
| --- |
| **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. |

**Lưu ý:** Mặc dù việc sử dụng máy ảo rất hữu ích khi điều tra các máy có khả năng bị nhiễm virus hoặc chạy phần mềm độc hại trong môi trường bị hạn chế nhưng vẫn có một số rủi ro. Ví dụ: một chương trình độc hại có thể thoát khỏi ảo hóa và truy cập vào máy chủ. Đây là lý do tại sao bạn không bao giờ nên tin tưởng hoàn toàn vào các hệ thống ảo hóa.

|  |
| --- |
| **Efficiency** |

**Hiệu quả**

|  |
| --- |
| 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. |

Sử dụng máy ảo cũng có thể là một cách hiệu quả và thuận tiện để thực hiện các tác vụ bảo mật. Bạn có thể mở nhiều máy ảo cùng một lúc và dễ dàng chuyển đổi giữa chúng. Điều này cho phép bạn hợp lý hóa các tác vụ bảo mật, chẳng hạn như thử nghiệm và khám phá các ứng dụng khác nhau.

|  |
| --- |
| 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. |

Bạn có thể so sánh hiệu quả của máy ảo với xe buýt thành phố. Một chiếc xe buýt thành phố có rất nhiều chỗ và là cách hiệu quả để vận chuyển nhiều người cùng một lúc. Nếu xe buýt thành phố không tồn tại thì mọi người trên xe buýt sẽ phải tự lái ô tô của mình. Điều này sử dụng nhiều xăng, ô tô và các tài nguyên khác hơn là đi xe buýt thành phố.

|  |
| --- |
| 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. |

Tương tự như số lượng người có thể đi một chuyến xe buýt, nhiều máy ảo có thể được lưu trữ trên cùng một máy vật lý. Bằng cách đó, các máy vật lý riêng biệt không cần thiết để thực hiện một số nhiệm vụ nhất định.

|  |
| --- |
| **Managing virtual machines** |

**Quản lý máy ảo**

|  |
| --- |
| 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. |

Máy ảo có thể được quản lý bằng phần mềm gọi là hypervisor. Hypervisor giúp người dùng quản lý nhiều máy ảo và kết nối phần cứng ảo và vật lý. Hypervisor cũng giúp phân bổ tài nguyên dùng chung của máy chủ vật lý cho một hoặc nhiều máy ảo.

|  |
| --- |
| 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. |

Một trình ảo hóa hữu ích mà bạn nên làm quen là Máy ảo dựa trên hạt nhân (KVM). KVM là một trình ảo hóa mã nguồn mở được hỗ trợ bởi hầu hết các bản phân phối Linux chính. Nó được tích hợp vào nhân Linux, có nghĩa là nó có thể được sử dụng để tạo các máy ảo trên bất kỳ máy nào chạy hệ điều hành Linux mà không cần phần mềm bổ sung.

|  |
| --- |
| **Other forms of virtualization** |

**Các hình thức ảo hóa khác**

|  |
| --- |
| 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. |

Ngoài máy ảo, còn có các hình thức ảo hóa khác. Một số công nghệ ảo hóa này không sử dụng hệ điều hành. Ví dụ: nhiều máy chủ ảo có thể được tạo từ một máy chủ vật lý. Mạng ảo cũng có thể được tạo để sử dụng hiệu quả hơn phần cứng của mạng vật lý.

|  |
| --- |
| **Key takeaways** |

**Bài học chính**

|  |
| --- |
| 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. |

Máy ảo là phiên bản ảo của máy tính vật lý và là một ví dụ về ảo hóa. Ảo hóa là một công nghệ quan trọng trong ngành bảo mật và điều quan trọng là các nhà phân tích bảo mật phải hiểu những điều cơ bản. Có nhiều lợi ích khi sử dụng máy ảo, chẳng hạn như cách ly phần mềm độc hại và các rủi ro bảo mật khác. Tuy nhiên, điều quan trọng cần nhớ là vẫn có nguy cơ phần mềm độc hại thoát khỏi môi trường ảo hóa.

***3.6. Test your knowledge: The operating system at work – Kiểm tra kiến ​​thức của bạn: Hệ điều hành đang hoạt động***

**4. The user interface – Giao diện người dùng**

***4.1. GUI versus CLI – GUI so với 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. |

Bây giờ bạn đã tìm hiểu hoạt động bên trong của máy tính,hãy thảo luận về cách người dùng vàhệ điều hành giao tiếp với nhau.Cho đến nay, bạn đã biết rằng máy tính cómột hệ điều hành, phần cứng và ứng dụng.Hãy nhớ rằng, hệ điều hànhgiao tiếp với phần cứng để thực hiện nhiệm vụ.Trong video này, bạn sẽ tìm hiểu cáchngười dùng—chính là bạn—tương tác vớihệ điều hành đểgửi nhiệm vụ đến phần cứng.

|  |
| --- |
| 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. |

Người dùng giao tiếp vớihệ điều hành thông qua một giao diện.Giao diện người dùng là một chương trình cho phépngười dùng điều khiển các chức năng của hệ điều hành.Hai giao diện người dùng mà chúng ta sẽ thảo luận làgiao diện người dùng đồ họa, hoặcGUI và giao diện dòng lệnh hoặc CLI.Hãy trình bày các giao diện này chi tiết hơn.

|  |
| --- |
| 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. |

GUI là giao diện người dùng sử dụng các biểu tượng trênmàn hình để quản lý các tác vụ khác nhau trên máy tính.Hầu hết các hệ điều hành có thểđược sử dụng với giao diện người dùng đồ họa.Nếu bạn đã sử dụng máy tính cá nhân hoặc điện thoại di động,bạn đã có kinh nghiệm vận hành GUI.Hầu hết các GUI bao gồm các thành phần sau:menu bắt đầu với các nhóm chương trình,thanh tác vụ để khởi chạy chương trình,và một màn hình nền có các biểu tượng và lối tắt.Tất cả những thành phần này giúp bạngiao tiếp với hệ điều hành để thực hiện các tác vụ.Ngoài việc nhấp vào biểu tượng,khi bạn sử dụng GUI,bạn cũng có thể tìm kiếm các tập tin hoặccác ứng dụng từ menu bắt đầu.Bạn chỉ cần nhớ biểu tượng hoặc têncủa chương trình để kích hoạt một ứng dụng.

|  |
| --- |
| 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. |

Bây giờ hãy thảo luận về giao diện dòng lệnh.Để so sánh, giao diện dòng lệnh hoặc CLI,là giao diện người dùng dựa trên văn bảnsử dụng các lệnh để tương tác với máy tính.Các lệnh này giao tiếp vớihệ điều hành và thực thicác công việc như mở chương trình.Giao diện dòng lệnh làmột cấu trúc rất kháchơn giao diện người dùng đồ họa.Khi bạn sử dụng CLI,bạn sẽ ngay lập tức nhận thấy sự khác biệt.Không có biểu tượng hoặc đồ họa trên màn hình.Giao diện dòng lệnh trông giống nhưdòng mã sử dụng các ngôn ngữ văn bản nhất định.CLI linh hoạt hơn và mạnh hơn GUI.Hãy suy nghĩ về việc sử dụng CLIthích tạo ra bất kỳ bữa ăn nào bạn muốntừ những nguyên liệu mua ở cửa hàng tạp hóa.Điều này mang lại cho bạn nhiều quyền kiểm soát vàtùy chỉnh về những gì bạn sẽ ăn.

|  |
| --- |
| 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. |

Để so sánh,sử dụng GUI giống như gọi đồ ăn từ nhà hàng hơn.Bạn chỉ có thể gọi những gì trên menu.Nếu bạn muốn cả món mì và pizza,nhưng nhà hàng đầu tiên bạn tới chỉ có pizza,bạn sẽ phải đi đến một nhà hàng khácđể gọi món mì.Với giao diện người dùng đồ họa,bạn phải làm một nhiệm vụ tại một thời điểmNhưng giao diện dòng lệnh cho phép tùy chỉnh,cho phép bạn hoàn thành nhiều nhiệm vụ cùng một lúc.Ví dụ, hãy tưởng tượng bạncó một thư mục với hàng trăm tập tincác loại tệp khác nhau và bạn cần phảichỉ di chuyển các tệp JPEG sang một thư mục mới.Hãy suy nghĩ về việc chậm vàđiều này sẽ tẻ nhạt khi bạn sử dụng GUI đểtìm từng tệp JPEG trongthư mục này và chuyển nó vào thư mục mới.Mặt khác, CLI sẽ cho phép bạnhợp lý hóa quá trình này và di chuyển tất cả chúng cùng một lúc.

|  |
| --- |
| 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? |

Như bạn có thể thấy, cósự khác biệt rất lớn tronghai loại giao diện người dùng này.Là một nhà phân tích chứng khoán,một số công việc của bạn có thể liên quan đến giao diện dòng lệnh.Khi phân tích nhật ký hoặcxác thực và ủy quyền cho người dùng,các nhà phân tích chứng khoán thường sử dụngCLI trong công việc hàng ngày của họ.Trong video này, chúng ta đã thảo luận về hai loại giao diện người dùng.Bạn đã học được rằng bạn đã cótrải nghiệm sử dụng giao diện người dùng đồ họa,vì hầu hết máy tính cá nhân và điện thoại di động đều sử dụng GUI.Bạn đã được giới thiệu về giao diện dòng lệnh.Sau đó trong chương trình,bạn sẽ học cách sử dụng CLI trong Linux và cáchnó có liên quan đến công việc hàng ngày của bạn với tư cách là nhà phân tích bảo mật.Bạn sẽ có được trải nghiệm thực tếgiao tiếp thông qua dòng lệnh. Khá thú vị phải không?

***4.2. The command line in use – Dòng lệnh đang được sử dụng***

|  |
| --- |
| **The command line in use** |

**Dòng lệnh đang được sử dụng**

|  |
| --- |
| 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. |

Trước đây, bạn đã khám phá giao diện đồ họa người dùng (GUI) và giao diện dòng lệnh (CLI). Trong bài đọc này, bạn sẽ so sánh hai giao diện này và tìm hiểu thêm về cách chúng được sử dụng trong an ninh mạng.

|  |
| --- |
| **CLI vs. GUI** |

**CLI so với 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. |

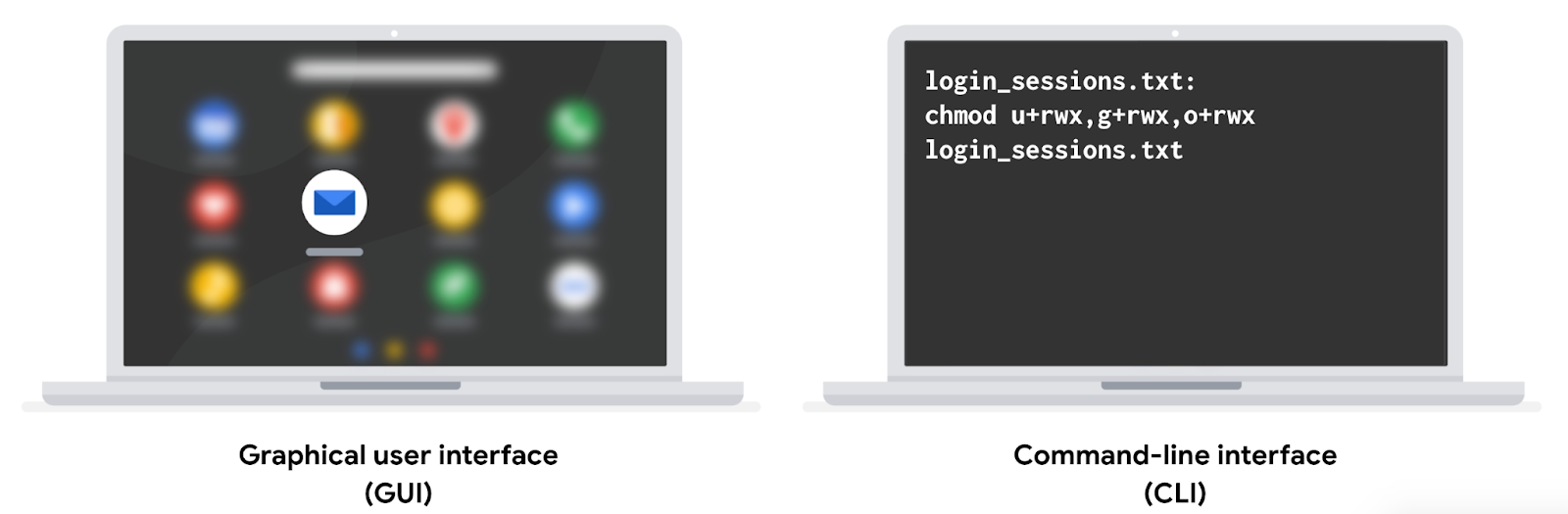
Giao diện **đồ họa người dùng (GUI)** là giao diện người dùng sử dụng các biểu tượng trên màn hình để quản lý các tác vụ khác nhau trên máy tính. Giao **diện dòng lệnh (CLI)** là giao diện người dùng dựa trên văn bản sử dụng các lệnh để tương tác với máy tính.

|  |
| --- |
| **Display** |

**Trưng bày**

|  |
| --- |
| 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. |

Một điểm khác biệt đáng chú ý giữa hai giao diện này là cách chúng xuất hiện trên màn hình. GUI có đồ họa và biểu tượng, chẳng hạn như các biểu tượng trên màn hình nền hoặc thanh tác vụ để khởi chạy chương trình. Ngược lại, CLI chỉ có văn bản. Nó trông giống như các dòng mã.



|  |
| --- |
| **Function** |

**Chức năng**

|  |
| --- |
| 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. |

Hai giao diện này cũng khác nhau về cách chúng hoạt động. GUI là một giao diện chỉ cho phép bạn thực hiện một yêu cầu tại một thời điểm. Tuy nhiên, CLI cho phép bạn thực hiện nhiều yêu cầu cùng một lúc.

|  |
| --- |
| **Advantages of a CLI in cybersecurity** |

**Ưu điểm của CLI trong an ninh mạng**

|  |
| --- |
| 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. |

Lựa chọn giữa việc sử dụng GUI hoặc CLI một phần dựa trên sở thích cá nhân, nhưng các nhà phân tích bảo mật có thể sử dụng cả hai giao diện. Sử dụng CLI có thể mang lại những lợi ích nhất định.

|  |
| --- |
| **Efficiency** |

**Hiệu quả**

|  |
| --- |
| 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. |

Một số thích CLI vì nó có thể được sử dụng nhanh hơn khi bạn biết cách quản lý giao diện này. Đối với người dùng mới, GUI có thể hiệu quả hơn vì người mới bắt đầu sử dụng GUI dễ dàng điều hướng hơn.

|  |
| --- |
| 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. |

Vì CLI có thể chấp nhận nhiều yêu cầu cùng một lúc nên nó sẽ mạnh mẽ hơn khi bạn cần thực hiện nhiều tác vụ một cách hiệu quả. Ví dụ: nếu bạn phải tạo nhiều tệp mới trong hệ thống của mình, bạn có thể nhanh chóng thực hiện tác vụ này trong CLI. Nếu bạn đang sử dụng GUI, quá trình này có thể mất nhiều thời gian hơn vì bạn phải lặp lại các bước tương tự cho mỗi tệp mới.

|  |
| --- |
| **History file** |

**Tập tin lịch sử**

|  |
| --- |
| 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. |

Đối với các nhà phân tích bảo mật, việc sử dụng Linux CLI rất hữu ích vì nó ghi lại tệp lịch sử của tất cả các lệnh và hành động trong CLI. Nếu bạn đang sử dụng GUI, hành động của bạn không nhất thiết phải được lưu trong tệp lịch sử.

|  |
| --- |
| 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. |

Ví dụ: bạn có thể rơi vào tình huống phải ứng phó với một sự cố bằng cách sử dụng cẩm nang. Hướng dẫn của playbook yêu cầu bạn chạy một loạt lệnh khác nhau. Nếu bạn đã sử dụng CLI, bạn có thể quay lại lịch sử và đảm bảo tất cả các lệnh đều được sử dụng chính xác. Điều này có thể hữu ích nếu xảy ra sự cố khi sử dụng sổ tay và bạn phải xem lại các bước mình đã thực hiện trong dòng lệnh.

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

Ngoài ra, nếu bạn nghi ngờ kẻ tấn công đã xâm phạm hệ thống của mình, bạn có thể theo dõi hành động của họ bằng tệp lịch sử.

|  |
| --- |
| **Key takeaways** |

**Bài học chính**

|  |
| --- |
| 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. |

GUI và CLI là hai loại giao diện người dùng mà các nhà phân tích bảo mật nên làm quen. Có nhiều điểm khác biệt giữa GUI và CLI, bao gồm cả cách hiển thị và cách chúng hoạt động. Khi làm việc trong lĩnh vực an ninh mạng, CLI thường được ưu tiên hơn GUI vì nó có thể xử lý nhiều tác vụ cùng lúc và bao gồm tệp lịch sử.

***4.3. Activity: Select the user interface – Hoạt động: Chọn giao diện người dùng***

***4.4. Ellen: My path into cybersecurity – Ellen: Con đường đến với an ninh mạng của tôi***

|  |
| --- |
| [MUSIC] 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. |

[ÂM NHẠC]Tên tôi là Ellen và tôi là giám đốc kỹ thuật bảo mật tại tập trung vào Googlevề cách Google sử dụng đám mây.An ninh mạng không phải là một lĩnh vực khi tôi bắt đầu làm việc trong lĩnh vực công nghệ,một cái gì đó tôi đã đến sau này.Tôi bắt đầu làm việc trong lĩnh vực công nghệ khi đang làm việc bán lẻ tại một cửa hàng áp phích.Và chúng tôi cần xây dựng một trang web và chân tôi bị đau và tôi thực sự cần phải ngồi xuống.Và thế là tôi đã nhờ bạn bè dạy tôi cách làm HTML đểTôi có thể ngồi xuống trong khi làm việc và có thể để các vết phồng rộp của mình được nghỉ ngơi.Khi tôi đang ở cửa hàng áp phích, một trong những khách hàng của chúng tôi làm việc tại một công ty khởi nghiệp vàthường đóng khung ảnh của nhân viên và họ yêu cầu họphản hồi trên trang web của tôi và cuối cùng họ đã cho tôi một cơ hội thực tập.Một trong những chuyên môn mà tôi đã học là thiết kế API hoặcthiết kế giao diện để nhà phát triển giao tiếp với máy.Là một phần của công việc đó, tôi đã nhận được công việc thiết kế một phiên bản thu nhỏ củamột hệ điều hành dành cho công nghệ bảo mật vàbắt đầu học bảo mật từ đó.Hầu hết những người tôi biết về an ninh mạng, đặc biệt là trong những ngày đầu,không có bằng cấp nào cả.Hoặc nếu có, họ cũng có bằng cấp như tôi về triết học hoặc thơ ca.Hầu hết mọi người đều tự học bằng cách thử nghiệm,bằng cách nói chuyện với mọi người, bằng cách đọc sách.Và vì vậy tôi sẽ nói rằng không cần có nền tảng kỹ thuật.Và trên thực tế, có một nền tảng mà bạn đã quen với thế giới thựcđôi khi có thể làm cho an ninh mạng có ý nghĩa hơn vàgiúp bạn đưa ra những lựa chọn cân bằng hơn.Ở hầu hết các khu vực, bạn có thể tìm thấy một cộng đồng bảo mật.Tìm hiểu xem họ đang ở đâu, tìm kiếm các hội nghị địa phương, bắt đầu nói chuyện với mọi người.Học theo cách đó thú vị hơn rất nhiều so với học trong chân không.Tôi nhận thấy rằng hầu hết mọi người nếu bạn đến gặp họ và nói, này, bạn thực sự giỏi vềnày, bạn có phiền nếu tôi mua cho bạn một ly cà phê và bạn chỉ cho tôi cách làm không?Rằng họ sẽ luôn nói đồng ý.Lời khuyên tôi dành cho những người không có kiến ​​thức về kỹ thuật, lời khuyên đầu tiên là,Tôi sẽ không sợ công nghệ.Có vẻ như chỉ có ai đó có bằng khoa học máy tính mới có thểhiểu mọi thứ, nhưng những khái niệm này,những công nghệ này ai cũng có thể hiểu được.Và vì vậy đừng bao giờ để thực tế là bạn có thể không có nền tảng kỹ thuậtNhân tiện, chỉ cần chọn một lĩnh vực mà bạn quan tâm và bắt đầu khám phá.Và miễn là bạn tò mò, và miễn là bạn thấy nó thú vị, bạn sẽ,bạn sẽ học công nghệ.

***4.5. Test your knowledge: The user interface – Kiểm tra kiến ​​thức của bạn: Giao diện người dùng***

**5. Review: Introduction to operating systems – Ôn tập: Giới thiệu hệ điều hành**

***5.1. Wrap-up – Gói lại***

|  |
| --- |
| 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. |

Chúng ta làm được rồi!Thật là một phần học tập tuyệt vời!Điều tuyệt vời nhất là chúng ta đã cùng nhau làm điều này vàbao gồm một số chủ đề rất hữu ích.Hãy tóm tắt lại các bài học của phần này.Là một nhà phân tích chứng khoán,điều quan trọng là bạn hiểu hệ thống mà bạn đang làm việc cùng.Hiểu biết cơ bản về máy tính sẽ giúp bạn thực hiện công việc hiệu quả hơn vàmột cách hiệu quả.Trong phần này, chúng tôi đề cập đến các hệ điều hành phổ biến.Chúng ta cũng đã thảo luận về các chức năng chính của hệ điều hành.Điều quan trọng là bạn đã tìm hiểu về mối quan hệ giữa các hệ điều hành,ứng dụng và phần cứng.Thật tuyệt khi biết cách họ kết hợp với nhau như một dàn nhạc.Ngoài ra, bạn đã tìm hiểu về sự khác biệt giữa người dùng đồ họagiao diện và giao diện dòng lệnh.Việc hiểu rõ giao diện dòng lệnh sẽ rất quan trọng cho công việc của bạn.

|  |
| --- |
| 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. |

Tôi rất thích khám phá thế giới hệ điều hành cùng bạn.Biết hệ điều hành hoạt động như thế nào là một bước quan trọng trong việc chuẩn bị chovị trí là nhà phân tích chứng khoán.Bạn đang làm rất tốt!Hãy tiếp tục tiến về phía trước với chương trình này.Trong phần tiếp theo,chúng tôi sẽ tập trung đặc biệt vào hệ điều hành Linux.

***5.2. Glossary terms from module 1 –Thuật ngữ thuật ngữ từ mô-đun 1***

|  |
| --- |
| **Glossary terms from module 1** |

**Thuật ngữ thuật ngữ từ mô-đun 1**

|  |
| --- |
| **Terms and definitions from Course 4, Module 1** |

**Các thuật ngữ và định nghĩa trong Khóa 4, Học phần 1**

|  |
| --- |
| **Application:** A program that performs a specific task |

**Ứng dụng:** Một chương trình thực hiện một nhiệm vụ cụ thể

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

**Hệ thống đầu vào/đầu ra cơ bản (BIOS):** Một vi mạch chứa các hướng dẫn tải cho máy tính và phổ biến trong các hệ thống cũ hơn

|  |
| --- |
| **Bootloader:** A software program that boots the operating system |

**Bootloader:** Một chương trình phần mềm khởi động hệ điều hành

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

**Giao diện dòng lệnh (CLI):** Giao diện người dùng dựa trên văn bản sử dụng các lệnh để tương tác với máy tính

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

**Giao diện người dùng đồ họa (GUI):** Giao diện người dùng sử dụng các biểu tượng trên màn hình để quản lý các tác vụ khác nhau trên máy tính

|  |
| --- |
| **Hardware:** The physical components of a computer |

**Phần cứng:** Các thành phần vật lý của máy tính

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

**Hệ điều hành kế thừa:** Hệ điều hành đã lỗi thời nhưng vẫn đang được sử dụng

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

**Hệ điều hành (OS)** : Giao diện giữa phần cứng máy tính và người dùng

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

**Bộ nhớ truy cập ngẫu nhiên (RAM):** Một thành phần phần cứng được sử dụng cho bộ nhớ ngắn hạn

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

**Giao diện phần mềm mở rộng hợp nhất (UEFI):** Một vi mạch chứa hướng dẫn tải cho máy tính và thay thế BIOS trên các hệ thống hiện đại hơn

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

**Giao diện người dùng:** Một chương trình cho phép người dùng điều khiển các chức năng của hệ điều hành

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

**Máy ảo (VM)** : Phiên bản ảo của máy tính vật lý

***5.3. Module 1 challenge – Thử thách mô-đun 1***

**Module 2: The Linux operating system – Hệ điều hành Linux**

|  |
| --- |
| 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 syste |

Bạn sẽ được giới thiệu về hệ điều hành Linux và tìm hiểu cách nó được sử dụng phổ biến trong an ninh mạng. Bạn cũng sẽ tìm hiểu về kiến ​​trúc Linux và các bản phân phối Linux phổ biến. Ngoài ra, bạn sẽ được giới thiệu về Linux shell và tìm hiểu cách nó cho phép bạn giao tiếp với hệ điều hành.

|  |
| --- |
| **Learning Objectives**   * Discuss why Linux is commonly used in the security profession. * Describe the architecture of the Linux operating system. * Identify the unique features of common Linux distributions. * Describe how a shell provides an interface for the user to interact with the operating system. |

**Mục tiêu học tập**

* Thảo luận tại sao Linux thường được sử dụng trong ngành bảo mật.
* Mô tả kiến ​​trúc của hệ điều hành Linux.
* Xác định các tính năng độc đáo của các bản phân phối Linux phổ biến.
* Mô tả cách shell cung cấp giao diện để người dùng tương tác với hệ điều hành.

**1. All about Linux – Tất cả về Linux**

***1.1. Welcome to module 2 – Chào mừng đến với mô-đun 2***

|  |
| --- |
| Welcome back! We have another important topic to explore. Previously, you learned about operating systems and user interfaces. You learned how operating systems work and how resources are allocated in computers. We also reviewed several common operating systems. You may already have a favorite operating system. It's common to hear that people are fans of one over another, but in the security world, Linux is commonly used. |

Chào mừng trở lại! Chúng ta có một chủ đề quan trọng khác cần khám phá.Trước đây bạn đã tìm hiểu vềhệ điều hành và giao diện người dùng.Bạn đã học cách hệ điều hành hoạt động vàtài nguyên được phân bổ như thế nào trong máy tính.Chúng tôi cũng đã xem xét một số hệ điều hành phổ biến.Bạn có thể đã có một hệ điều hành yêu thích.Người ta thường nghe nói rằng mọi người là fan của mộthơn người khác, nhưng trong thế giới an ninh,Linux được sử dụng phổ biến.

|  |
| --- |
| In this section, you'll be learning more about the Linux operating system and how it's used in everyday tasks in security. First, you'll learn about the architecture of Linux. After this, we'll compare the different distributions of Linux that are available. Lastly, you'll explore the shell, a key Linux component that allows you to communicate with the system. I remember when I first learned about the Linux OS, and I'm really happy to explore it with you now. |

Trong phần này, bạn sẽ tìm hiểu thêm vềhệ điều hành Linux và cách thứcnó được sử dụng trong các công việc hàng ngày về bảo mật.Đầu tiên, bạn sẽ tìm hiểu về kiến ​​trúc của Linux.Sau này chúng ta sẽ so sánhcác bản phân phối khác nhau của Linux hiện có.Cuối cùng, bạn sẽ khám phá lớp vỏ,một thành phần quan trọng của Linuxcho phép bạn giao tiếp với hệ thống.Tôi nhớ lần đầu tiên tôi biết vềhệ điều hành Linux và tôithực sự rất vui khi được khám phá nó cùng bạn bây giờ.

***1.2. Introduction to Linux – Giới thiệu về Linux***

|  |
| --- |
| You might have seen or heard the name Linux in the past. But did you know Linux is the most-used operating system in security today? Let's start by taking a look at Linux and how it's used in security. |

Bạn có thể đã từng thấy hoặc nghe đến cái tên Linux trước đây.Nhưng bạn có biết Linux là hệ điều hành được sử dụng nhiều nhất trong lĩnh vực bảo mật hiện nay không?Hãy bắt đầu bằng cách xem xét Linux và cách nó được sử dụng trong lĩnh vực bảo mật.

|  |
| --- |
| Linux is an open-source operating system. It was created in two parts. In the early 1990s, two different people were working separately on projects to improve computer engineering. The first person was Linus Torvalds. At the time, the UNIX operating system was already in use. He wanted to improve it and make it open source and accessible to anyone. What was revolutionary was his introduction of the Linux kernel. We're going to learn what the kernel does later. |

Linux là một hệ điều hành nguồn mở.Nó được tạo ra thành hai phần.Vào đầu những năm 1990, hai người khác nhau làm việc riêng biệt trong các dự án nhằmcải thiện kỹ thuật máy tính.Người đầu tiên là Linus Torvalds.Vào thời điểm đó, hệ điều hành UNIX đã được sử dụng.Anh ấy muốn cải thiện nó và làm cho nó trở thành nguồn mở và mọi người đều có thể truy cập được.Điều mang tính cách mạng là việc ông giới thiệu nhân Linux.Chúng ta sẽ tìm hiểu kernel làm gì sau này.

|  |
| --- |
| Around the same time, Richard Stallman started working on GNU. GNU was also an operating system based on UNIX. Stallman shared Torvalds' goal of creating software that was free and open to anyone. After working on GNU for a few years, the missing element for the software was a kernel. Together, Torvalds' and Stallman’s innovations made what is commonly referred to as Linux. |

Cùng lúc đó, Richard Stallman bắt đầu nghiên cứu GNU.GNU cũng là một hệ điều hành dựa trên UNIX.Stallman chia sẻ mục tiêu của Torvalds là tạo ra phần mềm miễn phí vàmở cửa cho bất cứ ai.Sau khi làm việc trên GNU được vài năm, phần tử còn thiếu chophần mềm là một hạt nhân.Cùng với nhau, những đổi mới của Torvalds và Stallman đã tạo ra những gì thường được gọi lànhư Linux.

|  |
| --- |
| Now that you've learned the history behind Linux, let's take a look at what makes Linux unique. As mentioned before, Linux is open source, meaning anyone can have access to the operating system and the source code. Linux and many of the programs that come with Linux are licensed under the terms of the GNU Public License, which allow you to use, share, and modify them freely. Thanks to Linux's open-source philosophy as well as a strong feature set, an entire community of developers has adopted this operating system. These developers are able to collaborate on projects and advance computing together. As a security analyst, you'll discover that Linux is used at different organizations. More specifically, Linux is used in many security programs. Another unique feature about Linux is the different distributions, or varieties, that have been developed. Because of the large community contribution, there are over 600 distributions of Linux. Later you'll learn more about distributions. |

Bây giờ bạn đã tìm hiểu về lịch sử đằng sau Linux,chúng ta hãy xem điều gì làm cho Linux trở nên độc đáo.Như đã đề cập trước đó, Linux là nguồn mở,nghĩa là bất kỳ ai cũng có thể có quyền truy cập vào hệ điều hành và mã nguồn.Linux và nhiều chương trình đi kèm với Linux được cấp phép theo các điều khoảncủa Giấy phép Công cộng GNU, cho phép bạn sử dụng, chia sẻ và sửa đổi chúng một cách tự do.Nhờ triết lý nguồn mở của Linux cũng như bộ tính năng mạnh mẽ,toàn bộ cộng đồng các nhà phát triển đã áp dụng hệ điều hành này.Những nhà phát triển này có thể cộng tác trong các dự án vàcùng nhau nâng cao tính toán.Là một nhà phân tích chứng khoán,bạn sẽ phát hiện ra rằng Linux được sử dụng ở nhiều tổ chức khác nhau.Cụ thể hơn, Linux được sử dụng trong nhiều chương trình bảo mật.Một tính năng độc đáo khác về Linux là các bản phân phối khác nhau, hoặcgiống đã được phát triển.Nhờ sự đóng góp to lớn của cộng đồng,có hơn 600 bản phân phối Linux.Sau này bạn sẽ tìm hiểu thêm về phân phối.

|  |
| --- |
| Finally, let's take a look at how you would use Linux in an entry-level security position. As a security analyst, you'll use many tools and programs in everyday work. You might examine different types of logs to identify what's going on in the system. For example, you might find yourself looking at an error log when investigating an issue. Another place where you will use Linux is to verify access and authorization in an identity and access management system. In security, managing access is key in order to ensure a secure system. We'll take a closer look into access and authorization later. |

Cuối cùng, hãy xem bạn sẽ sử dụng Linux như thế nào ở cấp độ cơ bảnvị trí an ninh.Là nhà phân tích bảo mật, bạn sẽ sử dụng nhiều công cụ và chương trình trong công việc hàng ngày.Bạn có thể kiểm tra các loại nhật ký khác nhau để xác định điều gì đang diễn ra trong hệ thống.Ví dụ,bạn có thể thấy mình đang xem nhật ký lỗi khi điều tra sự cố.Một nơi khác mà bạn sẽ sử dụng Linux là xác minh quyền truy cập vàủy quyền trong hệ thống quản lý danh tính và truy cập.Trong bảo mật, quản lý quyền truy cập là chìa khóa để đảm bảo một hệ thống an toàn.Chúng ta sẽ xem xét kỹ hơn về quyền truy cập và ủy quyền sau.

|  |
| --- |
| Finally, as an analyst, you might find yourself working with specific distributions designed for a particular task. For example, you might use a distribution that has a digital forensic tool to investigate what happened in an event alert. You might also use a distribution that's for pen testing in offensive security to look for vulnerabilities in the system. Distributions are created to fit the needs of their users. I hope you're excited to learn more about Linux. This will be a very useful skill in the security field. |

Cuối cùng, với tư cách là một nhà phân tích, bạn có thể thấy mình đang làm việcvới các bản phân phối cụ thể được thiết kế cho một nhiệm vụ cụ thể.Ví dụ: bạn có thể sử dụng bản phân phối có công cụ điều tra kỹ thuật sốđể điều tra những gì đã xảy ra trong một cảnh báo sự kiện.Bạn cũng có thể sử dụng một bản phân phối dành chopen testing trong tấn công bảo mật để tìm kiếm lỗ hổng trong hệ thống.Các bản phân phối được tạo ra để phù hợp với nhu cầu của người dùng.Tôi hy vọng bạn hào hứng tìm hiểu thêm về Linux.Đây sẽ là một kỹ năng rất hữu ích trong lĩnh vực bảo mật.

***1.3. Phil: Learn and grow in the cybersecurity field – Phil: Học hỏi và phát triển trong lĩnh vực an ninh mạng***

|  |
| --- |
| Hi, I'm Phil I'm the Chief Information Security Officer for Google Cloud, and a big part of that is, of course, cybersecurity. So, in cyber you've always got to learn, you've always got to stay up to date for the simple reason that technology and business and the world of our, kind of digital lives is just always changing. The online services that you use today are probably very different even just when what they were 12 months ago. In the mid '90s, I worked on one of the world's first internet banking systems. And essentially we were building and coding all of the security ourselves. I remember working on the first web browsers, the first web servers, the first implementations of encryption on the Internet. This was even before Google even existed. And so this was the very beginning of the Internet and we were literally kind of assembling and building this and learning how to do it as we went along. When you are first getting into cybersecurity, it's important to not get overwhelmed. It's a very big space. And all of us started off at where you are today. And we had to learn into that. At one point, I didn't know Linux, I didn't know how to program. I didn't know various parts of other operating systems. And I had to learn step-by-step, how all of that worked and gradually build up that knowledge over time. And even now I still have to look things up occasionally because I don't keep everything in my head all at once and that's totally fine. When you're approaching a new situation, you're always going to have a degree of anxiety about whether you're going to be able to learn it quickly enough. And generally, with enough experience, you're gradually comfortable that you will. But again, this is important to remember that you don't have to learn everything about everything all at once. Most of the time you learn enough to be enough of value in the initial part of the process, then you learn as you go. Start off by writing a few lines of simple code or looking at somebody else's code and trying to understand what it does and then change it a little bit and just incrementally work into this. Build that foundation of knowledge that gives you the ability to learn other things, and I think things will stem from that. |

Xin chào, tôi là Phil, tôi là Trưởng phòngNhân viên bảo mật thông tin của Google Cloud,và một phần lớn trong số đó tất nhiên là an ninh mạng.Vì vậy, trong mạng bạn luôn phải học hỏi,bạn phải luôn cập nhậtlý do đơn giản là công nghệ vàkinh doanh và thế giới củacuộc sống số của chúng ta luôn thay đổi.Các dịch vụ trực tuyến mà bạn sử dụnghôm nay có lẽ rất khácngay cả khi họ giống như 12 tháng trước.Vào giữa những năm 90, tôi đã làm việc trên một trong nhữnghệ thống ngân hàng trực tuyến đầu tiên trên thế giới.Và về cơ bản chúng tôi đang xây dựng vàtự mình mã hóa tất cả các biện pháp bảo mật.Tôi nhớ mình đã làm việc trên những trình duyệt web đầu tiên,máy chủ web đầu tiên,triển khai mã hóa đầu tiên trên Internet.Điều này thậm chí còn xảy ra trước khi Google tồn tại.Và đây chính là sự khởi đầu củaInternet và chúng tôi thực sự đang tập hợp lạivà xây dựng cái này và học cách làmnó khi chúng tôi đi cùng.Khi bạn lần đầu tiên bước vào lĩnh vực an ninh mạng,điều quan trọng là không bị choáng ngợp.Đó là một không gian rất lớn.Và tất cả chúng tôi đều bắt đầu ở vị trí của bạn ngày hôm nay.Và chúng tôi phải tìm hiểu về điều đó.Có một thời điểm, tôi không biết Linux,Tôi không biết cách lập trình.Tôi không biết nhiều phần khác nhau của các hệ điều hành khác.Và tôi phải học từng bước một,tất cả những điều đó đã hoạt động như thế nào vàdần dần xây dựng kiến ​​thức đó theo thời gian.Và ngay cả bây giờ tôi vẫn phảithỉnh thoảng tra cứu mọi thứ vìTôi không giữ mọi thứ trong đầutất cả cùng một lúc và điều đó hoàn toàn ổn.Khi bạn tiếp cận một tình huống mới,bạn sẽ luôn có một mức độ lo lắngvề việc liệu bạn có định trở thànhcó thể học nó đủ nhanh.Và nói chung, với đủ kinh nghiệm,bạn dần dần cảm thấy thoải mái rằng bạn sẽ làm được.Nhưng một lần nữa, điều quan trọng cần nhớ là bạn khôngphải học mọi thứ về mọi thứ cùng một lúc.Hầu hết thời gian bạn học đủ đểcó đủ giá trị trong phần đầu của quá trình,sau đó bạn học khi bạn đi.Hãy bắt đầu bằng việc viết vài dòngmã đơn giản hoặc nhìn vàomã của người khác và cố gắnghiểu nó làm gì và sau đó thay đổi nómột chút và chỉ cần thực hiện dần dần việc này.Xây dựng nền tảng kiến ​​thức đómang đến cho bạn khả năng học hỏi những thứ khác,và tôi nghĩ mọi chuyện sẽ bắt nguồn từ đó.

***1.4. Linux architecture – Kiến trúc Linux***

|  |
| --- |
| Let me start with a quick question that may seem unrelated to security. Do you have a favorite building? And what is it about its architecture that impresses you the most? The windows? The structure of the walls? Just like buildings, operating systems also have an architecture and are made up of discrete components that work together to form the whole. In this video, we're going to look at all the components that together make up Linux. |

Hãy để tôi bắt đầu bằng một câu hỏi nhanh có thểdường như không liên quan đến bảo mật.Bạn có một tòa nhà yêu thích?Và nó nói về cái gìkiến trúc của nó làm bạn ấn tượng nhất?Những cửa sổ? Cấu trúc của bức tường?Cũng giống như các tòa nhà, hệ điều hành cũng cómột kiến ​​trúc và được tạo thành từthành phần riêng biệt phối hợp với nhau để tạo thành tổng thể.Trong video này, chúng ta sẽ xem xéttất cả các thành phần cùng nhau tạo nên Linux.

|  |
| --- |
| The components of Linux include the user, applications, the shell, the Filesystem Hierarchy Standard, the kernel, and the hardware. Don't worry—we'll go into these components one by one together. |

Các thành phần của Linux bao gồm người dùng, ứng dụng,shell, Tiêu chuẩn phân cấp hệ thống tập tin,hạt nhân và phần cứng.Đừng lo lắng—chúng ta sẽ đi sâu vàocác thành phần này lần lượt với nhau.

|  |
| --- |
| First, you are the user. The user is the person interacting with the computer. In Linux, you're the first element to the architecture of the operating system. You're initiating the tasks or commands that the OS is going to execute. Linux is a multi-user system. This means that more than one user can use the system's resources at the same time. |

Đầu tiên, bạn là người dùng.Người dùng là người tương tác với máy tính.Trong Linux, bạn là thành phần đầu tiênđến kiến ​​trúc của hệ điều hành.Bạn đang bắt đầu nhiệm vụ hoặccác lệnh mà hệ điều hành sẽ thực thi.Linux là một hệ thống đa người dùng.Điều này có nghĩa là nhiều người dùng có thểsử dụng tài nguyên của hệ thống cùng một lúc.

|  |
| --- |
| The second element of the architecture is the applications within a system. An application is a program that performs a specific task, such as a word processor or a calculator. You might hear the word "applications" and "programs" used interchangeably. As an example, one popular Linux application that we'll learn more about later is Nano. Nano is a text editor. This simple application helps you keep notes on the screen. Linux applications are commonly distributed through package managers. We'll learn more about this process later. |

Yếu tố thứ hai của kiến ​​trúclà các ứng dụng trong một hệ thống.Ứng dụng là một chương trìnhthực hiện một nhiệm vụ cụ thể,chẳng hạn như một trình xử lý văn bản hoặc một máy tính.Bạn có thể nghe thấy từ "ứng dụng"và "chương trình" được sử dụng thay thế cho nhau.Như một ví dụ,một ứng dụng Linux phổ biếnsau này chúng ta sẽ tìm hiểu thêm về Nano.Nano là một trình soạn thảo văn bản.Ứng dụng đơn giản này giúpbạn giữ ghi chú trên màn hình.Các ứng dụng Linux thường đượcđược phân phối thông qua các nhà quản lý gói.Chúng ta sẽ tìm hiểu thêm về quá trình này sau.

|  |
| --- |
| The next component in the architecture of Linux is the shell. This is an important element because it is how you will communicate with the system. The shell is a command line interpreter. It processes commands and outputs the results. This might sound familiar. Previously, we learned about the two types of user interfaces: the GUI and the CLI. You can think of the shell as a CLI. |

Thành phần tiếp theo trong kiến ​​trúccủa Linux là shell.Đây là một yếu tố quan trọng vìđó là cách bạn sẽ giao tiếp với hệ thống.Shell là một trình thông dịch dòng lệnh.Nó xử lý các lệnh và đưa ra kết quả.Điều này nghe có vẻ quen thuộc.Trước đây chúng ta đã họcvề hai loại giao diện người dùng:GUI và CLI.Bạn có thể coi shell như một CLI.

|  |
| --- |
| Another element of the architecture of Linux is the Filesystem Hierarchy Standard, or FHS. It's the component of the Linux OS that organizes data. An easy way for you to think about the FHS is to think about it as a filing cabinet of data. The FHS is how data is stored in a system. It's a way to organize data so that it can be found when the data is accessed by the system. |

Một yếu tố khác của kiến ​​trúcLinux là Tiêu chuẩn phân cấp hệ thống tập tin,hoặc FHS. Của nóthành phần của hệ điều hành Linux tổ chức dữ liệu.Một cách dễ dàng để bạn suy nghĩFHS phải coi nó như một tủ chứa dữ liệu.FHS là cách dữ liệu được lưu trữ trong một hệ thống.Đó là một cách để tổ chức dữ liệu sao cho nó có thể đượcđược tìm thấy khi dữ liệu được hệ thống truy cập.

|  |
| --- |
| That brings us to the kernel. The kernel is a component of the Linux OS that manages processes and memory. The kernel communicates with the hardware to execute the commands sent by the shell. The kernel uses drivers to enable applications to execute tasks. The Linux kernel helps ensure that the system allocates resources more efficiently and makes the system work faster. |

Điều đó đưa chúng ta đến kernel.Hạt nhân là một thành phần củaHệ điều hành Linux quản lý các tiến trình và bộ nhớ.Hạt nhân giao tiếp với phần cứngđể thực thi các lệnh được gửi bởi shell.Hạt nhân sử dụng trình điều khiển để kích hoạtcác ứng dụng để thực hiện nhiệm vụ.Nhân Linux giúp đảm bảo rằng hệ thốngphân bổ nguồn lực hiệu quả hơnvà làm cho hệ thống hoạt động nhanh hơn.

|  |
| --- |
| Finally, the last component of the architecture is the hardware. Hardware refers to the physical components of a computer. You can compare this to software applications which can be downloaded into a system. The hardware in your computer are things like the CPU, mouse, and keyboard. |

Cuối cùng, thành phần cuối cùng củakiến trúc là phần cứng.Phần cứng đề cập đến các thành phần vật lý của máy tính.Bạn có thể so sánh điều này với các ứng dụng phần mềmcó thể được tải xuống hệ thống.Phần cứng trong máy tính của bạn là những thứnhư CPU, chuột và bàn phím.

|  |
| --- |
| Congratulations! We've now covered the architecture of Linux. An understanding of these components will help you become increasingly familiar with Linux. |

Chúc mừng!Bây giờ chúng ta đã đề cập đến kiến ​​trúccủa Linux. Một sự hiểu biết vềnhững thành phần này sẽ giúp bạnngày càng trở nên quen thuộc với Linux.

***1.5. Linux architecture explained – Giải thích Kiến trúc Linux***

|  |
| --- |
| **Linux architecture explained** |

**Giải thích kiến trúc Linux**

|  |
| --- |
| Understanding the Linux architecture is important for a security analyst. When you understand how a system is organized, it makes it easier to understand how it functions. In this reading, you’ll learn more about the individual components in the Linux architecture. A request to complete a task starts with the user and then flows through applications, the shell, the Filesystem Hierarchy Standard, the kernel, and the hardware. |

Hiểu kiến ​​trúc Linux rất quan trọng đối với một nhà phân tích bảo mật. Khi bạn hiểu cách một hệ thống được tổ chức, bạn sẽ dễ hiểu cách thức hoạt động của nó hơn. Trong bài đọc này, bạn sẽ tìm hiểu thêm về các thành phần riêng lẻ trong kiến ​​trúc Linux. Yêu cầu hoàn thành một tác vụ bắt đầu từ người dùng và sau đó đi qua các ứng dụng, shell, Tiêu chuẩn phân cấp hệ thống tập tin, kernel và phần cứng.

|  |
| --- |
| **User** |

**Người dùng**

|  |
| --- |
| The **user** is the person interacting with a computer. They initiate and manage computer tasks. Linux is a multi-user system, which means that multiple users can use the same resources at the same time. |

Người **dùng** là người tương tác với máy tính. Họ khởi tạo và quản lý các tác vụ của máy tính. Linux là một hệ thống nhiều người dùng, có nghĩa là nhiều người dùng có thể sử dụng cùng một tài nguyên cùng một lúc.

|  |
| --- |
| **Applications** |

**Các ứng dụng**

|  |
| --- |
| An **application** is a program that performs a specific task. There are many different applications on your computer. Some applications typically come pre-installed on your computer, such as calculators or calendars. Other applications might have to be installed, such as some web browsers or email clients. In Linux, you'll often use a package manager to install applications. A **package manager** is a tool that helps users install, manage, and remove packages or applications. A **package** is a piece of software that can be combined with other packages to form an application. |

Ứng **dụng** là một chương trình thực hiện một nhiệm vụ cụ thể. Có rất nhiều ứng dụng khác nhau trên máy tính của bạn. Một số ứng dụng thường được cài đặt sẵn trên máy tính của bạn, chẳng hạn như máy tính hoặc lịch. Các ứng dụng khác có thể phải được cài đặt, chẳng hạn như một số trình duyệt web hoặc ứng dụng email. Trong Linux, bạn sẽ thường xuyên sử dụng trình quản lý gói để cài đặt ứng dụng. Trình **quản lý gói** là một công cụ giúp người dùng cài đặt, quản lý và xóa các gói hoặc ứng dụng. Gói là một phần mềm có thể được kết hợp với các gói khác để tạo thành một ứng dụng **.**

|  |
| --- |
| **Shell** |

**Shell**

|  |
| --- |
| The **shell** is the command-line interpreter. Everything entered into the shell is text based. The shell allows users to give commands to the kernel and receive responses from it. You can think of the shell as a translator between you and your computer. The shell translates the commands you enter so that the computer can perform the tasks you want. |

Shell **là** trình thông dịch dòng lệnh. Mọi thứ được nhập vào shell đều dựa trên văn bản. Shell cho phép người dùng đưa ra lệnh cho kernel và nhận phản hồi từ nó. Bạn có thể coi shell như một công cụ dịch giữa bạn và máy tính. Shell dịch các lệnh bạn nhập để máy tính có thể thực hiện các tác vụ bạn muốn.

|  |
| --- |
| **Filesystem Hierarchy Standard (FHS)** |

**Tiêu chuẩn phân cấp hệ thống tập tin (FHS)**

|  |
| --- |
| The **Filesystem Hierarchy Standard (FHS)** is the component of the Linux OS that organizes data. It specifies the location where data is stored in the operating system. |

Tiêu **chuẩn phân cấp hệ thống tập tin (FHS)** là thành phần của hệ điều hành Linux giúp tổ chức dữ liệu. Nó chỉ định vị trí lưu trữ dữ liệu trong hệ điều hành.

|  |
| --- |
| A **directory** is a file that organizes where other files are stored. Directories are sometimes called “folders,” and they can contain files or other directories. The FHS defines how directories, directory contents, and other storage is organized so the operating system knows where to find specific data. |

Thư **mục** là một tệp tổ chức nơi các tệp khác được lưu trữ. Các thư mục đôi khi được gọi là “thư mục” và chúng có thể chứa các tệp hoặc thư mục khác. FHS xác định cách tổ chức các thư mục, nội dung thư mục và các bộ lưu trữ khác để hệ điều hành biết nơi tìm dữ liệu cụ thể.

|  |
| --- |
| **Kernel** |

**Kernel**

|  |
| --- |
| The **kernel** is the component of the Linux OS that manages processes and memory. It communicates with the applications to route commands. The Linux kernel is unique to the Linux OS and is critical for allocating resources in the system. The kernel controls all major functions of the hardware, which can help get tasks expedited more efficiently. |

Kernel là thành phần của hệ điều hành Linux quản lý các tiến trình và bộ nhớ **.** Nó giao tiếp với các ứng dụng để định tuyến các lệnh. Nhân Linux là duy nhất cho hệ điều hành Linux và rất quan trọng trong việc phân bổ tài nguyên trong hệ thống. Hạt nhân kiểm soát tất cả các chức năng chính của phần cứng, có thể giúp thực hiện các tác vụ nhanh chóng hiệu quả hơn.

|  |
| --- |
| **Hardware** |

**Phần cứng**

|  |
| --- |
| The **hardware** is the physical components of a computer. You might be familiar with some hardware components, such as hard drives or CPUs. Hardware is categorized as either peripheral or internal. |

Phần **cứng** là các thành phần vật lý của máy tính. Bạn có thể quen thuộc với một số thành phần phần cứng, chẳng hạn như ổ cứng hoặc CPU. Phần cứng được phân loại là ngoại vi hoặc nội bộ.

|  |
| --- |
| **Peripheral devices** |

**Thiết bị ngoại vi**

|  |
| --- |
| **Peripheral devices** are hardware components that are attached and controlled by the computer system. They are not core components needed to run the computer system. Peripheral devices can be added or removed freely. Examples of peripheral devices include monitors, printers, the keyboard, and the mouse. |

**Thiết bị ngoại vi** là các thành phần phần cứng được gắn và điều khiển bởi hệ thống máy tính. Chúng không phải là thành phần cốt lõi cần thiết để chạy hệ thống máy tính. Các thiết bị ngoại vi có thể được thêm vào hoặc gỡ bỏ một cách tự do. Ví dụ về các thiết bị ngoại vi bao gồm màn hình, máy in, bàn phím và chuột.

|  |
| --- |
| **Internal hardware** |

**Phần cứng bên trong**

|  |
| --- |
| **Internal hardware** are the components required to run the computer. Internal hardware includes a main circuit board and all components attached to it. This main circuit board is also called the motherboard. Internal hardware includes the following: |

**Phần cứng bên trong** là những thành phần cần thiết để chạy máy tính. Phần cứng bên trong bao gồm một bảng mạch chính và tất cả các thành phần gắn liền với nó. Bảng mạch chính này còn được gọi là bo mạch chủ. Phần cứng bên trong bao gồm:

|  |
| --- |
| * The **Central Processing Unit (CPU)** is a computer’s main processor, which is used to perform general computing tasks on a computer. The CPU executes the instructions provided by programs, which enables these programs to run. * **Random Access Memory (RAM)** is a hardware component used for short-term memory. It’s where data is stored temporarily as you perform tasks on your computer. For example, if you’re writing a report on your computer, the data needed for this is stored in RAM. After you’ve finished writing the report and closed down that program, this data is deleted from RAM. Information in RAM cannot be accessed once the computer has been turned off. The CPU takes the data from RAM to run programs. * The **hard drive** is a hardware component used for long-term memory. It’s where programs and files are stored for the computer to access later. Information on the hard drive can be accessed even after a computer has been turned off and on again. A computer can have multiple hard drives. |

* Bộ **xử lý trung tâm (CPU)** là bộ xử lý chính của máy tính, được sử dụng để thực hiện các tác vụ tính toán chung trên máy tính. CPU thực thi các hướng dẫn được cung cấp bởi các chương trình, cho phép các chương trình này chạy.
* **Bộ nhớ truy cập ngẫu nhiên (RAM)** là thành phần phần cứng được sử dụng cho bộ nhớ ngắn hạn. Đó là nơi dữ liệu được lưu trữ tạm thời khi bạn thực hiện các tác vụ trên máy tính của mình. Ví dụ: nếu bạn đang viết báo cáo trên máy tính, dữ liệu cần thiết cho việc này sẽ được lưu trữ trong RAM. Sau khi bạn viết xong báo cáo và đóng chương trình đó, dữ liệu này sẽ bị xóa khỏi RAM. Thông tin trong RAM không thể truy cập được khi máy tính đã tắt. CPU lấy dữ liệu từ RAM để chạy chương trình.
* Ổ **cứng** là một thành phần phần cứng được sử dụng cho bộ nhớ dài hạn. Đó là nơi lưu trữ các chương trình và tập tin để máy tính truy cập sau này. Thông tin trên ổ cứng có thể được truy cập ngay cả sau khi máy tính đã tắt và bật lại. Một máy tính có thể có nhiều ổ cứng.

|  |
| --- |
| **Key takeaways** |

**Bài học chính**

|  |
| --- |
| It’s important for security analysts to understand the Linux architecture and how these components are organized. The components of the Linux architecture are the user, applications, shell, Filesystem Hierarchy Standard, kernel, and hardware. Each of these components is important in how Linux functions. |

Điều quan trọng đối với các nhà phân tích bảo mật là phải hiểu kiến ​​trúc Linux và cách tổ chức các thành phần này. Các thành phần của kiến ​​trúc Linux là người dùng, ứng dụng, shell, Tiêu chuẩn phân cấp hệ thống tập tin, kernel và phần cứng. Mỗi thành phần này đều quan trọng trong cách thức hoạt động của Linux.

***1.6. Explore: Components of the Linux OS – Khám phá: Các thành phần của hệ điều hành Linux***

|  |  |
| --- | --- |
| User  A person sits at a desk working on a computer. | The user decides to create a new file. |

|  |  |
| --- | --- |
| User  A person sits at a desk working on a computer. | Người dùng quyết định tạo một tập tin mới. |

|  |  |
| --- | --- |
| Application  The person opens an application on the computer. | The user opens the application for communicating with the shell. |

|  |  |
| --- | --- |
| Application  The person opens an application on the computer. | Người dùng mở ứng dụng để giao tiếp với shell. |

|  |  |
| --- | --- |
| Shell  The person types command copy on the computer keyboard, and this copy is shown on the computer monitor. | The user enters commands in the shell to indicate they want to create a new file. |

|  |  |
| --- | --- |
| Shell  The person types command copy on the computer keyboard, and this copy is shown on the computer monitor. | Người dùng nhập các lệnh trong shell để cho biết họ muốn tạo một tệp mới. |

|  |  |
| --- | --- |
| Filesystem Hierarchy Standard (FHS) | The shell creates the new file in the FHS. |

|  |  |
| --- | --- |
| Filesystem Hierarchy Standard (FHS) | Shell tạo tệp mới trong FHS. |

|  |  |
| --- | --- |
| Kernel  Mechanical gears. | The contents and location of the new file are passed to the kernel. |

|  |  |
| --- | --- |
| Kernel  Mechanical gears. | Nội dung và vị trí của tệp mới được chuyển tới kernel. |

|  |  |
| --- | --- |
| Hardware  A hard drive. | The kernel tells the hardware how and where to save this new file. |

|  |  |
| --- | --- |
| Hardware  A hard drive. | Hạt nhân cho phần cứng biết cách thức và nơi lưu tệp mới này. |

***1.7. Test your knowledge: All about Linux – Kiểm tra kiến ​​thức của bạn: Tất cả về Linux***

**2. Linux distributions – Bản phân phối Linux**

***2.1. Linux distributions – Bản phân phối Linux***

|  |
| --- |
| Let's learn a little bit more about Linux and what you need to know about this operating system when working as a security analyst. Linux is a very customizable operating system. Unlike other operating systems, there are different versions available for you to use. These different versions of Linux are called distributions. You might also hear them called distros or flavors of Linux. It's essential for you to understand the distribution that you're using so you know what tools and apps are available to you. For example, Debian is a distro that has different tools than the Ubuntu distribution. |

Hãy tìm hiểu thêm một chút về Linux vànhững điều bạn cần biết về hệ điều hành này khi làm nhà phân tích bảo mật.Linux là một hệ điều hành có khả năng tùy biến rất cao.Không giống như các hệ điều hành khác, có nhiều phiên bản khác nhau dành chobạn sử dụng.Các phiên bản Linux khác nhau này được gọi là bản phân phối.Bạn cũng có thể nghe thấy chúng được gọi là bản phân phối hoặc phiên bản Linux.Điều cần thiết là bạn phải hiểu bản phân phối mà bạn đang sử dụngđể bạn biết những công cụ và ứng dụng nào có sẵn cho bạn.Ví dụ,Debian là một bản phân phối có các công cụ khác với bản phân phối Ubuntu.

|  |
| --- |
| Let's use an analogy to describe Linux distributions. Think of the OS as a vehicle. First, we'll start with its engine—that would be the kernel. Just as the engine makes a vehicle run, the kernel is the most important component of the Linux OS. Because the Linux kernel is open source, anyone can take the kernel and modify it to build a new distribution. This is comparable to a vehicle manufacturer taking an engine and creating different types of vehicles: trucks, cars, vans, convertibles, busses, airplanes, and so on. These different types of vehicles can be compared to different Linux distributions. A bus is used to transport lots of people. A truck is used to transport a large number of goods across vast distances. An aircraft transports passengers or goods by air. |

Hãy sử dụng một sự tương tự để mô tả các bản phân phối Linux.Hãy nghĩ về hệ điều hành như một phương tiện.Đầu tiên, chúng ta sẽ bắt đầu với engine của nó—đó sẽ là kernel. Cũng giống như động cơlàm cho một chiếc xe chạy được, kernel là thành phần quan trọng nhất của hệ điều hành Linux.Vì nhân Linux là nguồn mở nên bất kỳ ai cũng có thể lấy nhân Linux vàsửa đổi nó để xây dựng một bản phân phối mới.Điều này có thể so sánh với việc một nhà sản xuất ô tô lấy một động cơ vàtạo ra các loại phương tiện khác nhau: xe tải,ô tô, xe tải, xe mui trần, xe buýt, máy bay, v.v.Những loại phương tiện khác nhau này có thể được so sánh với các bản phân phối Linux khác nhau.Một chiếc xe buýt được sử dụng để vận chuyển rất nhiều người.Một chiếc xe tải được sử dụng để vận chuyển một số lượng lớn hàng hóa trên một khoảng cách rộng lớn.Một chiếc máy bay vận chuyển hành khách hoặc hàng hóa bằng đường hàng không.

|  |
| --- |
| Just as each vehicle serves its own purpose, different distributions are used for different reasons. Additionally, vehicles all have different components which distinguish them from each other. Aircrafts have control panels with buttons and knobs. Regular cars have four tires, but trucks can have more. Similarly, different Linux distributions contain different preinstalled programs, user interfaces, and much more. A lot of this is based on what the Linux user needs, but some distros are also chosen based on preference—the same way a sports car might be chosen as a vehicle. |

Giống như mỗi phương tiện phục vụ mục đích riêng của nó,các phân phối khác nhau được sử dụng vì những lý do khác nhau.Ngoài ra, các phương tiện đều có các bộ phận khác nhau để phân biệt chúng vớinhau.Máy bay có bảng điều khiển với các nút bấm và núm xoay.Ô tô thông thường có bốn lốp, nhưng xe tải có thể có nhiều hơn.Tương tự, các bản phân phối Linux khác nhau chứa các chương trình được cài đặt sẵn khác nhau,giao diện người dùng và nhiều hơn nữa.Phần lớn điều này dựa trên những gì người dùng Linux cần, nhưngmột số bản phân phối cũng được chọn dựa trên sở thích—bảngiống như cách một chiếc xe thể thao có thể được chọn làm phương tiện đi lại.

|  |
| --- |
| The advantage of using Linux as an OS is that you can customize it. Distributions include the Linux kernel, utilities, a package management system, and an installer. We learned earlier that Linux is open source, and anyone can contribute to adding to the source code. That is how new distributions are created. |

Ưu điểm của việc sử dụng Linux làm HĐH là bạn có thể tùy chỉnh nó.Các bản phân phối bao gồm nhân Linux, các tiện ích,một hệ thống quản lý gói và một trình cài đặt.Chúng ta đã biết trước đó rằng Linux là nguồn mở vàbất cứ ai cũng có thể đóng góp để thêm vào mã nguồn.Đó là cách các bản phân phối mới được tạo ra.

|  |
| --- |
| All distros are derived from another distro, but there are a few that are considered parent distributions. Red Hat® is the parent of CentOS, and Slackware® is the parent of SUSE®. Both Ubuntu and KALI LINUX™ are derived from Debian. |

Tất cả các bản phân phối đều có nguồn gốc từ một bản phân phối khác, nhưngcó một số ít được coi là phân phối gốc.Red Hat® là cha mẹ của CentOS và Slackware® là cha mẹ của SUSE®.Cả Ubuntu và KALI LINUX™ đều có nguồn gốc từ Debian.

|  |
| --- |
| As we continue, we're going to take a look at some of the distributions most commonly used by security analysts. The more you understand these distributions, the easier your work will be. |

Khi tiếp tục, chúng ta sẽ xem xét một số cách phân phối phổ biến nhấtđược các nhà phân tích chứng khoán sử dụng.Bạn càng hiểu rõ những sự phân bổ này,công việc của bạn sẽ càng dễ dàng hơn.

***2.2. KALI LINUX ™ – KALI LINUX ™***

|  |
| --- |
| In this section, we're going to cover a Linux distribution that's widely used in security and discuss KALI LINUX™. KALI LINUX™ is a trademark of Offensive Security and is Debian derived. This open-source distro was made specifically with penetration testing and digital forensics in mind. There are many tools pre-installed into KALI LINUX™. It's important to note that KALI LINUX™ should be used on a virtual machine. This prevents damage to your system in the event its tools are used improperly. An additional benefit is that using a virtual machine gives you the ability to revert to a previous state. |

Trong phần này, chúng tôi sẽ đề cập đến một bản phân phối Linux được sử dụng rộng rãi trongbảo mật và thảo luận về KALI LINUX™.KALI LINUX™ là nhãn hiệu của Bảo mật tấn công và có nguồn gốc từ Debian.Bản phân phối nguồn mở này được thực hiện đặc biệt bằng thử nghiệm thâm nhập vàpháp y kỹ thuật số trong tâm trí.Có nhiều công cụ được cài đặt sẵn trong KALI LINUX™.Điều quan trọng cần lưu ý là nên sử dụng KALI LINUX™ trên máy ảo.Điều này ngăn ngừa thiệt hại cho hệ thống của bạn trong trường hợp các công cụ của nó được sử dụng không đúng cách.Một lợi ích nữa là việc sử dụng máy ảo mang lại cho bạn khả năngtrở lại trạng thái trước đó.

|  |
| --- |
| As security professionals advance in their careers, some specialize in penetration testing. A penetration test is a simulated attack that helps identify vulnerabilities in systems, networks, websites, applications, and processes. KALI LINUX™ has numerous tools that are useful during penetration testing. Let's look at a few examples. |

Khi các chuyên gia bảo mật thăng tiến trong sự nghiệp, một số chuyên gia về thử nghiệm thâm nhập.Kiểm tra thâm nhập là một cuộc tấn công mô phỏng giúp xác định các lỗ hổng tronghệ thống, mạng, trang web, ứng dụng và quy trình.KALI LINUX™ có nhiều công cụ hữu ích trong quá trình thử nghiệm thâm nhập.Hãy xem xét một vài ví dụ.

|  |
| --- |
| To begin, Metasploit can be used to look for and exploit vulnerabilities on machines. Burp Suite is another tool that helps to test for weaknesses in web applications. And finally, John the Ripper is a tool used to guess passwords. As a security analyst, your work might involve digital forensics. Digital forensics is the process of collecting and analyzing data to determine what has happened after an attack. For example, you might take an investigative look at data related to network activity. KALI LINUX™ is also a useful distribution for security professionals who are involved in digital forensic work. It has a large number of tools that can be used for this. As one example, tcpdump is a command-line packet analyzer. It's used to capture network traffic. Another tool commonly used in the security profession is Wireshark. It has a graphical user interface that can be used to analyze live and captured network traffic. And as a final example, Autopsy is a forensic tool used to analyze hard drives and smartphones. These are just a few tools included with KALI LINUX™. This distribution has many tools used to conduct pen testing and digital forensics. |

Để bắt đầu, Metasploit có thể được sử dụng để tìm kiếm và khai thác các lỗ hổng trên máy.Burp Suite là một công cụ khác giúp kiểm tra điểm yếu trong ứng dụng web.Và cuối cùng, John the Ripper là công cụ dùng để đoán mật khẩu.Là một nhà phân tích bảo mật, công việc của bạn có thể liên quan đến pháp y kỹ thuật số.Pháp y kỹ thuật số là quá trình thu thập vàphân tích dữ liệu để xác định điều gì đã xảy ra sau một cuộc tấn công.Ví dụ,bạn có thể xem xét điều tra dữ liệu liên quan đến hoạt động mạng.KALI LINUX™ cũng là một bản phân phối hữu ích chocác chuyên gia bảo mật có liên quan đến công việc pháp y kỹ thuật số.Nó có một số lượng lớn các công cụ có thể được sử dụng cho việc này. Như một ví dụ,tcpdump là một trình phân tích gói dòng lệnh. Nó được sử dụng để nắm bắt lưu lượng mạng.Một công cụ khác thường được sử dụng trong ngành bảo mật là Wireshark.Nó có giao diện người dùng đồ họa có thể được sử dụng để phân tích trực tiếp vàbắt được lưu lượng mạng.Và như một ví dụ cuối cùng,Khám nghiệm tử thi là một công cụ pháp y được sử dụng để phân tích ổ cứng và điện thoại thông minh.Đây chỉ là một số công cụ đi kèm với KALI LINUX™.Bản phân phối này có nhiều công cụ được sử dụng để tiến hành kiểm tra bút và điều tra kỹ thuật số.

|  |
| --- |
| We've explored how KALI LINUX™ is an important distribution that's widely used in security, but there are other distributions that security professionals use as well. Next we'll explore a few more distributions. |

Chúng tôi đã khám phá cách KALI LINUX™ trở thành một bản phân phối quan trọng được sử dụng rộng rãiđược sử dụng trong an ninh,nhưng cũng có những bản phân phối khác mà các chuyên gia bảo mật sử dụng.Tiếp theo chúng ta sẽ khám phá thêm một vài bản phân phối.

***2.3. More Linux distributions – Các bản phân phối Linux khác***

|  |
| --- |
| **More Linux distributions** |

**Các bản phân phối Linux khác**

|  |
| --- |
| Previously, you were introduced to the different distributions of Linux. This included KALI LINUX ™. (KALI LINUX ™ is a trademark of OffSec.) In addition to KALI LINUX ™, there are multiple other Linux distributions that security analysts should be familiar with. In this reading, you’ll learn about additional Linux distributions. |

Trước đây, bạn đã được giới thiệu về các bản phân phối khác nhau của Linux. Điều này bao gồm KALI LINUX ™. (KALI LINUX ™ là nhãn hiệu của OffSec.) Ngoài KALI LINUX ™, còn có nhiều bản phân phối Linux khác mà các nhà phân tích bảo mật nên làm quen. Trong bài đọc này, bạn sẽ tìm hiểu về các bản phân phối Linux bổ sung.

|  |
| --- |
| **KALI LINUX ™** |

**KALI LINUX ™**

|  |
| --- |
| **KALI LINUX ™** is an open-source distribution of Linux that is widely used in the security industry. This is because KALI LINUX ™, which is Debian-based, is pre-installed with many useful tools for penetration testing and digital forensics. A **penetration test** is a simulated attack that helps identify vulnerabilities in systems, networks, websites, applications, and processes. **Digital forensics** is the practice of collecting and analyzing data to determine what has happened after an attack. These are key activities in the security industry. |

**KALI LINUX™** là một bản phân phối mã nguồn mở của Linux được sử dụng rộng rãi trong ngành bảo mật. Điều này là do KALI LINUX ™, dựa trên Debian, được cài đặt sẵn nhiều công cụ hữu ích để kiểm tra thâm nhập và điều tra kỹ thuật số. Kiểm **tra thâm nhập** là một cuộc tấn công mô phỏng giúp xác định các lỗ hổng trong hệ thống, mạng, trang web, ứng dụng và quy trình. **Điều tra kỹ thuật số** là hoạt động thu thập và phân tích dữ liệu để xác định điều gì đã xảy ra sau một cuộc tấn công. Đây là những hoạt động trọng điểm trong ngành an ninh.

|  |
| --- |
| However, KALI LINUX ™ is not the only Linux distribution that is used in cybersecurity. |

Tuy nhiên, KALI LINUX™ không phải là bản phân phối Linux duy nhất được sử dụng trong an ninh mạng.

|  |
| --- |
| **Ubuntu** |

**Ubuntu**

|  |
| --- |
| **Ubuntu** is an open-source, user-friendly distribution that is widely used in security and other industries. It has both a command-line interface (CLI) and a graphical user interface (GUI). Ubuntu is also Debian-derived and includes common applications by default. Users can also download many more applications from a package manager, including security-focused tools. Because of its wide use, Ubuntu has an especially large number of community resources to support users. |

**Ubuntu** là một bản phân phối mã nguồn mở, thân thiện với người dùng, được sử dụng rộng rãi trong ngành bảo mật và các ngành khác. Nó có cả giao diện dòng lệnh (CLI) và giao diện người dùng đồ họa (GUI). Ubuntu cũng có nguồn gốc từ Debian và bao gồm các ứng dụng phổ biến theo mặc định. Người dùng cũng có thể tải xuống nhiều ứng dụng khác từ trình quản lý gói, bao gồm các công cụ tập trung vào bảo mật. Vì được sử dụng rộng rãi nên Ubuntu có một lượng tài nguyên cộng đồng đặc biệt lớn để hỗ trợ người dùng.

|  |
| --- |
| Ubuntu is also widely used for cloud computing. As organizations migrate to cloud servers, cybersecurity work may more regularly involve Ubuntu derivatives. |

Ubuntu cũng được sử dụng rộng rãi cho điện toán đám mây. Khi các tổ chức chuyển sang máy chủ đám mây, công việc an ninh mạng có thể liên quan đến các sản phẩm phái sinh Ubuntu thường xuyên hơn.

|  |
| --- |
| **Parrot** |

**Parrot – Con vẹt**

|  |
| --- |
| **Parrot** is an open-source distribution that is commonly used for security. Similar to KALI LINUX ™, Parrot comes with pre-installed tools related to penetration testing and digital forensics. Like both KALI LINUX ™ and Ubuntu, it is based on Debian. |

**Parrot** là một bản phân phối nguồn mở thường được sử dụng để bảo mật. Tương tự như KALI LINUX ™, Parrot đi kèm với các công cụ được cài đặt sẵn liên quan đến kiểm tra thâm nhập và pháp y kỹ thuật số. Giống như cả KALI LINUX ™ và Ubuntu, nó dựa trên Debian.

|  |
| --- |
| Parrot is also considered to be a user-friendly Linux distribution. This is because it has a GUI that many find easy to navigate. This is in addition to Parrot’s CLI. |

Parrot cũng được coi là bản phân phối Linux thân thiện với người dùng. Điều này là do nó có GUI nên nhiều người thấy dễ điều hướng. Điều này bổ sung cho CLI của Parrot.

|  |
| --- |
| **Red Hat® Enterprise Linux®** |

**Red Hat® Enterprise Linux®**

|  |
| --- |
| **Red Hat Enterprise Linux** is a subscription-based distribution of Linux built for enterprise use. Red Hat is not free, which is a major difference from the previously mentioned distributions. Because it’s built and supported for enterprise use, Red Hat also offers a dedicated support team for customers to call about issues. |

**Red Hat Enterprise Linux** là bản phân phối Linux dựa trên đăng ký được xây dựng để sử dụng cho doanh nghiệp. Red Hat không miễn phí, đây là điểm khác biệt lớn so với các bản phân phối đã đề cập trước đó. Vì được xây dựng và hỗ trợ cho mục đích sử dụng của doanh nghiệp nên Red Hat cũng cung cấp một nhóm hỗ trợ riêng để khách hàng gọi điện khi có vấn đề.

|  |
| --- |
| **CentOS** |

**CentOS**

|  |
| --- |
| **CentOS** is an open-source distribution that is closely related to Red Hat. It uses source code published by Red Hat to provide a similar platform. However, CentOS does not offer the same enterprise support that Red Hat provides and is supported through the community. |

**CentOS** là một bản phân phối nguồn mở có liên quan chặt chẽ với Red Hat. Nó sử dụng mã nguồn do Red Hat xuất bản để cung cấp một nền tảng tương tự. Tuy nhiên, CentOS không cung cấp hỗ trợ doanh nghiệp giống như Red Hat cung cấp và được hỗ trợ thông qua cộng đồng.

|  |
| --- |
| **Key takeaways** |

**Bài học chính**

|  |
| --- |
| KALI LINUX ™, Ubuntu, Parrot, Red Hat, and CentOS are all widely used Linux distributions. It’s important for security analysts to be aware of these distributions that they might encounter in their career. |

KALI LINUX ™, Ubuntu, Parrot, Red Hat và CentOS đều là những bản phân phối Linux được sử dụng rộng rãi. Điều quan trọng là các nhà phân tích chứng khoán phải nhận thức được những sự phân bố này mà họ có thể gặp phải trong sự nghiệp của mình.

***2.4. Package managers for installing applications – Trình quản lý gói để cài đặt ứng dụng***

|  |
| --- |
| **Package managers for installing applications** |

**Trình quản lý gói để cài đặt ứng dụng**

|  |
| --- |
| Previously, you learned about Linux distributions and that different distributions derive from different sources, such as Debian or Red Hat Enterprise Linux distribution. You were also introduced to package managers, and learned that Linux applications are commonly distributed through package managers. In this reading, you’ll apply this knowledge to learn more about package managers. |

Trước đây, bạn đã tìm hiểu về các bản phân phối Linux và các bản phân phối khác nhau bắt nguồn từ các nguồn khác nhau, chẳng hạn như bản phân phối Debian hoặc Red Hat Enterprise Linux. Bạn cũng đã được giới thiệu về các trình quản lý gói và biết rằng các ứng dụng Linux thường được phân phối thông qua các trình quản lý gói. Trong bài đọc này, bạn sẽ áp dụng kiến ​​thức này để tìm hiểu thêm về trình quản lý gói.

|  |
| --- |
| **Introduction to package managers** |

**Giới thiệu về trình quản lý gói**

|  |
| --- |
| A **package** is a piece of software that can be combined with other packages to form an application. Some packages may be large enough to form applications on their own. |

Gói là một phần mềm có thể được kết hợp với các gói khác để tạo thành một ứng dụng **.** Một số gói có thể đủ lớn để tự tạo ứng dụng.

|  |
| --- |
| Packages contain the files necessary for an application to be installed. These files include dependencies, which are supplemental files used to run an application. |

Các gói chứa các tập tin cần thiết để cài đặt một ứng dụng. Các tệp này bao gồm các phần phụ thuộc, là các tệp bổ sung được sử dụng để chạy một ứng dụng.

|  |
| --- |
| Package managers can help resolve any issues with dependencies and perform other management tasks. A **package manager** is a tool that helps users install, manage, and remove packages or applications. Linux uses multiple package managers. |

Người quản lý gói có thể giúp giải quyết mọi vấn đề với phần phụ thuộc và thực hiện các nhiệm vụ quản lý khác. Trình **quản lý gói** là một công cụ giúp người dùng cài đặt, quản lý và xóa các gói hoặc ứng dụng. Linux sử dụng nhiều trình quản lý gói.

|  |
| --- |
| **Note:** It’s important to use the most recent version of a package when possible. The most recent version has the most up-to-date bug fixes and security patches. These help keep your system more secure. |

**Lưu ý:** Điều quan trọng là sử dụng phiên bản mới nhất của gói khi có thể. Phiên bản mới nhất có các bản sửa lỗi và bản vá bảo mật cập nhật nhất. Những điều này giúp giữ cho hệ thống của bạn an toàn hơn.

|  |
| --- |
| **Types of package managers** |

**Các loại trình quản lý gói**

|  |
| --- |
| Many commonly used Linux distributions are derived from the same parent distribution. For example, KALI LINUX ™, Ubuntu, and Parrot all come from Debian. CentOS comes from Red Hat. |

Nhiều bản phân phối Linux thường được sử dụng đều có nguồn gốc từ cùng một bản phân phối gốc. Ví dụ: KALI LINUX ™, Ubuntu và Parrot đều đến từ Debian. CentOS đến từ Red Hat.

|  |
| --- |
| This knowledge is useful when installing applications because certain package managers work with certain distributions. For example, the Red Hat Package Manager (RPM) can be used for Linux distributions derived from Red Hat, and package managers such as dpkg can be used for Linux distributions derived from Debian. |

Kiến thức này hữu ích khi cài đặt ứng dụng vì một số trình quản lý gói nhất định hoạt động với các bản phân phối nhất định. Ví dụ: Trình quản lý gói Red Hat (RPM) có thể được sử dụng cho các bản phân phối Linux có nguồn gốc từ Red Hat và các trình quản lý gói như dpkg có thể được sử dụng cho các bản phân phối Linux có nguồn gốc từ Debian.

|  |
| --- |
| Different package managers typically use different file extensions. For example, Red Hat Package Manager (RPM) has files which use the **.rpm** file extension, such as **Package-Version-Release\_Architecture.rpm**. Package managers for Debian-derived Linux distributions, such as dpkg, have files which use the **.deb** file extension, such as **Package\_Version-Release\_Architecture.deb**. |

Các trình quản lý gói khác nhau thường sử dụng các phần mở rộng tệp khác nhau. Ví dụ: Trình quản lý gói Red Hat (RPM) có các tệp sử dụng phần mở rộng tệp **.rpm** , chẳng hạn như **Package-Version-Release\_Architecture.rpm** . Trình quản lý gói cho các bản phân phối Linux có nguồn gốc từ Debian, chẳng hạn như dpkg, có các tệp sử dụng phần mở rộng tệp **.deb** , chẳng hạn như **Package\_Version-Release\_Architecture.deb** .

|  |
| --- |
| **Package management tools** |

**Công cụ quản lý gói**

|  |
| --- |
| In addition to package managers like RPM and dpkg, there are also package management tools that allow you to easily work with packages through the shell. Package management tools are sometimes utilized instead of package managers because they allow users to more easily perform basic tasks, such as installing a new package. Two notable tools are the Advanced Package Tool (APT) and Yellowdog Updater Modified (YUM). |

Ngoài các trình quản lý gói như RPM và dpkg, còn có các công cụ quản lý gói cho phép bạn dễ dàng làm việc với các gói thông qua shell. Các công cụ quản lý gói đôi khi được sử dụng thay vì trình quản lý gói vì chúng cho phép người dùng thực hiện các tác vụ cơ bản dễ dàng hơn, chẳng hạn như cài đặt gói mới. Hai công cụ đáng chú ý là Advanced Package Tool (APT) và Yellowdog Updater Modified (YUM).

|  |
| --- |
| **Advanced Package Tool (APT)** |

**Công cụ gói nâng cao (APT)**

|  |
| --- |
| APT is a tool used with Debian-derived distributions. It is run from the command-line interface to manage, search, and install packages. |

APT là một công cụ được sử dụng với các bản phân phối có nguồn gốc từ Debian. Nó được chạy từ giao diện dòng lệnh để quản lý, tìm kiếm và cài đặt các gói.

|  |
| --- |
| **Yellowdog Updater Modified (YUM)** |

**Trình cập nhật Yellowdog đã sửa đổi (YUM)**

|  |
| --- |
| YUM is a tool used with Red Hat-derived distributions. It is run from the command-line interface to manage, search, and install packages. YUM works with **.rpm** files. |

YUM là một công cụ được sử dụng với các bản phân phối có nguồn gốc từ Red Hat. Nó được chạy từ giao diện dòng lệnh để quản lý, tìm kiếm và cài đặt các gói. YUM hoạt động với các tệp **.rpm** .

|  |
| --- |
| **Key takeaways** |

**Bài học chính**

|  |
| --- |
| A package is a piece of software that can be combined with other packages to form an application. Packages can be managed using a package manager. There are multiple package managers and package management tools for different Linux distributions. Package management tools allow users to easily work with packages through the shell. Debian-derived Linux distributions use package managers like dpkg as well as package management tools like Advanced Package Tool (APT). Red Hat-derived distributions use the Red Hat Package Manager (RPM) or tools like Yellowdog Updater Modified (YUM). |

Gói là một phần mềm có thể được kết hợp với các gói khác để tạo thành một ứng dụng. Các gói có thể được quản lý bằng trình quản lý gói. Có nhiều trình quản lý gói và công cụ quản lý gói cho các bản phân phối Linux khác nhau. Các công cụ quản lý gói cho phép người dùng dễ dàng làm việc với các gói thông qua shell. Các bản phân phối Linux có nguồn gốc từ Debian sử dụng các trình quản lý gói như dpkg cũng như các công cụ quản lý gói như Advanced Package Tool (APT). Các bản phân phối có nguồn gốc từ Red Hat sử dụng Trình quản lý gói Red Hat (RPM) hoặc các công cụ như Yellowdog Updater Modified (YUM).

***2.5. Resources for completing Linux labs – Tài nguyên để hoàn thành phòng thí nghiệm Linux***

|  |
| --- |
| **Resources for completing Linux labs** |

**Tài nguyên để hoàn thành phòng thí nghiệm Linux**

|  |
| --- |
| This course features hands-on lab activities where you’ll have the opportunity to practice Linux commands in the terminal. You’ll use a platform called Qwiklabs to complete these labs. In this reading, you’ll learn how to use Qwiklabs. |

Khóa học này có các hoạt động thực hành trong phòng thí nghiệm, nơi bạn sẽ có cơ hội thực hành các lệnh Linux trong thiết bị đầu cuối. Bạn sẽ sử dụng nền tảng có tên Qwiklabs để hoàn thành các phòng thí nghiệm này. Trong bài đọc này, bạn sẽ học cách sử dụng Qwiklabs.

|  |
| --- |
| This reading first provides a section on how to use Qwiklabs, which includes details on how to launch a lab, how to interact within the Qwiklabs environment, and how to end a lab. This is followed by another section on helpful navigation tips and keyboard shortcuts; these may be useful when working in the terminal. |

Bài đọc này trước tiên cung cấp phần về cách sử dụng Qwiklabs, bao gồm chi tiết về cách khởi chạy phòng thí nghiệm, cách tương tác trong môi trường Qwiklabs và cách kết thúc phòng thí nghiệm. Tiếp theo là phần khác về các mẹo điều hướng hữu ích và phím tắt; những điều này có thể hữu ích khi làm việc trong thiết bị đầu cuối.

|  |
| --- |
| **Note**: You will not launch Qwiklabs directly from this reading and instead will do this through lab activities and exemplars that you encounter throughout the course. |

**Lưu ý** : Bạn sẽ không khởi chạy Qwiklabs trực tiếp từ bài đọc này mà thay vào đó sẽ thực hiện việc này thông qua các hoạt động trong phòng thí nghiệm và các ví dụ mà bạn gặp trong suốt khóa học.

|  |
| --- |
| **How to use Qwiklabs** |

**Cách sử dụng Qwiklabs**

|  |
| --- |
| **Launching Qwiklabs** |

**Ra mắt Qwiklabs**

|  |
| --- |
| When you select a lab, you start from a Coursera page. You will need to click **Launch App** on that page. After you click **Launch App**, a new tab will open with a Qwiklabs page that contains instructions for that particular lab. |

Khi bạn chọn một phòng thí nghiệm, bạn bắt đầu từ trang Coursera. Bạn sẽ cần nhấp vào **Khởi chạy ứng dụng** trên trang đó. Sau khi bạn nhấp vào **Khởi chạy ứng dụng** , một tab mới sẽ mở ra với trang Qwiklabs chứa hướng dẫn cho phòng thí nghiệm cụ thể đó.

|  |
| --- |
| **Start Lab button** |

**Nút bắt đầu phòng thí nghiệm**

|  |
| --- |
| On the Qwiklabs page, you must click **Start Lab** to open a temporary terminal. The instructions for the lab will move to the right side of the screen. |

Trên trang Qwiklabs, bạn phải nhấp vào **Start Lab** để mở thiết bị đầu cuối tạm thời. Các hướng dẫn cho phòng thí nghiệm sẽ di chuyển sang phía bên phải của màn hình.



|  |
| --- |
| Read the instructions and complete all the tasks in the lab by entering commands in the terminal. |

Đọc hướng dẫn và hoàn thành tất cả các nhiệm vụ trong phòng thí nghiệm bằng cách nhập lệnh trong thiết bị đầu cuối.

|  |
| --- |
| **Note**: It may take a moment for the terminal to start. |

**Lưu ý** : Có thể mất một chút thời gian để thiết bị đầu cuối khởi động.

|  |
| --- |
| **Lab control dialog box** |

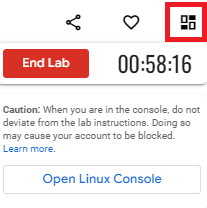
**Hộp thoại điều khiển phòng thí nghiệm**

|  |
| --- |
| After you click **Start Lab**, the lab control dialog box opens. It contains the **End Lab** button, the **timer**, and the **Open Linux Console** button. |

Sau khi bạn nhấn **Start Lab** , hộp thoại điều khiển lab sẽ mở ra. Nó chứa nút **End Lab**  , **bộ hẹn giờ** và nút **Open Linux Console** .

|  |
| --- |
| You can hide or unhide the dialog box by clicking the following icon in the red box: |

Bạn có thể ẩn hoặc hiện hộp thoại bằng cách nhấp vào biểu tượng sau trong hộp màu đỏ:



|  |
| --- |
| **The timer** |

**Đồng hồ bấm giờ**

|  |
| --- |
| The **timer** starts when the terminal has loaded. The timer keeps track of the amount of time you have left to complete a lab. The timer counts down until it reaches 00:00:00. When it does, your temporary terminal and resources are deleted. |

Bộ **đếm thời gian** bắt đầu khi thiết bị đầu cuối đã được tải. Bộ đếm thời gian theo dõi lượng thời gian bạn còn lại để hoàn thành phòng thí nghiệm. Đồng hồ đếm ngược cho đến khi về 00:00:00. Khi đó, thiết bị đầu cuối và tài nguyên tạm thời của bạn sẽ bị xóa.

|  |
| --- |
| You will have ample time to complete the labs. But, stay focused on completing the tasks to ensure you use your time well. |

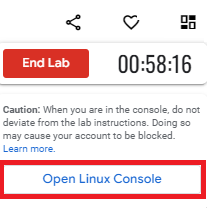
Bạn sẽ có nhiều thời gian để hoàn thành các bài thí nghiệm. Tuy nhiên, hãy tập trung hoàn thành nhiệm vụ để đảm bảo bạn sử dụng tốt thời gian của mình.

|  |
| --- |
| **Open Linux Console button** |

**Nút mở bảng điều khiển Linux**

|  |
| --- |
| When you click the button to **Open Linux Console**, the terminal opens in a new browser window: |

Khi bạn nhấp vào nút **Open Linux Console** , terminal sẽ mở trong cửa sổ trình duyệt mới:



|  |
| --- |
| Use this feature if you want a full-screen view of the terminal. You can close this window at any time. Closing the window does not end your lab, and you can continue working in the terminal in the original tab. |

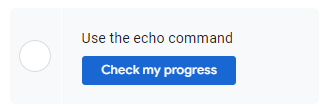
Sử dụng tính năng này nếu bạn muốn xem toàn màn hình của thiết bị đầu cuối. Bạn có thể đóng cửa sổ này bất cứ lúc nào. Việc đóng cửa sổ không kết thúc phòng thí nghiệm của bạn và bạn có thể tiếp tục làm việc trong thiết bị đầu cuối trong tab ban đầu.

|  |
| --- |
| **Check progress** |

**Kiểm tra tiến độ**

|  |
| --- |
| You can check your progress by clicking **Check my progress** at the end of each task. |

Bạn có thể kiểm tra tiến độ của mình bằng cách nhấp vào **Kiểm tra tiến độ của tôi** ở cuối mỗi nhiệm vụ.



|  |
| --- |
| If you haven’t yet completed a task, you’ll receive hints on what you must do to complete it. |

Nếu bạn chưa hoàn thành nhiệm vụ, bạn sẽ nhận được gợi ý về những gì bạn phải làm để hoàn thành nhiệm vụ đó.

|  |
| --- |
| You can click **Check my progress** whenever you want to check the completion status of a task or receive a hint. |

Bạn có thể nhấp vào **Kiểm tra tiến trình của tôi** bất cứ khi nào bạn muốn kiểm tra trạng thái hoàn thành của một nhiệm vụ hoặc nhận gợi ý.

|  |
| --- |
| **Using copy/paste commands** |

**Sử dụng lệnh sao chép/dán**

|  |
| --- |
| The first time you try to use copy or paste keyboard shortcuts (such as **CTRL + C**), you’ll receive a pop-up requesting permission to use your device’s clipboard:  “**googlecoursera.qwiklabs.com wants to see text and images copied to the clipboard.**” Please click **Allow** if you would like to be able to use these shortcuts in the Qwiklabs platform. If you choose not to allow Qwiklabs access to your clipboard, you cannot use keyboard shortcuts but you can still complete the lab. |

Lần đầu tiên bạn cố gắng sử dụng các phím tắt sao chép hoặc dán (chẳng hạn như **CTRL + C** ), bạn sẽ nhận được một cửa sổ bật lên yêu cầu quyền sử dụng bảng nhớ tạm của thiết bị: “ **googlecoursera.qwiklabs.com muốn xem văn bản và hình ảnh được sao chép sang bảng nhớ tạm.** ” Vui lòng nhấp vào **Cho phép** nếu bạn muốn có thể sử dụng các phím tắt này trong nền tảng Qwiklabs. Nếu bạn chọn không cho phép Qwiklabs truy cập vào khay nhớ tạm của mình, bạn không thể sử dụng phím tắt nhưng vẫn có thể hoàn thành bài thí nghiệm.

|  |
| --- |
| **Code block** |

**Khối mã**

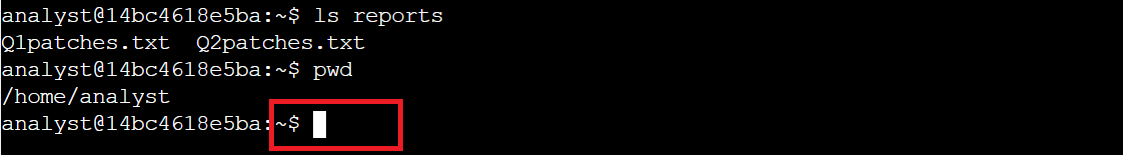
|  |
| --- |
| Certain steps may include a code block. Click the copy button to copy the code provided and then paste it into the terminal. |

Một số bước nhất định có thể bao gồm một khối mã. Nhấp vào nút sao chép để sao chép mã được cung cấp rồi dán vào thiết bị đầu cuối.



|  |
| --- |
| To paste code or other text content that you have copied from the instructions into the terminal, activate the terminal by clicking anywhere inside it. The terminal is active when the cursor in the terminal changes from a static empty outline to a flashing solid block. |

Để dán mã hoặc nội dung văn bản khác mà bạn đã sao chép từ hướng dẫn vào thiết bị đầu cuối, hãy kích hoạt thiết bị đầu cuối bằng cách nhấp vào bất kỳ đâu bên trong thiết bị đầu cuối. Thiết bị đầu cuối hoạt động khi con trỏ trong thiết bị đầu cuối thay đổi từ đường viền trống tĩnh sang khối rắn nhấp nháy.



|  |
| --- |
| Once the terminal is active, use the keyboard shortcut **CTRL + V** (hold down the **CTRL** key and press the **V** key) to insert the copied text into the terminal at the location of the flashing cursor. |

Khi thiết bị đầu cuối hoạt động, hãy sử dụng phím tắt **CTRL + V** (giữ phím **CTRL** và nhấn phím **V** ) để chèn văn bản đã sao chép vào thiết bị đầu cuối tại vị trí con trỏ nhấp nháy.

|  |
| --- |
| **Scrolling** |

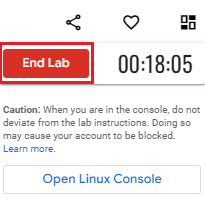
**Cuộn**

|  |
| --- |
| In certain situations, you may want to scroll within the terminal window. To do so, use the scroll wheel on your mouse or the touchpad of your computer. |

Trong một số trường hợp nhất định, bạn có thể muốn cuộn trong cửa sổ terminal. Để làm như vậy, hãy sử dụng con lăn trên chuột hoặc bàn di chuột của máy tính.

|  |
| --- |
| **End Lab button** |

**Nút kết thúc phòng thí nghiệm**



|  |
| --- |
| Finally, click **End Lab** when you’ve completed the tasks in the lab. |

Cuối cùng, nhấp vào **End Lab** khi bạn đã hoàn thành các nhiệm vụ trong lab.

|  |
| --- |
| **Note**: Don't click **End Lab** until you're finished; you'll lose access to the work you've done throughout the lab. |

**Lưu ý** : Đừng nhấp vào **End Lab** cho đến khi bạn hoàn thành; bạn sẽ mất quyền truy cập vào công việc bạn đã thực hiện trong phòng thí nghiệm.

|  |
| --- |
| **Tracking progress on Coursera** |

**Theo dõi tiến trình trên Coursera**

|  |
| --- |
| If you complete a lab but your progress hasn’t been tracked on Coursera, you may need to refresh the page for your progress to be registered. Once you complete the lab and refresh the page, the green check mark should appear. |

Nếu bạn hoàn thành bài thí nghiệm nhưng tiến trình của bạn chưa được theo dõi trên Coursera, bạn có thể cần phải làm mới trang để đăng ký tiến trình của mình. Sau khi bạn hoàn thành bài thực hành và làm mới trang, dấu kiểm màu xanh lục sẽ xuất hiện.

|  |
| --- |
| **Helpful navigation tips and keyboard shortcuts** |

**Mẹo điều hướng hữu ích và phím tắt**

|  |
| --- |
| The following contains a list of navigation tips and keyboard shortcuts you may find useful when completing your Linux labs. Your cursor must be in the terminal window to use these navigation tips and keyboard shortcuts. |

Phần sau đây chứa danh sách các mẹo điều hướng và phím tắt mà bạn có thể thấy hữu ích khi hoàn thành các phòng thí nghiệm Linux của mình. Con trỏ của bạn phải ở trong cửa sổ terminal để sử dụng các mẹo điều hướng và phím tắt này.

|  |
| --- |
| * **CTRL + C**: Terminates a command that is currently running; from the instructions portion of Qwiklabs, you can use **CTRL + C** to copy, but within the terminal, it will only terminate a command and if one isn't running, it will display **^C** at the prompt * **CTRL + V**: Pastes text * **clear**: Clears the terminal screen; this can also be done by entering **CTRL + L** * **CTRL + A**: Sets your cursor at the beginning of a command * **CTRL + E**: Sets your cursor at the end of a command * **Left arrow key**: Moves left within a command * **Right arrow key**: Moves right within a command * **Up arrow** **key**: Provides the last command you entered into the command line; can be entered multiple times to go through multiple commands from the command history * **Down arrow key**: Provides the next command in the command history; must be after using the **up arrow** key * **Tab** **key**: Provides available suggestions for completing your text |

* **CTRL + C** : Chấm dứt lệnh hiện đang chạy; từ phần hướng dẫn của Qwiklabs, bạn có thể sử dụng **CTRL + C** để sao chép, nhưng trong thiết bị đầu cuối, nó sẽ chỉ chấm dứt một lệnh và nếu một lệnh không chạy, nó sẽ hiển thị **^C** tại dấu nhắc
* **CTRL + V** : Dán văn bản
* **clear** : Xóa màn hình terminal; điều này cũng có thể được thực hiện bằng cách nhập **CTRL + L**
* **CTRL + A** : Đặt con trỏ của bạn ở đầu lệnh
* **CTRL + E** : Đặt con trỏ của bạn ở cuối lệnh
* **Phím mũi tên trái** : Di ​​chuyển sang trái trong lệnh
* **Phím mũi tên phải** : Di ​​chuyển sang phải trong lệnh
* **Phím mũi tên lên** : Cung cấp lệnh cuối cùng bạn đã nhập vào dòng lệnh; có thể được nhập nhiều lần để đi qua nhiều lệnh từ lịch sử lệnh
* **Phím mũi tên xuống** : Cung cấp lệnh tiếp theo trong lịch sử lệnh; phải sau khi sử dụng phím **mũi tên lên**
* **Phím tab** : Cung cấp các gợi ý có sẵn để hoàn thành văn bản của bạn

|  |
| --- |
| **Key takeaways** |

**Bài học chính**

|  |
| --- |
| Knowing how to navigate Qwiklabs will be useful as you complete the labs throughout this course. These labs can help you practice what you’ve learned in an interactive environment. |

Biết cách điều hướng Qwiklabs sẽ hữu ích khi bạn hoàn thành các phòng thí nghiệm trong suốt khóa học này. Những phòng thí nghiệm này có thể giúp bạn thực hành những gì bạn đã học trong môi trường tương tác.

***2.6. Lab tips and troubleshooting steps – Mẹo trong phòng thí nghiệm và các bước khắc phục sự cố***

|  |
| --- |
| **Lab tips and troubleshooting steps** |

**Mẹo trong phòng thí nghiệm và các bước khắc phục sự cố**

|  |
| --- |
| Throughout this certificate you will use Qwiklabs and Jupyter Notebooks to complete hands-on activities that  include Linux command line, packet capture, and Python programming tasks. In this reading, we will cover some tips and troubleshooting steps for using Qwiklabs and Jupyter Notebooks on your computer. |

Trong suốt chứng chỉ này, bạn sẽ sử dụng Qwiklabs và Jupyter Notebook để hoàn thành các hoạt động thực hành bao gồm dòng lệnh Linux, chụp gói và các tác vụ lập trình Python. Trong bài đọc này, chúng tôi sẽ đề cập đến một số mẹo và các bước khắc phục sự cố khi sử dụng Qwiklabs và Jupyter Notebook trên máy tính của bạn.

|  |
| --- |
| **Browser compatibility** |

**Tính tương thích của trình duyệt web**

|  |
| --- |
| Make sure your internet browser is updated regularly. Qwiklabs and Jupyter Notebooks require the latest version of Google Chrome, Firefox, or Microsoft Edge. If your browser is outdated or you are using a browser that is not supported by Qwiklabs or Jupyter Notebooks, you may encounter a problem. If your browser is up to date and you are using one of the browsers listed above and still encountering problems try restarting your browser or clearing your browser’s cache and cookies. You can also use incognito mode which prevents your browser from storing cookies and other temporary data. |

Đảm bảo trình duyệt internet của bạn được cập nhật thường xuyên. Qwiklabs và Jupyter Notebook yêu cầu phiên bản mới nhất của Google Chrome, Firefox hoặc Microsoft Edge. Nếu trình duyệt của bạn đã lỗi thời hoặc bạn đang sử dụng trình duyệt không được Qwiklabs hoặc Jupyter Notebooks hỗ trợ, bạn có thể gặp phải sự cố. Nếu trình duyệt của bạn được cập nhật và bạn đang sử dụng một trong các trình duyệt được liệt kê ở trên mà vẫn gặp sự cố, hãy thử khởi động lại trình duyệt hoặc xóa bộ nhớ đệm và cookie của trình duyệt. Bạn cũng có thể sử dụng chế độ ẩn danh để ngăn trình duyệt của bạn lưu trữ cookie và dữ liệu tạm thời khác.

|  |
| --- |
| **Note:** The Qwiklabs user interface works best with Google Chrome. |

**Lưu ý:** Giao diện người dùng Qwiklabs hoạt động tốt nhất với Google Chrome.

|  |
| --- |
| **Internet connection** |

**kết nối Internet**

|  |
| --- |
| Qwiklabs and Jupyter Notebooks require a stable internet connection. If you are experiencing problems starting or completing Qwiklabs or Jupyter Notebooks, your internet connection may be slow or unreliable. Some signs of an unstable internet connection may be freezing labs, difficulty connecting to virtual machines, or the inability to type or enter commands within the lab environment. |

Máy tính xách tay Qwiklabs và Jupyter yêu cầu kết nối Internet ổn định. Nếu bạn gặp sự cố khi bắt đầu hoặc hoàn thành Sổ ghi chép Qwiklabs hoặc Jupyter thì kết nối Internet của bạn có thể chậm hoặc không đáng tin cậy. Một số dấu hiệu của kết nối Internet không ổn định có thể là phòng thí nghiệm bị treo, khó kết nối với máy ảo hoặc không thể nhập hoặc nhập lệnh trong môi trường phòng thí nghiệm.

|  |
| --- |
| **Pro Tip:** If you are unable to complete a Qwiklab or Jupyter Notebooks lab on one device, try using another device. |

**Mẹo của chuyên gia:** Nếu bạn không thể hoàn thành lab Qwiklab hoặc Jupyter Notebooks trên một thiết bị, hãy thử sử dụng một thiết bị khác.

|  |
| --- |
| **Troubleshooting steps** |

**Các bước khắc phục sự cố**

|  |
| --- |
| To summarize, here are the troubleshooting steps to try if you encounter a problem with Qwiklabs or Jupyter Notebooks. |

Tóm lại, đây là các bước khắc phục sự cố để thử nếu bạn gặp sự cố với Qwiklabs hoặc Jupyter Notebook.

|  |
| --- |
| 1. Make sure you are using the latest version of a supported browser: Google Chrome, Firefox, or Microsoft Edge. 2. Restart your browser and clear your browser’s cache and cookies. You can also use incognito mode. 3. Check your internet connection and make sure it is stable. You can try restarting your router and modem to regain a stable connection. 4. Try restarting Qwiklabs or Jupyter Notebooks again. 5. **For Qwiklabs only:** If problems persist or you receive a message stating that you have exceeded the quota for a Qwiklab, submit this [form](https://qwiklab.zendesk.com/hc/en-us/requests/new) to Qwiklabs support for assistance. |

1. Đảm bảo bạn đang sử dụng phiên bản mới nhất của trình duyệt được hỗ trợ: Google Chrome, Firefox hoặc Microsoft Edge.
2. Khởi động lại trình duyệt của bạn và xóa bộ nhớ cache và cookie của trình duyệt. Bạn cũng có thể sử dụng chế độ ẩn danh.
3. Kiểm tra kết nối internet của bạn và đảm bảo nó ổn định. Bạn có thể thử khởi động lại bộ định tuyến và modem để lấy lại kết nối ổn định.
4. Hãy thử khởi động lại Qwiklabs hoặc Jupyter Notebook một lần nữa.
5. **Chỉ dành cho Qwiklabs:** Nếu sự cố vẫn tiếp diễn hoặc bạn nhận được thông báo cho biết rằng bạn đã vượt quá hạn ngạch cho Qwiklab, hãy gửi thông báo này[hình thức](https://qwiklab.zendesk.com/hc/en-us/requests/new)tới bộ phận hỗ trợ của Qwiklabs để được hỗ trợ.

***2.7. Activity: Install software in a Linux distribution – Hoạt động: Cài đặt phần mềm trên bản phân phối Linux***

***2.8. Optional Exemplar: Install software in a Linux distribution – Mẫu tùy chọn: Cài đặt phần mềm trong bản phân phối Linux***

***2.9. Test your knowledge: Linux distributions – Kiểm tra kiến ​​thức của bạn: Bản phân phối Linux***

**3. The shell – Shell**

***3.1. Introduction to the shell – Giới thiệu về shell***

|  |
| --- |
| Welcome back! In this video, we're going to discuss the Linux shell. This part of the Linux architecture is where the action will happen for you as a security analyst. We introduced the shell with other components of the Linux OS earlier, but let's take a deeper look at what the shell is and what it does. |

Chào mừng trở lại! Trong video này, chúng ta sẽ thảo luận về Linux shell.Phần này của kiến ​​trúc Linux là nơi hành động sẽ diễn rabạn với tư cách là một nhà phân tích bảo mật.Chúng tôi đã giới thiệu shell với các thành phần khác của hệ điều hành Linux trước đó,nhưng chúng ta hãy nhìn sâu hơn xem shell là gì và nó làm gì.

|  |
| --- |
| The shell is the command-line interpreter. That means it helps you communicate with the operating system through the command line. Previously, we discussed a command-line interface. This is essentially the shell. The shell provides the command-line interface for you to interact with the OS. To tell the OS what to do, you enter commands into this interface. A command is an instruction telling the computer to do something. The shell communicates with the kernel to execute these commands. |

Shell là trình thông dịch dòng lệnh.Điều đó có nghĩa là nó giúp bạn giao tiếp với hệ điều hành thông quadòng lệnh.Trước đây, chúng ta đã thảo luận về giao diện dòng lệnh.Đây thực chất là vỏ.Shell cung cấp giao diện dòng lệnh để bạn tương tác với hệ điều hành.Để báo cho HĐH biết phải làm gì, bạn nhập lệnh vào giao diện này.Lệnh là một lệnh yêu cầu máy tính làm một việc gì đó.Shell giao tiếp với kernel để thực thi các lệnh này.

|  |
| --- |
| Earlier, we discussed how the operating system helps humans and computers speak with each other. The shell is the part of the OS that allows you to do this. Think of this as a very helpful language interpreter between you and your system. Since you do not speak computer language or binary, you can't directly communicate with your system. This is where the shell comes in to help you. Your OS doesn't need the shell for most of its work, but it is an interface between you and what your system can offer. It allows you to perform math, run tests, and execute applications. More importantly, it allows you to combine these operations and connect applications to each other to perform complex and automated tasks. |

Trước đó, chúng ta đã thảo luận về cách hệ điều hành giúp đỡ con người vàmáy tính nói chuyện với nhau.Shell là một phần của hệ điều hành cho phép bạn thực hiện việc này.Hãy coi đây như một trình thông dịch ngôn ngữ rất hữu ích giữa bạn và hệ thống của bạn.Vì bạn không nói được ngôn ngữ máy tính hoặc hệ nhị phân,bạn không thể giao tiếp trực tiếp với hệ thống của mình.Đây là nơi Shell đến để giúp bạn.Hệ điều hành của bạn không cần shell cho hầu hết công việc của nó, nhưngnó là một giao diện giữa bạn và những gì hệ thống của bạn có thể cung cấp.Nó cho phép bạn thực hiện phép toán, chạy thử nghiệm và thực thi các ứng dụng.Quan trọng hơn, nó cho phép bạn kết hợp các hoạt động này vàkết nối các ứng dụng với nhauđể thực hiện các nhiệm vụ phức tạp và tự động.

|  |
| --- |
| Just as there are many Linux distributions, there are many different types of shells. We'll primarily focus on the Bash shell in this course. Let's continue to learn more about the shell. |

Cũng như có nhiều bản phân phối Linux,có rất nhiều loại vỏ khác nhau.Chúng tôi sẽ chủ yếu tập trung vào shell Bash trong khóa học này.Hãy tiếp tục tìm hiểu thêm về shell.

***3.2. Different types of shells – Các loại shell khác nhau***

|  |
| --- |
| **Different types of shells** |

**Các loại shell khác nhau**

|  |
| --- |
| Knowing how to work with Linux shells is an important skill for cybersecurity professionals. Shells can be used for many common tasks. Previously, you were introduced to shells and their functions. This reading will review shells and introduce you to different types, including the one that you'll use in this course. |

Biết cách làm việc với shell Linux là một kỹ năng quan trọng đối với các chuyên gia an ninh mạng. Shell có thể được sử dụng cho nhiều nhiệm vụ thông thường. Trước đây, bạn đã được giới thiệu về shell và các chức năng của chúng. Bài đọc này sẽ xem xét các shell và giới thiệu cho bạn các loại khác nhau, bao gồm cả loại bạn sẽ sử dụng trong khóa học này.

|  |
| --- |
| **Communicate through a shell** |

**Giao tiếp qua shell**

|  |
| --- |
| As you explored previously, the **shell** is the command-line interpreter. You can think of a shell as a translator between you and the computer system. Shells allow you to give commands to the computer and receive responses from it. When you enter a command into a shell, the shell executes many internal processes to interpret your command, send it to the kernel, and return your results. |

Như bạn đã khám phá trước đó, **shell** là trình thông dịch dòng lệnh. Bạn có thể coi shell như một công cụ dịch thuật giữa bạn và hệ thống máy tính. Shell cho phép bạn đưa ra lệnh cho máy tính và nhận phản hồi từ nó. Khi bạn nhập lệnh vào shell, shell sẽ thực thi nhiều quy trình nội bộ để diễn giải lệnh của bạn, gửi lệnh đó đến kernel và trả về kết quả của bạn.

|  |
| --- |
| **Types of shells** |

**Các loại shell**

|  |
| --- |
| The many different types of Linux shells include the following:   * Bourne-Again Shell (bash) * C Shell (csh) * Korn Shell (ksh) * Enhanced C shell (tcsh) * Z Shell (zsh) |

Nhiều loại shell Linux khác nhau bao gồm:

* Bourne-Again Shell (bash)
* C Shell (csh)
* Korn Shell (ksh)
* Enhanced C shell (tcsh)
* Z Shell (zsh)

|  |
| --- |
| All Linux shells use common Linux commands, but they can differ in other features. For example, ksh and bash use the dollar sign (**$**) to indicate where users type in their commands. Other shells, such as zsh, use the percent sign (**%**) for this purpose. |

Tất cả các shell Linux đều sử dụng các lệnh Linux phổ biến, nhưng chúng có thể khác nhau ở các tính năng khác. Ví dụ: ksh và bash sử dụng ký hiệu đô la ( **$** ) để cho biết nơi người dùng nhập lệnh của họ. Các shell khác, chẳng hạn như zsh, sử dụng dấu phần trăm ( **%** ) cho mục đích này.

|  |
| --- |
| **Bash** |

Bash

|  |
| --- |
| **Bash** is the default shell in most Linux distributions. It’s considered a user-friendly shell. You can use bash for basic Linux commands as well as larger projects. |

**Bash** là shell mặc định trong hầu hết các bản phân phối Linux. Nó được coi là một lớp vỏ thân thiện với người dùng. Bạn có thể sử dụng bash cho các lệnh Linux cơ bản cũng như các dự án lớn hơn.

|  |
| --- |
| Bash is also the most popular shell in the cybersecurity profession. You’ll use bash throughout this course as you learn and practice Linux commands. |

Bash cũng là shell phổ biến nhất trong ngành an ninh mạng. Bạn sẽ sử dụng bash trong suốt khóa học này khi học và thực hành các lệnh Linux.

|  |
| --- |
| **Key takeaways** |

**Bài học chính**

|  |
| --- |
| Shells are a fundamental part of the Linux operating system. Shells allow you to give commands to the computer and receive responses from it. They can be thought of as a translator between you and your computer system. There are many different types of shells, but the bash shell is the most commonly used shell in the cybersecurity profession. You’ll learn how to enter Linux commands through the bash shell later in this course. |

Shell là một phần cơ bản của hệ điều hành Linux. Shell cho phép bạn đưa ra lệnh cho máy tính và nhận phản hồi từ nó. Họ có thể được coi là người phiên dịch giữa bạn và hệ thống máy tính của bạn. Có nhiều loại shell khác nhau nhưng bash shell là loại shell được sử dụng phổ biến nhất trong ngành an ninh mạng. Bạn sẽ học cách nhập lệnh Linux thông qua bash shell ở phần sau của khóa học này.

***3.3. Input and output in the shell – Đầu vào và đầu ra trong shell***

|  |
| --- |
| Hello again! In this video, we're going to learn a little more about the shell and how to communicate with it. Communicating with a computer is like having a conversation with your friend. One person asks a question and the other person answers with a response. If you don't know the answer, you can just say you don't know the answer. When you communicate with the shell, the commands in the shell can take input, give output, or give error messages. |

Xin chào lần nữa! Trong video này,chúng ta sẽ tìm hiểu thêm một chút vềshell và cách giao tiếp với nó.Giao tiếp với máy tính làgiống như đang trò chuyện với bạn của bạn.Một người đặt một câu hỏivà người kia trả lời bằng một câu trả lời.Nếu bạn không biết câu trả lời,bạn chỉ có thể nói rằng bạn không biết câu trả lời.Khi bạn giao tiếp với shell,các lệnh trong shell có thể nhận đầu vào,đưa ra đầu ra hoặc đưa ra thông báo lỗi.

|  |
| --- |
| Let's explore standard input, standard output, and error messages in more detail. Standard input consists of information received by the OS via the command line. This is like you asking your friend a question during a conversation. The information is input from your keyboard to the shell. If the shell can interpret your request, it asks the kernel for the resources it needs to execute the related task. |

Hãy khám phá đầu vào tiêu chuẩn,đầu ra tiêu chuẩn và thông báo lỗi chi tiết hơn.Đầu vào tiêu chuẩn bao gồm thông tinđược hệ điều hành nhận thông qua dòng lệnh.Điều này giống như bạn hỏi bạn của bạnmột câu hỏi trong cuộc trò chuyện.Thông tin được nhập từ bàn phím của bạn tới shell.Nếu shell có thể giải thích yêu cầu của bạn,nó yêu cầu kernel cung cấp tài nguyêncần thực hiện nhiệm vụ liên quan.

|  |
| --- |
| Let's take a look at this through echo, a Linux command that outputs a specified string of text. String data is data consisting of an ordered sequence of characters. In our example, we'll just have it output the string of: hello. So, as input, we'll type: echo hello into the shell. Later, when we press enter, we'll get the output. But before we do that, let's first discuss the concept of output in more detail. |

Chúng ta hãy xem xét điều này thông qua tiếng vang,một lệnh Linux xuất ra một chuỗi văn bản được chỉ định.Dữ liệu chuỗi là dữ liệu bao gồmcủa một chuỗi ký tự có thứ tự.Trong ví dụ của chúng tôi, chúng tôi sẽ chỉ cónó xuất ra chuỗi: hello.Vì vậy, khi làm đầu vào, chúng ta sẽ gõ: echo hello vào shell.Sau này, khi chúng ta nhấn enter, chúng ta sẽ nhận được kết quả.Nhưng trước khi chúng ta làm điều đó,trước tiên hãy thảo luận chi tiết hơn về khái niệm đầu ra.

|  |
| --- |
| Standard output is the information returned by the OS through the shell. In the same way that your friend gives an answer to your question, output is a computer's response to the command you input. Output is what you receive. Let's pick up where we left off in our example and send the input of: echo hello to the OS by pressing enter. Immediately, the shell returns the output of: hello. |

Đầu ra tiêu chuẩn là thông tinđược hệ điều hành trả về thông qua shell.Tương tự như cách mà bạn của bạnđưa ra câu trả lời cho câu hỏi của bạn,đầu ra là phản hồi của máy tính đối với lệnh bạn nhập vào.Đầu ra là những gì bạn nhận được.Hãy bắt đầu từ nơi chúng ta đã dừng lại trong ví dụ của mình và gửiđầu vào của: echo hello to the OS bằng cách nhấn enter.Ngay lập tức, shell trả về kết quả: hello.

|  |
| --- |
| Finally, standard error contains error messages returned by the OS through the shell. Just like your friend might indicate that they can't answer a question, the system responds with an error message if they can't respond to your command. Sometimes this might occur when we misspell a command or the system doesn't know the response to the command. Other times, it might happen because we don't have the appropriate permissions to perform a command. |

Cuối cùng, lỗi tiêu chuẩn chứathông báo lỗi được hệ điều hành trả về thông qua shell.Giống như bạn của bạn có thểcho biết họ không thể trả lời một câu hỏi,hệ thống phản hồi vớimột thông báo lỗi nếu họ không thể đáp ứng lệnh của bạn.Đôi khi điều này có thể xảy ra khi chúng ta viết sai chính tảmột lệnh hoặc hệ thốngkhông biết phản ứng với lệnh.Những lần khác, điều đó có thể xảy ra vì chúng ta không cócác quyền thích hợp để thực hiện một lệnh.

|  |
| --- |
| We'll explore another example that demonstrates standard error. Let's input: eco hello into the shell. Notice I intentionally misspelled echo as e-c-o. When we press enter, an error message appears. |

Chúng ta sẽ khám phá một ví dụ khácđiều đó thể hiện lỗi tiêu chuẩn.Hãy nhập: eco hello vào shell.Lưu ý rằng tôi cố tình viết sai chính tả echo là eco.Khi chúng ta nhấn enter,một thông báo lỗi xuất hiện.

|  |
| --- |
| To wrap up, we've covered the basics of communication with the shell. Communication with the shell can only go in one of three ways: the system receives a command—this is input; the system responds to the command and produces output; and finally, the system doesn't know how to respond, resulting in an error. Later, you'll become much more familiar with this as we explore commands useful for security professionals. |

Để kết thúc, chúng tôi đã đề cậpnhững điều cơ bản của giao tiếp với shell.Giao tiếp với shell chỉ có thể thực hiện bằng một trong cácba cách: hệ thốngnhận được lệnh—đây là đầu vào;hệ thống phản hồi lệnh và tạo đầu ra;và cuối cùng, hệ thống không biết phản hồi thế nào,dẫn đến một lỗi.Sau này, bạn sẽ trở nên quen thuộc hơn với điều này vìchúng tôi khám phá các lệnh hữu ích cho các chuyên gia bảo mật.

***3.4. Activity: Examine input and output in the shell – Hoạt động: Kiểm tra đầu vào và đầu ra trong shell***

***3.5. Optional Exemplar: Examine input and output in the shell – Mẫu tùy chọn: Kiểm tra đầu vào và đầu ra trong shell***

***3.6. Test your knowledge: The shell – Kiểm tra kiến ​​thức của bạn: Shell***

***3.7. Strategies to learn new skills – Chiến lược học các kỹ năng mới***

**4. Review: The Linux operating system – Đánh giá: Hệ điều hành Linux**

***4.1. Wrap-up – Gói lại***

|  |
| --- |
| We've made it to the end of this section. Great work! Let's recap what you've just completed. |

Chúng ta đã đi đến cuối phần này.Công việc tuyệt vời!Hãy tóm tắt lại những gì bạn vừa hoàn thành.

|  |
| --- |
| In this section, you learned about the Linux operating system. We examined the architecture of Linux. In our exploration of the different distributions of Linux, we discussed some of the most widely used distros in security. You were introduced to KALI LINUX™, Ubuntu, Parrot, Red Hat, and CentOS distributions. Finally, you learned about the shell and its role as an interpreter between the user and operating system. |

Trong phần này, bạn đã họcvề hệ điều hành Linux.Chúng tôi đã kiểm tra kiến ​​trúc của Linux.Trong cuộc khám phá của chúng tôi vềcác bản phân phối khác nhau của Linux, chúng tôiđã thảo luận về một số điều nhấtcác bản phân phối được sử dụng rộng rãi trong bảo mật.Bạn đã được giới thiệu về KALI LINUX™, Ubuntu,Các bản phân phối Parrot, Red Hat và CentOS.Cuối cùng, bạn đã tìm hiểu về shell vàvai trò của nó như một thông dịch viêngiữa người dùng và hệ điều hành.

|  |
| --- |
| Congratulations! You're doing great, and we have more useful topics to come. In the next part of the program, you'll learn specific commands to use within the shell while working as a security analyst. Let's continue on. |

Chúc mừng! Bạn đang làmtuyệt vời và chúng tôi sắp có nhiều chủ đề hữu ích hơn.Trong phần tiếp theo của chương trình,bạn sẽ học các lệnh cụ thể để sử dụng trongvỏ trong khi làm việc nhưmột nhà phân tích bảo mật. Hãy tiếp tục nào.

***4.2. Glossary terms from module 2 – Thuật ngữ trong học phần 2***

|  |
| --- |
| **Glossary terms from module 2** |

**Thuật ngữ trong học phần 2**

|  |
| --- |
| **Terms and definitions from Course 4, Module 2** |

**Các thuật ngữ và định nghĩa trong Khóa 4, Học phần 2**

|  |
| --- |
| **Application:** A program that performs a specific task |

**Ứng dụng:** Một chương trình thực hiện một nhiệm vụ cụ thể

|  |
| --- |
| **Bash:** The default shell in most Linux distributions |

**Bash:** Shell mặc định trong hầu hết các bản phân phối Linux

|  |
| --- |
| **CentOS:** An open-source distribution that is closely related to Red Hat |

**CentOS:** Một bản phân phối nguồn mở có liên quan chặt chẽ với Red Hat

|  |
| --- |
| **Central Processing Unit (CPU):** A computer’s main processor, which is used to perform general computing tasks on a computer |

**Bộ xử lý trung tâm (CPU):** Bộ xử lý chính của máy tính, được sử dụng để thực hiện các tác vụ tính toán chung trên máy tính

|  |
| --- |
| **Command:** An instruction telling the computer to do something |

**Lệnh:** Lệnh yêu cầu máy tính làm một việc gì đó

|  |
| --- |
| **Digital forensics:** The practice of collecting and analyzing data to determine what has happened after an attack |

**Điều tra kỹ thuật số:** Việc thực hành thu thập và phân tích dữ liệu để xác định điều gì đã xảy ra sau một cuộc tấn công

|  |
| --- |
| **Directory:** A file that organizes where other files are stored |

**Thư mục:** Một tệp tổ chức nơi các tệp khác được lưu trữ

|  |
| --- |
| **Distributions:** The different versions of Linux |

**Phân phối:** Các phiên bản khác nhau của Linux

|  |
| --- |
| **File path:** The location of a file or directory |

**Đường dẫn tệp:** Vị trí của tệp hoặc thư mục

|  |
| --- |
| **Filesystem Hierarchy Standard (FHS):** The component of the Linux OS that organizes data |

**Tiêu chuẩn phân cấp hệ thống tập tin (FHS):** Thành phần của hệ điều hành Linux tổ chức dữ liệu

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

**Giao diện người dùng đồ họa (GUI):** Giao diện người dùng sử dụng các biểu tượng trên màn hình để quản lý các tác vụ khác nhau trên máy tính

|  |
| --- |
| **Hard drive:** A hardware component used for long-term memory |

**Ổ cứng:** Một thành phần phần cứng được sử dụng cho bộ nhớ dài hạn

|  |
| --- |
| **Hardware**: The physical components of a computer |

**Phần cứng** : Các thành phần vật lý của máy tính

|  |
| --- |
| **Internal hardware:** The components required to run the computer |

**Phần cứng bên trong:** Các thành phần cần thiết để chạy máy tính

|  |
| --- |
| **Kali Linux ™**: An open-source distribution of Linux that is widely used in the security industry |

**Kali Linux™** : Một bản phân phối mã nguồn mở của Linux được sử dụng rộng rãi trong ngành bảo mật

|  |
| --- |
| **Kernel:** The component of the Linux OS that manages processes and memory |

**Kernel:** Thành phần của hệ điều hành Linux quản lý các tiến trình và bộ nhớ

|  |
| --- |
| **Linux:** An open source operating system |

**Linux:** Một hệ điều hành mã nguồn mở

|  |
| --- |
| **Package:** A piece of software that can be combined with other packages to form an application |

**Package:** Một phần mềm có thể kết hợp với các gói khác để tạo thành một ứng dụng

|  |
| --- |
| **Package manager:** A tool that helps users install, manage, and remove packages or applications |

**Trình quản lý gói:** Công cụ giúp người dùng cài đặt, quản lý và xóa các gói hoặc ứng dụng

|  |
| --- |
| **Parrot:** An open-source distribution that is commonly used for security |

**Parrot:** Một bản phân phối nguồn mở thường được sử dụng để bảo mật

|  |
| --- |
| **Penetration test (pen test):** A simulated attack that helps identify vulnerabilities in systems, networks, websites, applications, and processes |

**Kiểm tra thâm nhập (pen test):** Cuộc tấn công mô phỏng giúp xác định các lỗ hổng trong hệ thống, mạng, trang web, ứng dụng và quy trình

|  |
| --- |
| **Peripheral devices:** Hardware components that are attached and controlled by the computer system |

**Thiết bị ngoại vi:** Các thành phần phần cứng được gắn và điều khiển bởi hệ thống máy tính

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

**Bộ nhớ truy cập ngẫu nhiên (RAM):** Một thành phần phần cứng được sử dụng cho bộ nhớ ngắn hạn

|  |
| --- |
| **Red Hat® Enterprise Linux®** (also referred to simply as Red Hat in this course)**:** A subscription-based distribution of Linux built for enterprise use |

**Red Hat® Enterprise Linux®** (còn được gọi đơn giản là Red Hat trong khóa học này) **:** Một bản phân phối Linux dựa trên đăng ký được xây dựng để sử dụng cho doanh nghiệp

|  |
| --- |
| **Shell:** The command-line interpreter |

**Shell:** Trình thông dịch dòng lệnh

|  |
| --- |
| **Standard error:** An error message returned by the OS through the shell |

**Lỗi tiêu chuẩn:** Thông báo lỗi được hệ điều hành trả về thông qua shell

|  |
| --- |
| **Standard input:** Information received by the OS via the command line |

**Đầu vào tiêu chuẩn:** Thông tin được HĐH nhận thông qua dòng lệnh

|  |
| --- |
| **Standard output:** Information returned by the OS through the shell |

**Đầu ra tiêu chuẩn:** Thông tin được hệ điều hành trả về thông qua shell

|  |
| --- |
| **String data:** Data consisting of an ordered sequence of characters |

**Dữ liệu chuỗi:** Dữ liệu bao gồm một chuỗi ký tự được sắp xếp

|  |
| --- |
| **Ubuntu:** An open-source, user-friendly distribution that is widely used in security and other industries |

**Ubuntu:** Một bản phân phối mã nguồn mở, thân thiện với người dùng, được sử dụng rộng rãi trong ngành bảo mật và các ngành khác

|  |
| --- |
| **User:** The person interacting with a computer |

**Người dùng:** Người tương tác với máy tính

***4.3 . Module 2 challenge – Thử thách mô-đun 2***

# **Module 3: Linux commands in the Bash shell – Các lệnh Linux trong shell Bash**

|  |
| --- |
| 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. |

Bạn sẽ được giới thiệu các lệnh Linux được nhập thông qua shell Bash. Bạn sẽ sử dụng shell Bash để điều hướng và quản lý hệ thống tệp cũng như ủy quyền và xác thực người dùng. Bạn cũng sẽ biết nơi cần trợ giúp khi làm việc với các lệnh Linux mới.

|  |
| --- |
| **Learning Objectives**   * Navigate the file system using Linux commands via the Bash shell. * Manage the file system using Linux commands via the Bash shell. * Describe how Linux handles file permissions. * Use Linux commands via the Bash shell to authenticate and authorize users. * Use sudo to provide root user permissions. * Access resources that provide support on using Linux commands. |

**Mục tiêu học tập**

* Điều hướng hệ thống tệp bằng các lệnh Linux thông qua shell Bash.
* Quản lý hệ thống tệp bằng lệnh Linux thông qua shell Bash.
* Mô tả cách Linux xử lý quyền truy cập tệp.
* Sử dụng các lệnh Linux thông qua shell Bash để xác thực và ủy quyền cho người dùng.
* Sử dụng sudo để cung cấp quyền cho người dùng root.
* Truy cập các tài nguyên cung cấp hỗ trợ về cách sử dụng các lệnh Linux.

**1. Navigate the Linux file system – Điều hướng hệ thống tệp Linux**

***1.1. Welcome to module 3 – Chào mừng đến với mô-đun 3***

|  |
| --- |
| Learning to communicate in a new way can be exciting. Maybe you've learned a new language and can remember this feeling. Perhaps a lot of us share this excitement with young children as they are expanding their vocabulary. Others, including me, remember a sense of wonder when we first used a specialized language to communicate with their computer. In this section, we'll continue to learn more about Linux and how to communicate with the OS through its shell. |

Học cách giao tiếp theo một cách mới có thể rất thú vị.Có thể bạn đã học được một ngôn ngữ mớivà có thể nhớ cảm giác này.Có lẽ nhiều người trong chúng ta cùng chia sẻ sự phấn khích này vớitrẻ nhỏ khi chúng đang mở rộng vốn từ vựng của mình.Những người khác, kể cả tôi, vẫn nhớ cảm giác ngạc nhiên khi chúng tôilần đầu tiên sử dụng một ngôn ngữ chuyên biệtđể giao tiếp với máy tính của họ.Trong phần này chúng ta sẽ tiếp tục tìm hiểu thêm vềLinux và cách thực hiệngiao tiếp với hệ điều hành thông qua lớp vỏ của nó.

|  |
| --- |
| You'll utilize the command line to communicate with the OS. You'll learn how to input commands in the shell and learn about some of the core Linux commands that you'll use as a security analyst. Specifically, this includes navigating and managing the file system. You'll also focus on authenticating and authorizing users. This means you'll be able to use a command line to add and delete users from the system and to control what they have access to. Finally, there's always more to learn. We'll cover accessing resources that support learning new Linux commands. |

Bạn sẽ sử dụng dòng lệnhđể giao tiếp với hệ điều hành.Bạn sẽ học cách nhập liệucác lệnh trong shell và tìm hiểu về một sốcác lệnh Linux cốt lõi mà bạn sẽsử dụng như một nhà phân tích bảo mật.Cụ thể, điều này bao gồmđiều hướng và quản lý hệ thống tập tin.Bạn cũng sẽ tập trung vàoxác thực và ủy quyền cho người dùng.Điều này có nghĩa là bạn sẽ có thểsử dụng một dòng lệnh để thêm vàxóa người dùng khỏi hệ thống vàđể kiểm soát những gì họ có quyền truy cập.Cuối cùng, luôn có nhiều điều để học hỏi.Chúng tôi sẽ đề cập đến việc truy cập các tài nguyênhỗ trợ học các lệnh Linux mới.

|  |
| --- |
| I remember when I first learned about the command line and was shocked at the capabilities it provided. I didn't need to click through multiple screens to get tasks done. Although it took some practice and time to get used to, it has been one of the biggest tools at my disposal. After this section, you'll have a practical experience in an area important to the work of a security analyst: using Linux commands. |

Tôi nhớ lần đầu tiên tôi biết về dòng lệnhvà bị sốc trước khả năng mà nó mang lại.Tôi không cần phải nhấp quanhiều màn hình để hoàn thành nhiệm vụ.Mặc dù phải mất một thời gian luyện tập và làm quen,nó là một trong những công cụ lớn nhất mà tôi có thể sử dụng.Sau phần này, bạn sẽ cómột kinh nghiệm thực tế trong một khu vựcquan trọng đối với công việc củamột nhà phân tích bảo mật: sử dụng các lệnh Linux.

***1.2. Linux commands via the Bash shell – Các lệnh Linux thông qua shell Bash***

|  |
| --- |
| Welcome back. Before we get into specific Linux commands, let's explore in more detail the basics of communicating with the OS through the shell. Being able to utilize Linux commands is a foundational skill for all security professionals. As a security analyst, you will work with server logs and you'll need to know how to navigate, manage and analyze files remotely without a graphical user interface. In addition, you'll need to know how to verify and configure users and group access. You'll also need to give authorization and set file permissions. That means that developing skills with the command line is essential for your work as a security analyst. When we learned about the Linux architecture, we learned that the shell is one of the main components of an operating system. We also learned that there are different shells. In this section, we'll utilize the Bash shell. |

Chào mừng trở lại. Trước khi chúng tôi nhận đượcvào các lệnh Linux cụ thể, hãykhám phá chi tiết hơn những điều cơ bản củagiao tiếp với hệ điều hành thông qua shell.Có thể sử dụng các lệnh Linux làmột kỹ năng nền tảng cho tất cả các chuyên gia bảo mật.Là một nhà phân tích bảo mật, bạn sẽ làm việc vớinhật ký máy chủ và bạn sẽ cần biết cách điều hướng,quản lý và phân tích tập tintừ xa mà không có giao diện người dùng đồ họa.Ngoài ra, bạn cần biết cáchxác minh và định cấu hình quyền truy cập của người dùng và nhóm.Bạn cũng sẽ cần phải cấp quyềnvà đặt quyền truy cập tập tin.Điều đó có nghĩa là việc phát triển kỹ năng sử dụng dòng lệnhlà điều cần thiết cho công việc của bạn với tư cách là một nhà phân tích bảo mật.Khi chúng tôi biết về Linuxkiến trúc, chúng tôi đã học được rằngvỏ là một trong những thành phần chínhcủa một hệ điều hành.Chúng tôi cũng biết được rằng có nhiều loại vỏ khác nhau.Trong phần này, chúng ta sẽ sử dụng shell Bash.

|  |
| --- |
| Bash is the default shell in most Linux distributions. For the most part, the key Linux commands that you'll be learning in this section are the same across shells. Now that you know what shell you'll be using, let's go into how to write in Bash. As we discussed in a previous section, communicating with your OS is like a conversation. You type in commands, and the OS responds with an answer to your command. A command is an instruction telling the computer to do something. |

Bash là shell mặc định trong hầu hết các bản phân phối Linux.Phần lớn, các lệnh Linux chính mà bạn sẽviệc học trong phần này đều giống nhau trên các shell.Bây giờ bạn đã biết bạn sẽ là cái vỏ nàosử dụng, chúng ta hãy đi vào cách viết bằng Bash.Như chúng ta đã thảo luận ở phần trước,giao tiếp với hệ điều hành của bạn giống như một cuộc trò chuyện.Bạn gõ lệnh và hệ điều hànhđáp lại bằng một câu trả lời cho lệnh của bạn.Một lệnh là một hướng dẫnyêu cầu máy tính làm điều gì đó.

|  |
| --- |
| We'll try out a command in Bash. Notice a dollar sign before the cursor. This is your prompt to enter a new command. Some commands might tell the computer to find something like a specific file. Others might tell it to launch a program. Or, it might be to output a specific string of text. In the last section, when we discussed input and output, we explored how the echo command did this. |

Chúng ta sẽ thử một lệnh trong Bash.Chú ý ký hiệu đô la trước con trỏ.Đây là lời nhắc của bạn để nhập một lệnh mới.Một số lệnh có thể yêu cầu máy tính thực hiệntìm một cái gì đó giống như một tập tin cụ thể.Những người khác có thể bảo nó khởi chạy một chương trình.Hoặc có thể là xuất ra một chuỗi văn bản cụ thể.Trong phần cuối cùng,khi chúng ta thảo luận về đầu vào và đầu ra,chúng tôi đã khám phá cách lệnh echo thực hiện điều này.

|  |
| --- |
| Let's input the echo command again. You may notice that the command we just input is not complete. If we're going to use the echo command to output a specific string of texts, we need to specify what the string of text is. This is what arguments are for. An argument is specific information needed by a command. Some commands take multiple arguments. So now let's complete the echo command with an argument. We're learning some pretty technical stuff, so how about we output the words: "You are doing great!" We'll add this argument, and then we'll press enter to get the output. |

Hãy nhập lại lệnh echo.Bạn có thể nhận thấy rằng lệnhchúng tôi chỉ nhập vào là chưa hoàn thành.Nếu chúng ta định sử dụng lệnh echođể xuất ra một chuỗi cụ thể củatext, chúng ta cần xác định chuỗi văn bản là gì.Đây chính là lý do để tranh luận.Đối số là thông tin cụ thể cần thiết cho một lệnh.Một số lệnh có nhiều đối số.Vì vậy bây giờ chúng ta hãy hoàn thành lệnh echo bằng một đối số.Chúng tôi đang học một số nội dung khá kỹ thuật,vậy sao chúng ta không xuất ra dòng chữ: "Bạn đang làm rất tốt!"Chúng tôi sẽ thêm đối số này vàsau đó chúng ta sẽ nhấn enter để có kết quả.

|  |
| --- |
| In this example, our argument was a string of text. Arguments can provide other types of information as well. One thing that is really important in Linux is that all commands and arguments are case sensitive. This includes file and directory names. Keep that in mind as you learn more about how to use Linux in your day-to-day tasks as a security analyst. Okay, now that we've covered the basics of entering Linux commands and arguments through the Bash shell, we're ready to learn some specific commands. This is exciting, so let's get to our next video! |

Trong ví dụ này, đối số của chúng tôi là một chuỗi văn bản.Các lập luận cũng có thể cung cấp các loại thông tin khác.Một điều thực sự quan trọng trong Linux làtất cả các lệnh và đối số đều phân biệt chữ hoa chữ thường.Điều này bao gồm tên tập tin và thư mục.Hãy ghi nhớ điều đó khi bạn tìm hiểu thêm về cáchsử dụng Linux trong công việc hàng ngày của bạn với tư cách là nhà phân tích bảo mật.Được rồi, bây giờ chúng ta đã trình bày những điều cơ bản vềnhập các lệnh và đối số Linuxthông qua vỏ Bash, chúng tôi đã sẵn sàngđể tìm hiểu một số lệnh cụ thể.Điều này thật thú vị, vì vậy hãy chuyển sang video tiếp theo của chúng tôi!

***1.3. Core commands for navigation and reading files – Các lệnh cốt lõi để điều hướng và đọc tệp***

|  |
| --- |
| 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. |

Chào mừng trở lại. Tôi hy vọng bạn đang họcrất nhiều về cách giao tiếp với hệ điều hành Linux.Khi chúng tôi tiếp tục cuộc hành trình vàosử dụng dòng lệnh Linux,chúng tôi sẽ tập trung vào cách điều hướng hệ thống tệp Linux.

|  |
| --- |
| 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. |

Bây giờ tôi muốn bạn tưởng tượng một cái cây.Bạn chú ý đến điều gì đầu tiên ở cái cây?Bạn sẽ nói thân cây hay cành cây?Những điều này chắc chắn có thể thu hút sự chú ý của bạn,nhưng còn gốc rễ của nó thì sao?Mọi thứ về một cái cây đều bắt đầu từ rễ.Điều tương tự xảy ra khi chúng tahãy nghĩ về hệ thống tập tin Linux.

|  |
| --- |
| 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. |

Trước đây chúng ta đã tìm hiểu vềcác thành phần của kiến ​​trúc Linux.Tiêu chuẩn phân cấp hệ thống tập tin,hoặc FHS, làthành phần của hệ điều hành Linux tổ chức dữ liệu.Hệ thống tập tin này làmột phần rất quan trọng của Linux vìmọi thứ chúng tôi làm trong Linux đều được xem xétmột tập tin ở đâu đó trong thư mục của hệ thống.FHS là một hệ thống phân cấp,và giống như với một cái cây,mọi thứ đều phát triển và đâm nhánh từ gốc.Thư mục gốc làthư mục cấp cao nhất trong Linux.Nó được chỉ định bởi một dấu gạch chéo duy nhất.Các thư mục con phân nhánh từ thư mục gốc.Các thư mục con phân nhánhngày càng xa khỏi thư mục gốc.Khi mô tả cấu trúc thư mục trong Linux, dấu gạch chéođược sử dụng khi truy tìmxuyên qua các nhánh này để trở về gốc.Ví dụ, ở đây,dấu gạch chéo đầu tiên cho biết thư mục gốc.Sau đó, nó phân nhánh một cấp vào thư mục con chính.Một dấu gạch chéo khác cho biết nó đang phân nhánh trở lại.Lần này là đểthư mục con của nhà phân tích nằm trong nhà.Khi làm việc trong lĩnh vực an ninh,điều cần thiết là bạn phải học cách định hướngmột hệ thống tập tin để định vị và phân tích nhật ký,chẳng hạn như các tập tin nhật ký.Bạn sẽ phân tích các tệp nhật ký này đểsử dụng và xác thực ứng dụng.

|  |
| --- |
| 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. |

Với nền tảng đó, giờ đây chúng ta đã sẵn sàng để họccác lệnh thường dùngđể điều hướng hệ thống tập tin.Đầu tiên, pwd in thư mục làm việc lên màn hình.Khi bạn sử dụng lệnh này,đầu ra cho bạn biết bạn hiện đang ở thư mục nào.Tiếp theo, ls hiển thị tên của các tập tin vàthư mục trong thư mục làm việc hiện tại. Và cuối cùng,cd điều hướng giữa các thư mục.Đây là lệnh bạn sẽ sử dụngkhi bạn muốn thay đổi thư mục.

|  |
| --- |
| 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. |

Hãy sử dụng các lệnh này trong Bash.Đầu tiên chúng ta sẽ gõ lệnhpwd để hiển thị vị trí hiện tại rồi nhấn enter.Đầu ra là đường dẫn đếnthư mục phân tích nơi chúng tôi hiện đang làm việc.Tiếp theo, hãy nhập ls để hiển thịcác tập tin và thư mục trong thư mục phân tích.Đầu ra là tên củabốn thư mục: logs, oldreports,dự án, báo cáo và một tệp có tên Updates.txt.Vì vậy, giả sử bây giờ chúng ta muốn đi sâu vàothư mục nhật ký để kiểm tra truy cập trái phép.Chúng tôi sẽ nhập: nhật ký cdđể thay đổi thư mục.Chúng tôi sẽ không nhận được bất kỳ đầu ra nàotrên màn hình từ lệnh cd,nhưng nếu chúng ta nhập lại pwd,đầu ra của nó chỉ ra rằng thư mục làm việc là nhật ký.Nhật ký là thư mục con của thư mục phân tích.

|  |
| --- |
| 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. |

Là một nhà phân tích chứng khoán,bạn cũng sẽ cần biết cáchđọc nội dung tập tin trong Linux.Ví dụ, bạn có thể cần đọccác tập tin chứa cài đặt cấu hình đểxác định các lỗ hổng tiềm ẩn. Hoặc, bạn có thể nhìntại báo cáo truy cập của người dùngtrong khi điều tra truy cập trái phép.Khi đọc nội dung tập tin,có một số lệnh sẽ giúp bạn.Đầu tiên, cat hiển thị nội dung của một tập tin.Điều này rất hữu ích nhưng đôi khi bạnsẽ không muốn toàn bộ nội dung của một tệp lớn.Trong những trường hợp này, bạn có thể sử dụng lệnh head.Nó chỉ hiển thị phần đầu củamột tập tin, theo mặc định mười dòng.

|  |
| --- |
| 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. |

Hãy thử các lệnh này.Hãy tưởng tượng rằng chúng ta muốn đọc nội dung củaaccess.txt và chúng tôiđã có trong thư mục làm việc nơi nó nằm.Đầu tiên, chúng ta nhập lệnh catrồi theo sau là tên của tập tin,truy cập.txt. VàBash trả về toàn bộ nội dung của tệp này.Hãy so sánh điều đó với lệnh head.Khi chúng ta nhập lệnh head theo sau là tên tệp của chúng ta,chỉ có 10 dòng đầu tiên của tập tin này được hiển thị.

|  |
| --- |
| 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. |

Wow, phần này có rất nhiềuhành động, và đó mới chỉ là sự khởi đầu!Tôi rất vui vì bạn đã biết cách các nhà phân tích chứng khoán có thể sử dụngcác lệnh cần thiết để điều hướng hệ thống.Tiếp theo, chúng ta sẽ khám phá cách quản lý hệ thống.

***1.4. Navigate Linux and read file content – Điều hướng Linux và đọc nội dung tệp***

|  |
| --- |
| **Navigate Linux and read file content** |

**Điều hướng Linux và đọc nội dung tệp**

|  |
| --- |
| In this reading, you’ll review how to navigate the file system using Linux commands in Bash. You’ll further explore the organization of the Linux Filesystem Hierarchy Standard, review several common Linux commands for navigation and reading file content, and learn a couple of new commands. |

Trong bài đọc này, bạn sẽ xem lại cách điều hướng hệ thống tệp bằng các lệnh Linux trong Bash. Bạn sẽ khám phá thêm về cách tổ chức Tiêu chuẩn phân cấp hệ thống tệp Linux, xem xét một số lệnh Linux phổ biến để điều hướng và đọc nội dung tệp cũng như tìm hiểu một số lệnh mới.

|  |
| --- |
| **Filesystem Hierarchy Standard (FHS)** |

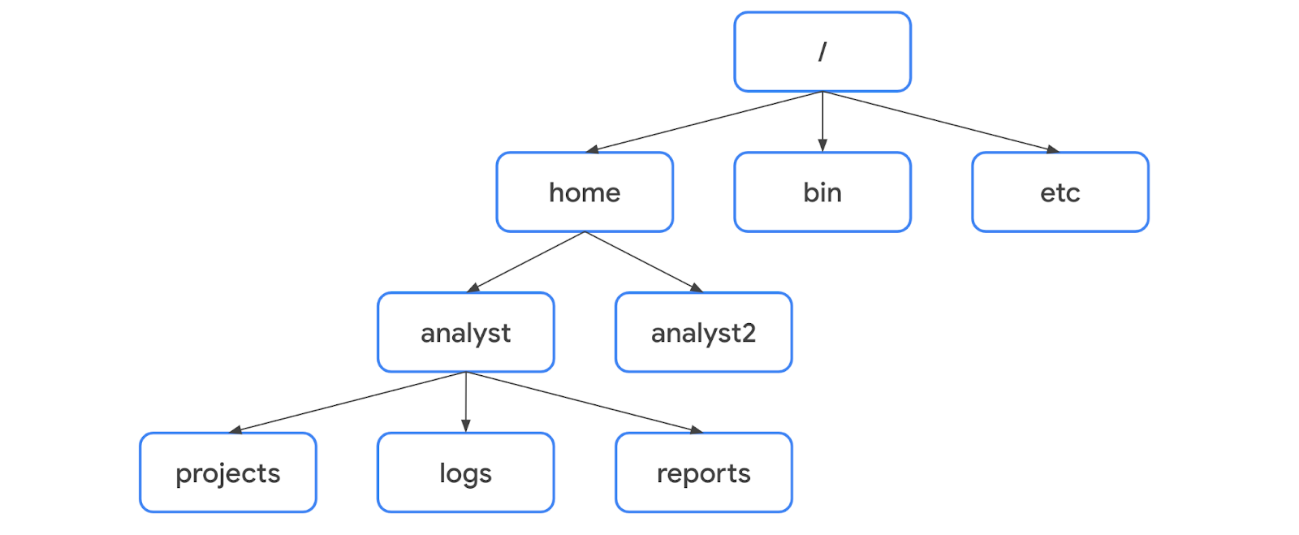
**Tiêu chuẩn phân cấp hệ thống tập tin (FHS)**

|  |
| --- |
| Previously, you learned that the **Filesystem Hierarchy Standard** **(FHS)** is the component of Linux that organizes data. The FHS is important because it defines how directories, directory contents, and other storage is organized in the operating system. |

Trước đây, bạn đã biết rằng **Tiêu chuẩn phân cấp hệ thống tập tin (FHS)** là thành phần của Linux giúp tổ chức dữ liệu. FHS rất quan trọng vì nó xác định cách tổ chức các thư mục, nội dung thư mục và các bộ lưu trữ khác trong hệ điều hành.

|  |
| --- |
| This diagram illustrates the hierarchy of relationships under the FHS: |

Sơ đồ này minh họa hệ thống phân cấp của các mối quan hệ trong FHS:



|  |
| --- |
| Under the FHS, a file’s location can be described by a file path. A **file path** is the location of a file or directory. In the file path, the different levels of the hierarchy are separated by a forward slash (**/**). |

Theo FHS, vị trí của tệp có thể được mô tả bằng đường dẫn tệp. Đường **dẫn tệp** là vị trí của tệp hoặc thư mục. Trong đường dẫn tệp, các cấp độ khác nhau của hệ thống phân cấp được phân tách bằng dấu gạch chéo lên ( **/** ).

|  |
| --- |
| **Root directory** |

**Thư mục gốc**

|  |
| --- |
| The **root directory** is the highest-level directory in Linux, and it’s always represented with a forward slash (**/**).  All subdirectories branch off the root directory. Subdirectories can continue branching out to as many levels as necessary. |

Thư **mục gốc** là thư mục cấp cao nhất trong Linux và nó luôn được biểu thị bằng dấu gạch chéo lên ( **/** ). Tất cả các thư mục con đều phân nhánh ra khỏi thư mục gốc. Các thư mục con có thể tiếp tục phân nhánh theo nhiều cấp độ nếu cần thiết.

|  |
| --- |
| **Standard FHS directories** |

**Thư mục FHS tiêu chuẩn**

|  |
| --- |
| Directly below the root directory, you’ll find standard FHS directories. In the diagram, **home**, **bin**, and **etc** are standard FHS directories. Here are a few examples of what standard directories contain: |

Ngay bên dưới thư mục gốc, bạn sẽ tìm thấy các thư mục FHS tiêu chuẩn. Trong sơ đồ, **home** , **bin** , **v.v.** là các thư mục FHS tiêu chuẩn. Dưới đây là một vài ví dụ về những gì thư mục tiêu chuẩn chứa:

|  |
| --- |
| * **/home**: Each user in the system gets their own home directory. * **/bin**: This directory stands for “binary” and contains binary files and other executables. Executables are files that contain a series of commands a computer needs to follow to run programs and perform other functions. * **/etc**: This directory stores the system’s configuration files. * **/tmp**: This directory stores many temporary files. The **/tmp** directory is commonly used by attackers because anyone in the system can modify data in these files. * **/mnt**: This directory stands for “mount” and stores media, such as USB drives and hard drives. |

* **/home** : Mỗi người dùng trong hệ thống có thư mục chính của riêng mình.
* **/bin** : Thư mục này là viết tắt của “nhị phân” và chứa các tệp nhị phân và các tệp thực thi khác. Tệp thực thi là các tệp chứa một loạt lệnh mà máy tính cần tuân theo để chạy chương trình và thực hiện các chức năng khác.
* **/etc** : Thư mục này lưu trữ các file cấu hình của hệ thống.
* **/tmp** : Thư mục này lưu trữ nhiều file tạm thời. Thư mục **/tmp** thường được những kẻ tấn công sử dụng vì bất kỳ ai trong hệ thống đều có thể sửa đổi dữ liệu trong các tệp này.
* **/mnt** : Thư mục này là viết tắt của “mount” và lưu trữ phương tiện, chẳng hạn như ổ USB và ổ cứng.

|  |
| --- |
| **Pro Tip**: You can use the **man hier** command to learn more about the FHS and its standard directories. |

**Mẹo chuyên nghiệp** : Bạn có thể sử dụng lệnh **man hier** để tìm hiểu thêm về FHS và các thư mục tiêu chuẩn của nó.

|  |
| --- |
| **User-specific subdirectories** |

**Thư mục con dành riêng cho người dùng**

|  |
| --- |
| Under **home** are subdirectories for specific users. In the diagram, these users are  **analyst** and **analyst2**. Each user has their own personal subdirectories, such as **projects**, **logs**, or **reports**. |

Dưới **nhà** là các thư mục con dành cho người dùng cụ thể. Trong sơ đồ, những người dùng này là   **nhà phân tích** và **nhà phân tích2** . Mỗi người dùng có các thư mục con cá nhân của riêng họ, chẳng hạn như **dự án** , **nhật ký** hoặc **báo cáo** .

|  |
| --- |
| **Note:** When the path leads to a subdirectory below the user’s home directory, the user’s home directory can be represented as the tilde (**~**). For example, **/home/analyst/logs** can also be represented as **~/logs**. |

**Lưu ý:** Khi đường dẫn dẫn đến thư mục con bên dưới thư mục chính của người dùng, thư mục chính của người dùng có thể được biểu thị dưới dạng dấu ngã ( **~** ). Ví dụ: **/home/analyst/logs** cũng có thể được biểu diễn dưới dạng **~/logs** .

|  |
| --- |
| You can navigate to specific subdirectories using their absolute or relative file paths. The **absolute file path** is the full file path, which starts from the root. For example, **/home/analyst/projects** is an absolute file path. The **relative file path** is the file path that starts from a user's current directory. |

Bạn có thể điều hướng đến các thư mục con cụ thể bằng cách sử dụng đường dẫn tệp tuyệt đối hoặc tương đối của chúng. Đường **dẫn tệp tuyệt đối** là đường dẫn tệp đầy đủ, bắt đầu từ thư mục gốc. Ví dụ: **/home/analyst/projects** là đường dẫn tệp tuyệt đối. Đường **dẫn tệp tương đối** là đường dẫn tệp bắt đầu từ thư mục hiện tại của người dùng.

|  |
| --- |
| **Note:** Relative file paths can use a dot (**.**) to represent the current directory, or two dots (**..**) to represent the parent of the current directory. An example of a relative file path could be **../projects**. |

**Lưu ý:** Đường dẫn tệp tương đối có thể sử dụng dấu chấm ( **.** ) để biểu thị thư mục hiện tại hoặc hai dấu chấm ( **..** ) để biểu thị thư mục mẹ của thư mục hiện tại. Một ví dụ về đường dẫn tệp tương đối có thể là **../projects** .

|  |
| --- |
| **Key commands for navigating the file system** |

**Các lệnh chính để điều hướng hệ thống tập tin**

|  |
| --- |
| The following Linux commands can be used to navigate the file system: **pwd**, **ls**, and **cd**. |

Các lệnh Linux sau đây có thể được sử dụng để điều hướng hệ thống tệp: **pwd** , **ls** và **cd**.

|  |
| --- |
| **pwd** |

**pwd**

|  |
| --- |
| The **pwd** command prints the working directory to the screen. Or in other words, it returns the directory that you’re currently in. |

Lệnh **pwd** in thư mục làm việc ra màn hình. Hay nói cách khác, nó trả về thư mục mà bạn hiện đang ở.

|  |
| --- |
| The output gives you the absolute path to this directory. For example, if you’re in your **home** directory and your username is **analyst**, entering **pwd** returns **/home/analyst**. |

Đầu ra cung cấp cho bạn đường dẫn tuyệt đối đến thư mục này. Ví dụ: nếu bạn đang ở trong thư mục **chính** và tên người dùng của bạn là **nhà phân tích** , việc nhập **pwd** sẽ trả về **/home/analyst** .

|  |
| --- |
| **Pro Tip**: To learn what your username is, use the **whoami** command. The **whoami** command returns the username of the current user. For example, if your username is **analyst**, entering **whoami** returns **analyst**. |

**Mẹo chuyên nghiệp** : Để tìm hiểu tên người dùng của bạn là gì, hãy sử dụng lệnh **whoami** . Lệnh **whoami** trả về tên người dùng của người dùng hiện tại. Ví dụ: nếu tên người dùng của bạn là **nhà phân tích** , nhập **whoami** sẽ trả về **nhà phân tích** .

|  |
| --- |
| **ls** |

**ls**

|  |
| --- |
| The **ls** command displays the names of the files and directories in the current working directory. For example, in the video, **ls** returned directories such as **logs**, and a file called **updates.txt**. |

Lệnh **ls** hiển thị tên của các tập tin và thư mục trong thư mục làm việc hiện tại. Ví dụ: trong video, **ls** trả về các thư mục như **logs** và một tệp có tên **Updates.txt** .

|  |
| --- |
| **Note**: If you want to return the contents of a directory that’s not your current working directory, you can add an argument after **ls** with the absolute or relative file path to the desired directory. For example, if you’re in the **/home/analyst** directory but want to list the contents of its **projects** subdirectory, you can enter **ls /home/analyst/projects** or just **ls projects**. |

**Lưu ý** : Nếu bạn muốn trả về nội dung của một thư mục không phải là thư mục làm việc hiện tại của bạn, bạn có thể thêm một đối số sau **ls** với đường dẫn tệp tuyệt đối hoặc tương đối vào thư mục mong muốn. Ví dụ: nếu bạn đang ở trong thư mục **/home/analyst** nhưng muốn liệt kê nội dung của thư mục **con dự án** của nó , bạn có thể nhập **ls /home/analyst/projects** hoặc chỉ **lsprojects** .

|  |
| --- |
| **cd** |

**đĩa CD**

|  |
| --- |
| The **cd** command navigates between directories. When you need to change directories, you should use this command. |

Lệnh **cd** điều hướng giữa các thư mục. Khi bạn cần thay đổi thư mục, bạn nên sử dụng lệnh này.

|  |
| --- |
| To navigate to a subdirectory of the current directory, you can add an argument after **cd** with the subdirectory name. For example, if you’re in the **/home/analyst** directory and want to navigate to its **projects** subdirectory, you can enter **cd projects**. |

Để điều hướng đến thư mục con của thư mục hiện tại, bạn có thể thêm đối số sau **cd** với tên thư mục con. Ví dụ: nếu bạn đang ở trong thư mục **/home/analyst** và muốn điều hướng đến thư mục **con dự án** của nó , bạn có thể nhập **dự án cd** .

|  |
| --- |
| You can also navigate to any specific directory by entering the absolute file path. For example, if you’re in **/home/analyst/projects**, entering **cd /home/analyst/logs** changes your current directory to **/home/analyst/logs**. |

Bạn cũng có thể điều hướng đến bất kỳ thư mục cụ thể nào bằng cách nhập đường dẫn tệp tuyệt đối. Ví dụ: nếu bạn đang ở **/home/analyst/projects** , việc nhập **cd /home/analyst/logs** sẽ thay đổi thư mục hiện tại của bạn thành **/home/analyst/logs** .

|  |
| --- |
| **Pro Tip**: You can use the relative file path and enter **cd ..** to go up one level in the file structure. For example, if the current directory is **/home/analyst/projects**, entering **cd ..** would change your working directory to **/home/analyst**. |

**Mẹo chuyên nghiệp** : Bạn có thể sử dụng đường dẫn tệp tương đối và nhập **cd ..** để tăng một cấp trong cấu trúc tệp. Ví dụ: nếu thư mục hiện tại là **/home/analyst/projects** , việc nhập **cd ..** sẽ thay đổi thư mục làm việc của bạn thành **/home/analyst** .

|  |
| --- |
| **Common commands for reading file content** |

**Các lệnh phổ biến để đọc nội dung file**

|  |
| --- |
| The following Linux commands are useful for reading file content: **cat**, **head**, **tail**, and **less**. |

Các lệnh Linux sau đây rất hữu ích để đọc nội dung tệp: **cat** , **head** , **tail** và **less** .

|  |
| --- |
| **cat** |

**cat**

|  |
| --- |
| The **cat** command displays the content of a file. For example, entering **cat updates.txt** returns everything in the **updates.txt** file. |

Lệnh **cat** hiển thị nội dung của một tập tin. Ví dụ: nhập **catupdates.txt** sẽ trả về mọi thứ trong tệp **Updates.txt** .

|  |
| --- |
| **head** |

**head**

|  |
| --- |
| The **head** command displays just the beginning of a file, by default 10 lines. The **head** command can be useful when you want to know the basic contents of a file but don’t need the full contents. Entering **head updates.txt** returns only the first 10 lines of the **updates.txt** file. |

Lệnh **head** chỉ hiển thị phần đầu của tệp, theo mặc định là 10 dòng. Lệnh **head** có thể hữu ích khi bạn muốn biết nội dung cơ bản của một tập tin nhưng không cần nội dung đầy đủ. Nhập **headupdate.txt** chỉ trả về 10 dòng đầu tiên của **fileupdate.txt** .

|  |
| --- |
| **Pro Tip**: If you want to change the number of lines returned by **head**, you can specify the number of lines by including **-n**. For example, if you only want to display the first five lines of the **updates.txt** file, enter **head -n 5 updates.txt**. |

**Mẹo chuyên nghiệp** : Nếu bạn muốn thay đổi số dòng được trả về bởi **head** , bạn có thể chỉ định số dòng bằng cách bao gồm **-n** . Ví dụ: nếu bạn chỉ muốn hiển thị năm dòng đầu tiên của tệp **Updates.txt** , hãy nhập **head -n 5 Updates.txt** .

|  |
| --- |
| **tail** |

**tail**

|  |
| --- |
| The **tail** command does the opposite of **head**. This command can be used to display just the end of a file, by default 10 lines. Entering **tail updates.txt** returns only the last 10 lines of the **updates.txt** file. |

Lệnh **tail** thực hiện ngược lại với **head** . Lệnh này có thể được sử dụng để chỉ hiển thị phần cuối của tệp, theo mặc định là 10 dòng. Nhập **tailupdates.txt** chỉ trả về 10 dòng cuối cùng của **fileupdate.txt** .

|  |
| --- |
| **Pro Tip**: You can use **tail** to read the most recent information in a log file. |

**Mẹo chuyên nghiệp** : Bạn có thể sử dụng **tail** để đọc thông tin mới nhất trong tệp nhật ký.

|  |
| --- |
| **less** |

**less**

|  |
| --- |
| The **less** command returns the content of a file one page at a time. For example, entering **less updates.txt** changes the terminal window to display the contents of **updates.txt** one page at a time. This allows you to easily move forward and backward through the content. |

Lệnh **less** trả về nội dung của một tệp tại một thời điểm. Ví dụ: nhập **less Updates.txt** sẽ thay đổi cửa sổ terminal để hiển thị nội dung của **Updates.txt** từng trang một. Điều này cho phép bạn dễ dàng di chuyển tiến và lùi thông qua nội dung.

|  |
| --- |
| Once you’ve accessed your content with the **less** command, you can use several keyboard controls to move through the file: |

Sau khi truy cập nội dung của mình bằng lệnh **less** , bạn có thể sử dụng một số điều khiển bàn phím để di chuyển qua tệp:

|  |
| --- |
| * **Space bar**: Move forward one page * **b**: Move back one page * **Down arrow**: Move forward one line * **Up arrow**: Move back one line * **q**: Quit and return to the previous terminal window |

* **Phím cách** : Di chuyển về phía trước một trang
* **b** : Lùi lại một trang
* **Mũi tên xuống** : Tiến lên một dòng
* **Mũi tên lên** : Di chuyển lùi một dòng
* **q** : Thoát và quay lại cửa sổ terminal trước đó

|  |
| --- |
| **Key takeaways** |

**Bài học chính**

|  |
| --- |
| It’s important for security analysts to be able to navigate Linux and the file system of the FHS. Some key commands for navigating the file system include **pwd**, **ls**, and **cd**. Reading file content is also an important skill in the security profession. This can be done with commands such as **cat**, **head**, **tail**, and **less**. |

Điều quan trọng đối với các nhà phân tích bảo mật là có thể điều hướng Linux và hệ thống tệp của FHS. Một số lệnh chính để điều hướng hệ thống tệp bao gồm **pwd** , **ls** và **cd** . Đọc nội dung file cũng là một kỹ năng quan trọng trong nghề bảo mật. Điều này có thể được thực hiện bằng các lệnh như **cat** , **head** , **tail** và **less** .

***1.5. Activity: Find files with Linux commands – Hoạt động: Tìm file bằng lệnh Linux***

***1.6. Optional Exemplar: Find files with Linux commands – Mẫu tùy chọn: Tìm tệp bằng lệnh Linux***

***1.7. Test your knowledge: Navigate the Linux file system in Bash – Kiểm tra kiến ​​thức của bạn: Điều hướng hệ thống tệp Linux trong Bash***

**2. Manage file content in Bash – Quản lý nội dung file trong Bash**

***2.1. Find what you need with Linux – Tìm những gì bạn cần với Linux***

|  |
| --- |
| Now that we covered: pwd, ls, and cd and are familiar with these basic commands for navigating the Linux file system, let's look at a couple of ways to find what you need within this system. As a security analyst, your work will likely involve filtering for the information you need. Filtering means searching your system for specific information that can help you solve complex problems. For example, imagine that your team determines a piece of malware contains a string of characters. You might be tasked with finding other files with the same string to determine if those files contain the same malware. Later, we'll learn more about how you can use SQL to filter a database, but Linux is a good place to start basic filtering. |

Bây giờ chúng ta đã đề cập đến: pwd, ls,và cd và quen thuộc vớinhững lệnh cơ bản này đểđiều hướng hệ thống tập tin Linux,chúng ta hãy xem xét một vài cách đểtìm thấy những gì bạn cần trong hệ thống này.Là một nhà phân tích chứng khoán,công việc của bạn có thể sẽ liên quan đếnlọc thông tin bạn cần.Lọc có nghĩa là tìm kiếm hệ thống của bạnthông tin cụ thể có thểgiúp bạn giải quyết những vấn đề phức tạp.Ví dụ, hãy tưởng tượng rằng nhóm của bạnxác định một phầnphần mềm độc hại chứa một chuỗi ký tự.Bạn có thể được giao nhiệm vụ tìm các tệp khác bằngcùng một chuỗi để xác định xemnhững tệp đó chứa cùng một phần mềm độc hại.Sau này chúng ta sẽ tìm hiểu thêm về cáchbạn có thể sử dụng SQL để lọc cơ sở dữ liệu,nhưng Linux là nơi tốt để bắt đầu quá trình lọc cơ bản.

|  |
| --- |
| First, we'll start with grep. The grep command searches a specified file and returns all lines in the file containing a specified string. Here's an example of this. Let's say we have a file called updates.txt, and we're currently looking for lines that contain the word: OS. If the file is large, it would take a long time to visually scan for this. Instead, after navigating to the directory that contains updates.txt, we'll type the command: grep OS updates.txt into the shell. Notice how the grep command is followed by two arguments. The first argument is the string we're searching for; in this case, OS. The second argument is the name of the file we're searching through, updates.txt. When we press enter, Bash returns all lines containing the word OS. |

Đầu tiên, chúng ta sẽ bắt đầu với grep.Lệnh grep tìm kiếm một tệp được chỉ định vàtrả về tất cả các dòng trongtập tin chứa một chuỗi được chỉ định.Đây là một ví dụ về điều này.Giả sử chúng ta có một tệp có tên là update.txt,và chúng tôi hiện đang tìm kiếm những dòngchứa từ: OS.Nếu tập tin lớn,sẽ mất nhiều thời gian để quét trực quan cho điều này.Thay vào đó, sau khi điều hướng đếnthư mục chứa Updates.txt,chúng ta sẽ gõ lệnh:grep OSupdates.txt vào shell.Lưu ý lệnh grep được theo sau bởi hai đối số.Đối số đầu tiên là chuỗi chúng ta đang tìm kiếm;trong trường hợp này, hệ điều hành.Đối số thứ hai là tên của tập tinchúng tôi đang tìm kiếm thông qua,update.txt.Khi chúng ta nhấn enter,Bash trả về tất cả các dòng có chứa từ OS.

|  |
| --- |
| Now let's talk about piping. Piping is a Linux command that can be used for a variety of purposes. In a moment, we'll focus on how it can be used for filtering. But first, let's talk about the general idea of piping. The piping command sends a standard output of one command as standard input into another command for further processing. It's represented by the vertical bar character. In our context, we can refer to this as the pipe character. Take a moment and imagine a physical pipe. Physical pipes have two ends. On one end, for example, water might enter the pipe from a hot water tank. Then, it travels through the pipe and comes out on the other end in a sink. Similarly, in Linux, piping also involves redirection. Output from one command is sent through the pipe and then is used on the other side of the pipe. Earlier in this video, I explained how grep can be used to filter for strings of characters within a file. Grep can also be incorporated after a pipe. |

Bây giờ hãy nói về đường ống.Piping là một lệnh Linuxcó thể được sử dụng cho nhiều mục đích khác nhau.Trong giây lát, chúng ta sẽ tập trung vàolàm thế nào nó có thể được sử dụng để lọc.Nhưng trước tiên, hãy nói về ý tưởng chung về đường ống.Lệnh đường ống gửi một đầu ra tiêu chuẩn củamột lệnh làm đầu vào tiêu chuẩnvào một lệnh khác để xử lý tiếp.Nó được biểu thị bằng ký tự thanh dọc.Trong bối cảnh của chúng tôi,chúng ta có thể gọi đây là ký tự ống.Hãy dành một chút thời gian và tưởng tượng một đường ống vật lý.Ống vật lý có hai đầu.Ở một đầu, ví dụ,nước có thể đi vào đường ống từ bình nước nóng.Sau đó, nó đi qua đường ống vàđi ra ở đầu bên kia trong bồn rửa.Tương tự, trong Linux,đường ống cũng liên quan đến việc chuyển hướng.Đầu ra từ một lệnh được gửi quađường ống và sau đó được sử dụng ở phía bên kia của đường ống.Trước đó trong video này,Tôi đã giải thích cách sử dụng grep để lọcchuỗi ký tự trong một tập tin.Grep cũng có thể được kết hợp sau một đường ống.

|  |
| --- |
| Let's focus on this example. The first command, ls, instructs the operating system to output the file and directory contents of their reports subdirectory. But because the command is followed by the pipe, the output isn't returned to the screen. Instead, it's sent to the next command. As we just learned, grep searches for a specified string of characters; in this case, it's users. But where is it searching? Since grep follows a pipe, the output of the previous command indicates where to search. In this case, that output is a list of files and directories within the reports subdirectory. It will return all files and directories that contain the word: users. |

Hãy tập trung vào ví dụ này.Lệnh đầu tiên, ls,hướng dẫn hệ điều hành xuất tập tinvà nội dung thư mục của thư mục con báo cáo của họ.Nhưng vì lệnh được theo sau bởi đường ống,đầu ra không được trả về màn hình.Thay vào đó, nó được gửi đến lệnh tiếp theo.Như chúng ta vừa học,grep tìm kiếm một chuỗi ký tự được chỉ định;trong trường hợp này, đó là người dùng.Nhưng nó đang tìm kiếm ở đâu?Vì grep đi theo một đường ống,đầu ra của lệnh trướccho biết nơi để tìm kiếm.Trong trường hợp này, đầu ra đó là một danh sáchtập tin và thư mục trong thư mục con báo cáo.Nó sẽ trả về tất cả các tập tin vàcác thư mục chứa từ: user.

|  |
| --- |
| Let's explore this in Bash. So we can better understand how the filter works, let's first output everything in the reports directory. If we were already in the directory, we would just need to input ls. But since we're not, we'll also specify the path to this directory. When we press enter, the output indicates there are seven files in the reports directory. Because we want to return only the files that contain the word users, we'll combine this ls command with piping and the grep command. As the output demonstrates, Linux has been instructed to return only files that contain the word users. The two files that don't contain this string no longer appear. |

Hãy khám phá điều này trong Bash.Để chúng ta có thể hiểu rõ hơn cách thức hoạt động của bộ lọc,trước tiên hãy xuất mọi thứ trong thư mục báo cáo.Nếu chúng ta đã có trong thư mục,chúng ta chỉ cần nhập ls.Nhưng vì chúng tôi không như vậy nên chúng tôi cũng sẽchỉ định đường dẫn đến thư mục này.Khi chúng ta nhấn enter,đầu ra cho biết cóbảy tập tin trong thư mục báo cáo.Bởi vì chúng tôi muốn quay trở lạichỉ những tệp chứa từ người dùng,chúng ta sẽ kết hợp lệnh ls nàyvới đường ống và lệnh grep.Như đầu ra chứng minh,Linux đã được hướng dẫn quay trở lạichỉ các tệp có chứa từ người dùng.Hai tập tin không chứachuỗi này không còn xuất hiện nữa.

|  |
| --- |
| So now you have two different ways that you can filter in Linux while working as an analyst. Navigating through files and filtering are just part of what you need to know. Let's keep exploring the Linux command line. |

Vì vậy bây giờ bạn có hai cách khác nhau để bạn có thểfilter trong Linux khi đang làm nhà phân tích.Điều hướng qua các tập tin vàlọc chỉ là một phần của những gì bạn cần biết.Hãy tiếp tục khám phá dòng lệnh Linux.

***2.2. Filter content in Linux – Lọc nội dung trong Linux***

|  |
| --- |
| **Filter content in Linux** |

**Lọc nội dung trong Linux**

|  |
| --- |
| In this reading, you’ll continue exploring Linux commands, which can help you filter for the information you need. You’ll learn a new Linux command, **find**, which can help you search files and directories for specific information. |

Trong bài đọc này, bạn sẽ tiếp tục khám phá các lệnh Linux, lệnh này có thể giúp bạn lọc thông tin bạn cần. Bạn sẽ học một lệnh Linux mới, **find** , lệnh này có thể giúp bạn tìm kiếm các tệp và thư mục để biết thông tin cụ thể.

|  |
| --- |
| **Filtering for information** |

**Lọc thông tin**

|  |
| --- |
| You previously explored how filtering for information is an important skill for security analysts. **Filtering** is selecting data that match a certain condition. For example, if you had a virus in your system that only affected the **.txt** files, you could use filtering to find these files quickly. Filtering allows you to search based on specific criteria, such as file extension or a string of text. |

Trước đây bạn đã khám phá việc lọc thông tin là một kỹ năng quan trọng như thế nào đối với các nhà phân tích bảo mật. **Lọc** là chọn dữ liệu phù hợp với một điều kiện nhất định. Ví dụ: nếu hệ thống của bạn có vi-rút chỉ ảnh hưởng đến các tệp **.txt** , bạn có thể sử dụng tính năng lọc để tìm các tệp này một cách nhanh chóng. Tính năng lọc cho phép bạn tìm kiếm dựa trên các tiêu chí cụ thể, chẳng hạn như đuôi tệp hoặc một chuỗi văn bản.

|  |
| --- |
| **grep** |

**grep**

|  |
| --- |
| The **grep** command searches a specified file and returns all lines in the file containing a specified string or text. The **grep** command commonly takes two arguments: a specific string to search for and a specific file to search through. |

Lệnh **grep** tìm kiếm một tệp được chỉ định và trả về tất cả các dòng trong tệp chứa chuỗi hoặc văn bản được chỉ định. Lệnh **grep** thường có hai đối số: một chuỗi cụ thể để tìm kiếm và một tệp cụ thể để tìm kiếm.

|  |
| --- |
| For example, entering **grep** **OS** **updates**.**txt** returns all lines containing **OS** in the **updates**.**txt** file. In this example, **OS** is the specific string to search for, and **updates.txt** is the specific file to search through. |

Ví dụ: nhập **grep OSupdates . txt** trả về tất cả các dòng chứa **hệ điều hành** trong **bản cập nhật** . tập tin **txt** . Trong ví dụ này, **OS** là chuỗi cụ thể để tìm kiếm và **Updates.txt** là tệp cụ thể để tìm kiếm.

|  |
| --- |
| Let’s look at another example: **grep error time\_logs.txt**. Here grep is used to search for the text pattern. **error** is the term you are looking for in the **time\_logs.txt** file. When you run this command, grep will scan the time\_logs.txt file and print only the lines containing the word **error**. |

Hãy xem một ví dụ khác: **grep error time\_logs.txt** . Ở đây grep được sử dụng để tìm kiếm mẫu văn bản. **error** là thuật ngữ bạn đang tìm kiếm trong tệp **time\_logs.txt** . Khi bạn chạy lệnh này, grep sẽ quét file time\_logs.txt và chỉ in những dòng chứa từ **error** .

|  |
| --- |
| **Piping** |

**Piping**

|  |
| --- |
| The pipe command is accessed using the pipe character (**|**). **Piping** sends the standard output of one command as standard input to another command for further processing. As a reminder, **standard output** is information returned by the OS through the shell, and **standard input** is information received by the OS via the command line. |

Lệnh ống được truy cập bằng ký tự ống ( **|** ). **Piping** gửi đầu ra tiêu chuẩn của một lệnh làm đầu vào tiêu chuẩn cho lệnh khác để xử lý tiếp. Xin nhắc lại, **đầu ra tiêu chuẩn** là thông tin được HĐH trả về thông qua shell và **đầu vào tiêu chuẩn** là thông tin được HĐH nhận được thông qua dòng lệnh.

|  |
| --- |
| The pipe character (**|**) is located in various places on a keyboard. On many keyboards, it’s located on the same key as the backslash character (**\**). On some keyboards, the **|** can look different and have a small space through the middle of the line. If you can’t find the **|**, search online for its location on your particular keyboard. |

Ký tự ống ( **|** ) nằm ở nhiều vị trí khác nhau trên bàn phím. Trên nhiều bàn phím, nó nằm trên cùng phím với ký tự dấu gạch chéo ngược ( **\** ). Trên một số bàn phím, **|** có thể trông khác và có một khoảng trống nhỏ ở giữa dòng. Nếu bạn không thể tìm thấy **|** , tìm kiếm trực tuyến vị trí của nó trên bàn phím cụ thể của bạn.

|  |
| --- |
| When used with **grep**, the pipe can help you find directories and files containing a specific word in their names. For example, **ls /home/analyst/reports | grep users** returns the file and directory names in the **reports** directory that contain **users**. Before the pipe, **ls** indicates to list the names of the files and directories in **reports**. Then, it sends this output to the command after the pipe. In this case, **grep users** returns all of the file or directory names containing **users** from the input it received. |

Khi được sử dụng với **grep** , pipe có thể giúp bạn tìm các thư mục và tệp chứa một từ cụ thể trong tên của chúng. Ví dụ: **ls /home/analyst/reports | Người dùng grep** trả về tên tệp và thư mục trong thư mục **báo cáo** chứa **người dùng** . Trước đường ống, **ls** biểu thị danh sách tên của các tập tin và thư mục trong **báo cáo** . Sau đó, nó gửi đầu ra này tới lệnh sau đường ống. Trong trường hợp này, **grep user** trả về tất cả tên tệp hoặc thư mục chứa **người dùng** từ dữ liệu đầu vào mà nó nhận được.

|  |
| --- |
| **Note:** Piping is a general form of redirection in Linux and can be used for multiple tasks other than filtering. You can think of piping as a general tool that you can use whenever you want the output of one command to become the input of another command. |

**Lưu ý:** Đường ống là một dạng chuyển hướng chung trong Linux và có thể được sử dụng cho nhiều tác vụ khác ngoài việc lọc. Bạn có thể coi đường ống như một công cụ chung mà bạn có thể sử dụng bất cứ khi nào bạn muốn đầu ra của một lệnh trở thành đầu vào của lệnh khác.

|  |
| --- |
| **find** |

**find**

|  |
| --- |
| The **find** command searches for directories and files that meet specified criteria. There’s a wide range of criteria that can be specified with **find**. For example, you can search for files and directories that |

Lệnh **find** tìm kiếm các thư mục và tập tin đáp ứng các tiêu chí đã chỉ định. Có rất nhiều tiêu chí có thể được chỉ định bằng **find** . Ví dụ: bạn có thể tìm kiếm các tập tin và thư mục

|  |
| --- |
| * Contain a specific string in the name, * Are a certain file size, or * Were last modified within a certain time frame. |

* Chứa một chuỗi cụ thể trong tên,
* Là một kích thước tập tin nhất định, hoặc
* Được sửa đổi lần cuối trong một khung thời gian nhất định.

|  |
| --- |
| When using **find**, the first argument after **find** indicates where to start searching. For example, entering **find /home/analyst/projects** searches for everything starting at the **projects** directory. |

Khi sử dụng **find** , đối số đầu tiên sau **find** cho biết nơi bắt đầu tìm kiếm. Ví dụ: nhập **find /home/analyst/projects** để tìm kiếm mọi thứ bắt đầu từ thư mục **dự án** .

|  |
| --- |
| After this first argument, you need to indicate your criteria for the search. If you don’t include a specific search criteria with your second argument, your search will likely return a lot of directories and files. |

Sau đối số đầu tiên này, bạn cần chỉ ra tiêu chí tìm kiếm của mình. Nếu bạn không bao gồm tiêu chí tìm kiếm cụ thể với đối số thứ hai, tìm kiếm của bạn có thể sẽ trả về nhiều thư mục và tệp.

|  |
| --- |
| Specifying criteria involves options. **Options** modify the behavior of a command and commonly begin with a hyphen (**-**). |

Việc chỉ định tiêu chí liên quan đến các tùy chọn. **Các tùy chọn** sửa đổi hành vi của lệnh và thường bắt đầu bằng dấu gạch nối ( **-** ).

|  |
| --- |
| **-name and -iname** |

**-name và -iname**

|  |
| --- |
| One key criteria analysts might use with **find** is to find file or directory names that contain a specific string. The specific string you’re searching for must be entered in quotes after the **-name** or **-iname** options. The difference between these two options is that **-name** is case-sensitive, and **-iname** is not. |

Một tiêu chí chính mà các nhà phân tích có thể sử dụng với **find** là tìm tên tệp hoặc thư mục có chứa một chuỗi cụ thể. Chuỗi cụ thể mà bạn đang tìm kiếm phải được nhập trong dấu ngoặc kép sau các tùy chọn **-name** hoặc **-iname** . Sự khác biệt giữa hai tùy chọn này là **-name** phân biệt chữ hoa chữ thường, còn **-iname** thì không.

|  |
| --- |
| For example, you might want to find all files in the **projects** directory that contain the word “log” in the file name. To do this, you’d enter **find /home/analyst/projects -name "\*log\*"**. You could also enter **find /home/analyst/projects -iname "\*log\*"**. |

Ví dụ: bạn có thể muốn tìm tất cả các tệp trong thư mục **dự án** có chứa từ “log” trong tên tệp. Để thực hiện việc này, bạn phải nhập **find /home/analyst/projects -name "\*log\*"** . Bạn cũng có thể nhập **find /home/analyst/projects -iname "\*log\*"** .

|  |
| --- |
| In these examples, the output would be all files in the **projects** directory that contain **log** surrounded by zero or more characters. The **"\*log\*"** portion of the command is the search criteria that indicates to search for the string “log”. When **-name** is the option, files with names that include **Log** or **LOG**, for example, wouldn’t be returned because this option is case-sensitive. However, they would be returned when **-iname** is the option. |

Trong các ví dụ này, đầu ra sẽ là tất cả các tệp trong thư mục **dự án** chứa **nhật ký** được bao quanh bởi 0 hoặc nhiều ký tự. Phần **"\*log\*"** của lệnh là tiêu chí tìm kiếm cho biết tìm kiếm chuỗi “log”. Ví dụ: khi **-name** là tùy chọn, các tệp có tên bao gồm **Log** hoặc **LOG** sẽ không được trả về vì tùy chọn này phân biệt chữ hoa chữ thường. Tuy nhiên, chúng sẽ được trả về khi **-iname** là tùy chọn.

|  |
| --- |
| **Note**: An asterisk (**\***) is used as a wildcard to represent zero or more unknown characters. |

**Lưu ý** : Dấu hoa thị ( **\*** ) được sử dụng làm ký tự đại diện để biểu thị 0 hoặc nhiều ký tự không xác định.

|  |
| --- |
| **-mtime** |

**-mtime**

|  |
| --- |
| Security analysts might also use **find** to find files or directories last modified within a certain time frame. The **-mtime** option can be used for this search. For example, entering **find /home/analyst/projects -mtime -3** returns all files and directories in the **projects** directory that have been modified within the past three days. |

Các nhà phân tích bảo mật cũng có thể sử dụng **tính năng tìm kiếm** để tìm các tệp hoặc thư mục được sửa đổi lần cuối trong một khung thời gian nhất định. Tùy chọn **-mtime** có thể được sử dụng cho tìm kiếm này. Ví dụ: nhập **find /home/analyst/projects -mtime -3** sẽ trả về tất cả các tệp và thư mục trong thư mục **dự án** đã được sửa đổi trong vòng ba ngày qua.

|  |
| --- |
| The **-mtime** option search is based on days, so entering **-mtime +1** indicates all files or directories last modified more than one day ago, and entering **-mtime -1** indicates all files or directories last modified less than one day ago. |

Tìm kiếm tùy chọn **-mtime** dựa trên số ngày, do đó, nhập **-mtime +1** cho biết tất cả các tệp hoặc thư mục được sửa đổi lần cuối cách đây hơn một ngày và nhập **-mtime -1** cho biết tất cả các tệp hoặc thư mục được sửa đổi lần cuối cách đây chưa đầy một ngày.

|  |
| --- |
| **Note:** The option **-mmin** can be used instead of **-mtime** if you want to base the search on minutes rather than days. |

**Lưu ý:** Tùy chọn **-mmin** có thể được sử dụng thay vì **-mtime** nếu bạn muốn tìm kiếm dựa trên số phút thay vì ngày.

|  |
| --- |
| **Key takeaways** |

**Bài học chính**

|  |
| --- |
| Filtering for information using Linux commands is an important skill for security analysts so that they can customize data to fit their needs. Three key Linux commands for this are **grep**, piping (**|**), and **find**. These commands can be used to navigate and filter for information in the file system. |

Lọc thông tin bằng lệnh Linux là một kỹ năng quan trọng đối với các nhà phân tích bảo mật để họ có thể tùy chỉnh dữ liệu cho phù hợp với nhu cầu của mình. Ba lệnh Linux chính cho việc này là **grep** , pipe ( **|** ) và **find** . Các lệnh này có thể được sử dụng để điều hướng và lọc thông tin trong hệ thống tệp.

***2.3. Activity: Filter with grep – Hoạt động: Lọc bằng grep***

***2.4. Optional Exemplar: Filter with grep – Mẫu tùy chọn: Lọc bằng grep***

***2.5. Create and modify directories and files – Tạo và sửa đổi thư mục và tập tin***

|  |
| --- |
| Let's make some branches! What do I mean by that? Well, in a previous video, we discussed root directories and how other subdirectories branch off of the root directory. Let's think again about the file directory system as a tree. The subdirectories are the branches of the tree. They're all connected from the same root but can grow to make a complex tree. In this video, we'll create directories and files and learn how to modify them. |

Hãy làm một số nhánh!Ý tôi là gì?À, trong video trước,chúng tôi đã thảo luận về thư mục gốc vàcác thư mục con khác phân nhánh như thế nàora khỏi thư mục gốc.Chúng ta hãy suy nghĩ lại vềhệ thống thư mục tập tin dưới dạng cây.Các thư mục con là các nhánh của cây.Tất cả đều được kết nối từ cùng một gốcnhưng có thể phát triển để tạo thành một cây phức tạp.Trong video này, chúng ta sẽ tạothư mục và tập tin cũng như tìm hiểu cách sửa đổi chúng.

|  |
| --- |
| When it comes to working with data in security, organization is key. If we know where information is located, it makes it easier to detect issues and keep information safe. In a previous video, we've already discussed navigating between directories, but let's take a moment to examine directories more closely. It's possible you're familiar with the concept of folders for organizing information. In Linux, we have directories. Directories help organize files and subdirectories. For example, within a directory for reports, an analyst may need to create two subdirectories: one for drafts and one for final reports. |

Khi nói đến việc làm việc với dữ liệu trongan ninh, tổ chức là chìa khóa.Nếu chúng ta biết thông tin nằm ở đâu,nó làm cho nó dễ dàng hơn để phát hiệnvấn đề và giữ thông tin an toàn.Trong video trước,chúng ta đã thảo luận về việc điều hướng giữa các thư mục,nhưng chúng ta hãy dành một chút thời gian đểkiểm tra các thư mục chặt chẽ hơn.Có thể bạn đã quen với khái niệm nàycác thư mục để tổ chức thông tin.Trong Linux, chúng ta có các thư mục.Thư mục giúp tổ chức các tập tin và thư mục con.Ví dụ: trong một thư mục dành cho các báo cáo,một nhà phân tích có thể cần tạo hai thư mục con:một cho bản dự thảo và một cho các báo cáo cuối cùng.

|  |
| --- |
| Now that we know why we need directories, let's take a look at some essential Linux commands for managing directories and files. First, let's take note of commands for creating and removing directories. The mkdir command creates a new directory. In contrast, rmdir removes or deletes a directory. A helpful feature of this command is its built-in warning that lets you know a directory is not empty. This saves you from accidentally deleting files. Next, you'll use other commands for creating and removing files. The touch command creates a new file, and then the rm command removes or deletes a file. And last, we have our commands for copying and moving files or directories. The mv command moves a file or directory to new location, and cp copies a file or directory into a new location. |

Bây giờ chúng ta đã biết tại sao chúng ta cần thư mục,chúng ta hãy nhìn vàomột số lệnh Linux cần thiết choquản lý thư mục và tập tin.Đầu tiên chúng ta hãy chú ý đếnlệnh tạo và xóa thư mục.Lệnh mkdir tạo một thư mục mới.Ngược lại, rmdir loại bỏ hoặc xóa một thư mục.Một tính năng hữu ích của lệnh này làcảnh báo tích hợp của nó cho phép bạnbiết một thư mục không trống.Điều này giúp bạn tránh việc vô tình xóa các tập tin.Tiếp theo, bạn sẽ sử dụngcác lệnh khác để tạo và xóa tập tin.Lệnh touch tạo một tập tin mới,và sau đó lệnh rm sẽ loại bỏ hoặc xóa một tập tin.Và cuối cùng, chúng ta có các lệnh để sao chépvà di chuyển tập tin hoặc thư mục.Lệnh mv di chuyển một tập tin hoặc thư mục tới vị trí mới,và cp sao chép một tập tin hoặc thư mục vào một vị trí mới.

|  |
| --- |
| Now, we're ready to try out these commands. First, let's use the pwd command, and then let's display the names of the files and directories in the analyst directory with the ls command. Imagine that we no longer need the oldreports directory that appears among the file contents. Let's take a look at how to remove it. We input the rmdir command and follow it with the name of the directory we want to remove: oldreports. We can use the ls command to confirm that oldreports has been deleted and no longer appears among the contents. |

Bây giờ, chúng ta đã sẵn sàng để thử các lệnh này.Đầu tiên, hãy sử dụng lệnh pwd,sau đó hãy hiển thị tên của các tập tin vàthư mục trong thư mục phân tích bằng lệnh ls.Hãy tưởng tượng rằng chúng ta không còn cầnthư mục oldreports đóxuất hiện giữa các nội dung tập tin.Chúng ta hãy xem làm thế nào để loại bỏ nó.Chúng tôi nhập lệnh rmdir và làm theo nó vớitên của thư mục chúng tôi muốn xóa: oldreports.Chúng ta có thể sử dụng lệnh ls để xác nhận rằngbáo cáo cũ đã bị xóavà không còn xuất hiện trong số các nội dung.

|  |
| --- |
| Now, let's make another change. We want a new directory for drafts of reports. We need to use the command: mkdir and specify a name for this directory: drafts. If we input ls again, we'll notice the new directory drafts included among the contents of the analyst directory. Let's change into this new directory by entering: cd drafts. If we run ls, it doesn't return any output, indicating that this directory is currently empty. But next, we'll add some files to it. Let's say we want to draft new reports on recently installed email and OS patches. To create these files, we input: touch email\_patches.txt and then: touch OS\_patches.txt. |

Bây giờ, hãy thực hiện một thay đổi khác.Chúng tôi muốn có một thư mục mới cho các bản thảo báo cáo.Chúng ta cần sử dụng lệnh: mkdirvà chỉ định tên cho thư mục này: bản nháp.Nếu chúng ta nhập lại ls,chúng ta sẽ chú ý đến các bản nháp thư mục mớiđược bao gồm trong nội dung của thư mục phân tích.Hãy thay đổi vào thư mục mới nàybằng cách nhập: bản nháp cd.Nếu chúng ta chạy ls,nó không trả về bất kỳ đầu ra nào,cho biết thư mục này hiện đang trống.Nhưng tiếp theo, chúng ta sẽ thêm một số file vào đó.Giả sử chúng ta muốn soạn thảo báo cáo mới vềcác bản vá email và hệ điều hành được cài đặt gần đây.Để tạo các tập tin này,chúng tôi nhập: touch email\_patches.txtvà sau đó: chạm vào OS\_patches.txt.

|  |
| --- |
| Running ls indicates that these files are now in the drafts directory. What if we realize that we only need a new report on OS patches and we want to delete the email patches report? To do this, we input the rm command and specify the file to delete as: email\_patches.txt. Running ls confirms that it's been deleted. Now, let's focus on our commands for moving and copying. We realized that we have a file called email policy in the reports folder that is currently in draft format. We want to move it into the newly created drafts folder. To do this, we need to change into the directory that currently has that file. |

Chạy ls chỉ ra rằngnhững tập tin này bây giờ nằm ​​trong thư mục bản nháp.Điều gì sẽ xảy ra nếu chúng tôi nhận ra rằng chúng tôi chỉ cần một báo cáo mới vềCác bản vá hệ điều hành và chúng tôi muốnđể xóa báo cáo bản vá email?Để thực hiện việc này, chúng tôi nhập lệnh rm và chỉ định tệpđể xóa dưới dạng: email\_patches.txt.Chạy ls xác nhận rằng nó đã bị xóa.Bây giờ, hãy tập trung vào các lệnh di chuyển và sao chép của chúng ta.Chúng tôi nhận ra rằng chúng tôi có một tệp có tên emailchính sách trong thư mục báo cáohiện đang ở dạng bản nháp.Chúng tôi muốn chuyển nó vào thư mục bản nháp mới tạo.Để làm điều này, chúng ta cần thay đổivào thư mục hiện có tập tin đó.

|  |
| --- |
| Running ls in that directory indicates that it contains several files, including email\_policy.txt. Then to move that file, we'll enter the mv command followed by two arguments. The first argument after mv identifies the file to be moved. The second argument indicates where to move it. If we change directories into drafts and then display its contents, we'll notice that the email policy file has been moved to this directory. We'll change back into reports. Displaying the file contents confirms that email\_policy is no longer there. |

Chạy ls trong thư mục đó chỉ ra rằng nó chứamột số tệp, bao gồm email\_policy.txt.Sau đó, để di chuyển tập tin đó,chúng ta sẽ nhập lệnh mv theo sau là hai đối số.Đối số đầu tiênsau mv xác định tập tin cần di chuyển.Đối số thứ hai cho biết nơi để di chuyển nó.Nếu chúng ta thay đổi thư mục thànhbản nháp và sau đó hiển thị nội dung của nó,chúng ta sẽ nhận thấy rằng tệp chính sách emailđã được chuyển đến thư mục này.Chúng ta sẽ chuyển lại thành báo cáo.Hiển thị nội dung tập tin xác nhận rằngemail\_policy không còn ở đó nữa.

|  |
| --- |
| Okay, one more thing. vulnerabilities.txt is a file that we want to keep in the reports directory. But since it affects an upcoming project, we also want to copy it into the project's directory. Since we're already in the directory that has this file, we'll use the cp command to copy it into the projects directory. Notice that the first argument indicates which file to copy, and the second argument provides the path to the directory that it will be copied into. When we press Enter, this copies the vulnerabilities file into the projects directory while also leaving the original within reports. Isn't it cool what we can do with these commands? |

Được rồi, còn một điều nữa. lỗ hổng.txt làmột tập tin mà chúng tôi muốn giữ trong thư mục báo cáo.Nhưng vì nó ảnh hưởng tới dự án sắp tới,chúng tôi cũng muốn sao chép nó vào thư mục của dự án.Vì chúng ta đã ở trong thư mục chứa tệp này,chúng ta sẽ sử dụng lệnh cp đểsao chép nó vào thư mục dự án.Lưu ý rằng đối số đầu tiêncho biết tập tin nào cần sao chép,và đối số thứ hai cung cấpđường dẫn đến thư mục mà nó sẽ được sao chép vào.Khi chúng ta nhấn Enter,cái này sao chép tệp lỗ hổng vàothư mục dự án đồng thờiđể lại bản gốc trong các báo cáo.Thật tuyệt vời khi chúng ta có thể làm được những lệnh này phải không?

|  |
| --- |
| Now, let's focus on one more concept related to modifying files. In addition to using commands, you can also use applications to help you edit files. As a security analyst, file editors are often necessary for your daily tasks, like writing or editing reports. A popular file editor is nano. It's good for beginners. You can access this tool through the nano command. Let's get familiar with nano together. We'll add a title to our new draft report: OS\_patches.txt. First, we change into the directory containing that file, then we input nano followed by the name of the file we want to edit: OS\_patches.txt. This brings up the nano file editor with that file open. For now, we'll just enter the title OS Patches by typing this into the editor. We need to save this before returning to the command line, and to do so, we press Ctrl+O and then enter to save it with the current file name. Then to exit, we press Ctrl+X. |

Bây giờ, hãy tập trung vàothêm một khái niệm liên quan đến sửa đổi tập tin.Ngoài việc sử dụng lệnhbạn cũng có thể sử dụng các ứng dụng để giúp bạn chỉnh sửa tập tin.Là một nhà phân tích chứng khoán,trình soạn thảo tập tin thường cần thiết chocông việc hàng ngày của bạn, như viết hoặc chỉnh sửa báo cáo.Một trình chỉnh sửa tập tin phổ biến là nano.Nó tốt cho người mới bắt đầu.Bạn có thể truy cập công cụ này thông qua lệnh nano.Hãy cùng làm quen với nano nhé.Chúng tôi sẽ thêm tiêu đề vàobáo cáo dự thảo mới của chúng tôi: OS\_patches.txt.Đầu tiên chúng ta đổi thànhthư mục chứa tập tin đó,sau đó chúng tôi nhập nanotheo sau là tên của tập tin chúng tôi muốnđể chỉnh sửa: OS\_patches.txt.Thao tác này sẽ hiển thị trình chỉnh sửa tệp nano khi tệp đó đang mở.Bây giờ chúng ta sẽ chỉ nhậptiêu đề Bản vá hệ điều hành bằng cách nhập phần này vào trình chỉnh sửa.Chúng ta cần lưu cái này trướcquay trở lại dòng lệnh và để làm như vậy,chúng ta nhấn Ctrl+Orồi enter để lưu với tên file hiện tại.Sau đó để thoát chúng ta nhấn Ctrl+X.

|  |
| --- |
| Great work! We've covered a lot of topics here—from creating and removing directories and files to copying or moving them, and just now, we've added editing files. You're well on your way to learning Linux commands! |

Công việc tuyệt vời!Chúng tôi đã đề cập đến rất nhiều chủ đề ở đây—từtạo và xóa thư mục và tập tinđể sao chép hoặc di chuyển chúng,và ngay bây giờ,chúng tôi đã thêm các tập tin chỉnh sửa.Bạn đang trên đường học các lệnh Linux!

***2.6. Manage directories and files – Quản lý thư mục và tập tin***

|  |
| --- |
| **Manage directories and files** |

**Quản lý thư mục và tập tin**

|  |
| --- |
| Previously, you explored how to manage the file system using Linux commands. The following commands were introduced: **mkdir**, **rmdir**, **touch**, **rm**, **mv**, and **cp**. In this reading, you’ll review these commands, the nano text editor, and learn another way to write to files. |

Trước đây, bạn đã khám phá cách quản lý hệ thống tệp bằng các lệnh Linux. Các lệnh sau đã được giới thiệu: **mkdir** , **rmdir** , **touch** , **rm** , **mv** và **cp** . Trong bài đọc này, bạn sẽ xem lại các lệnh này, trình soạn thảo văn bản nano và tìm hiểu một cách khác để ghi vào tệp.

|  |
| --- |
| **Creating and modifying directories** |

**Tạo và sửa đổi thư mục**

|  |
| --- |
| **mkdir** |

**mkdir**

|  |
| --- |
| The **mkdir** command creates a new directory. Like all of the commands presented in this reading, you can either provide the new directory as the absolute file path, which starts from the root, or as a relative file path, which starts from your current directory. |

Lệnh **mkdir** tạo một thư mục mới. Giống như tất cả các lệnh được trình bày trong bài đọc này, bạn có thể cung cấp thư mục mới dưới dạng đường dẫn tệp tuyệt đối, bắt đầu từ thư mục gốc hoặc dưới dạng đường dẫn tệp tương đối, bắt đầu từ thư mục hiện tại của bạn.

|  |
| --- |
| For example, if you want to create a new directory called **network** in your **/home/analyst/logs** directory, you can enter **mkdir /home/analyst/logs/network** to create this new directory. If you’re already in the **/home/analyst/logs** directory, you can also create this new directory by entering **mkdir network**. |

Ví dụ: nếu bạn muốn tạo một thư mục mới có tên **network** trong thư mục **/home/analyst/logs** của mình , bạn có thể nhập **mkdir /home/analyst/logs/network** để tạo thư mục mới này. Nếu bạn đã ở trong thư mục **/home/analyst/logs** , bạn cũng có thể tạo thư mục mới này bằng cách nhập **mkdir network** .

|  |
| --- |
| **Pro Tip**: You can use the **ls** command to confirm the new directory was added. |

**Mẹo chuyên nghiệp** : Bạn có thể sử dụng lệnh **ls** để xác nhận thư mục mới đã được thêm.

|  |
| --- |
| **rmdir** |

**rmdir**

|  |
| --- |
| The **rmdir** command removes, or deletes, a directory. For example, entering **rmdir /home/analyst/logs/network** would remove this empty directory from the file system. |

Lệnh **rmdir** loại bỏ hoặc xóa một thư mục. Ví dụ: nhập **rmdir /home/analyst/logs/network** sẽ xóa thư mục trống này khỏi hệ thống tệp.

|  |
| --- |
| **Note**: The **rmdir** command cannot delete directories with files or subdirectories inside. For example, entering **rmdir /home/analyst** returns an error message. |

**Lưu ý** : Lệnh **rmdir** không thể xóa các thư mục có file hoặc thư mục con bên trong. Ví dụ: nhập **rmdir /home/analyst** sẽ trả về thông báo lỗi.

|  |
| --- |
| **Creating and modifying files** |

**Tạo và sửa đổi tập tin**

|  |
| --- |
| **touch and rm** |

**touch and rm**

|  |
| --- |
| The **touch** command creates a new file. This file won’t have any content inside. If your current directory is **/home/analyst/reports**, entering **touch permissions.txt** creates a new file in the **reports** subdirectory called **permissions.txt**. |

Lệnh **touch** tạo một tập tin mới. Tập tin này sẽ không có bất kỳ nội dung nào bên trong. Nếu thư mục hiện tại của bạn là **/home/analyst/reports** , việc nhập **touch Permissions.txt** sẽ tạo một tệp mới trong thư mục con **báo cáo** có tên là **Permissions.txt** .

|  |
| --- |
| The **rm** command removes, or deletes, a file. This command should be used carefully because it’s not easy to recover files deleted with **rm**. To remove the permissions file you just created, enter **rm permissions.txt**. |

Lệnh **rm** loại bỏ hoặc xóa một tập tin. Lệnh này nên được sử dụng cẩn thận vì không dễ để khôi phục các tệp đã bị xóa bằng **rm** . Để xóa tệp quyền bạn vừa tạo, hãy nhập **rm Permissions.txt** .

|  |
| --- |
| **Pro Tip:** You can verify that **permissions.txt** was successfully created or removed by entering **ls**. |

**Mẹo chuyên nghiệp:** Bạn có thể xác minh rằng **Permissions.txt** đã được tạo hoặc xóa thành công bằng cách nhập **ls** .

|  |
| --- |
| **mv and cp** |

**mv và cp**

|  |
| --- |
| You can also use **mv** and **cp** when working with files. The **mv** command moves a file or directory to a new location, and the **cp** command copies a file or directory into a new location. The first argument after **mv** or **cp** is the file or directory you want to move or copy, and the second argument is the location you want to move or copy it to. |

Bạn cũng có thể sử dụng **mv** và **cp** khi làm việc với các tập tin. Lệnh **mv** di chuyển tệp hoặc thư mục đến vị trí mới và lệnh **cp** sao chép tệp hoặc thư mục vào vị trí mới. Đối số đầu tiên sau **mv** hoặc **cp** là tệp hoặc thư mục bạn muốn di chuyển hoặc sao chép và đối số thứ hai là vị trí bạn muốn di chuyển hoặc sao chép nó tới.

|  |
| --- |
| To move **permissions.txt** into the **logs** subdirectory, enter **mv permissions.txt /home/analyst/logs**. Moving a file removes the file from its original location. However, copying a file doesn’t remove it from its original location. To copy **permissions.txt** into the **logs** subdirectory while also keeping it in its original location, enter **cp permissions.txt /home/analyst/logs**. |

Để di chuyển **quyền.txt** vào thư mục **con nhật ký** , hãy nhập **mv Permissions.txt /home/analyst/logs** . Di chuyển tệp sẽ xóa tệp khỏi vị trí ban đầu của nó. Tuy nhiên, việc sao chép tệp không xóa tệp đó khỏi vị trí ban đầu. Để sao chép **quyền.txt** vào thư mục **con nhật ký** đồng thời giữ nó ở vị trí ban đầu, hãy nhập **cpquyền.txt /home/analyst/logs** .

|  |
| --- |
| **Note**: The **mv** command can also be used to rename files. To rename a file, pass the new name in as the second argument instead of the new location. For example, entering **mv permissions.txt perm.txt** renames the **permissions.txt** file to **perm.txt**. |

**Lưu ý** : Lệnh **mv** cũng có thể được sử dụng để đổi tên file. Để đổi tên tệp, hãy chuyển tên mới làm đối số thứ hai thay vì vị trí mới. Ví dụ: nhập **mv Pers.txt perm.txt** sẽ đổi tên tệp **Perm.txt** thành **perm.txt** .

|  |
| --- |
| **nano text editor** |

**soạn thảo văn bản nano**

|  |
| --- |
| **nano** is a command-line file editor that is available by default in many Linux distributions. Many beginners find it easy to use, and it’s widely used in the security profession. You can perform multiple basic tasks in nano, such as creating new files and modifying file contents. |

**nano** là trình chỉnh sửa tệp dòng lệnh có sẵn theo mặc định trong nhiều bản phân phối Linux. Nhiều người mới bắt đầu thấy nó dễ sử dụng và được sử dụng rộng rãi trong ngành bảo mật. Bạn có thể thực hiện nhiều tác vụ cơ bản trong nano, chẳng hạn như tạo tệp mới và sửa đổi nội dung tệp.

|  |
| --- |
| To open an existing file in nano from the directory that contains it, enter **nano** followed by the file name. For example, entering **nano permissions.txt** from the **/home/analyst/reports** directory opens a new nano editing window with the **permissions.txt** file open for editing. You can also provide the absolute file path to the file if you’re not in the directory that contains it. |

Để mở một tệp hiện có ở dạng nano từ thư mục chứa nó, hãy nhập **nano** theo sau là tên tệp. Ví dụ: nhập **nano Pers.txt** từ thư mục **/home/analyst/reports** sẽ mở ra một cửa sổ chỉnh sửa nano mới với tệp **Permissions.txt** được mở để chỉnh sửa. Bạn cũng có thể cung cấp đường dẫn tệp tuyệt đối tới tệp nếu bạn không có trong thư mục chứa tệp đó.

|  |
| --- |
| You can also create a new file in nano by entering **nano** followed by a new file name. For example, entering **nano authorized\_users.txt** from the **/home/analyst/reports** directory creates the **authorized\_users.txt** file within that directory and opens it in a new nano editing window. |

Bạn cũng có thể tạo một tệp mới bằng nano bằng cách nhập **nano** theo sau là tên tệp mới. Ví dụ: nhập **nano ủy quyền\_users.txt** từ thư mục **/home/analyst/reports** sẽ tạo tệp **ủy quyền\_users.txt** trong thư mục đó và mở tệp trong cửa sổ chỉnh sửa nano mới.

|  |
| --- |
| Since there isn't an auto-saving feature in nano, it’s important to save your work before exiting. To save a file in nano, use the keyboard shortcut **Ctrl + O**. You’ll be prompted to confirm the file name before saving. To exit out of nano, use the keyboard shortcut **Ctrl + X**. |

Vì không có tính năng tự động lưu trong nano nên điều quan trọng là bạn phải lưu tác phẩm của mình trước khi thoát. Để lưu tệp ở dạng nano, hãy sử dụng phím tắt **Ctrl + O** . Bạn sẽ được nhắc xác nhận tên tệp trước khi lưu. Để thoát khỏi nano, hãy sử dụng phím tắt **Ctrl +** X.

|  |
| --- |
| **Note**: Vim and Emacs are also popular command-line text editors. |

**Lưu ý** : Vim và Emacs cũng là những trình soạn thảo văn bản dòng lệnh phổ biến.

|  |
| --- |
| **Standard output redirection** |

**Chuyển hướng đầu ra tiêu chuẩn**

|  |
| --- |
| There’s an additional way you can write to files. Previously, you learned about standard input and standard output. **Standard input** is information received by the OS via the command line, and **standard output** is information returned by the OS through the shell. |

Có một cách bổ sung để bạn có thể ghi vào tập tin. Trước đây, bạn đã tìm hiểu về đầu vào tiêu chuẩn và đầu ra tiêu chuẩn. **Đầu vào tiêu chuẩn** là thông tin được HĐH nhận được thông qua dòng lệnh và **đầu ra tiêu chuẩn** là thông tin được HĐH trả về thông qua shell.

|  |
| --- |
| You’ve also learned about piping. **Piping** sends the standard output of one command as standard input to another command for further processing. It uses the pipe character (**|**). |

Bạn cũng đã học về đường ống. **Đường ống** gửi đầu ra tiêu chuẩn của một lệnh làm đầu vào tiêu chuẩn cho lệnh khác để xử lý tiếp. Nó sử dụng ký tự ống ( **|** ).

|  |
| --- |
| In addition to the pipe (**|**), you can also use the right angle bracket (**>**) and double right angle bracket (**>>**) operators to redirect standard output. |

Ngoài dấu ngoặc vuông ( **|** ), bạn cũng có thể sử dụng toán tử dấu ngoặc vuông ( **>** ) và dấu ngoặc vuông kép ( **>>** ) để chuyển hướng đầu ra tiêu chuẩn.

|  |
| --- |
| When used with **echo**, the **>** and **>>** operators can be used to send the output of **echo** to a specified file rather than the screen. The difference between the two is that **>** overwrites your existing file, and **>>** adds your content to the end of the existing file instead of overwriting it. The **>** operator should be used carefully, because it’s not easy to recover overwritten files. |

Khi được sử dụng với **echo** , các toán tử **>** và **>>** có thể được sử dụng để gửi đầu ra của **echo** tới một tệp được chỉ định thay vì màn hình. Sự khác biệt giữa hai điều này là **>** ghi đè lên tệp hiện có của bạn và **>>** thêm nội dung của bạn vào cuối tệp hiện có thay vì ghi đè lên nó. Toán tử **>** nên được sử dụng cẩn thận vì không dễ để khôi phục các tệp bị ghi đè.

|  |
| --- |
| When you’re inside the directory containing the **permissions.txt** file, entering **echo "last updated date" >> permissions.txt** adds the string “last updated date” to the file contents. Entering **echo "time" > permissions.txt** after this command overwrites the entire file contents of **permissions.txt** with the string “time”. |

Khi bạn ở trong thư mục chứa tệp **Persences.txt** , hãy nhập **echo "ngày cập nhật cuối cùng" >> Persence.txt** sẽ thêm chuỗi “ngày cập nhật cuối cùng” vào nội dung tệp. Nhập **echo "time" > Permission.txt** sau lệnh này sẽ ghi đè toàn bộ nội dung tệp của **Permissions.txt** bằng chuỗi “time”.

|  |
| --- |
| **Note:** Both the **>** and **>>** operators will create a new file if one doesn’t already exist with your specified name. |

**Lưu ý:** Cả hai toán tử **>** và **>>** sẽ tạo một tệp mới nếu tệp đó chưa tồn tại với tên bạn chỉ định.

|  |
| --- |
| **Key takeaways** |

**Bài học chính**

|  |
| --- |
| Knowing how to manage the file system in Linux is an important skill for security analysts. Useful commands for this include: **mkdir**, **rmdir**, **touch**, **rm**, **mv**, and **cp**. When security analysts need to write to files, they can use the nano text editor, or the **>** and **>>** operators. |

Biết cách quản lý hệ thống tệp trong Linux là một kỹ năng quan trọng đối với các nhà phân tích bảo mật. Các lệnh hữu ích cho việc này bao gồm: **mkdir** , **rmdir** , **touch** , **rm** , **mv** và **cp** . Khi các nhà phân tích bảo mật cần ghi vào tệp, họ có thể sử dụng trình soạn thảo văn bản nano hoặc toán tử **>** và **>>** .

***2.7. Identify: Key Linux commands – Xác định: Các lệnh Linux chính***

|  |  |
| --- | --- |
| **Command** | **Use** |
| mkdir | Creates a new directory |
| rmdir | Removes, or deletes, a directory |
| rm | Removes, or deletes, a file |
| touch | Creates a new file |
| mv | Moves a file or directory to a new location |
| cp | Copies a file or directory into a new location |

|  |  |
| --- | --- |
| **Lệnh** | **Ý nghĩa** |
| mkdir | Tạo một thư mục mới |
| rmdir | Loại bỏ hoặc xóa một thư mục |
| rm | Loại bỏ hoặc xóa một tập tin |
| touch | Tạo một tập tin mới |
| mv | Di chuyển một tập tin hoặc thư mục đến một vị trí mới |
| cp | Sao chép một tập tin hoặc thư mục vào một vị trí mới |

***2.8. Activity: Manage files with Linux commands – Hoạt động: Quản lý tập tin bằng lệnh Linux***

***2.9. Optional Exemplar: Manage files with Linux commands – Mẫu tùy chọn: Quản lý tệp bằng lệnh Linux***

***2.10. Test your knowledge: Manage file content in Bash – Kiểm tra kiến ​​thức của bạn: Quản lý nội dung file trong Bash***

**3. Authenticate and authorize users – Xác thực và ủy quyền người dùng**

***3.1. File permissions and ownership – Quyền và quyền sở hữu tập tin***

|  |
| --- |
| Hi there. It's great to have you back! Let's continue to learn more about how to work in Linux as a security analyst. In this video, we'll explore file and directory permissions. We'll learn how Linux represents permissions and how you can check for the permissions associated with files and directories. |

Chào bạn. Thật tuyệt khi có bạn trở lại!Hãy tiếp tục tìm hiểu thêm về cáchlàm việc trong Linux với tư cách là nhà phân tích bảo mật.Trong video này, chúng ta sẽ khám pháquyền tập tin và thư mục.Chúng ta sẽ tìm hiểu cách Linux thể hiện quyềnvà cách bạn có thể kiểm tra quyềnliên kết với các tập tin và thư mục.

|  |
| --- |
| Permissions are the type of access granted for a file or directory. Permissions are related to authorization. Authorization is the concept of granting access to specific resources in a system. Authorization allows you to limit access to specified files or directories. A good rule to follow is that data access is on a need-to-know basis. You can imagine the security risk it would impose if anyone could access or modify anything they wanted to on a system. |

Quyền là loạiquyền truy cập được cấp cho một tập tin hoặc thư mục.Quyền có liên quan đến ủy quyền.Ủy quyền là khái niệm cấptruy cập vào các tài nguyên cụ thể trong một hệ thống.Ủy quyền cho phép bạn hạn chếtruy cập vào các tập tin hoặc thư mục được chỉ định.Một quy tắc tốt để làm theo làtruy cập dữ liệu là trên cơ sở cần phải biết.Bạn có thể tưởng tượng rủi ro bảo mậtnó sẽ áp đặt nếu có aicó thể truy cập hoặc sửa đổibất cứ điều gì họ muốn trên một hệ thống.

|  |
| --- |
| There are three types of permissions in Linux that an authorized user can have. The first type of permission is read. On a file, read permissions means contents on the file can be read. On a directory, this permission means you can read all files in that directory. Next are write permissions. Write permissions on a file allow modifications of contents of the file. On a directory, write permissions indicate that new files can be created in that directory. Finally, there are also execute permissions. Execute permissions on files mean that the file can be executed if it's an executable file. Execute permissions on directories allow users to enter into a directory and access its files. |

Có ba loại quyền trongLinux mà người dùng được ủy quyền có thể có.Loại quyền đầu tiên được đọc.Trên một tập tin, quyền đọccó nghĩa là nội dung trên tập tin có thể được đọc.Trên một thư mục,sự cho phép này có nghĩa là bạn có thể đọctất cả các tập tin trong thư mục đó.Tiếp theo là quyền ghi.Cho phép ghi quyền trên một tập tinsửa đổi nội dung của tập tin.Trên một thư mục, quyền ghi chỉ ra rằngcác tập tin mới có thể được tạo trong thư mục đó.Cuối cùng, cũng có quyền thực thi.Thực thi quyền trên các tập tin có nghĩa làtệp có thể được thực thi nếu đó là tệp thực thi.Quyền thực thi trên các thư mục cho phép người dùngnhập vào một thư mục và truy cập các tập tin của nó.

|  |
| --- |
| Permissions are granted for three different types of owners. The first type is the user. The user is the owner of the file. When you create a file, you become the owner of the file, but the ownership can be changed. Group is the next type. Every user is a part of a certain group. A group consists of several users, and this is one way to manage a multi-user environment. Finally, there is other. Other can be considered all other users on the system. Basically, anyone else with access to the system belongs to this group. In Linux, file permissions are represented with a 10-character string. For a directory with full permissions for the user group, this string would be: drwxrwxrwx. |

Quyền được cấp choba loại chủ sở hữu khác nhau.Loại đầu tiên là người dùng.Người dùng là chủ sở hữu của tập tin.Khi bạn tạo một tập tin,bạn trở thành chủ sở hữu của tập tin,nhưng quyền sở hữu có thể được thay đổi.Nhóm là loại tiếp theo.Mỗi người dùng là một phần của một nhóm nhất định.Một nhóm bao gồm nhiều người dùng,và đây là một cách để quản lý môi trường nhiều người dùng.Cuối cùng, có cái khác.Khác có thể được coi là tất cả người dùng khác trên hệ thống.Về cơ bản, bất kỳ ai khác có quyền truy cậpvào hệ thống thuộc về nhóm này.Trong Linux, quyền truy cập tập tin làđược biểu diễn bằng chuỗi 10 ký tự.Đối với một thư mục có đầy đủ quyền cho nhóm người dùng,chuỗi này sẽ là: drwxrwxrwx.

|  |
| --- |
| Let's examine what this means more closely. The first character indicates the file type. As shown in this example, d is used to indicate it is a directory. If this character contains a hyphen instead, it would be a regular file. The second, third, and fourth characters indicate the permissions for the user. In this example, r indicates the user has read permissions, w indicates the user has write permissions, and x indicates the user has execute permissions. If one of these permissions was missing, there would be a hyphen instead of the letter. In the same way, the fifth, sixth, and seventh characters indicate permissions for the next owner type group. As it shows here, the type group also has read, write, and execute permissions. There are no hyphens to indicate that any of these permissions haven't been granted. Finally, the eighth through tenth characters indicate permissions for the last owner type: other. They also have read, write, and execute permissions in this example. |

Chúng ta hãy xem xét điều này có nghĩa gì chặt chẽ hơn.Ký tự đầu tiên cho biết loại tệp.Như được hiển thị trong ví dụ này,d được sử dụng để cho biết đó là một thư mục.Thay vào đó, nếu ký tự này chứa dấu gạch nối,nó sẽ là một tập tin thông thường.Thứ hai, thứ ba vàký tự thứ tư cho biết quyền của người dùng.Trong ví dụ này, rcho biết người dùng có quyền đọc,w cho biết người dùng có quyền ghi,và x cho biết người dùng có quyền thực thi.Nếu thiếu một trong những quyền này,sẽ có dấu gạch nối thay vì chữ cái.Tương tự như vậy, thứ năm, thứ sáu,và ký tự thứ bảy biểu thịquyền cho nhóm loại chủ sở hữu tiếp theo.Như nó cho thấy ở đây,nhóm loại cũng đã đọc,viết và thực thi quyền.Không có dấu gạch nối để chỉ ra rằngbất kỳ quyền nào trong số này chưa được cấp.Cuối cùng, ký tự thứ tám đến thứ mườichỉ ra quyền cho loại chủ sở hữu cuối cùng: khác.Họ cũng đã đọc, viết,và thực thi các quyền trong ví dụ này.

|  |
| --- |
| Ensuring files and directories are set with their appropriate access permissions is critical to protecting sensitive files and maintaining the overall security of a system. For example, payroll departments handle sensitive information. If someone outside of the payroll group could read this file, this would be a privacy concern. Another example is when the user, the group, and other can all write to a file. This type of file is considered a world-writable file. World-writable files can pose significant security risks. |

Đảm bảo các tập tin và thư mục được thiết lậpvới quyền truy cập thích hợp của họ làquan trọng để bảo vệ các tập tin nhạy cảm vàduy trì tính bảo mật tổng thể của hệ thống.Ví dụ, bộ phận tính lươngxử lý thông tin nhạy cảm.Nếu ai đó ở ngoàinhóm trả lương có thể đọc tập tin này,đây sẽ là một mối lo ngại về quyền riêng tư.Một ví dụ khác là khi người dùngnhóm và những người khác đều có thể ghi vào một tập tin.Loại tệp này được coi là tệp có thể ghi trên thế giới.Các tập tin có thể ghi trên thế giới có thể gây ra rủi ro bảo mật đáng kể.

|  |
| --- |
| So how do we check permissions? First, we need to understand what options are. Options modify the behavior of the command. The options for a command can be a single letter or a full word. Checking permissions involves adding options to the ls command. First, ls -l displays permissions to files and directories. You might also want to display hidden files and identify their permissions. Hidden files, which begin with a period before their name, don't normally appear when you use ls to display file contents. Entering ls -a displays hidden files. Then you can combine these two options to do both. Entering ls -la displays permissions to files and directories, including hidden files. |

Vậy làm cách nào để kiểm tra quyền?Đầu tiên chúng ta cần hiểu option là gì?Tùy chọn sửa đổi hành vi của lệnh.Các tùy chọn cho lệnhcó thể là một chữ cái hoặc một từ đầy đủ.Kiểm tra quyền liên quan đến việc thêmcác tùy chọn cho lệnh ls.Đầu tiên, ls -l hiển thịquyền đối với các tập tin và thư mục.Bạn cũng có thể muốn hiển thịtập tin ẩn và xác định quyền của họ.Các tập tin ẩn, bắt đầu bằngmột khoảng thời gian trước tên của họ, đừngthường xuất hiện khi bạn sử dụng ls để hiển thị nội dung tệp.Nhập ls -a sẽ hiển thị các tập tin ẩn.Sau đó, bạn có thể kết hợp hai tùy chọn này để làm cả hai.Nhập ls -la hiển thị quyềnvào các tập tin và thư mục, bao gồm cả các tập tin ẩn.

|  |
| --- |
| Let's get into Bash and try out these options. Right now, we're in the project subdirectory. First, let's use the ls command to display its contents. The output displays the files in this directory, but we don't know anything about their permissions. By using ls -l instead, we get expanded information on these files. Let's do this. The file names are now on the right side of each row. The first piece of information in each row shows the permissions in the format that we discussed earlier. Since these are all files and not directories, notice how the first character is a hyphen. Let's focus on one specific file: project1.txt. The second through fourth characters of its permissions show us the user has both read and write permissions but lacks execute permissions. In both the fifth through seventh characters and eighth through tenth characters, the sequence is r--. This means group and other have only read privileges. After the permissions, ls -l first displays the username. Here, that's us, analyst. Next comes the group name; in our case, the security group. Now let's use ls -a The output includes two more files—hidden files with the names: .hidden1.txt and .hidden2.txt Finally, we can also use ls -la to show the permissions for all files, including these hidden files. |

Hãy vào Bash và thử các tùy chọn này.Hiện tại, chúng ta đang ở trong thư mục con của dự án.Đầu tiên, hãy sử dụng lệnh ls để hiển thị nội dung của nó.Đầu ra hiển thị các tập tin trong thư mục này,nhưng chúng tôi không biết gì về quyền của họ.Bằng cách sử dụng ls -l thay vào đó,chúng tôi nhận được thông tin mở rộng vềnhững tập tin này. Làm thôi nào.Tên tệp bây giờ ở bên phải của mỗi hàng.Phần thông tin đầu tiên trong mỗi hànghiển thị các quyền trongđịnh dạng mà chúng ta đã thảo luận trước đó.Vì đây là tất cả các tập tin chứ không phải thư mục,chú ý ký tự đầu tiên là dấu gạch nối như thế nào.Hãy tập trung vào một tệp cụ thể: project1.txt.Ký tự thứ hai đến thứ tư của nóquyền cho chúng tôi thấy người dùngcó cả quyền đọc và quyền ghinhưng thiếu quyền thực thi.Trong cả thứ năm đếnký tự thứ bảy và ký tự thứ tám đến thứ mười,trình tự là r--.Điều này có nghĩa là nhóm và những người khác chỉ có đặc quyền đọc.Sau khi có quyền, ls -l trước tiên sẽ hiển thị tên người dùng.Đây là chúng tôi, nhà phân tích.Tiếp theo là tên nhóm;trong trường hợp của chúng tôi, nhóm bảo mật.Bây giờ hãy sử dụng ls -aĐầu ra bao gồm hai tệp nữa—ẩncác tệp có tên: .hidden1.txtvà .hidden2.txtCuối cùng, chúng ta cũng có thể sử dụngls -la để hiển thị quyền cho tất cả các tệp,bao gồm cả những tập tin ẩn này.

|  |
| --- |
| I thought that was pretty interesting. Did you? You now know a little more about file permissions and ownership. This will be helpful when working in security because monitoring and setting correct permissions is essential for protecting information. Take a small break and meet me in the next video. |

Tôi nghĩ điều đó khá thú vị. Bạn đã?Bây giờ bạn đã biết thêm một chút vềquyền và quyền sở hữu tập tin.Điều này sẽ hữu ích khi làm việc trongan ninh vì giám sát vàthiết lập quyền chính xác làcần thiết cho việc bảo vệ thông tin.Hãy nghỉ ngơi một chút và gặp tôi trong video tiếp theo.

***3.2. Change permissions – Thay đổi quyền***

|  |
| --- |
| Hi there! In the previous video, you learned how to check permissions for a user. In this video, we're going to learn about changing permissions. |

Chào bạn! Trong video trước,bạn đã học cách kiểm tra quyền của người dùng.Trong video này, chúng ta sẽ điđể tìm hiểu về cách thay đổi quyền.

|  |
| --- |
| When working as a security analyst, there may be many reasons to change permissions for a user. A user may have changed departments or been assigned to a different work group. A user might simply no longer be working on a project that requires certain permissions. These changes are necessary in order to protect system files from being accidentally or deliberately altered or deleted. |

Khi làm việc như một nhà phân tích chứng khoán,có thể có nhiều lý do đểthay đổi quyền cho người dùng.Một người dùng có thể đã thay đổi phòng banhoặc được phân công vào một nhóm công việc khác.Đơn giản là người dùng có thể không còn làm việc nữamột dự án yêu cầu một số quyền nhất định.Những thay đổi này là cần thiết để bảo vệtập tin hệ thống từbị thay đổi hoặc xóa một cách vô tình hoặc cố ý.

|  |
| --- |
| Let's explore a related command that helps control this access. In this video, we'll learn about chmod. chmod changes permissions on files and directories. The command chmod stands for change mode. |

Hãy khám phá một lệnh liên quangiúp kiểm soát quyền truy cập này.Trong video này, chúng ta sẽ tìm hiểu về chmod.chmod thay đổi quyền trên tập tin và thư mục.Lệnh chmod là viết tắt của chế độ thay đổi.

|  |
| --- |
| There are two modes for changing permissions, but we'll focus on symbolic. The best way to learn about how chmod works is through an example. I know this has a lot of details, but we'll break this down. Also, please keep in mind that, like many Linux commands, you don't have to memorize the information and can always find a reference. |

Có hai chế độ để thay đổi quyền,nhưng chúng ta sẽ tập trung vào biểu tượng. Cách tốt nhất đểtìm hiểu về cách hoạt động của chmod thông qua một ví dụ.Tôi biết điều này có rất nhiều chi tiết,nhưng chúng tôi sẽ chia nhỏ điều này.Ngoài ra, hãy nhớ rằng, giống như nhiều lệnh Linux,bạn không cần phải ghi nhớthông tin và luôn có thể tìm thấy một tài liệu tham khảo.

|  |
| --- |
| With chmod, you need to identify which file or directory you want to adjust permissions for. This is the final argument, in this case, a file named: access.txt. The first argument, added directly after the chmod command, indicates how to change permissions. Right now, this might seem hard to interpret, but soon we'll understand why this is called symbolic mode. |

Với chmod, bạn cần xác định cái nàotập tin hoặc thư mục mà bạn muốn điều chỉnh quyền.Đây là lý lẽ cuối cùng,trong trường hợp này là một tệp có tên: access.txt.Đối số đầu tiên, được thêm trực tiếp saulệnh chmod, cho biết cách thay đổi quyền.Hiện tại, điều này có vẻ khó diễn giải,nhưng chúng ta sẽ sớm hiểu tại saođây được gọi là chế độ tượng trưng.

|  |
| --- |
| Previously, we learned about the three types of owners: user, group, and other. To identify these with chmod, we use u to represent the user, g to represent the group, and o to represent other. In this particular example, g indicates we will make some changes to group permissions, and o to permissions for other. These owner types are separated by a comma in this argument. |

Trước đây chúng ta đã tìm hiểu về 3 loạicủa chủ sở hữu: người dùng, nhóm và người khác.Để xác định những thứ này bằng chmod,chúng tôi sử dụng bạn để đại diện cho người dùng,g đại diện cho nhóm,và o để đại diện cho người khác.Trong ví dụ cụ thể này,g cho biết chúng tôi sẽ thực hiệnmột số thay đổi về quyền của nhóm,và o để cấp quyền cho người khác.Các loại chủ sở hữu này được tách biệtbằng dấu phẩy trong lập luận này.

|  |
| --- |
| But do we want to add or take away permissions? Well, for this, we use mathematical operators. So, the plus sign after g means we want to add permissions for group. The minus sign after o means we want to take them away from other. And the last question is: what kind of changes? We've already learned that r represents read permissions, w represents write permissions, and x represents execute permissions. So in this case, the w indicates that we're adding write permissions to the group, and r indicates that we are taking away read permissions from other. This is still very complex. But now that we've broken it down, perhaps it doesn't seem quite so much like a foreign language. And remember, you don't have to memorize this all. |

Nhưng chúng ta muốn thêm hay bớt quyền?Vâng, để làm điều này, chúng tôi sử dụng các toán tử toán học.Vì vậy, dấu cộng sau gcó nghĩa là chúng tôi muốn thêm quyền cho nhóm.Dấu trừ sau ocó nghĩa là chúng ta muốn lấy chúng ra khỏi người khác.Và câu hỏi cuối cùng là: loại thay đổi nào?Chúng ta đã biết r đại diện cho quyền đọc,w đại diện cho quyền ghi,và x đại diện cho quyền thực thi.Vì vậy, trong trường hợp này, w chỉ rarằng chúng tôi đang thêm quyền ghi vào nhóm,và r chỉ ra rằng chúng tôi đang dùngbỏ quyền đọc từ người khác.Điều này vẫn còn rất phức tạp.Nhưng bây giờ chúng ta đã chia nhỏ nó ra,có lẽ nó có vẻ không hoàn toàngiống ngoại ngữ quáVà hãy nhớ rằng, bạn không cần phải ghi nhớ tất cả những điều này.

|  |
| --- |
| Let's give this new command a try. We'll start out in the logs sub-directory. If we use the ls -l command, it will output the permissions for the file. It shows the permissions for the only file in this directory: access.txt. Previously, we learned how to read these permissions. The second through fourth characters indicate that the user has read and write permissions. The fifth through seventh characters show the group only has read permissions. And the eighth to tenth characters show that other only has read permissions. We need to adjust these permissions. |

Hãy thử lệnh mới này.Chúng ta sẽ bắt đầu trong thư mục con logs.Nếu chúng ta sử dụng lệnh ls -l,nó sẽ xuất ra các quyền cho tập tin.Nó hiển thị các quyền cho tập tin duy nhấttrong thư mục này: access.txt.Trước đây, chúng tôi đã học cách đọc các quyền này.Ký tự thứ hai đến thứ tưcho biết người dùng có quyền đọc và ghi.Ký tự thứ năm đến thứ bảyhiển thị nhóm chỉ có quyền đọc.Và nhân vật thứ tám đến thứ mười hiển thịcái kia chỉ có quyền đọc.Chúng ta cần điều chỉnh các quyền này.

|  |
| --- |
| We want to ensure analysts in the security group have write permission, but takeaway read permissions from the owner-type other, so we add write permissions for group and remove read permissions for other. Let's run ls -l again. This shows a change in the permissions for access.txt. Notice how in the middle segment of permissions for the group, w has been added to give write permissions. And another change is that the r has been removed in the last segment, indicating that read permissions for other have been removed. As mentioned earlier, these hyphens indicate a lack of permissions. Now, other is lacking all permissions. |

Chúng tôi muốn đảm bảo các nhà phân tíchnhóm bảo mật có quyền viết,nhưng quyền đọc mang đi từ loại chủ sở hữu khác,vì vậy chúng tôi thêm quyền ghi chonhóm và loại bỏ quyền đọc cho người khác.Hãy chạy ls -l lần nữa.Điều này cho thấy sự thay đổi về quyền đối với access.txt.Chú ý như thế nào ở đoạn giữaquyền cho nhóm,w đã được thêm vào để cấp quyền ghi.Và một sự thay đổi khác đó làr đã bị xóa ở phân đoạn cuối cùng,chỉ ra rằng quyền đọcđối với những thứ khác đã bị loại bỏ.Như đã đề cập trước đó, những dấu gạch nối nàychỉ ra sự thiếu quyền.Bây giờ, cái khác đang thiếu tất cả các quyền.

|  |
| --- |
| Though it requires practice, working in Linux becomes more natural with time. I'm glad you're learning a little more about how to use Linux. |

Mặc dù nó đòi hỏi phải thực hành,làm việc trong Linux trở nên tự nhiên hơn theo thời gian.Tôi rất vui vì bạn đã học được một chútthêm về cách sử dụng Linux.

***3.3. Permission commands – Lệnh cấp phép***

|  |
| --- |
| **Permission commands** |

**Lệnh cấp phép**

|  |
| --- |
| Previously, you explored file permissions and the commands that you can use to display and change them.  In this reading, you’ll review these concepts and also focus on an example of how these commands work together when putting the principle of least privilege into practice. |

Trước đây, bạn đã khám phá các quyền đối với tệp và các lệnh mà bạn có thể sử dụng để hiển thị và thay đổi chúng. Trong bài đọc này, bạn sẽ xem lại các khái niệm này và cũng tập trung vào một ví dụ về cách các lệnh này phối hợp với nhau khi áp dụng nguyên tắc đặc quyền tối thiểu vào thực tế.

|  |
| --- |
| **Reading permissions** |

**Quyền đọc**

|  |
| --- |
| In Linux, permissions are represented with a 10-character string. Permissions include: |

Trong Linux, các quyền được biểu thị bằng chuỗi 10 ký tự. Quyền bao gồm:

|  |
| --- |
| * **read**: for files, this is the ability to read the file contents; for directories, this is the ability to read all contents in the directory including both files and subdirectories * **write**: for files, this is the ability to make modifications on the file contents; for directories, this is the ability to create new files in the directory * **execute**: for files, this is the ability to execute the file if it’s a program; for directories, this is the ability to enter the directory and access its files |

* **read** : đối với file, đây là khả năng đọc nội dung file; đối với thư mục, đây là khả năng đọc tất cả nội dung trong thư mục bao gồm cả tệp và thư mục con
* **write** : đối với các tập tin, đây là khả năng sửa đổi nội dung tập tin; đối với thư mục, đây là khả năng tạo tập tin mới trong thư mục
* **execute**: đối với tệp, đây là khả năng thực thi tệp nếu đó là chương trình; đối với thư mục, đây là khả năng vào thư mục và truy cập các tệp của nó

|  |
| --- |
| These permissions are given to these types of owners: |

Các quyền này được cấp cho các loại chủ sở hữu sau:

|  |
| --- |
| * **user**: the owner of the file * **group**: a larger group that the owner is a part of * **other**: all other users on the system |

* **user**: chủ sở hữu của tập tin
* **group**: một nhóm lớn hơn mà chủ sở hữu là một phần của
* **other** : tất cả người dùng khác trên hệ thống

|  |
| --- |
| Each character in the 10-character string conveys different information about these permissions. The following table describes the purpose of each character: |

Mỗi ký tự trong chuỗi 10 ký tự truyền tải thông tin khác nhau về các quyền này. Bảng sau mô tả mục đích của từng ký tự:

|  |  |  |
| --- | --- | --- |
| **Character** | **Example** | **Meaning** |
| 1st | **d**rwxrwxrwx | file type   * **d** for directory * **-** for a regular file |
| 2nd | d**r**wxrwxrwx | read permissions for the user   * **r** if the user has read permissions * **-** if the user lacks read permissions |
| 3rd | dr**w**xrwxrwx | write permissions for the user   * **w** if the user has write permissions * **-** if the user lacks write permissions |
| 4th | drw**x**rwxrwx | execute permissions for the user   * **x** if the user has execute permissions * **-** if the user lacks execute permissions |
| 5th | drwx**r**wxrwx | read permissions for the group   * **r** if the group has read permissions * **-** if the group lacks read permissions |
| 6th | drwxr**w**xrwx | write permissions for the group   * **w** if the group has write permissions * **-** if the group lacks write permissions |
| 7th | drwxrw**x**rwx | execute permissions for the group   * **x** if the group has execute permissions * **-** if the group lacks execute permissions |
| 8th | drwxrwx**r**wx | read permissions for other   * **r** if the other owner type has read permissions * **-** if the other owner type lacks read permissions |
| 9th | drwxrwxr**w**x | write permissions for other   * **w** if the other owner type has write permissions * **-** if the other owner type lacks write permissions |
| 10th | drwxrwxrw**x** | execute permissions for other   * **x** if the other owner type has execute permissions * **-** if the other owner type lacks execute permissions |

|  |  |  |
| --- | --- | --- |
| **Ký tự** | **Ví dụ** | **Nghĩa** |
| 1st | **d**rwxrwxrwx | loại tệp   * **d** cho thư mục * **-** đối với một tập tin thông thường |
| 2nd | d**r**wxrwxrwx | quyền đọc cho người dùng   * **r** nếu người dùng có quyền đọc * **-** nếu người dùng thiếu quyền đọc |
| 3rd | dr**w**xrwxrwx | quyền ghi cho người dùng   * **w** nếu người dùng có quyền ghi * **-** nếu người dùng thiếu quyền ghi |
| 4th | drw**x**rwxrwx | thực thi quyền cho người dùng   * **x** nếu người dùng có quyền thực thi * **-** nếu người dùng thiếu quyền thực thi |
| 5th | drwx**r**wxrwx | quyền đọc cho nhóm   * **r** nếu nhóm có quyền đọc * **-** nếu nhóm thiếu quyền đọc |
| 6th | drwxr**w**xrwx | quyền ghi cho nhóm   * **w** nếu nhóm có quyền ghi * **-** nếu nhóm thiếu quyền ghi |
| 7th | drwxrw**x**rwx | thực thi quyền cho nhóm   * **x** nếu nhóm có quyền thực thi * **-** nếu nhóm thiếu quyền thực thi |
| 8th | drwxrwx**r**wx | quyền đọc cho người khác   * **r** nếu loại chủ sở hữu khác có quyền đọc * **-** nếu loại chủ sở hữu khác thiếu quyền đọc |
| 9th | drwxrwxr**w**x | quyền ghi cho người khác   * **w** nếu loại chủ sở hữu khác có quyền ghi * **-** nếu loại chủ sở hữu khác thiếu quyền ghi |
| 10th | drwxrwxrw**x** | thực thi quyền cho người khác   * **x** nếu loại chủ sở hữu khác có quyền thực thi * **-** nếu loại chủ sở hữu khác thiếu quyền thực thi |

|  |
| --- |
| **Exploring existing permissions** |

**Khám phá các quyền hiện có**

|  |
| --- |
| You can use the **ls** command to investigate who has permissions on files and directories. Previously, you learned that **ls** displays the names of files in directories in the current working directory. |

Bạn có thể sử dụng lệnh **ls** để điều tra xem ai có quyền đối với các tệp và thư mục. Trước đây, bạn đã biết rằng **ls** hiển thị tên của các tập tin trong các thư mục trong thư mục làm việc hiện tại.

|  |
| --- |
| There are additional options you can add to the **ls** command to make your command more specific. Some of these options provide details about permissions. Here are a few important **ls** options for security analysts: |

Có các tùy chọn bổ sung mà bạn có thể thêm vào lệnh **ls** để làm cho lệnh của bạn cụ thể hơn. Một số tùy chọn này cung cấp thông tin chi tiết về quyền. Dưới đây là một số tùy chọn **ls** quan trọng dành cho các nhà phân tích bảo mật:

|  |
| --- |
| * **ls -a**: Displays hidden files. Hidden files start with a period (**.**) at the beginning. * **ls -l**: Displays permissions to files and directories. Also displays other additional information, including owner name, group, file size, and the time of last modification. * **ls -la**: Displays permissions to files and directories, including hidden files. This is a combination of the other two options. |

* **ls -a** : Hiển thị file ẩn. Các tệp ẩn bắt đầu bằng dấu chấm ( **.** ) ở đầu.
* **ls -l** : Hiển thị quyền đối với tập tin và thư mục. Đồng thời hiển thị các thông tin bổ sung khác, bao gồm tên chủ sở hữu, nhóm, kích thước tệp và thời gian sửa đổi lần cuối.
* **ls -la** : Hiển thị quyền đối với các tập tin và thư mục, bao gồm cả các tập tin ẩn. Đây là sự kết hợp của hai lựa chọn còn lại.

|  |
| --- |
| **Changing permissions** |

**Thay đổi quyền**

|  |
| --- |
| The **principle of least privilege** is the concept of granting only the minimal access and authorization required to complete a task or function. In other words, users should not have privileges that are beyond what is necessary. Not following the principle of least privilege can create security risks. |

Nguyên **tắc đặc quyền tối thiểu** là khái niệm chỉ cấp quyền truy cập và ủy quyền tối thiểu cần thiết để hoàn thành một nhiệm vụ hoặc chức năng. Nói cách khác, người dùng không nên có những đặc quyền vượt quá mức cần thiết. Không tuân theo nguyên tắc đặc quyền tối thiểu có thể tạo ra rủi ro về bảo mật.

|  |
| --- |
| The **chmod**  command can help you manage this authorization. The **chmod** command changes permissions on files and directories. |

Lệnh **chmod**   có thể giúp bạn quản lý việc ủy ​​quyền này. Lệnh **chmod** thay đổi quyền trên tập tin và thư mục.

|  |
| --- |
| **Using chmod** |

**Sử dụng chmod**

|  |
| --- |
| The **chmod** command requires two arguments. The first argument indicates how to change permissions, and the second argument indicates the file or directory that you want to change permissions for.  For example, the following command would add all permissions to **login\_sessions.txt**: |

Lệnh **chmod** yêu cầu hai đối số. Đối số đầu tiên cho biết cách thay đổi quyền và đối số thứ hai cho biết tệp hoặc thư mục mà bạn muốn thay đổi quyền. Ví dụ: lệnh sau sẽ thêm tất cả các quyền vào **login\_sessions.txt** :

|  |
| --- |
| **chmod u+rwx,g+rwx,o+rwx login\_sessions.txt** |

**chmod u+rwx,g+rwx,o+rwx login\_sessions.txt**

|  |
| --- |
| If you wanted to take all the permissions away, you could use |

Nếu bạn muốn lấy đi tất cả các quyền, bạn có thể sử dụng

|  |
| --- |
| **chmod u-rwx,g-rwx,o-rwx login\_sessions.txt** |

**chmod u-rwx,g-rwx,o-rwx login\_sessions.txt**

|  |
| --- |
| Another way to assign these permissions is to use the equals sign (**=**) in this first argument. Using **=** with **chmod** sets, or assigns, the permissions exactly as specified. For example, the following command would set read permissions for **login\_sessions.txt** for user, group, and other: |

Một cách khác để gán các quyền này là sử dụng dấu bằng ( **=** ) trong đối số đầu tiên này. Sử dụng **=** với bộ **chmod** hoặc gán các quyền chính xác như được chỉ định. Ví dụ: lệnh sau sẽ đặt quyền đọc **login\_sessions.txt** cho người dùng, nhóm và những người khác:

|  |
| --- |
| **chmod u=r,g=r,o=r login\_sessions.txt** |

**chmod u=r,g=r,o=r login\_sessions.txt**

|  |
| --- |
| This command overwrites existing permissions. For instance, if the user previously had write permissions, these write permissions are removed after you specify only read permissions with **=**. |

Lệnh này ghi đè các quyền hiện có. Ví dụ: nếu trước đây người dùng có quyền ghi thì các quyền ghi này sẽ bị xóa sau khi bạn chỉ định quyền đọc bằng **=** .

|  |
| --- |
| The following table reviews how each character is used within the first argument of **chmod**: |

Bảng sau đây xem xét cách sử dụng từng ký tự trong đối số đầu tiên của **chmod** :

|  |  |
| --- | --- |
| **Character** | **Description** |
| **u** | indicates changes will be made to user permissions |
| **g** | indicates changes will be made to group permissions |
| **o** | indicates changes will be made to other permissions |
| **+** | adds permissions to the user, group, or other |
| **-** | removes permissions from the user, group, or other |
| **=** | assigns permissions for the user, group, or other |

|  |  |
| --- | --- |
| **Ký tự** | **Đặc tả** |
| **u** | cho biết những thay đổi sẽ được thực hiện đối với quyền của người dùng |
| **g** | cho biết những thay đổi sẽ được thực hiện đối với quyền của nhóm |
| **o** | cho biết những thay đổi sẽ được thực hiện đối với các quyền khác |
| **+** | thêm quyền cho người dùng, nhóm hoặc người khác |
| **-** | xóa quyền của người dùng, nhóm hoặc người khác |
| **=** | gán quyền cho người dùng, nhóm hoặc người khác |

|  |
| --- |
| **Note:** When there are permission changes to more than one owner type, commas are needed to separate changes for each owner type. You should not add spaces after those commas. |

**Lưu ý:** Khi có các thay đổi về quyền đối với nhiều loại chủ sở hữu, cần có dấu phẩy để phân tách các thay đổi cho từng loại chủ sở hữu. Bạn không nên thêm dấu cách sau những dấu phẩy đó.

|  |
| --- |
| **The principle of least privilege in action** |

**Nguyên tắc đặc quyền tối thiểu trong hành động**

|  |
| --- |
| As a security analyst, you may encounter a situation like this one: There’s a file called **bonuses.txt** within a compensation directory. The owner of this file is a member of the Human Resources department with a username of **hrrep1**. It has been decided that **hrrep1** needs access to this file. But, since this file contains confidential information, no one else in the **hr** group needs access. |

Là một nhà phân tích bảo mật, bạn có thể gặp phải tình huống như thế này: Có một tệp tên là **bonus.txt** trong thư mục bồi thường. Chủ sở hữu của tệp này là thành viên của bộ phận Nhân sự với tên người dùng là **hrrep1** . Người ta đã quyết định rằng **HRrep1** cần quyền truy cập vào tệp này. Tuy nhiên, vì tệp này chứa thông tin bí mật nên không ai khác trong nhóm **nhân sự** cần quyền truy cập.

|  |
| --- |
| You run **ls -l** to check the permissions of files in the compensation directory and discover that the permissions for **bonuses.txt** are **-rw-rw----**. The group owner type has read and write permissions that do not align with the principle of least privilege. |

Bạn chạy **ls -l** để kiểm tra quyền của các tệp trong thư mục bồi thường và phát hiện ra rằng các quyền đối với **bonus.txt** là **-rw-rw----** . Loại chủ sở hữu nhóm có quyền đọc và ghi không phù hợp với nguyên tắc đặc quyền tối thiểu.

|  |
| --- |
| To remedy the situation, you input **chmod g-rw bonuses.txt**. Now, only the user who needs to access this file to carry out their job responsibilities can access this file. |

Để khắc phục tình trạng này, bạn nhập **chmod g-rw bonus.txt** . Bây giờ, chỉ người dùng cần truy cập tệp này để thực hiện trách nhiệm công việc của họ mới có thể truy cập tệp này.

|  |
| --- |
| **Key takeaways** |

**Bài học chính**

|  |
| --- |
| Managing directory and file permissions may be a part of your work as a security analyst. Using **ls** with the **-l** and **-la** options allows you to investigate directory and file permissions. Using **chmod** allows you to change user permissions and ensure they are aligned with the principle of least privilege. |

Quản lý quyền truy cập thư mục và tệp có thể là một phần công việc của bạn với tư cách là nhà phân tích bảo mật. Sử dụng **ls** với các tùy chọn **-l** và **-la** cho phép bạn điều tra các quyền của thư mục và tệp. Sử dụng **chmod** cho phép bạn thay đổi quyền của người dùng và đảm bảo chúng được căn chỉnh theo nguyên tắc đặc quyền tối thiểu.

***3.4. Activity: Manage authorization – Hoạt động: Quản lý ủy quyền***

***3.5. Optional Exemplar: Manage authorization – Mẫu tùy chọn: Quản lý ủy quyền***

***3.6. Portfolio Activity: Use Linux commands to manage file permissions – Hoạt động danh mục đầu tư: Sử dụng các lệnh Linux để quản lý quyền truy cập tệp***

|  |
| --- |
| **Activity Overview**  In this activity, you will create a new portfolio document to demonstrate your experience using Linux commands to manage file permissions. You can add this document to your cybersecurity portfolio, which you can share with prospective employers or recruiters. To review the importance of building a professional portfolio and options for creating your portfolio, read [Create a cybersecurity portfolio](https://www.coursera.org/learn/linux-and-sql/resources/wDFrc).  To create your portfolio document, you will review a scenario and follow a series of steps. This scenario is connected to [the lab](https://www.coursera.org/learn/linux-and-sql/ungradedLti/483Kl/activity-manage-authorization) you have just completed about how to examine and manage file permissions. You will explain the commands you used in that lab, and this will help you prepare for future job interviews and other steps in the hiring process.  Be sure to complete this activity and answer the questions that follow before moving on. The next course item will provide you with a completed exemplar to compare to your own work. |

**Tổng quan về hoạt động**

Trong hoạt động này, bạn sẽ tạo một tài liệu danh mục đầu tư mới để thể hiện trải nghiệm của mình bằng cách sử dụng các lệnh Linux để quản lý quyền truy cập tệp. Bạn có thể thêm tài liệu này vào danh mục an ninh mạng của mình để có thể chia sẻ với các nhà tuyển dụng hoặc nhà tuyển dụng tiềm năng. Để xem lại tầm quan trọng của việc xây dựng danh mục đầu tư chuyên nghiệp và các lựa chọn để tạo danh mục đầu tư của bạn, hãy đọc[Tạo danh mục đầu tư an ninh mạng](https://www.coursera.org/learn/linux-and-sql/resources/wDFrc).

Để tạo tài liệu portfolio, bạn sẽ xem xét một kịch bản và làm theo một loạt các bước. Kịch bản này được kết nối với[phòng thí nghiệm](https://www.coursera.org/learn/linux-and-sql/ungradedLti/483Kl/activity-manage-authorization)bạn vừa hoàn thành cách kiểm tra và quản lý quyền truy cập tệp. Bạn sẽ giải thích các lệnh bạn đã sử dụng trong phòng thí nghiệm đó và điều này sẽ giúp bạn chuẩn bị cho các cuộc phỏng vấn xin việc trong tương lai cũng như các bước khác trong quy trình tuyển dụng.

Hãy chắc chắn hoàn thành hoạt động này và trả lời các câu hỏi tiếp theo trước khi tiếp tục. Mục khóa học tiếp theo sẽ cung cấp cho bạn một ví dụ hoàn chỉnh để so sánh với công việc của chính bạn.

|  |
| --- |
| **Scenario**  Review the scenario below. Then, complete the step-by-step instructions.  You are a security professional at a large organization. You mainly work with their research team. Part of your job is to ensure users on this team are authorized with the appropriate permissions. This helps keep the system secure.  Your task is to examine existing permissions on the file system. You’ll need to determine if the permissions match the authorization that should be given. If they do not match, you’ll need to modify the permissions to authorize the appropriate users and remove any unauthorized access.  **Note:** This scenario involves investigating and updating the same file permissions as the ones in the [Manage authorization](https://www.coursera.org/learn/linux-and-sql/ungradedLti/483Kl/activity-manage-authorization) lab.  You can revisit the lab to get screenshots to include in your portfolio document. If you choose, it's also possible to complete this activity without revisiting the lab by typing your commands in the template. |

**Kịch bản**

Xem lại kịch bản dưới đây. Sau đó, hoàn thành các hướng dẫn từng bước.

Bạn là chuyên gia bảo mật tại một tổ chức lớn. Bạn chủ yếu làm việc với nhóm nghiên cứu của họ. Một phần công việc của bạn là đảm bảo người dùng trong nhóm này được ủy quyền với các quyền thích hợp. Điều này giúp giữ cho hệ thống an toàn.

Nhiệm vụ của bạn là kiểm tra các quyền hiện có trên hệ thống tập tin. Bạn sẽ cần xác định xem các quyền có khớp với ủy quyền cần được cấp hay không. Nếu chúng không khớp, bạn sẽ cần sửa đổi các quyền để cấp quyền cho người dùng phù hợp và xóa mọi quyền truy cập trái phép.

**Lưu ý:** Kịch bản này liên quan đến việc điều tra và cập nhật các quyền đối với tệp giống như các quyền trong[Quản lý ủy quyền](https://www.coursera.org/learn/linux-and-sql/ungradedLti/483Kl/activity-manage-authorization)phòng thí nghiệm. Bạn có thể quay lại phòng thí nghiệm để lấy ảnh chụp màn hình để đưa vào tài liệu danh mục đầu tư của mình. Nếu bạn chọn, bạn cũng có thể hoàn thành hoạt động này mà không cần quay lại phòng thí nghiệm bằng cách nhập các lệnh của mình vào mẫu.

|  |
| --- |
| **Step-By-Step Instructions**  Follow the instructions to complete each step of the activity. Then, answer the 8 questions at the end of the activity before going to the next course item to compare your work to a completed exemplar. |

**Hướng dẫn từng bước một**

Làm theo hướng dẫn để hoàn thành từng bước của hoạt động. Sau đó, trả lời 8 câu hỏi ở cuối hoạt động trước khi chuyển sang mục khóa học tiếp theo để so sánh bài làm của bạn với một bài mẫu đã hoàn thành.

|  |
| --- |
| **Step 1: Access the template**  To use the template for this course item, click the following link and select *Use Template*. (In this step, you will just open the template. More instructions for how to use the template will be included in later steps.)  Link to template: [File permissions in Linux](https://docs.google.com/document/d/1A3xiUi9wbXf5lGvRwm8oFsXq18Q8mP7FUDNndjj89zc/template/preview?usp=sharing) |

**Bước 1: Truy cập mẫu**

Để sử dụng mẫu cho mục khóa học này, hãy nhấp vào liên kết sau và chọn *Sử dụng Mẫu* . (Ở bước này, bạn sẽ chỉ mở mẫu. Hướng dẫn thêm về cách sử dụng mẫu sẽ được đưa vào các bước sau.)

Liên kết đến mẫu:[Quyền tập tin trong Linux](https://docs.google.com/document/d/1A3xiUi9wbXf5lGvRwm8oFsXq18Q8mP7FUDNndjj89zc/template/preview?usp=sharing)

|  |
| --- |
| **Step 2: Access supporting materials**  The following supporting materials will help you complete this activity. Keep them open as you proceed to the next steps.  To use the supporting materials for this course item, click the links.  The **Instructions for including Linux commands** document provides instructions and best practices for including samples of Linux commands in your portfolio activity.  Link to supporting material: [Instructions for including Linux commands](https://docs.google.com/document/d/1t-9o-bPndpOIh9577FJobiakS10kJxgIKrB6GG7EPwA/template/preview?usp=sharing&resourcekey=0-623w2JztdmNSu3nDbsQJcQ)  The **Current file permissions** document demonstrates how the file structure is built for this portfolio activity. The file permissions for each file or directory are also provided.  Link to supporting material: [Current file permissions](https://docs.google.com/document/d/1F3-8XQZsNagSzTkJwFzOGY5OHbGbMRtlb8GbmXE_gCc/template/preview?usp=sharing&resourcekey=0-UUEu0EyFFvMf0SAipcel6w)  **Note**: It is recommended that you use the **Manage authorization** lab to complete this portfolio activity. If you’re revisiting the lab, using the **Current file permissions** document is optional because this file structure has already been created for you. |

**Bước 2: Truy cập tài liệu hỗ trợ**

Các tài liệu hỗ trợ sau đây sẽ giúp bạn hoàn thành hoạt động này. Giữ chúng mở khi bạn tiến hành các bước tiếp theo.

Để sử dụng các tài liệu hỗ trợ cho mục khóa học này, hãy nhấp vào liên kết.

Tài **liệu Hướng dẫn bao gồm các lệnh Linux** cung cấp các hướng dẫn và cách thực hành tốt nhất để đưa các mẫu lệnh Linux vào hoạt động danh mục đầu tư của bạn.

Liên kết đến tài liệu hỗ trợ:[Hướng dẫn thêm lệnh Linux](https://docs.google.com/document/d/1t-9o-bPndpOIh9577FJobiakS10kJxgIKrB6GG7EPwA/template/preview?usp=sharing&resourcekey=0-623w2JztdmNSu3nDbsQJcQ)

Tài liệu **về quyền đối với tệp hiện tại** trình bày cách xây dựng cấu trúc tệp cho hoạt động danh mục đầu tư này. Quyền truy cập tệp cho từng tệp hoặc thư mục cũng được cung cấp.

Liên kết đến tài liệu hỗ trợ:[Quyền tập tin hiện tại](https://docs.google.com/document/d/1F3-8XQZsNagSzTkJwFzOGY5OHbGbMRtlb8GbmXE_gCc/template/preview?usp=sharing&resourcekey=0-UUEu0EyFFvMf0SAipcel6w)

**Lưu ý** : Bạn nên sử dụng phòng thí nghiệm **Quản lý ủy quyền** để hoàn thành hoạt động danh mục đầu tư này. Nếu bạn đang xem lại lab, việc sử dụng tài liệu **Quyền đối với tệp hiện tại** là tùy chọn vì cấu trúc tệp này đã được tạo cho bạn.

|  |
| --- |
| **Step 3: Check file and directory details**  In the **Manage authorization** lab, check the permissions set for files and subdirectories in the **projects** directory. Make sure you display all permissions, including hidden files. Or, use the content of [**Current file permissions**](https://docs.google.com/document/d/1F3-8XQZsNagSzTkJwFzOGY5OHbGbMRtlb8GbmXE_gCc/template/preview?usp=sharing&resourcekey=0-UUEu0EyFFvMf0SAipcel6w) document to determine the current permissions.  Describe the command you can use to check permissions in the **Check file and directory details** section of the **File permissions in Linux** template. From the lab, take a screenshot of the Linux command you used. Or, type this command directly into the template.  Then, use either the output of this command in the lab or the content or the **Current file permissions** document to indicate the current permissions. If using the **Current file permissions** document, write these in the 10-character string that would be part of the command's output. |

**Bước 3: Kiểm tra chi tiết file và thư mục**

Trong phòng thí nghiệm **Quản lý ủy quyền** , hãy kiểm tra các quyền được đặt cho tệp và thư mục con trong thư mục **dự án** . Đảm bảo bạn hiển thị tất cả các quyền, bao gồm cả các tệp ẩn. Hoặc sử dụng nội dung của[**Quyền tập tin hiện tại**](https://docs.google.com/document/d/1F3-8XQZsNagSzTkJwFzOGY5OHbGbMRtlb8GbmXE_gCc/template/preview?usp=sharing&resourcekey=0-UUEu0EyFFvMf0SAipcel6w)tài liệu để xác định các quyền hiện tại.

Mô tả lệnh bạn có thể sử dụng để kiểm tra quyền trong phần **Kiểm tra chi tiết tệp và thư mục** của mẫu **Quyền đối với tệp trong Linux** . Từ phòng thí nghiệm, chụp ảnh màn hình lệnh Linux bạn đã sử dụng. Hoặc gõ lệnh này trực tiếp vào mẫu.

Sau đó, sử dụng đầu ra của lệnh này trong lab hoặc nội dung hoặc tài liệu **về quyền đối với tệp hiện tại** để cho biết các quyền hiện tại. Nếu sử dụng tài liệu **Quyền đối với tệp hiện tại** , hãy viết chúng vào chuỗi 10 ký tự sẽ là một phần của đầu ra của lệnh.

|  |
| --- |
| **Step 4: Describe the permissions string**  Choose one example from the output in the previous step. In the **Describe the permissions string** section of the **File permissions in Linux** template, write a short description that explains the 10-character string in the example. You should describe what the 10-character string is for and what each character represents. |

**Bước 4: Mô tả chuỗi quyền**

Chọn một ví dụ từ đầu ra ở bước trước. Trong phần **Mô tả chuỗi quyền** của mẫu **Quyền đối với tệp trong Linux** , hãy viết mô tả ngắn giải thích chuỗi 10 ký tự trong ví dụ. Bạn nên mô tả chuỗi 10 ký tự dùng để làm gì và mỗi ký tự đại diện cho điều gì.

|  |
| --- |
| **Step 5: Change file permissions**  The organization does not allow other to have write access to any files. Based on the permissions established in Step 3, identify which file needs to have its permissions modified. Use a Linux command to modify these permissions.  Describe the command you used and its output in the **Change file permissions** section of the **File permissions in Linux** template. In the **Manage authorization** lab, take a screenshot of the Linux command you used. Or, type this command directly into the template. |

**Bước 5: Thay đổi quyền truy cập tệp**

Tổ chức không cho phép người khác có quyền ghi vào bất kỳ tệp nào. Dựa trên các quyền được thiết lập ở Bước 3, xác định tệp nào cần sửa đổi quyền. Sử dụng lệnh Linux để sửa đổi các quyền này.

Mô tả lệnh bạn đã sử dụng và đầu ra của lệnh đó trong phần **Thay đổi quyền đối với tệp** của mẫu **Quyền đối với tệp trong Linux** . Trong phòng thí nghiệm **Quản lý ủy quyền** , hãy chụp ảnh màn hình lệnh Linux mà bạn đã sử dụng. Hoặc gõ lệnh này trực tiếp vào mẫu.

|  |
| --- |
| **Step 6: Change file permissions on a hidden file**  The research team has archived **.project\_x.txt**, which is why it’s a hidden file. This file should not have write permissions for anyone, but the user and group should be able to read the file. Use a Linux command to assign **.project\_x.txt** the appropriate authorization.  Describe the command you used and its output in the **Change file permissions on a hidden file** section of the **File permissions in Linux** template. In the **Manage authorization** lab, take a screenshot of the Linux command you used. Or, type this command directly into the template. |

**Bước 6: Thay đổi quyền truy cập tệp trên tệp ẩn**

Nhóm nghiên cứu đã lưu trữ **.project\_x.txt** , đó là lý do tại sao nó là một tệp ẩn. Tệp này không được có quyền ghi đối với bất kỳ ai nhưng người dùng và nhóm sẽ có thể đọc tệp. Sử dụng lệnh Linux để gán **.project\_x.txt** ủy quyền thích hợp.

Mô tả lệnh bạn đã sử dụng và đầu ra của lệnh đó trong phần **Thay đổi quyền đối với tệp trên tệp ẩn** của mẫu **Quyền đối với tệp trong Linux** . Trong phòng thí nghiệm **Quản lý ủy quyền** , hãy chụp ảnh màn hình lệnh Linux mà bạn đã sử dụng. Hoặc gõ lệnh này trực tiếp vào mẫu.

|  |
| --- |
| **Step 7: Change directory permissions**  The files and directories in the projects directory belong to the **researcher2** user. Only **researcher2** should be allowed to access the **drafts** directory and its contents. Use a Linux command to modify the permissions accordingly.  Describe the command you used and its output in the **Change directory permissions** section of the **File permissions in Linux** template. In the **Manage authorization** lab, take a screenshot of the Linux command you used. Or, type this command directly into the template. |

**Bước 7: Thay đổi quyền thư mục**

Các tập tin và thư mục trong thư mục dự án thuộc về người dùng **Research2** . Chỉ có **nhà nghiên cứu2** mới được phép truy cập vào thư mục **bản nháp** và nội dung của nó. Sử dụng lệnh Linux để sửa đổi các quyền cho phù hợp.

Mô tả lệnh bạn đã sử dụng và đầu ra của lệnh đó trong phần **Thay đổi quyền thư mục** của mẫu **Quyền đối với tệp trong Linux** . Trong phòng thí nghiệm **Quản lý ủy quyền** , hãy chụp ảnh màn hình lệnh Linux mà bạn đã sử dụng. Hoặc gõ lệnh này trực tiếp vào mẫu.

|  |
| --- |
| **Step 8: Finalize your document**  To finalize the document and make its purpose clear to potential employers, be sure to complete the **Project description** and **Summary** sections of the **File permissions in Linux** template.  In the Project description section, give a general overview of the scenario and what you accomplish through Linux. Write two to four sentences.  In the Summary section, provide a short summary of the previous tasks and connect them to the scenario. Write approximately two to four sentences. |

**Bước 8: Hoàn thiện tài liệu của bạn**

Để hoàn thiện tài liệu và làm rõ mục đích của nó với các nhà tuyển dụng tiềm năng, hãy đảm bảo hoàn thành phần **Mô tả dự án** và **Tóm tắt** của mẫu **Quyền đối với tệp trong Linux** .

Trong phần Mô tả dự án, hãy đưa ra cái nhìn tổng quan chung về kịch bản và những gì bạn đạt được thông qua Linux. Viết hai đến bốn câu.

Trong phần Tóm tắt, hãy cung cấp bản tóm tắt ngắn gọn về các nhiệm vụ trước đó và kết nối chúng với kịch bản. Viết khoảng hai đến bốn câu.

|  |
| --- |
| **What to Include in Your Response** |

**Những gì cần bao gồm trong phản hồi của bạn**

|  |
| --- |
| Be sure to include the following in your completed activity:   * Screenshots of your commands or typed versions of the commands * Explanations of your commands * A project description at the beginning * A summary at the end * Details on using **chmod** to update file permissions * Details on checking file permissions with **ls -la** * Details on interpreting the 10-character string that represents file permissions * Details on hidden files and directories |

Hãy chắc chắn bao gồm những điều sau đây trong hoạt động đã hoàn thành của bạn:

* Ảnh chụp màn hình lệnh của bạn hoặc phiên bản đã nhập của lệnh
* Giải thích các lệnh của bạn
* Mô tả dự án ở phần đầu
* Tóm tắt ở cuối
* Chi tiết về cách sử dụng **chmod** để cập nhật quyền truy cập tệp
* Chi tiết về kiểm tra quyền truy cập tệp bằng **ls -la**
* Chi tiết về cách diễn giải chuỗi 10 ký tự thể hiện quyền đối với tệp
* Chi tiết về các tập tin và thư mục ẩn

|  |
| --- |
| **Step 9: Assess your activity**  The following is a  self-assessment for your **Use Linux commands to manage file permissions** portfolio activity. You will use these statements to review your own work. The self-assessment process is an important part of the learning experience because it allows you to *objectively* assess your **Use Linux commands to manage file permissions** portfolio activity.  There are a total of 8 points possible for this activity and each statement is worth 1 point.  To complete the self-assessment, first open your **Use Linux commands to manage file permissions** portfolio activity. Then respond yes or no to each statement.  When you complete and submit your responses, you will receive a percentage score. This score will help you confirm whether you completed the required steps of the activity. The recommended passing grade for this project is at least 80% (or 7/8 points). If you want to increase your score, you can revise your project and then resubmit your responses to reflect any changes you made. Try to achieve at least 7 points before continuing on to the next course item. |

**Bước 9: Đánh giá hoạt động của bạn**

Sau đây là phần tự đánh giá **các lệnh Sử dụng Linux của bạn để quản lý** hoạt động danh mục quyền đối với tệp. Bạn sẽ sử dụng những tuyên bố này để xem xét công việc của riêng bạn. Quá trình tự đánh giá là một phần quan trọng trong trải nghiệm học tập vì nó cho phép bạn đánh giá *khách quan* **các lệnh Sử dụng Linux** của mình để quản lý hoạt động danh mục quyền đối với tệp.

Có tổng cộng 8 điểm cho hoạt động này và mỗi câu có giá trị 1 điểm.

Để hoàn tất quá trình tự đánh giá, trước tiên hãy mở **lệnh Sử dụng Linux để quản lý** hoạt động danh mục quyền đối với tệp. Sau đó trả lời có hoặc không cho mỗi câu.

Khi bạn hoàn thành và gửi câu trả lời của mình, bạn sẽ nhận được điểm phần trăm. Điểm số này sẽ giúp bạn xác nhận xem bạn đã hoàn thành các bước yêu cầu của hoạt động hay chưa. Điểm đậu được đề xuất cho dự án này ít nhất là 80% (hoặc 7/8 điểm). Nếu muốn tăng điểm, bạn có thể sửa lại dự án của mình rồi gửi lại phản hồi để phản ánh bất kỳ thay đổi nào bạn đã thực hiện. Cố gắng đạt được ít nhất 7 điểm trước khi tiếp tục học mục tiếp theo của khóa học.

***3.7. Portfolio Activity Exemplar: Use Linux commands to manage file permissions – Ví dụ về hoạt động danh mục đầu tư: Sử dụng các lệnh Linux để quản lý quyền truy cập tệp***

***3.8. Add and delete users – Thêm và xóa người dùng***

|  |
| --- |
| Welcome back! In this video, we are going to discuss adding and deleting users. This is related to the concept of authentication. Authentication is the process of a user proving that they are who they say they are in the system. |

Chào mừng trở lại! Trong video này, chúng tôisẽ thảo luận về việc thêm và xóa người dùng.Điều này liên quan đến khái niệm xác thực.Xác thực là quá trình của người dùngchứng minh rằng họ đúng như những gì họ nóihọ đang ở trong hệ thống.

|  |
| --- |
| Just like in a physical building, not all users should be allowed in. Not all users should get access to the system. But we also want to make sure everyone who should have access to the system has it. That's why we need to add users. New users can be new to the organization or new to a group. This could be related to a change in organizational structure or simply a directive from management to move someone. |

Giống như trong một tòa nhà vật chất,không phải tất cả người dùng đều được phép vào.Không phải tất cả người dùng đều có quyền truy cập vào hệ thống.Nhưng chúng tôi cũng muốn đảm bảo rằng mọi ngườiai nên có quyền truy cập vào hệ thống có nó.Đó là lý do tại sao chúng ta cần thêm người dùng.Người dùng mới có thể là người mới sử dụngtổ chức hoặc người mới vào một nhóm.Điều này có thể liên quan đến sự thay đổi trongcơ cấu tổ chức hay đơn giản là một chỉ thịtừ quản lý để di chuyển một ai đó.

|  |
| --- |
| And also, when users leave the organization, they need to be deleted. They should no longer have access to any part of the system. Or if they simply changed groups, they should be deleted from groups that they are no longer a part of. |

Ngoài ra, khi người dùng rời khỏi tổ chức,chúng cần phải được xóa.Đáng lẽ họ không còn cótruy cập vào bất kỳ phần nào của hệ thống.Hoặc nếu họ chỉ đơn giản là thay đổi nhóm,họ nên bị xóa khỏi nhómmà họ không còn là một phần của nữa.

|  |
| --- |
| Now that we've sorted out why it's important to add and delete users, let's discuss a different type of user, the root user. A root user, or superuser, is a user with elevated privileges to modify the system. Regular users have limitations, where the root does not. |

Bây giờ chúng ta đã tìm ra lý do tại saoquan trọng để thêm và xóa người dùng,hãy thảo luận về một loại người dùng khác, người dùng root.Người dùng root hoặc superuserlà người dùng có đặc quyền nâng cao để sửa đổi hệ thống.Người dùng thông thường có những hạn chế,nơi mà gốc không có.

|  |
| --- |
| Individuals who need to perform specific tasks can be temporarily added as root users. Root users can create, modify, or delete any file and run any program. Only root users or accounts with root privileges can add new users. So you may be wondering how you become a superuser. Well, one way is logging in as the root user, but running commands as the root user is considered to be bad practice when using Linux. |

Các cá nhân cần thực hiệncác tác vụ cụ thể có thể được thêm tạm thời với tư cách là người dùng root.Người dùng root có thể tạo, sửa đổi,hoặc xóa bất kỳ tập tin nào và chạy bất kỳ chương trình nào.Chỉ người dùng root hoặc tài khoản cóđặc quyền root có thể thêm người dùng mới.Vì vậy, bạn có thể tự hỏi làm thế nào bạn có thể trở thành siêu người dùng.Vâng, một cách là đăng nhập với tư cách người dùng root,nhưng việc chạy lệnh với tư cách là người dùng rootđược coi là hành vi không tốt khi sử dụng Linux.

|  |
| --- |
| Why is running commands as a root user potentially problematic? The first problem with logging in as root is the security risks. Malicious actors will try to breach the root account. Since it's the most powerful account, to stay safe, the root account should have logins disabled. Another problem is that it's very easy to make irreversible mistakes. |

Tại sao các lệnh chạy nhưngười dùng root có khả năng gặp vấn đề?Vấn đề đầu tiên khi đăng nhậpnhư root là những rủi ro bảo mật.Những kẻ độc hại sẽ cố gắng xâm nhập vào tài khoản root.Vì đây là tài khoản mạnh mẽ nhất nên để giữ an toàn,tài khoản root sẽ bị vô hiệu hóa thông tin đăng nhập.Một vấn đề nữa là nó rấtdễ mắc phải những sai lầm không thể sửa chữa được.

|  |
| --- |
| It's very easy to type the wrong command in the CLI, and if you're running as the root user, you run a higher risk of making an irreversible mistake, such as permanently deleting a directory. Finally, there's the concern of accountability. In a multi-user environment like Linux, there are many users. If a user is running as root, there is no way to track who exactly ran a command. One solution to help solve this problem is sudo. |

Rất dễ gõ sai lệnh trong CLI,và nếu bạn đang chạy với tư cách người dùng root,bạn có nguy cơ mắc phải sai lầm không thể sửa chữa cao hơn,chẳng hạn như xóa vĩnh viễn một thư mục.Cuối cùng là mối quan tâm về trách nhiệm giải trình.Trong môi trường nhiều người dùng như Linux,có rất nhiều người dùng.Nếu người dùng đang chạy bằng root,không có cách nào để theo dõi chính xác ai đã thực hiện lệnh.Một giải pháp giúp giải quyết vấn đề này là sudo.

|  |
| --- |
| sudo is a command that temporarily grants elevated permissions to specific users. This provides more of a controlled approach compared to root, which runs every command with root privileges. sudo solves lots of problems associated with running as root. |

sudo là lệnh cấp tạm thờiquyền nâng cao cho người dùng cụ thể.Điều này cung cấp nhiều hơnmột cách tiếp cận có kiểm soát so với root,chạy mọi lệnh với quyền root.sudo giải quyết được rất nhiềucác vấn đề liên quan đến việc chạy bằng root.

|  |
| --- |
| sudo comes from super-user-do and lets you execute commands as an elevated user without having to sign in and out of another account. Running sudo will prompt you to enter the password for the user you're currently logged in as. Not all users on a system can become a superuser. Users must be granted sudo access through a configuration file called the sudoers file. |

sudo đến từ siêu người dùngvà cho phép bạn thực hiện các lệnh nhưmột người dùng nâng cao mà không cầnđể đăng nhập và đăng xuất khỏi tài khoản khác.Chạy sudo sẽ nhắc bạn nhậpmật khẩu cho người dùng mà bạn hiện đang đăng nhập.Không phải tất cả người dùng trên hệ thống đều có thể trở thành siêu người dùng.Người dùng phải được cấp quyền truy cập sudo thông quamột tệp cấu hình được gọi là tệp sudoers.

|  |
| --- |
| Now that we've learned about sudo, let's learn how we can use it with another command to add users. This command is useradd. useradd adds a user to the system. Only root or users with sudo privileges can use a useradd command. Let's look at a specific example in which we need to add a user. We'll imagine a new representative is joining the sales department and will be given the username of salesrep7. We're tasked with adding them to the system. |

Bây giờ chúng ta đã tìm hiểu về sudo,hãy tìm hiểu cách chúng ta có thể sử dụng nó vớimột lệnh khác để thêm người dùng.Lệnh này là useradd.useradd thêm người dùng vào hệ thống.Chỉ root hoặc người dùng cóđặc quyền sudo có thể sử dụng lệnh useradd.Hãy xem một ví dụ cụ thểtrong đó chúng tôi cần thêm người dùng.Chúng ta sẽ tưởng tượng một đại diện mới đang tham giabộ phận bán hàng và sẽ được traotên người dùng của salesrep7.Chúng tôi được giao nhiệm vụ thêm chúng vào hệ thống.

|  |
| --- |
| Let's try adding the new user. First, we need to use the sudo command, followed by the useradd command, and then last, the username we want to add, in this case, salesrep7. This command doesn't display anything on the screen. But since we get a new Bash cursor and not an error message, we can feel confident that the command worked successfully. If it didn't, an error message would have appeared. Sometimes an error has to do with something simple like misspelling useradd. Or, it might be because we didn't have sudo privileges. |

Hãy thử thêm người dùng mới.Đầu tiên, chúng ta cần sử dụng lệnh sudo,theo sau là lệnh useradd,và cuối cùng là tên người dùng mà chúng tôi muốn thêm,trong trường hợp này, salesrep7.Lệnh này không hiển thị bất cứ điều gì trên màn hình.Nhưng vì chúng ta có một con trỏ Bash mớivà không phải là một thông báo lỗi,chúng ta có thể cảm thấy tự tin rằnglệnh đã hoạt động thành công.Nếu không, một thông báo lỗi sẽ xuất hiện.Đôi khi một lỗi liên quan đếnmột cái gì đó đơn giản như lỗi chính tả useradd.Hoặc có thể là do chúng tôi không có đặc quyền sudo.

|  |
| --- |
| Now let's learn how to do the opposite. Let's learn how to delete a user with userdel. userdel deletes a user from the system. Similarly, we need root permissions that we'll access through sudo to use userdel. Let's go back to our example of the user we added. Let's imagine two months later, the sales representative that we just added to the system leaves the company. That user should no longer have access to the system. Let's delete that user from the system. |

Bây giờ hãy học cách làm điều ngược lại.Hãy tìm hiểu cách xóa người dùng bằng userdel.userdel xóa người dùng khỏi hệ thống.Tương tự, chúng tôi cần quyền root để có thểtruy cập thông qua sudo để sử dụng userdel.Hãy quay lại ví dụ về người dùng mà chúng tôi đã thêm.Hãy tưởng tượng hai tháng sau,đại diện bán hàng mà chúng tôi vừađược thêm vào hệ thống sẽ rời khỏi công ty.Người dùng đó sẽ không còn quyền truy cập vào hệ thống nữa.Hãy xóa người dùng đó khỏi hệ thống.

|  |
| --- |
| Again, the sudo command is used first, then we add the userdel command. Last, we add the name of the user we want to delete. Again, we know it ran successfully because there is a new Bash cursor and not an error message. |

Một lần nữa, lệnh sudo được sử dụng đầu tiên,sau đó chúng ta thêm lệnh userdel.Cuối cùng, chúng tôi thêm tên của người dùng mà chúng tôi muốn xóa.Một lần nữa, chúng tôi biết nó đã chạy thành công vìcó một con trỏ Bash mới và không có thông báo lỗi.

|  |
| --- |
| Now, we've covered how to add and delete users and how these actions require sudo. When using sudo, we have to use our best judgment. These special privileges must be used responsibly to ensure a secure system. |

Bây giờ, chúng ta đã đề cập đến cách thêm và xóangười dùng và cách những hành động này yêu cầu sudo.Khi sử dụng sudo, chúng ta phải sử dụng khả năng phán đoán tốt nhất của mình.Những đặc quyền này phải được sử dụngcó trách nhiệm đảm bảo một hệ thống an toàn.

***3.9.Responsible use of sudo – Sử dụng sudo có trách nhiệm***

|  |
| --- |
| **Responsible use of sudo** |

**Sử dụng sudo có trách nhiệm**

|  |
| --- |
| Previously, you explored authorization, authentication, and Linux commands with **sudo**, **useradd**, and **userdel**. The **sudo** command is important for security analysts because it allows users to have elevated permissions without risking the system by running commands as the root user. You’ll continue exploring authorization, authentication, and Linux commands in this reading and learn two more commands that can be used with **sudo**: **usermod** and **chown**. |

Trước đây, bạn đã khám phá các lệnh ủy quyền, xác thực và Linux bằng **sudo** , **useradd** và **userdel** . Lệnh **sudo** rất quan trọng đối với các nhà phân tích bảo mật vì nó cho phép người dùng có quyền nâng cao mà không gây rủi ro cho hệ thống bằng cách chạy các lệnh với tư cách là người dùng root. Bạn sẽ tiếp tục khám phá các lệnh ủy quyền, xác thực và Linux trong bài đọc này và tìm hiểu thêm hai lệnh có thể được sử dụng với **sudo** : **usermod** và **chown** .

|  |
| --- |
| **Responsible use of sudo** |

**Sử dụng sudo có trách nhiệm**

|  |
| --- |
| To manage authorization and authentication, you need to be a **root user,** or a user with elevated privileges to modify the system. The root user can also be called the “super user.” You become a root user by logging in as the root user. However, running commands as the root user is not recommended in Linux because it can create security risks if malicious actors compromise that account. It’s also easy to make irreversible mistakes, and the system can’t track who ran a command. For these reasons, rather than logging in as the root user, it’s recommended you use **sudo** in Linux when you need elevated privileges. |

Để quản lý ủy quyền và xác thực, bạn cần phải là **người dùng root** hoặc người dùng có đặc quyền nâng cao để sửa đổi hệ thống. Người dùng root cũng có thể được gọi là “siêu người dùng”. Bạn trở thành người dùng root bằng cách đăng nhập với tư cách là người dùng root. Tuy nhiên, việc chạy lệnh với tư cách người dùng root không được khuyến khích trong Linux vì nó có thể tạo ra rủi ro bảo mật nếu tác nhân độc hại xâm phạm tài khoản đó. Bạn cũng dễ mắc phải những lỗi không thể khắc phục được và hệ thống không thể theo dõi ai đã thực hiện lệnh. Vì những lý do này, thay vì đăng nhập với tư cách người dùng root, bạn nên sử dụng **sudo** trong Linux khi cần đặc quyền nâng cao.

|  |
| --- |
| The **sudo** command temporarily grants elevated permissions to specific users. The name of this command comes from “super user do.” Users must be given access in a configuration file to use **sudo**. This file is called the “sudoers file.” Although using **sudo** is preferable to logging in as the root user, it's important to be aware that users with the elevated permissions to use **sudo** might be more at risk in the event of an attack. |

Lệnh **sudo** tạm thời cấp quyền nâng cao cho người dùng cụ thể. Tên của lệnh này xuất phát từ “super user do”. Người dùng phải được cấp quyền truy cập vào tệp cấu hình để sử dụng **sudo** . Tệp này được gọi là “tệp sudoers”. Mặc dù sử dụng **sudo** tốt hơn là đăng nhập với tư cách người dùng root nhưng điều quan trọng cần lưu ý là những người dùng có quyền nâng cao để sử dụng **sudo** có thể gặp nhiều rủi ro hơn trong trường hợp bị tấn công.

|  |
| --- |
| You can compare this to a hotel with a master key. The master key can be used to access any room in the hotel. There are some workers at the hotel who need this key to perform their work. For example, to clean all the rooms, the janitor would scan their ID badge and then use this master key. However, if someone outside the hotel’s network gained access to the janitor’s ID badge and master key, they could access any room in the hotel. In this example, the janitor with the master key represents a user using **sudo** for elevated privileges. Because of the dangers of **sudo**, only users who really need to use it should have these permissions. |

Bạn có thể so sánh điều này với một khách sạn có chìa khóa chính. Chìa khóa chính có thể được sử dụng để vào bất kỳ phòng nào trong khách sạn. Có một số công nhân tại khách sạn cần chiếc chìa khóa này để thực hiện công việc của mình. Ví dụ: để dọn dẹp tất cả các phòng, người gác cổng sẽ quét thẻ căn cước của họ rồi sử dụng chìa khóa chính này. Tuy nhiên, nếu ai đó bên ngoài mạng của khách sạn có được quyền truy cập vào thẻ ID và chìa khóa chính của người gác cổng, họ có thể truy cập vào bất kỳ phòng nào trong khách sạn. Trong ví dụ này, người gác cổng có khóa chính đại diện cho người dùng sử dụng **sudo** để có các đặc quyền nâng cao. Vì sự nguy hiểm của **sudo** , chỉ những người dùng thực sự cần sử dụng nó mới có những quyền này.

|  |
| --- |
| Additionally, even if you need access to **sudo**, you should be careful about using it with only the commands you need and nothing more. Running commands with **sudo** allows users to bypass the typical security controls that are in place to prevent elevated access to an attacker. |

Ngoài ra, ngay cả khi bạn cần quyền truy cập vào **sudo** , bạn nên cẩn thận khi chỉ sử dụng nó với các lệnh bạn cần và không có gì hơn. Việc chạy lệnh bằng **sudo** cho phép người dùng bỏ qua các biện pháp kiểm soát bảo mật thông thường được áp dụng để ngăn chặn kẻ tấn công có quyền truy cập cao.

|  |
| --- |
| **Note**: Be aware of **sudo** if copying commands from an online source. It’s important you don’t use **sudo** accidentally. |

**Lưu ý** : Hãy lưu ý **sudo** nếu sao chép lệnh từ nguồn trực tuyến. Điều quan trọng là bạn không vô tình sử dụng **sudo** .

|  |
| --- |
| **Authentication and authorization with sudo** |

**Xác thực và ủy quyền với sudo**

|  |
| --- |
| You can use **sudo** with many authentication and authorization management tasks. As a reminder, **authentication** is the process of verifying who someone is, and **authorization** is the concept of granting access to specific resources in a system. Some of the key commands used for these tasks include the following: |

Bạn có thể sử dụng **sudo** với nhiều tác vụ quản lý xác thực và ủy quyền. Xin nhắc lại, **xác thực** là quá trình xác minh ai đó là ai và **ủy quyền** là khái niệm cấp quyền truy cập vào các tài nguyên cụ thể trong hệ thống. Một số lệnh chính được sử dụng cho các tác vụ này bao gồm:

|  |
| --- |
| **useradd** |

**useradd**

|  |
| --- |
| The **useradd** command adds a user to the system. To add a user with the username of **fgarcia** with **sudo**, enter **sudo useradd fgarcia**. There are additional options you can use with **useradd**: |

Lệnh **useradd** thêm người dùng vào hệ thống. Để thêm người dùng có tên người dùng **fgarcia** bằng **sudo** , hãy nhập **sudo useradd fgarcia** . Có các tùy chọn bổ sung mà bạn có thể sử dụng với **useradd** :

|  |
| --- |
| * **-g**: Sets the user’s default group, also called their primary group * **-G**: Adds the user to additional groups, also called supplemental or secondary groups |

* **-g** : Đặt nhóm mặc định của người dùng, còn được gọi là nhóm chính của họ
* **-G** : Thêm người dùng vào các nhóm bổ sung, còn được gọi là nhóm bổ sung hoặc nhóm phụ

|  |
| --- |
| To use the **-g** option, the primary group must be specified after **-g**. For example, entering **sudo useradd -g security fgarcia** adds **fgarcia** as a new user and assigns their primary group to be **security**. |

Để sử dụng tùy chọn **-g** , nhóm chính phải được chỉ định sau **-g** . Ví dụ: nhập **sudo useradd -g security fgarcia** sẽ thêm **fgarcia** làm người dùng mới và chỉ định nhóm chính của họ là **security** .

|  |
| --- |
| To use the **-G** option, the supplemental group must be passed into the command after **-G**. You can add more than one supplemental group at a time with the **-G** option. Entering **sudo useradd -G finance,admin fgarcia** adds **fgarcia** as a new user and adds them to the existing **finance** and **admin** groups. |

Để sử dụng tùy chọn **-G** , nhóm bổ sung phải được chuyển vào lệnh sau **-G** . Bạn có thể thêm nhiều nhóm bổ sung cùng một lúc bằng tùy chọn **-G** . Nhập **sudo useradd -G Finance,admin fgarcia** thêm **fgarcia** làm người dùng mới và thêm họ vào nhóm **tài chính** và **quản trị viên** hiện có .

|  |
| --- |
| **usermod** |

**usermod**

|  |
| --- |
| The **usermod** command modifies existing user accounts. The same **-g** and **-G** options from the **useradd** command can be used with **usermod** if a user already exists. |

Lệnh **usermod** sửa đổi tài khoản người dùng hiện có. Các tùy chọn **-g** và **-G** tương tự từ lệnh **useradd** có thể được sử dụng với **usermod** nếu người dùng đã tồn tại.

|  |
| --- |
| To change the primary group of an existing user, you need the **-g** option. For example, entering **sudo usermod -g executive fgarcia** would change **fgarcia**’s primary group to the **executive** group. |

Để thay đổi nhóm chính của người dùng hiện tại, bạn cần tùy chọn **-g** . Ví dụ: nhập **sudo usermod -g điều hành fgarcia** sẽ thay đổi nhóm chính của **fgarcia thành nhóm điều hành** .

|  |
| --- |
| To add a supplemental group for an existing user, you need the **-G** option. You also need a **-a** option, which appends the user to an existing group and is only used with the **-G** option. For example, entering **sudo usermod -a -G marketing fgarcia** would add the existing **fgarcia** user to the supplemental **marketing** group. |

Để thêm nhóm bổ sung cho người dùng hiện tại, bạn cần tùy chọn **-G** . Bạn cũng cần tùy chọn **-a** , tùy chọn này sẽ thêm người dùng vào nhóm hiện có và chỉ được sử dụng với tùy chọn **-G** . Ví dụ: nhập **sudo usermod -a -G marketing fgarcia** sẽ thêm người dùng **fgarcia** hiện tại vào nhóm **tiếp thị** bổ sung .

|  |
| --- |
| **Note:** When changing the supplemental group of an existing user, if you don't include the **-a** option, **-G** will replace any existing supplemental groups with the groups specified after **usermod**.  Using **-a** with **-G** ensures that the new groups are added but existing groups are not replaced. |

**Lưu ý:** Khi thay đổi nhóm bổ sung của người dùng hiện tại, nếu bạn không bao gồm tùy chọn **-a** , **-G** sẽ thay thế mọi nhóm bổ sung hiện có bằng các nhóm được chỉ định sau **usermod** . Sử dụng **-a** với **-G** đảm bảo rằng các nhóm mới được thêm vào nhưng các nhóm hiện có không bị thay thế.

|  |
| --- |
| There are other options you can use with **usermod** to specify how you want to modify the user, including: |

Có các tùy chọn khác mà bạn có thể sử dụng với **usermod** để chỉ định cách bạn muốn sửa đổi người dùng, bao gồm:

|  |
| --- |
| * **-d**: Changes the user’s home directory. * **-l**: Changes the user’s login name. * **-L**: Locks the account so the user can’t log in. |

* **-d** : Thay đổi thư mục chính của người dùng.
* **-l** : Thay đổi tên đăng nhập của người dùng.
* **-L** : Khóa tài khoản khiến người dùng không thể đăng nhập.

|  |
| --- |
| The option always goes after the **usermod** command. For example, to change **fgarcia**’s home directory to **/home/garcia\_f**, enter **sudo usermod -d /home/garcia\_f fgarcia**. The option **-d** directly follows the command **usermod** before the other two needed arguments. |

Tùy chọn này luôn đi sau lệnh **usermod** . Ví dụ: để thay đổi thư mục chính của **fgarcia thành /home/garcia\_f** , hãy nhập **sudo usermod -d /home/garcia\_f fgarcia** . Tùy chọn **-d** trực tiếp theo sau lệnh **usermod** trước hai đối số cần thiết khác.

|  |
| --- |
| **userdel** |

**userdel**

|  |
| --- |
| The **userdel** command deletes a user from the system. For example, entering **sudo userdel fgarcia** deletes **fgarcia** as a user. Be careful before you delete a user using this command. |

Lệnh **userdel** xóa người dùng khỏi hệ thống. Ví dụ: nhập **sudo userdel fgarcia** sẽ xóa **fgarcia** với tư cách người dùng. Hãy cẩn thận trước khi bạn xóa người dùng bằng lệnh này.

|  |
| --- |
| The **userdel** command doesn’t delete the files in the user’s home directory unless you use the **-r** option. Entering **sudo userdel -r fgarcia** would delete **fgarcia** as a user and delete all files in their home directory. Before deleting any user files, you should ensure you have backups in case you need them later. |

Lệnh **userdel** không xóa các tập tin trong thư mục chính của người dùng trừ khi bạn sử dụng tùy chọn **-r** . Nhập **sudo userdel -r fgarcia** sẽ xóa **fgarcia** với tư cách người dùng và xóa tất cả các tệp trong thư mục chính của họ. Trước khi xóa bất kỳ tệp người dùng nào, bạn nên đảm bảo có bản sao lưu phòng trường hợp sau này bạn cần chúng.

|  |
| --- |
| **Note**: Instead of deleting the user, you could consider deactivating their account with **usermod -L**. This prevents the user from logging in while still giving you access to their account and associated permissions. For example, if a user left an organization, this option would allow you to identify which files they have ownership over, so you could move this ownership to other users. |

**Lưu ý** : Thay vì xóa người dùng, bạn có thể cân nhắc việc vô hiệu hóa tài khoản của họ bằng **usermod -L** . Điều này ngăn người dùng đăng nhập trong khi vẫn cấp cho bạn quyền truy cập vào tài khoản của họ và các quyền liên quan. Ví dụ: nếu người dùng rời khỏi tổ chức, tùy chọn này sẽ cho phép bạn xác định những tệp họ có quyền sở hữu để bạn có thể chuyển quyền sở hữu này cho những người dùng khác.

|  |
| --- |
| **chown** |

**chown**

|  |
| --- |
| The **chown** command changes ownership of a file or directory. You can use **chown** to change user or group ownership. To change the user owner of the **access.txt** file to **fgarcia**, enter **sudo chown fgarcia access.txt**. To change the group owner of **access.txt** to **security**, enter **sudo chown :security access.txt**. You must enter a colon (**:**) before **security** to designate it as a group name. |

Lệnh **chown** thay đổi quyền sở hữu của một tập tin hoặc thư mục. Bạn có thể sử dụng **chown** để thay đổi quyền sở hữu của người dùng hoặc nhóm. Để thay đổi chủ sở hữu người dùng của tệp **access.txt** thành **fgarcia** , hãy nhập **sudo chown fgarcia access.txt** . Để thay đổi chủ sở hữu nhóm của **access.txt** thành **security** , hãy nhập **sudo chown :security access.txt** . Bạn phải nhập dấu hai chấm ( **:** ) trước **phần bảo mật** để chỉ định đó là tên nhóm.

|  |
| --- |
| Similar to **useradd**, **usermod**, and **userdel**, there are additional options that can be used with **chown**. |

Tương tự như **useradd** , **usermod** và **userdel** , có những tùy chọn bổ sung có thể được sử dụng với **chown** .

|  |
| --- |
| **Key takeaways** |

**Bài học chính**

|  |
| --- |
| Authentication is the process of a user verifying their identity, and authorization is the process of determining what they have access to. You can use the **sudo** command to temporarily run commands with elevated privileges to complete authentication and authorization management tasks. Specifically, **useradd**, **userdel,** **usermod**, and **chown** can be used to manage users and file ownership. |

Xác thực là quá trình người dùng xác minh danh tính của họ và ủy quyền là quá trình xác định những gì họ có quyền truy cập. Bạn có thể sử dụng lệnh **sudo** để tạm thời chạy các lệnh có đặc quyền nâng cao nhằm hoàn thành các tác vụ quản lý ủy quyền và xác thực. Cụ thể, **useradd** , **userdel , usermod** và **chown** có thể được sử dụng để quản lý người dùng và quyền sở hữu tệp.

***3.10. Activity: Add and manage users with Linux commands – Hoạt động: Thêm và quản lý người dùng bằng lệnh Linux***

***3.11. Optional Exemplar: Add and manage users with Linux commands – Mẫu tùy chọn: Thêm và quản lý người dùng bằng các lệnh Linux***

***3.12. Test your knowledge: Authenticate and authorize users – Kiểm tra kiến ​​thức của bạn: Xác thực và ủy quyền cho người dùng***

**4. Get help in Linux – Nhận trợ giúp về Linux**

***4.1. Damar: My journey into Linux commands – Damar: Hành trình của tôi vào các lệnh Linux***

|  |
| --- |
| [MUSIC] My name is Damar, I'm a security engineer here at Google. I've always wanted to get into cybersecurity since I was a kid. A lot of the cartoons I watched, they had like floppy disks or flash drives, and they would put that in the computer and kind of like cause havoc. [LAUGH] So I always thought that was really cool. I've had quite a bit of jobs before coming to Google. I originally started out making smoothies at Jamba Juice. I got my first IT technological kind of job at Geek Squad and then eventually came here and became a security engineer. My advice to people trying to get into cybersecurity is it may be a lot easier than you think. [LAUGH] It definitely was a lot easier than I thought. Something that I learned jumping in myself is that you're not going to be able to learn everything all at once, and you're not going to need to know everything all at once. Linux is very important because it's broadly used across pretty much every company. You may use Linux to curate logs. It's a very common practice you may also use Linux to set up bash jobs that will help with routine tasks within Linux. I first got interested in learning Linux from the Jurassic Park movie. There's a scene in the movie where they need to reactivate the electrical doors, and they have to use a UNIX operating system to do so. So later on, I learned what UNIX was and how Linux came from it, and it inspired me to learn more about Linux. The best advice I can give someone that's trying to learn Linux and Linux commands is, don't get discouraged by any small hiccups that come up. Just keep with it. Stick with it. Think of it as when you first learned to swim, right, you probably weren't that great at it. [LAUGH] It was frustrating, and you were probably a little scared, but you're stuck with it and I hope that you're able to swim now. [LAUGH] There are a plethora of support resources when learning Linux. One good example is the discussion forum in the certificate course. Another avenue of support for learning Linux is just googling answers using Stack Overflow, maybe even making a Reddit post. I love working in cybersecurity. It's pretty satisfying to know that me and my team and then like all the other security teams here at Google are helping protect people online from things they may not even know about. [SOUND] |

[ÂM NHẠC]Tên tôi là Damar, tôi là kỹ sư bảo mật tại Google.Tôi luôn muốn tham gia vào lĩnh vực an ninh mạng từ khi còn nhỏ.Rất nhiều phim hoạt hình tôi đã xem, chúng có dạng đĩa mềm hoặc ổ đĩa flash, vàhọ sẽ đặt nó vào máy tính và kiểu như gây ra sự tàn phá.[CƯỜI] Vì vậy, tôi luôn nghĩ điều đó thật tuyệt.Tôi đã làm khá nhiều công việc trước khi đến với Google.Ban đầu tôi bắt đầu làm sinh tố tại Jamba Juice.Tôi nhận được công việc công nghệ CNTT đầu tiên tại Geek Squad vàrồi cuối cùng đến đây và trở thành kỹ sư bảo mật.Lời khuyên của tôi dành cho những người đang cố gắng tham gia vào lĩnh vực an ninh mạng là nó có thể dễ dàng hơn rất nhiềuhơn bạn nghĩ.[CƯỜI] Nó chắc chắn dễ dàng hơn tôi nghĩ rất nhiều.Điều mà tôi đã học được khi tự mình nhảy vào là bạn sẽ không thểhọc tất cả mọi thứ cùng một lúc, vàbạn sẽ không cần phải biết tất cả mọi thứ cùng một lúc.Linux rất quan trọng vì nó được sử dụng rộng rãiđược sử dụng ở hầu hết mọi công ty.Bạn có thể sử dụng Linux để quản lý nhật ký.Đó là một thực tế rất phổ biến mà bạn cũng có thể sử dụng Linux để thiết lậpcác công việc bash sẽ giúp thực hiện các tác vụ thông thường trong Linux.Lần đầu tiên tôi quan tâm đến việc học Linux từ bộ phim Công viên kỷ Jura.Có một cảnh trong phim họ cần kích hoạt lại cửa điện,và họ phải sử dụng hệ điều hành UNIX để làm việc đó.Vì vậy sau này tôi đã biết UNIX là gì và Linux hình thành từ nó như thế nào,và nó truyền cảm hứng cho tôi tìm hiểu thêm về Linux.Lời khuyên tốt nhất tôi có thể đưa ra cho ai đó đang cố gắng học Linux vàCác lệnh của Linux là đừng nản lòng trước bất kỳ trục trặc nhỏ nào xảy ra.Cứ giữ nó đi.Hãy kiên trì với nó.Hãy nghĩ về nó như lần đầu tiên bạn học bơi, phải không,có lẽ bạn không giỏi việc đó lắm.[CƯỜI] Thật là bực bội và có lẽ bạn cũng hơi sợ hãi, nhưngbạn đang mắc kẹt với nó và tôi hy vọng rằng bây giờ bạn có thể bơi được.[CƯỜI] Có rất nhiều tài nguyên hỗ trợ khi học Linux.Một ví dụ điển hình là diễn đàn thảo luận trong khóa học cấp chứng chỉ.Một cách khác để hỗ trợ việc học Linux là tìm câu trả lời trên Google bằng cách sử dụngTràn ngăn xếp, thậm chí có thể tạo một bài đăng trên Reddit.Tôi thích làm việc trong lĩnh vực an ninh mạng.Thật là hài lòng khi biết rằng tôi và nhóm của tôi vàthì giống như tất cả các nhóm bảo mật khác tại Google đang giúp bảo vệ mọi ngườitrực tuyến từ những điều họ thậm chí có thể không biết.[ÂM THANH]

***4.2. The Linux community – Cộng đồng Linux***

|  |
| --- |
| There are so many others just like you who will be using the command line. Linux's popularity and ease of use has created a large online community that constantly publishes information to help users learn how to operate Linux. Since Linux is open-source, it has become a global community of users that contribute frequently. |

Có rất nhiều người khác giống như bạnai sẽ sử dụng dòng lệnh.Sự phổ biến và dễ sử dụng của Linuxđã tạo ra một cộng đồng trực tuyến lớnliên tục công bố thông tin tớigiúp người dùng học cách vận hành Linux.Vì Linux là mã nguồn mở nênnó đã trở thành một cộng đồng toàn cầu củangười dùng đóng góp thường xuyên.

|  |
| --- |
| This global community is a huge resource for all Linux users because users can find answers for everyday tasks. Just searching on the internet will provide many answers. The easiest way to troubleshoot a task is to search and read about how someone else has done it. Looking for resources on how to execute a task is a good way for beginners to continue learning. |

Cộng đồng toàn cầu này là một nguồn tài nguyên khổng lồ chotất cả người dùng Linux vì người dùngcó thể tìm thấy câu trả lời cho công việc hàng ngày.Chỉ cần search trên mạng sẽ có nhiều câu trả lời.Cách dễ nhất để khắc phục sự cố của một tác vụ là tìm kiếm vàđọc về cách người khác đã làm điều đó.Tìm kiếm tài nguyên về cách thực hiệnmột nhiệm vụ là một cách tốt để người mới bắt đầu tiếp tục học tập.

|  |
| --- |
| So far, you've learned how to add users, but imagine if later you want to add a new group. One way to learn how to do this is to search online. Let's give this a try through a Google search. The search results give us many options for adding a group in Linux. |

Cho đến nay, bạn đã học được cách thêm người dùng,nhưng hãy tưởng tượng nếu sau này bạn muốn thêm một nhóm mới.Một cách để tìm hiểu cách thực hiện việc này là tìm kiếm trực tuyến.Hãy thử điều này thông qua tìm kiếm trên Google.Kết quả tìm kiếm cho chúng tanhiều tùy chọn để thêm nhóm trong Linux.

|  |
| --- |
| Another reputable source is a Unix & Linux Stack Exchange. Their answers are ranked with points to display high-quality answers. Many questions relate to more advanced users and are geared towards troubleshooting. |

Một nguồn uy tín khác làTrao đổi ngăn xếp Unix & Linux.Câu trả lời của họ được xếp hạng vớiđiểm để hiển thị câu trả lời chất lượng cao.Nhiều câu hỏi liên quan đếnngười dùng cao cấp hơn vàđang hướng tới việc khắc phục sự cố.

|  |
| --- |
| Well, now you know where to get some extra support whenever in doubt about topics in Linux. There is a lot of support just a click away. Coming up, we'll learn how to get support from within the command line itself. Join me. |

Chà, bây giờ bạn biết nơi để nhận được sự hỗ trợ thêmbất cứ khi nào có nghi ngờ về các chủ đề trong Linux.Có rất nhiều hỗ trợ chỉ bằng một cú nhấp chuột.Sắp tới, chúng ta sẽ tìm hiểu cách nhận được sự hỗ trợtừ bên trong dòng lệnh. Tham gia với tôi.

***4.3. Man pages within the shell – Các trang Man bên trong shell***

|  |
| --- |
| Welcome back! In this video, we're going to discuss some resources that are available directly through the shell and can help you while working in Linux. One of the great things about Linux is that you can get help right through the command line. The first command that can help you in this way is: man. |

Chào mừng trở lại! Trong video này,chúng ta sẽ thảo luận về một số tài nguyên có sẵntrực tiếp qua vỏ và có thểgiúp đỡ bạn khi làm việc trên Linux.Một trong những điều tuyệt vời về Linux làrằng bạn có thể nhận trợ giúp ngay thông qua dòng lệnh.Lệnh đầu tiên có thể giúp bạn theo cách này là: man.

|  |
| --- |
| man displays information on other commands and how they work. The name of this command comes from the word manual. Let's examine this more closely by using man to get information about the usermod command. After man, we type the name of this command. The information that man returns includes a general description. It also contains information about each of usermod's options. For example, the option -d can be added to usermod to change a user's home directory. man provides a lot of information, but sometimes we just need a quick reference on what a command does. In that case, you use whatis. whatis displays a description of a command on a single line. |

man hiển thị thông tin trêncác lệnh khác và cách chúng hoạt động.Tên của lệnh này xuất phát từ hướng dẫn từ.Hãy kiểm tra điều này chặt chẽ hơn bằng cách sử dụngman để lấy thông tin về lệnh usermod.Sau man, chúng ta gõ tên của lệnh này.Thông tin người đàn ông đótrả về bao gồm một mô tả chung.Nó cũng chứa thông tinvề từng tùy chọn của usermod.Ví dụ: tùy chọn -d có thể làđược thêm vào usermod để thay đổi thư mục chính của người dùng.con người cung cấp rất nhiều thông tin,nhưng đôi khi chúng ta chỉ cầnmột tài liệu tham khảo nhanh về những gì một lệnh làm.Trong trường hợp đó, bạn sử dụng whatis.whatis hiển thị mô tảcủa một lệnh trên một dòng.

|  |
| --- |
| Let's say you heard a co-worker mention a command like tail. You've never heard of this command before, but you can find out what it does. Simply use the command, whatis tail, and learn that it outputs the last part of files. |

Giả sử bạn đã nghe thấy một đồng nghiệpđề cập đến một lệnh như tail.Bạn chưa bao giờ nghe lệnh này trước đây,nhưng bạn có thể tìm hiểu xem nó làm gì.Đơn giản chỉ cần sử dụng lệnh,đuôi là gì và tìm hiểu điều đónó xuất ra phần cuối cùng của tập tin.

|  |
| --- |
| Sometimes we might not even know what command to look up. This is where apropos can help us. apropos searches the manual page descriptions for a specified string. Let's try it out. Let's say you have a task that requires you to change a password, but you're not quite sure how to do this. If we use the apropos command with the string password, this will display a large number of commands with that word. This helps somewhat, but it still may be difficult to find what we need. But we can filter this by adding the -a option and an additional string. This option will return only the commands that contain both strings. In our case, since we want to change the password, let's look for commands with both: change and password. Now, the output has been limited to the most relevant commands. |

Đôi khi chúng ta thậm chí có thể không biết nên tra cứu lệnh nào.Đây là nơi apropos có thể giúp chúng tôi.apropos tìm kiếm các mô tả trang thủ côngcho một chuỗi được chỉ định. Hãy thử nó.Giả sử bạn có một nhiệm vụyêu cầu bạn thay đổi mật khẩu,nhưng bạn không chắc chắn về cách thực hiện việc này.Nếu chúng ta sử dụng lệnh apropos với mật khẩu chuỗi,điều này sẽ hiển thị một số lượng lớncác lệnh có từ đó.Điều này giúp ích phần nào,nhưng vẫn có thể khó tìm được thứ chúng ta cần.Nhưng chúng ta có thể lọc cái này bằng cách thêmtùy chọn -a và một chuỗi bổ sung.Tùy chọn này sẽ trở lạichỉ các lệnh có chứa cả hai chuỗi.Trong trường hợp của chúng tôi, vì chúng tôi muốn thay đổi mật khẩu,hãy tìm các lệnh có cả hai: thay đổi và mật khẩu.Bây giờ, đầu ra đã đượcgiới hạn ở các lệnh có liên quan nhất.

|  |
| --- |
| These commands make it a lot easier to navigate the Linux command line. As a new analyst, you won't have all the answers all the time, but you can learn where to find them. |

Những lệnh này làm cho nó rất nhiềudễ dàng hơn để điều hướng dòng lệnh Linux.Là một nhà phân tích mới,không phải lúc nào bạn cũng có được mọi câu trả lời,nhưng bạn có thể tìm hiểu nơi để tìm thấy chúng.

***4.4. Linux resources – Tài nguyên Linux***

|  |
| --- |
| **Linux resources** |

**Tài nguyên Linux**

|  |
| --- |
| Previously, you were introduced to the Linux community and some resources that exist to help Linux users. Linux has many options available to give users the information they need. This reading will review these resources. When you’re aware of the resources available to you, you can continue to learn Linux independently. You can also discover even more ways that Linux can support your work as a security analyst. |

Trước đây, bạn đã được giới thiệu về cộng đồng Linux và một số tài nguyên hiện có để trợ giúp người dùng Linux. Linux có sẵn nhiều tùy chọn để cung cấp cho người dùng thông tin họ cần. Bài đọc này sẽ xem xét các tài nguyên này. Khi bạn biết về các tài nguyên có sẵn cho mình, bạn có thể tiếp tục học Linux một cách độc lập. Bạn cũng có thể khám phá thêm nhiều cách mà Linux có thể hỗ trợ công việc của bạn với tư cách là nhà phân tích bảo mật.

|  |
| --- |
| **Linux community** |

**cộng đồng Linux**

|  |
| --- |
| Linux has a large online community, and this is a huge resource for Linux users of all levels. You can likely find the answers to your questions with a simple online search. Troubleshooting issues by searching and reading online is an effective way to discover how others approached your issue. It’s also a great way for beginners to learn more about Linux. |

Linux có một cộng đồng trực tuyến rộng lớn và đây là nguồn tài nguyên khổng lồ dành cho người dùng Linux ở mọi cấp độ. Bạn có thể tìm thấy câu trả lời cho câu hỏi của mình bằng cách tìm kiếm trực tuyến đơn giản. Khắc phục sự cố bằng cách tìm kiếm và đọc trực tuyến là cách hiệu quả để khám phá cách người khác tiếp cận vấn đề của bạn. Đây cũng là một cách tuyệt vời để người mới bắt đầu tìm hiểu thêm về Linux.

|  |
| --- |
| The [UNIX and Linux Stack Exchange](https://unix.stackexchange.com/) is a trusted resource for troubleshooting Linux issues. The Unix and Linux Stack Exchange is a question and answer website where community members can ask and answer questions about Linux. Community members vote on answers, so the higher quality answers are displayed at the top. Many of the questions are related to specific topics from advanced users, and the topics might help you troubleshoot issues as you continue using Linux. |

Các[Trao đổi ngăn xếp UNIX và Linux](https://unix.stackexchange.com/)là một nguồn tài nguyên đáng tin cậy để khắc phục sự cố Linux. Unix and Linux Stack Exchange là trang web hỏi đáp nơi các thành viên cộng đồng có thể hỏi và trả lời các câu hỏi về Linux. Các thành viên cộng đồng bỏ phiếu cho các câu trả lời nên những câu trả lời có chất lượng cao hơn sẽ được hiển thị ở trên cùng. Nhiều câu hỏi liên quan đến các chủ đề cụ thể từ người dùng nâng cao và các chủ đề này có thể giúp bạn khắc phục sự cố khi bạn tiếp tục sử dụng Linux.

|  |
| --- |
| **Integrated Linux support** |

**Hỗ trợ Linux tích hợp**

|  |
| --- |
| Linux also has several commands that you can use for support. |

Linux cũng có một số lệnh mà bạn có thể sử dụng để hỗ trợ.

|  |
| --- |
| **man** |

**man**

|  |
| --- |
| The **man** command displays information on other commands and how they work. It’s short for “manual.” To search for information on a command, enter the command after **man**. For example, entering **man chown** returns detailed information about **chown**, including the various options you can use with it. The output of the **man** command is also called a “man page.” |

Lệnh **man** hiển thị thông tin về các lệnh khác và cách chúng hoạt động. Nó là viết tắt của “thủ công”. Để tìm kiếm thông tin về lệnh, hãy nhập lệnh sau **man** . Ví dụ: nhập **man chown** sẽ trả về thông tin chi tiết về **chown** , bao gồm các tùy chọn khác nhau mà bạn có thể sử dụng với nó. Đầu ra của lệnh **man** còn được gọi là “trang man”.

|  |
| --- |
| **apropos** |

**apropos**

|  |
| --- |
| The **apropos** command searches the man page descriptions for a specified string. Man pages can be lengthy and difficult to search through if you’re looking for a specific keyword. To use **apropos**, enter the keyword after **apropos**. |

Lệnh **apropos** tìm kiếm các mô tả trang man cho một chuỗi được chỉ định. Các trang hướng dẫn có thể dài và khó tìm kiếm nếu bạn đang tìm kiếm một từ khóa cụ thể. Để sử dụng **apropos** , bạn nhập từ khóa sau **apropos** .

|  |
| --- |
| You can also include the **-a** option to search for multiple words. For example, entering **apropos -a graph editor** outputs man pages that contain both the words “graph" and "editor” in their descriptions. |

Bạn cũng có thể thêm tùy chọn **-a** để tìm kiếm nhiều từ. Ví dụ: nhập **apropos -a trình soạn thảo biểu đồ** sẽ xuất ra các trang man chứa cả từ “biểu đồ” và “trình chỉnh sửa” trong mô tả của chúng.

|  |
| --- |
| **whatis** |

**whatis**

|  |
| --- |
| The **whatis** command displays a description of a command on a single line. For example, entering **whatis nano** outputs the description of **nano**. This command is useful when you don't need a detailed description, just a general idea of the command. This might be as a reminder. Or, it might be after you discover a new command through a colleague or online resource and want to know more. |

Lệnh **whatis** hiển thị mô tả lệnh trên một dòng. Ví dụ: nhập **nano là gì** sẽ đưa ra mô tả về **nano** . Lệnh này hữu ích khi bạn không cần mô tả chi tiết mà chỉ cần ý tưởng chung về lệnh. Đây có thể coi như một lời nhắc nhở. Hoặc có thể là sau khi bạn phát hiện ra một lệnh mới thông qua đồng nghiệp hoặc tài nguyên trực tuyến và muốn biết thêm.

|  |
| --- |
| **Key takeaways** |

**Bài học chính**

|  |
| --- |
| There are many resources available for troubleshooting issues or getting support for Linux. Linux has a large global community of users who ask and answer questions on online resources, such as the Unix and Linux Stack Exchange. You can also use integrated support commands in Linux, such as **man**, **apropos**, and **whatis**. |

Có nhiều tài nguyên có sẵn để khắc phục sự cố hoặc nhận hỗ trợ cho Linux. Linux có một cộng đồng người dùng toàn cầu rộng lớn, những người hỏi và trả lời các câu hỏi về các tài nguyên trực tuyến, chẳng hạn như Unix và Linux Stack Exchange. Bạn cũng có thể sử dụng các lệnh hỗ trợ tích hợp trong Linux, chẳng hạn như **man** , **apropos** và **whatis** .

|  |
| --- |
| **Resources for more information** |

**Tài nguyên để biết thêm thông tin**

|  |
| --- |
| There are many resources available online that can help you learn new Linux concepts, review topics, or ask and answer questions with the global Linux community. The [Unix and Linux Stack Exchange](https://unix.stackexchange.com/) is one example, and you can search online to find others. |

Có rất nhiều tài nguyên trực tuyến có thể giúp bạn tìm hiểu các khái niệm Linux mới, xem lại các chủ đề hoặc hỏi và trả lời các câu hỏi với cộng đồng Linux toàn cầu. Các[Trao đổi ngăn xếp Unix và Linux](https://unix.stackexchange.com/)là một ví dụ và bạn có thể tìm kiếm trực tuyến để tìm những người khác.

***4.5. Activity: Get help in the command line – Hoạt động: Nhận trợ giúp về dòng lệnh***

***4.6. Optional Exemplar: Get help in the command line – Mẫu tùy chọn: Nhận trợ giúp trong dòng lệnh***

***4.7. Apply Linux commands as a cybersecurity professional – Áp dụng các lệnh Linux như một chuyên gia an ninh mạng***

***4.8. Test your knowledge: Get help in Linux – Kiểm tra kiến ​​thức của bạn: Nhận trợ giúp về Linux***

**5. Review: Linux commands in the Bash shell – Đánh giá: Các lệnh Linux trong Bash shell**

***5.1. Wrap-up – Gói lại***

|  |
| --- |
| Congratulations! You completed another section in this course. Take a minute to think about what you've achieved. You learned a lot in this section. Let's recap what we covered. |

Chúc mừng! Bạn đã hoàn thành một phần khác trong khóa học này.Hãy dành một phút để suy nghĩ về những gì bạn đã đạt được.Bạn đã học được rất nhiều trong phần này. Hãy tóm tắt lại những gì chúng tôi đã đề cập.

|  |
| --- |
| In this section, you utilized the command line to communicate with the OS. Part of this was using commands for navigating and managing the file system. And you used other commands for authenticating and authorizing users. These are all tasks that a security analyst is likely to encounter. |

Trong phần này, bạn đã sử dụng dòng lệnh để giao tiếp với HĐH.Một phần của việc này là sử dụng các lệnh để điều hướng và quản lý hệ thống tệp.Và bạn đã sử dụng các lệnh khác để xác thực và cấp phép cho người dùng.Đây là tất cả các nhiệm vụ mà một nhà phân tích bảo mật có thể gặp phải.

|  |
| --- |
| Finally, you learned about accessing resources that support learning new Linux commands. With this knowledge, you'll be able to continue learning more and more about using the command line. |

Cuối cùng, bạn đã học về cách truy cập các tài nguyên hỗ trợhọc các lệnh Linux mới.Với kiến ​​thức này, bạn sẽ có thể tiếp tục học hỏi nhiều hơn vàthêm về cách sử dụng dòng lệnh.

|  |
| --- |
| We did it! we learned how to communicate with Linux. That's a great accomplishment, and one that will be very useful to you in your career as a security analyst. You should be proud of the work that you've done so far. |

Chúng ta làm được rồi! chúng tôi đã học cách giao tiếp với Linux.Đó là một thành tựu to lớn vàmột thứ sẽ rất hữu ích cho bạn trong sự nghiệp phân tích chứng khoán.Bạn nên tự hào về công việc bạn đã làm cho đến nay.

***5.2. Reference guide: Linux – Hướng dẫn tham khảo: Linux***

|  |
| --- |
| **Reference guide: Linux** |

**Hướng dẫn tham khảo: Linux**

|  |
| --- |
| The Linux reference guide contains key Linux commands security professionals use to perform basic job duties. The reference guide is divided into six different categories of useful Linux commands for security-related tasks: |

Hướng dẫn tham khảo Linux chứa các lệnh Linux chính mà các chuyên gia bảo mật sử dụng để thực hiện các nhiệm vụ công việc cơ bản. Hướng dẫn tham khảo được chia thành sáu loại lệnh Linux hữu ích khác nhau cho các tác vụ liên quan đến bảo mật:

|  |
| --- |
| * Navigate the file system * Read files * Manage the file system * Filter content * Manage users and their permissions * Get help in Linux |

* Điều hướng hệ thống tập tin
* Đọc tập tin
* Quản lý hệ thống tập tin
* Lọc nội dung
* Quản lý người dùng và quyền của họ
* Nhận trợ giúp về Linux

|  |
| --- |
| Within each category, commands are organized alphabetically. |

Trong mỗi danh mục, các lệnh được sắp xếp theo thứ tự bảng chữ cái.

|  |
| --- |
| **Access and save the guide** |

**Truy cập và lưu hướng dẫn**

|  |
| --- |
| You can save a copy of this guide for future reference. You can use it as a resource for additional practice or in your future professional projects. |

Bạn có thể lưu một bản sao của hướng dẫn này để tham khảo sau này. Bạn có thể sử dụng nó như một nguồn tài liệu để thực hành bổ sung hoặc cho các dự án chuyên môn trong tương lai của mình.

|  |
| --- |
| To access a downloadable version of this course item, click the following link and select *Use Template*.  [Reference guide: Linux](https://docs.google.com/document/d/1flGzGBZBo8vtX6Wiphf0K78yeL9OhQ-o9ShCX8K58CA/template/preview?usp=sharing) |

Để truy cập phiên bản có thể tải xuống của mục khóa học này, hãy nhấp vào liên kết sau và chọn *Sử dụng Mẫu* .

[Hướng dẫn tham khảo: Linux](https://docs.google.com/document/d/1flGzGBZBo8vtX6Wiphf0K78yeL9OhQ-o9ShCX8K58CA/template/preview?usp=sharing)

***5.3. Glossary terms from module 3 – Thuật ngữ trong học phần 3***

|  |
| --- |
| **Glossary terms from module 3** |

**Thuật ngữ trong học phần 3**

|  |
| --- |
| **Terms and definitions from Course 4, Module 3** |

**Các thuật ngữ và định nghĩa trong Khóa 4, Học phần 3**

|  |
| --- |
| **Absolute file path:** The full file path, which starts from the root |

**Đường dẫn tệp tuyệt đối:** Đường dẫn tệp đầy đủ, bắt đầu từ thư mục gốc

|  |
| --- |
| **Argument (Linux):** Specific information needed by a command |

**Đối số (Linux):** Thông tin cụ thể cần thiết cho một lệnh

|  |
| --- |
| **Authentication:** The process of verifying who someone is |

**Xác thực:** Quá trình xác minh ai đó là ai

|  |
| --- |
| **Authorization:** The concept of granting access to specific resources in a system |

**Ủy quyền:** Khái niệm cấp quyền truy cập vào các tài nguyên cụ thể trong hệ thống

|  |
| --- |
| **Bash:** The default shell in most Linux distributions |

**Bash:** Shell mặc định trong hầu hết các bản phân phối Linux

|  |
| --- |
| **Command:** An instruction telling the computer to do something |

**Lệnh:** Lệnh yêu cầu máy tính làm một việc gì đó

|  |
| --- |
| **File path:** The location of a file or directory |

**Đường dẫn tệp:** Vị trí của tệp hoặc thư mục

|  |
| --- |
| **Filesystem Hierarchy Standard (FHS):** The component of the Linux OS that organizes data |

**Tiêu chuẩn phân cấp hệ thống tập tin (FHS):** Thành phần của hệ điều hành Linux tổ chức dữ liệu

|  |
| --- |
| **Filtering:** Selecting data that match a certain condition |

**Lọc:** Chọn dữ liệu phù hợp với một điều kiện nhất định

|  |
| --- |
| **nano:** A command-line file editor that is available by default in many Linux distributions |

**nano:** Trình chỉnh sửa tệp dòng lệnh có sẵn theo mặc định trong nhiều bản phân phối Linux

|  |
| --- |
| **Options:** Input that modifies the behavior of a command |

**Tùy chọn:** Đầu vào sửa đổi hành vi của lệnh

|  |
| --- |
| **Permissions:** The type of access granted for a file or directory |

**Quyền:** Loại quyền truy cập được cấp cho tệp hoặc thư mục

m

|  |
| --- |
| **Principle of least privilege:** The concept of granting only the minimal access and authorization required to complete a task or function |

**Nguyên tắc đặc quyền tối thiểu:** Khái niệm chỉ cấp quyền truy cập và ủy quyền tối thiểu cần thiết để hoàn thành một nhiệm vụ hoặc chức năng

|  |
| --- |
| **Relative file path:** A file path that starts from the user's current directory |

**Đường dẫn tệp tương đối:** Đường dẫn tệp bắt đầu từ thư mục hiện tại của người dùng

|  |
| --- |
| **Root directory:** The highest-level directory in Linux |

**Thư mục gốc:** Thư mục cấp cao nhất trong Linux

|  |
| --- |
| **Root user (or superuser):** A user with elevated privileges to modify the system |

**Người dùng root (hoặc siêu người dùng):** Người dùng có đặc quyền nâng cao để sửa đổi hệ thống

|  |
| --- |
| **Standard input:** Information received by the OS via the command line |

**Đầu vào tiêu chuẩn:** Thông tin được HĐH nhận thông qua dòng lệnh

|  |
| --- |
| **Standard output:** Information returned by the OS through the shell |

**Đầu ra tiêu chuẩn:** Thông tin được hệ điều hành trả về thông qua shell

***5.4. Module 3 challenge – Thử thách mô-đun 3***

# **Module 4: Databases and SQL – Cơ sở dữ liệu và SQL**

|  |
| --- |
| 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. |

Bạn sẽ thực hành sử dụng SQL để giao tiếp với cơ sở dữ liệu. Bạn sẽ tìm hiểu cách truy vấn cơ sở dữ liệu và lọc kết quả. Bạn cũng sẽ tìm hiểu cách SQL có thể nối nhiều bảng lại với nhau trong một truy vấn.

|  |
| --- |
| **Learning Objectives**   * Discuss how SQL is used within the security profession. * Describe how a relational database is organized. * Use SQL to retrieve information from a database. * Apply filters to SQL queries. * Use SQL joins to combine multiple tables into a query. |

**Mục tiêu học tập**

* Thảo luận về cách SQL được sử dụng trong ngành bảo mật.
* Mô tả cách tổ chức cơ sở dữ liệu quan hệ.
* Sử dụng SQL để lấy thông tin từ cơ sở dữ liệu.
* Áp dụng bộ lọc cho truy vấn SQL.
* Sử dụng các phép nối SQL để kết hợp nhiều bảng thành một truy vấn.

**1. Introduction to SQL and Databases – Giới thiệu về SQL và Cơ sở dữ liệu**

***1.1. Welcome to module 4 – Chào mừng đến với mô-đun 4***

|  |
| --- |
| In the world of security, diversity is important. Diverse perspectives are often needed to find effective solutions. This is also true of the tools we use. Your job will often require you to use a lot of diverse tools. In the last section, we studied the Linux command line and learned how this tool can help you search and filter through data, navigate through the Linux file system, and authenticate users. Now, we'll learn about another tool. |

Trong thế giới an ninh, sự đa dạng là quan trọng.Những quan điểm đa dạng thườngcần tìm giải pháp hữu hiệu.Điều này cũng đúng với các công cụ chúng tôi sử dụng.Công việc của bạn thường sẽ yêu cầubạn sử dụng rất nhiều công cụ đa dạng.Trong phần cuối cùng,chúng tôi đã nghiên cứu dòng lệnh Linux và tìm hiểu cáchcông cụ này có thể giúp bạn tìm kiếm và lọc dữ liệu,điều hướng qua hệ thống tệp Linux,và xác thực người dùng.Bây giờ chúng ta sẽ tìm hiểu về một công cụ khác.

|  |
| --- |
| In this section, we'll explore SQL and how it allows you to analyze data in a way needed for your role as a security analyst. We're going to start off by learning about relational databases and how they're structured. From there, we're going to introduce SQL queries and how to use them to access data from databases. We then move on to SQL filters, which help us refine our queries to get the exact information we need. Lastly, we'll explore SQL joins, which allow you to combine tables together. |

Trong phần này, chúng ta sẽ khám phá SQL và cách nó cho phépbạn phân tích dữ liệu theo cáchcần thiết cho vai trò của bạn với tư cách là nhà phân tích bảo mật.Chúng ta sẽ bắt đầu bằng việc tìm hiểu vềcơ sở dữ liệu quan hệ và cách chúng được cấu trúc.Từ đó chúng tôi sẽ giới thiệuTruy vấn SQL và cách sử dụngchúng để truy cập dữ liệu từ cơ sở dữ liệu.Sau đó chúng tôi chuyển sang bộ lọc SQL,giúp chúng tôi tinh chỉnh các truy vấn của mìnhđể có được thông tin chính xác mà chúng tôi cần.Cuối cùng, chúng ta sẽ khám phá các phép nối SQL,cho phép bạn kết hợp các bảng lại với nhau.

|  |
| --- |
| When I'm presented with a problem or a project at work, I often have to sift through a large amount of data. When I use SQL, I'm able to review data quickly and provide results with confidence since the queries are consistent and easily executed. |

Khi tôi gặp phải một vấn đề hoặc một dự án ở nơi làm việc,Tôi thường phải sàng lọc một lượng lớn dữ liệu.Khi tôi sử dụng SQL,Tôi có thể xem lại dữ liệu một cách nhanh chóng và cung cấp kết quả vớisự tự tin vì các truy vấn đượcnhất quán và dễ thực hiện.

|  |
| --- |
| SQL is a very powerful and flexible tool. Throughout this section, you'll learn how to use the parts of it you need as a security analyst and gain hands-on experience. Good luck, and I'll join you for the rest of the course! |

SQL là một công cụ rất mạnh mẽ và linh hoạt.Trong suốt phần này, bạn sẽhọc cách sử dụng các phần của nó bạncần trở thành một nhà phân tích bảo mật và tích lũy kinh nghiệm thực tế.Chúc may mắn và tôi sẽ tham gia cùng bạn trong phần còn lại của khóa học!

***1.2. Introduction to databases – Giới thiệu về cơ sở dữ liệu***

|  |
| --- |
| Our modern world is filled with data and that data almost always guides us in making important decisions. When working with large amounts of data, we need to know how to store it, so it's organized and quick to access and process. The solution to this is through databases, and that's what we're exploring in this video! |

Thế giới hiện đại của chúng ta chứa đầy dữ liệu vàdữ liệu đó hầu như luôn hướng dẫn chúng ta đưa ra những quyết định quan trọng.Khi làm việc với lượng lớn dữ liệu, chúng ta cần biết cách lưu trữ nó, vì vậynó được tổ chức và truy cập và xử lý nhanh chóng.Giải pháp cho vấn đề này là thông qua cơ sở dữ liệu vàđó là những gì chúng ta đang khám phá trong video này!

|  |
| --- |
| To start us off, we can define a database as an organized collection of information or data. Databases are often compared to spreadsheets. Some of you may have used Google Sheets or another common spreadsheet program in the past. While these programs are convenient ways to store data, spreadsheets are often designed for a single user or a small team to store less data. In contrast, databases can be accessed by multiple people simultaneously and can store massive amounts of data. Databases can also perform complex tasks while accessing data. As a security analyst, you'll often need to access databases containing useful information. For example, these could be databases containing information on login attempts, software and updates, or machines and their owners. |

Để bắt đầu chúng ta,chúng ta có thể định nghĩa cơ sở dữ liệu là một tập hợp thông tin hoặc dữ liệu có tổ chức.Cơ sở dữ liệu thường được so sánh với bảng tính.Một số bạn có thể đã sử dụng Google Trang tính hoặcmột chương trình bảng tính phổ biến khác trong quá khứ.Mặc dù các chương trình này là cách thuận tiện để lưu trữ dữ liệu nhưng bảng tínhthường được thiết kế cho một người dùng hoặc một nhóm nhỏ để lưu trữ ít dữ liệu hơn.Ngược lại, cơ sở dữ liệu có thể được nhiều người truy cập đồng thời vàcó thể lưu trữ một lượng lớn dữ liệu.Cơ sở dữ liệu cũng có thể thực hiện các tác vụ phức tạp trong khi truy cập dữ liệu.Là một nhà phân tích chứng khoán,bạn thường sẽ cần truy cập cơ sở dữ liệu chứa thông tin hữu ích.Ví dụ: đây có thể là cơ sở dữ liệu chứa thông tin về các lần thử đăng nhập,phần mềm và các bản cập nhật, hoặc máy móc và chủ sở hữu của chúng.

|  |
| --- |
| Now that we know how important databases are for us, let's talk about how they're organized and how we can interact with them. Using databases allow us to store large amounts of data while keeping it quick and easy to access. There are lots of different ways we can structure a database, but in this course, we'll be working with relational databases. A relational database is a structured database containing tables that are related to each other. |

Bây giờ chúng ta đã biết cơ sở dữ liệu quan trọng như thế nào đối với chúng ta,hãy nói về cách họ được tổ chức và cách chúng ta có thể tương tác với họ.Việc sử dụng cơ sở dữ liệu cho phép chúng ta lưu trữ một lượng lớn dữ liệu trong khi vẫn đảm bảo tốc độ vàdê dang truy cập.Có rất nhiều cách khác nhau để chúng ta có thể cấu trúc cơ sở dữ liệu, nhưng trong khóa học này,chúng ta sẽ làm việc với cơ sở dữ liệu quan hệ.Cơ sở dữ liệu quan hệ là cơ sở dữ liệu có cấu trúc chứa các bảngcó liên quan với nhau.

|  |
| --- |
| Let's learn more about what makes a relational database. We'll start by examining an individual table in a larger database of organizational information. Each table contains fields of information. For example, in this table on employees, these would include fields like employee\_id, device\_id, and username. |

Hãy cùng tìm hiểu thêm về những gì tạo nên một cơ sở dữ liệu quan hệ.Chúng ta sẽ bắt đầu bằng cách kiểm tra một bảng riêng lẻ trongmột cơ sở dữ liệu lớn hơn về thông tin tổ chức.Mỗi bảng chứa các trường thông tin.Ví dụ: trong bảng này về nhân viên,chúng sẽ bao gồm các trường như user\_id, device\_id và tên người dùng.

|  |
| --- |
| These are the columns of the tables. In addition, tables contain rows also called records. Rows are filled with specific data related to the columns in the table. For example, our first row is a record for an employee whose id is 1,000 and who works in the marketing department. |

Đây là các cột của bảng.Ngoài ra, bảng còn chứa các hàng còn được gọi là bản ghi.Các hàng chứa đầy dữ liệu cụ thể liên quan đến các cột trong bảng.Ví dụ: hàng đầu tiên của chúng tôi là bản ghi cho một nhân viên có id là 1.000 vàngười làm việc ở bộ phận tiếp thị.

|  |
| --- |
| Relational databases often have multiple tables. Consider an example where we have two tables from a larger database, one with employees of the company and another with machines given to those employees. We can connect two tables if they share a common column. In this example, we establish a relationship between them with a common employee\_id column. The columns that relate two tables to each other are called keys. There are two types of keys. The first is called a primary key. The primary key refers to a column where every row has a unique entry. The primary key must not have any duplicate values, or any null or empty values. The primary key allows us to uniquely identify every row in our table. For the table of employees, employee\_id is a primary key. Every employee\_id is unique and there are no employee\_ids that are duplicate or empty. |

Cơ sở dữ liệu quan hệ thường có nhiều bảng.Hãy xem xét một ví dụ trong đó chúng ta có hai bảng từ cơ sở dữ liệu lớn hơn, một bảng cónhân viên của công ty và một người khác có máy móc được trao cho những nhân viên đó.Chúng ta có thể kết nối hai bảng nếu chúng có chung một cột.Trong ví dụ này,chúng tôi thiết lập mối quan hệ giữa chúng bằng cột member\_id chung.Các cột liên kết hai bảng với nhau được gọi là khóa.Có hai loại chìa khóa.Đầu tiên được gọi là khóa chính.Khóa chính đề cập đến một cột trong đó mỗi hàng có một mục nhập duy nhất.Khóa chính không được có bất kỳ giá trị trùng lặp nào hoặc bất kỳ giá trị rỗng hoặccác giá trị trống.Khóa chính cho phép chúng tôi xác định duy nhất mọi hàng trong bảng của mình.Đối với bảng nhân viên, user\_id là khóa chính.Mỗi ID nhân viên là duy nhất và không có ID nhân viên nào trùng lặp hoặctrống.

|  |
| --- |
| The second type of key is a foreign key. The foreign key is a column in a table that is a primary key in another table. Foreign keys, unlike primary keys, can have empty values and duplicates. The foreign key allows us to connect two tables together. In our example, we can look at the employee\_id column in the machines table. We previously identified this as a primary key in the employees table, so we can use this to connect every machine to their corresponding employee. |

Loại khóa thứ hai là khóa ngoại.Khóa ngoại là một cột trong bảng và là khóa chính trong bảng khác.Khóa ngoại, không giống như khóa chính, có thể có giá trị trống và trùng lặp.Khóa ngoại cho phép chúng ta kết nối hai bảng với nhau.Trong ví dụ của chúng ta, chúng ta có thể xem cột member\_id trong bảng máy.Trước đây chúng tôi đã xác định đây là khóa chính trong bảng nhân viên, vì vậychúng ta có thể sử dụng điều này để kết nối mọi máy với nhân viên tương ứng của họ.

|  |
| --- |
| It's also important to know that a table can only have one primary key, but multiple foreign keys. |

Điều quan trọng cần biết là một bảng chỉ có thể có một khóa chính, nhưngnhiều khóa ngoại.

|  |
| --- |
| With this information, we're ready to move on to the basics of SQL, the language that lets us work with databases. Throughout this section, we'll gain hands-on experience working with the concepts we just covered! |

Với thông tin này, chúng ta đã sẵn sàng chuyển sang những kiến ​​thức cơ bản về SQL,ngôn ngữ cho phép chúng ta làm việc với cơ sở dữ liệu.Xuyên suốt phần này,chúng ta sẽ có được kinh nghiệm thực tế khi làm việc với các khái niệm mà chúng ta vừa đề cập!

***1.3. Query databases with SQL – Truy vấn cơ sở dữ liệu bằng SQL***

|  |
| --- |
| As a security analyst, you'll need to be familiar both with databases and the tools used to access them. Now that we know the basics of databases, let's focus on an important tool used to work with them, SQL, and learn more about how analysts like yourself might utilize it. SQL, or as it's also pronounced, S-Q-L, stands for Structured Query Language. SQL is a programming language used to create, interact with, and request information from a database. |

Là một nhà phân tích bảo mật, bạn sẽ cần phải làm quen với cả cơ sở dữ liệu vàcác công cụ được sử dụng để truy cập chúng.Bây giờ chúng ta đã biết những điều cơ bản về cơ sở dữ liệu,hãy tập trung vào một công cụ quan trọng được sử dụng để làm việc với chúng, SQL vàtìm hiểu thêm về cách các nhà phân tích như bạn có thể sử dụng nó.SQL, hay như nó cũng được phát âm là SQL, là viết tắt của Ngôn ngữ truy vấn có cấu trúc.SQL là ngôn ngữ lập trình được sử dụng để tạo, tương tác vàyêu cầu thông tin từ cơ sở dữ liệu.

|  |
| --- |
| Before learning more about SQL, we need to define what query means. A query is a request for data from a database table or a combination of tables. Nearly all relational databases rely on some version of SQL to query data. The different versions of SQL only have slight differences in their structure, like where to place quotation marks. Whatever variety of SQL you use, you'll find it to be a very important tool in your work as a security analyst. |

Trước khi tìm hiểu thêm về SQL, chúng ta cần xác định ý nghĩa của truy vấn.Truy vấn là yêu cầu dữ liệu từ bảng cơ sở dữ liệu hoặc kết hợp các bảng.Gần như tất cả các cơ sở dữ liệu quan hệ đều dựa vào một số phiên bản SQL để truy vấn dữ liệu.Các phiên bản SQL khác nhau chỉ có sự khác biệt nhỏ về cấu trúc,như nơi đặt dấu ngoặc kép.Dù bạn sử dụng loại SQL nào,bạn sẽ thấy nó là một công cụ rất quan trọng trong công việc của bạn với tư cách là nhà phân tích bảo mật.

|  |
| --- |
| First, let's discuss how SQL can help you retrieve logs. A log is a record of events that occur within an organization's systems. As a security analyst, you might be tasked with reviewing logs for various reasons. For example, some logs might contain details on machines used in a company, and as an analyst, |

Trước tiên, hãy thảo luận về cách SQL có thể giúp bạn truy xuất nhật ký.Nhật ký là bản ghi các sự kiện xảy ra trong hệ thống của tổ chức.Là nhà phân tích bảo mật, bạn có thể được giao nhiệm vụ xem xét nhật ký vì nhiều lý do.Ví dụ: một số nhật ký có thể chứa thông tin chi tiết về các máy được sử dụng trong công ty,và với tư cách là một nhà phân tích,

|  |
| --- |
| you would need to find those machines that weren't configured properly. Other logs might describe the visitors to your website or web app and the tasks they perform. In that case, |

bạn sẽ cần tìm những máy không được cấu hình đúng cách.Các nhật ký khác có thể mô tả khách truy cập vào trang web hoặc ứng dụng web của bạn vànhững nhiệm vụ họ thực hiện.Trong trường hợp đó,

|  |
| --- |
| you might be looking for unusual patterns that may point to malicious activity. Security logs are often very large and hard to process. There are millions of data points, and it's very time consuming to find what you need. But this is where SQL comes in! It can search through millions of data points to extract relevant rows of data using one query that takes seconds to run. That's pretty useful, right? |

bạn có thể đang tìm kiếm các mẫu bất thường có thể chỉ ra hoạt động độc hại.Nhật ký bảo mật thường rất lớn và khó xử lý.Có hàng triệu điểm dữ liệu vàrất tốn thời gian để tìm thấy những gì bạn cần.Nhưng đây chính là lúc SQL xuất hiện! Nó có thể tìm kiếm thông qua hàng triệu điểm dữ liệu đểtrích xuất các hàng dữ liệu có liên quan bằng một truy vấn mất vài giây để chạy.Điều đó khá hữu ích phải không?

|  |
| --- |
| SQL is also a very common language used for basic data analytics, another set of skills that will set you apart as a security analyst. As a security analyst, you can use SQL's filtering to find data to support security-related decisions and analyze when things may go wrong. For instance, you can identify what machines haven't received the latest patch. This is important because patches are updates that help secure against attacks. As another example, you can use SQL to determine the best time to update a machine based on when it's least used. |

SQL cũng là một ngôn ngữ rất phổ biến được sử dụng để phân tích dữ liệu cơ bản,một bộ kỹ năng khác sẽ giúp bạn trở thành một nhà phân tích bảo mật.Là nhà phân tích bảo mật, bạn có thể sử dụng tính năng lọc của SQL để tìm dữ liệu hỗ trợcác quyết định liên quan đến bảo mật và phân tích khi có sự cố xảy ra.Ví dụ,bạn có thể xác định những máy nào chưa nhận được bản vá mới nhất.Điều này rất quan trọng vì các bản vá là bản cập nhật giúp bảo mật trước các cuộc tấn công.Một ví dụ khác, bạn có thể sử dụng SQL để xác định thời điểm tốt nhấtđể cập nhật máy dựa trên thời điểm máy ít được sử dụng nhất.

|  |
| --- |
| Now that we know why SQL is important to us, we're going to start making basic queries to a sample database! This is definitely exciting, and I'll meet you in the next video. |

Bây giờ chúng ta đã biết tại sao SQL lại quan trọng đối với chúng ta,chúng ta sẽ bắt đầu thực hiện các truy vấn cơ bản tới cơ sở dữ liệu mẫu!Điều này chắc chắn rất thú vị và tôi sẽ gặp bạn trong video tiếp theo.

***1.4. SQL filtering versus Linux filtering – Lọc SQL so với lọc Linux***

|  |
| --- |
| **SQL filtering versus Linux filtering** |

**Lọc SQL so với lọc Linux**

|  |
| --- |
| Previously, you explored the Linux commands that allow you to filter for specific information contained within files or directories. And, more recently, you examined how SQL helps you efficiently filter for the information you need. In this reading, you'll explore differences between the two tools as they relate to filtering. You'll also learn that one way to access SQL is through the Linux command line. |

Trước đây, bạn đã khám phá các lệnh Linux cho phép bạn lọc thông tin cụ thể có trong các tệp hoặc thư mục. Và gần đây hơn, bạn đã kiểm tra cách SQL giúp bạn lọc thông tin bạn cần một cách hiệu quả. Trong bài đọc này, bạn sẽ khám phá sự khác biệt giữa hai công cụ vì chúng liên quan đến việc lọc. Bạn cũng sẽ biết rằng một cách để truy cập SQL là thông qua dòng lệnh Linux.

|  |
| --- |
| **Accessing SQL** |

**Truy cập SQL**

|  |
| --- |
| There are many interfaces for accessing SQL and many different versions of SQL. One way to access SQL is through the Linux command line. |

Có nhiều giao diện để truy cập SQL và nhiều phiên bản SQL khác nhau. Một cách để truy cập SQL là thông qua dòng lệnh Linux.

|  |
| --- |
| To access SQL from Linux, you need to type in a command for the version of SQL that you want to use. For example, if you want to access SQLite, you can enter the command **sqlite3** in the command line. |

Để truy cập SQL từ Linux, bạn cần nhập lệnh cho phiên bản SQL mà bạn muốn sử dụng. Ví dụ: nếu bạn muốn truy cập SQLite, bạn có thể nhập lệnh **sqlite3** vào dòng lệnh.

|  |
| --- |
| After this, any commands typed in the command line will be directed to SQL instead of Linux commands. |

Sau này, mọi lệnh được nhập vào dòng lệnh sẽ được chuyển hướng tới SQL thay vì các lệnh Linux.

|  |
| --- |
| **Differences between Linux and SQL filtering** |

**Sự khác biệt giữa lọc Linux và SQL**

|  |
| --- |
| Although both Linux and SQL allow you to filter through data, there are some differences that affect which one you should choose. |

Mặc dù cả Linux và SQL đều cho phép bạn lọc dữ liệu, nhưng có một số khác biệt ảnh hưởng đến việc bạn nên chọn cái nào.

|  |
| --- |
| **Purpose** |

**Mục đích**

|  |
| --- |
| Linux filters data in the context of files and directories on a computer system. It’s used for tasks like searching  for specific files, manipulating file permissions, or managing processes. |

Linux lọc dữ liệu theo ngữ cảnh của các tệp và thư mục trên hệ thống máy tính. Nó được sử dụng cho các tác vụ như tìm kiếm các tệp cụ thể, thao tác quyền truy cập tệp hoặc quản lý quy trình.

|  |
| --- |
| SQL is used to filter data within a database management system. It’s used for querying and manipulating data stored in tables and retrieving specific information based on defined criteria. |

SQL được sử dụng để lọc dữ liệu trong hệ thống quản lý cơ sở dữ liệu. Nó được sử dụng để truy vấn và thao tác dữ liệu được lưu trữ trong bảng và truy xuất thông tin cụ thể dựa trên các tiêu chí đã xác định.

|  |
| --- |
| **Syntax** |

**Cú pháp**

|  |
| --- |
| Linux uses various commands and command-line options specific to each filtering tool. Syntax varies depending on the tool and purpose. Some examples of Linux commands are find, sed, cut, e grep |

Linux sử dụng nhiều lệnh và tùy chọn dòng lệnh khác nhau dành riêng cho từng công cụ lọc. Cú pháp khác nhau tùy thuộc vào công cụ và mục đích. Một số ví dụ về lệnh Linux là find, sed, cut, e grep

|  |
| --- |
| SQL uses the Structured Query Language (SQL), a standardized language with specific keywords and clauses for filtering data across different SQL databases. Some examples of SQL keywords and clauses are WHERE, SELECT, JOIN |

SQL sử dụng Ngôn ngữ truy vấn có cấu trúc (SQL), một ngôn ngữ được tiêu chuẩn hóa với các từ khóa và mệnh đề cụ thể để lọc dữ liệu trên các cơ sở dữ liệu SQL khác nhau. Một số ví dụ về từ khóa và mệnh đề SQL là WHERE, SELECT, JOIN

|  |
| --- |
| **Structure** |

**Kết cấu**

|  |
| --- |
| SQL offers a lot more structure than Linux, which is more free-form and not as tidy. |

SQL cung cấp nhiều cấu trúc hơn Linux, có dạng tự do hơn và không gọn gàng bằng.

|  |
| --- |
| For example, if you wanted to access a log of employee log-in attempts, SQL would have each record separated into columns. Linux would print the data as a line of text without this organization. As a result, selecting a specific column to analyze would be easier and more efficient in SQL. |

Ví dụ: nếu bạn muốn truy cập nhật ký các lần đăng nhập của nhân viên, SQL sẽ tách mỗi bản ghi thành các cột. Linux sẽ in dữ liệu dưới dạng dòng văn bản mà không cần tổ chức này. Do đó, việc chọn một cột cụ thể để phân tích sẽ dễ dàng và hiệu quả hơn trong SQL.

|  |
| --- |
| In terms of structure, SQL provides results that are more easily readable and that can be adjusted more quickly than when using Linux. |

Về mặt cấu trúc, SQL cung cấp kết quả dễ đọc hơn và có thể điều chỉnh nhanh hơn so với khi sử dụng Linux.

|  |
| --- |
| **Joining tables** |

**Tham gia các bảng**

|  |
| --- |
| Some security-related decisions require information from different tables. SQL allows the analyst to join multiple tables together when returning data. Linux doesn’t have that same functionality; it doesn’t allow data to be connected to other information on your computer. This is more restrictive for an analyst going through security logs. |

Một số quyết định liên quan đến bảo mật yêu cầu thông tin từ các bảng khác nhau. SQL cho phép nhà phân tích nối nhiều bảng lại với nhau khi trả về dữ liệu. Linux không có chức năng tương tự; nó không cho phép dữ liệu được kết nối với thông tin khác trên máy tính của bạn. Điều này hạn chế hơn đối với nhà phân tích khi xem qua nhật ký bảo mật.

|  |
| --- |
| **Best uses** |

**Sử dụng tốt nhất**

|  |
| --- |
| As a security analyst, it’s important to understand when you can use which tool. Although SQL has a more organized structure and allows you to join tables, this doesn’t mean that there aren’t situations that would require you to filter data in Linux. |

Là một nhà phân tích bảo mật, điều quan trọng là phải hiểu khi nào bạn có thể sử dụng công cụ nào. Mặc dù SQL có cấu trúc có tổ chức hơn và cho phép bạn nối các bảng nhưng điều này không có nghĩa là không có trường hợp nào yêu cầu bạn lọc dữ liệu trong Linux.

|  |
| --- |
| A lot of data used in cybersecurity will be stored in a database format that works with SQL. However, other logs might be in a format that is not compatible with SQL. For instance, if the data is stored in a text file, you cannot search through it with SQL. In those cases, it is useful to know how to filter in Linux. |

Rất nhiều dữ liệu được sử dụng trong an ninh mạng sẽ được lưu trữ ở định dạng cơ sở dữ liệu hoạt động với SQL. Tuy nhiên, các nhật ký khác có thể có định dạng không tương thích với SQL. Ví dụ: nếu dữ liệu được lưu trữ trong tệp văn bản, bạn không thể tìm kiếm bằng SQL. Trong những trường hợp đó, việc biết cách lọc trong Linux sẽ rất hữu ích.

|  |
| --- |
| **Key takeaways** |

**Bài học chính**

|  |
| --- |
| Linux filtering focuses on managing files and directories on a system, while SQL filtering focuses on structured data manipulation within databases. To work with SQL, you can access it from multiple different interfaces, such as the Linux command line. Both SQL and Linux allow you to filter for specific data, but SQL offers the advantages of structuring the data and allowing you to join data from multiple tables. |

Lọc Linux tập trung vào việc quản lý các tệp và thư mục trên hệ thống, trong khi lọc SQL tập trung vào thao tác dữ liệu có cấu trúc trong cơ sở dữ liệu. Để làm việc với SQL, bạn có thể truy cập nó từ nhiều giao diện khác nhau, chẳng hạn như dòng lệnh Linux. Cả SQL và Linux đều cho phép bạn lọc dữ liệu cụ thể, nhưng SQL mang lại lợi ích về cấu trúc dữ liệu và cho phép bạn nối dữ liệu từ nhiều bảng.

***1.5. Adedayo: SQL in cybersecurity – Adedayo: SQL trong an ninh mạng***

|  |
| --- |
| My name is Adedayo, and I'm a Security Engineer at Google. A lot of people think you need to have a degree in computer science, right to be able to get into cybersecurity. I don't think that's true. Take me for an example, I started learning IT from Lagos, Nigeria where I was born and raised, and then I'm all the way here now in Silicon Valley, working for Google. I think that's just amazing and a dream come true. You taking this certificate is a first step to you making a commitment to switching your career to cybersecurity. Kudos to you on that. SQL is one of the skillset you need to have in your toolbox as a cybersecurity professional because you can very quickly make decisions, not just off the bat, but make decisions with data backing you, and be able to communicate with your team, with stakeholders about why you made a decision because it's one thing to be able to say, we need to do this, it's another thing to say we need to do this and here's the data that I wrote my SQL statements about. I learned SQL by, first, as a coursework in school, that was really great, but I think I forgot everything about that after school. The next step that I took was taking online courses, such as the one you're taking right now to learn SQL and the fundamentals about it and how to really use it. Then the first time I used SQL practically was at Google. You really need to practice. I think with anything else, practice makes perfect. Being able to, even if it's just a few hours a week, put aside time to practice writing SQL statement. Having that skill is something that will be very applicable to your first job, and you can use that to make data-driven decisions. I feel very fulfilled working in cybersecurity. I feel very energized, come into work every day. Not only because I get to work on really complex problems and try to figure out solutions for them, but I also have great teammates that we all come together and tackle the problem. Being able to go to bed at night, knowing that the work that I do is for the better of Google users and Google employees is a very rewarding feeling for me. |

Tên tôi là Adedayo,và tôi là Kỹ sư bảo mật tại Google.Nhiều người nghĩ rằng bạn cần phải có bằng cấp vềkhoa học máy tính, quyền có thể có đượcvào an ninh mạng. Tôi không nghĩ điều đó đúng.Hãy lấy tôi làm ví dụ,Tôi bắt đầu học CNTT từ Lagos,Nigeria nơi tôi sinh ra và lớn lên,và rồi bây giờ tôi đã đến đâyở Thung lũng Silicon, làm việc cho Google.Tôi nghĩ điều đó thật tuyệt vời và một giấc mơ đã trở thành hiện thực.Việc lấy chứng chỉ này là bước đi đầu tiên của bạncam kết chuyển đổisự nghiệp của bạn đối với an ninh mạng. Kudos cho bạn về điều đó.SQL là một trongbộ kỹ năng bạn cần có trong hộp công cụ của mình với tư cách là mộtchuyên gia an ninh mạng vì bạn có thểđưa ra quyết định rất nhanh chóng,không chỉ là ngẫu nhiên,nhưng đưa ra quyết định với sự hỗ trợ của dữ liệu,và có thể giao tiếp với nhóm của bạn,với các bên liên quan về lý do tại sao bạn thực hiệnmột quyết định bởi vì đó là một điều có thể nói,chúng ta cần phải làm điều này, đó làmột điều nữa để nói rằng chúng ta cần phải làm điều nàyvà đây là dữ liệu mà tôi đã viết các câu lệnh SQL của mình.Đầu tiên tôi học SQL bằng cáchnhư một bài tập ở trường, điều đó thực sự tuyệt vời,nhưng tôi nghĩ tôi đã quên hết chuyện đó sau giờ học.Bước tiếp theo tôi thực hiện là tham gia các khóa học trực tuyến,chẳng hạn như cái bạn đang học bây giờSQL và các nguyên tắc cơ bảnvề nó và cách thực sự sử dụng nó.Sau đó, lần đầu tiên tôi sử dụng SQL thực tế là ở Google.Bạn thực sự cần phải luyện tập.Tôi nghĩ với bất cứ điều gì khác, luyện tập sẽ tạo nên sự hoàn hảo.Có thể, ngay cả khi chỉ vài giờ một tuần,dành thời gian để thực hành viết câu lệnh SQL.Có được kỹ năng đó là điều sẽrất phù hợp với công việc đầu tiên của bạn,và bạn có thể sử dụng điều đó để đưa ra quyết định dựa trên dữ liệu.Tôi cảm thấy rất hài lòng khi làm việc trong lĩnh vực an ninh mạng.Tôi cảm thấy rất tràn đầy năng lượng,đi làm mỗi ngày.Không chỉ vì tôi được làm việcnhững vấn đề thực sự phức tạp vàcố gắng tìm ra giải pháp cho họ,nhưng tôi cũng có những đồng đội tuyệt vời mà chúng tôitất cả cùng nhau giải quyết vấn đề.Có thể đi ngủ vào ban đêm,biết rằng công việc tôi làm là vì lợi ích củaNgười dùng Google và nhân viên Googlelà một cảm giác rất bổ ích đối với tôi.

***1.6. Test your knowledge: SQL and databases – Kiểm tra kiến ​​thức của bạn: SQL và cơ sở dữ liệu***

**2. SQL queries – Truy vấn SQL**

***2.1. Basic queries – Truy vấn cơ bản***

|  |
| --- |
| In this video, we're going to be running our very first SQL query! This query will be based on a common work task that you might encounter as a security analyst. We're going to determine which computer has been assigned to a certain employee. Let's say we have access to the employees table. The employees table has five columns. Two of them, employee\_id and device\_id, contain the information that we need. We'll write a query to this table that returns only those two columns from the table. |

Trong video này, chúng ta sẽđang chạy truy vấn SQL đầu tiên của chúng tôi!Truy vấn này sẽ dựa trênmột nhiệm vụ công việc chung mà bạn có thểgặp phải với tư cách là một nhà phân tích bảo mật.Chúng ta sẽ xác địnhmáy tính nào đã được giao cho một nhân viên nhất định.Giả sử chúng ta có quyền truy cập vào bảng nhân viên.Bảng nhân viên có năm cột.Hai trong số đó, user\_id và device\_id,chứa thông tin mà chúng ta cần.Chúng tôi sẽ viết một truy vấn vào bảng nàychỉ trả về hai cột đó từ bảng.

|  |
| --- |
| The two SQL keywords we need for basic SQL queries are SELECT and FROM. SELECT indicates which columns to return. FROM indicates which table to query. The use of these keywords in SQL is very similar to how we would use these words in everyday language. For example, we can ask a friend to select apples and bananas from the big box when going out to buy fruit. This is already very similar to SQL. |

Hai từ khóa SQL chúng ta cần chocác truy vấn SQL cơ bản là CHỌN và TỪ.CHỌN cho biết cột nào sẽ trả về.FROM cho biết bảng nào cần truy vấn.Cách sử dụng các từ khóa này trong SQL rất giống nhauvề cách chúng ta sử dụng những từ này trong ngôn ngữ hàng ngày.Ví dụ: chúng ta có thể nhờ một người bạn chọntáo và chuối từhộp lớn khi đi ra ngoài mua trái cây.Điều này đã rất giống với SQL.

|  |
| --- |
| So let's go ahead and use SELECT and FROM in SQL to return the information we need on employees and the computers they use. We start off by typing in the SQL statement. After FROM, we've identified that the information will be pulled from the employees table. And after SELECT, employee\_id and device\_id indicate the two columns we want to return from this table. Notice how a comma separates the two columns that we want to return. |

Vì vậy, hãy tiếp tục và sử dụng SELECT và FROM trong SQL đểtrả lại thông tin chúng tôi cần trênnhân viên và máy tính họ sử dụng.Chúng tôi bắt đầu bằng cách gõ câu lệnh SQL.Sau FROM, chúng tôi đã xác định đượcrằng thông tin sẽ đượckéo ra khỏi bàn nhân viên.Và sau CHỌN, nhân viên\_id và device\_idchỉ ra hai cột chúng tôimuốn trở về từ bảng này.Chú ý cách phân tách bằng dấu phẩyhai cột mà chúng tôi muốn trả về.

|  |
| --- |
| It's also worth mentioning a couple of key aspects related to the syntax of SQL here. Syntax refers to the rules that determine what is correctly structured in a computing language. In SQL, keywords are not case-sensitive, so you could also write select and from in lowercase, but we're placing them in capital letters because it makes the query easier to understand. Another aspect of this syntax is that semicolons are placed at the end of the statement. |

Cũng đáng đề cập đến một vàicác khía cạnh chính liên quan đến cú pháp của SQL ở đây.Cú pháp đề cập đến các quy tắc xác địnhnhững gì được cấu trúc chính xác trong một ngôn ngữ máy tính.Trong SQL, từ khóa không phân biệt chữ hoa chữ thường, vì vậybạn cũng có thể viết select và from bằng chữ thường,nhưng chúng tôi đặt chúng bằng chữ in hoa vìnó làm cho truy vấn dễ hiểu hơn.Một khía cạnh khác của cú pháp nàyđó là dấu chấm phẩyđặt ở cuối tuyên bố.

|  |
| --- |
| And now, we'll run the query by pressing Enter. The output gives us the information we need to match employees to their computers. We just ran our very first SQL query! |

Và bây giờ, chúng ta sẽ chạy truy vấn bằng cách nhấn Enter.Đầu ra cung cấp cho chúng tôi thông tin mà chúng tôicần phải kết hợp nhân viên với máy tính của họ.Chúng tôi vừa chạy truy vấn SQL đầu tiên của mình!

|  |
| --- |
| Suppose you wanted to know what department the employee using the computer is from, or their username, or the office they work in. To do that, we can use SQL to make another statement that prints out all of the columns from the table. We can do this by placing an asterisk after SELECT. This is commonly referred to as select all. Now, let's run this query to the employees table in SQL. And now we have the full table in the output. |

Giả sử bạn muốn biếtnhân viên sử dụng bộ phận nàomáy tính đến từ hoặc của họtên người dùng hoặc văn phòng họ làm việc.Để làm điều đó, chúng ta có thể sử dụng SQL để tạomột tuyên bố khác in ratất cả các cột trong bảng.Chúng ta có thể làm điều này bằng cách đặt dấu hoa thị sau CHỌN.Điều này thường được gọi là chọn tất cả.Bây giờ, hãy chạy truy vấn này tới bảng nhân viên trong SQL.Và bây giờ chúng ta có bảng đầy đủ ở đầu ra.

|  |
| --- |
| You just made it through a basic query in SQL, congratulations! In the next video, we'll learn how to add filters to our queries, so I'll meet you there! |

Bạn vừa thực hiện nó thông qua một truy vấn cơ bảntrong SQL, xin chúc mừng!Trong video tiếp theo,chúng ta sẽ tìm hiểu cách thêm bộ lọc vàocâu hỏi của chúng tôi, vì vậy tôi sẽ gặp bạn ở đó!

***2.2. Query a database – Truy vấn cơ sở dữ liệu***

|  |
| --- |
| **Query a database** |

**Truy vấn cơ sở dữ liệu**

|  |
| --- |
| Previously, you explored how SQL is an important tool in the world of cybersecurity and is essential when querying databases. You examined a few basic SQL queries and keywords used to extract needed information from a database. In this reading, you’ll review those basic SQL queries and learn a new keyword that will help you organize your output. You'll also learn about the Chinook database, which this course uses for queries in readings and quizzes. |

Trước đây, bạn đã khám phá SQL là một công cụ quan trọng như thế nào trong thế giới an ninh mạng và cần thiết khi truy vấn cơ sở dữ liệu. Bạn đã kiểm tra một số truy vấn SQL cơ bản và từ khóa được sử dụng để trích xuất thông tin cần thiết từ cơ sở dữ liệu. Trong bài đọc này, bạn sẽ xem lại các truy vấn SQL cơ bản đó và tìm hiểu một từ khóa mới sẽ giúp bạn sắp xếp đầu ra của mình. Bạn cũng sẽ tìm hiểu về cơ sở dữ liệu **Chinook** mà khóa học này sử dụng cho các truy vấn trong bài đọc và câu hỏi.

|  |
| --- |
| **Basic SQL query** |

**Truy vấn SQL cơ bản**

|  |
| --- |
| There are two essential keywords in any SQL query: **SELECT** and **FROM**. You will use these keywords every time you want to query a SQL database. Using them together helps SQL identify what data you need from a database and the table you are returning it from. |

Có hai từ khóa thiết yếu trong bất kỳ truy vấn SQL nào: **SELECT** và **FROM** . Bạn sẽ sử dụng những từ khóa này mỗi khi bạn muốn truy vấn cơ sở dữ liệu SQL. Việc sử dụng chúng cùng nhau giúp SQL xác định dữ liệu nào bạn cần từ cơ sở dữ liệu và bảng mà bạn đang trả về dữ liệu đó.

|  |
| --- |
| The video demonstrated this SQL query: |

Video minh họa truy vấn SQL này:

|  |
| --- |
| **SELECT employee\_id, device\_id** |

**SELECT employee\_id, device\_id**

|  |
| --- |
| **FROM employees;** |

**FROM employees;**

|  |
| --- |
| In readings and quizzes, this course uses a sample database called the **Chinook** database to run queries. The **Chinook** database includes data that might be created at a digital media company. A security analyst employed by this company might need to query this data.  For example, the database contains eleven tables, including an **employees** table, a **customers** table, and an **invoices** table. These tables include data such as names and addresses. |

Trong các bài đọc và câu hỏi, khóa học này sử dụng cơ sở dữ liệu mẫu có tên là cơ sở dữ liệu **Chinook** để chạy truy vấn. Cơ sở dữ liệu **Chinook** bao gồm dữ liệu có thể được tạo tại một công ty truyền thông kỹ thuật số. Một nhà phân tích bảo mật được công ty này tuyển dụng có thể cần truy vấn dữ liệu này. Ví dụ: cơ sở dữ liệu chứa 11 bảng, bao gồm bảng **nhân viên** , bảng **khách hàng** và bảng **hóa đơn** . Các bảng này bao gồm dữ liệu như tên và địa chỉ.

|  |
| --- |
| As an example, you can run this query to return data from the **customers** table of the **Chinook** database:  SELECT customerid, city, country  FROM customers; |

Ví dụ: bạn có thể chạy truy vấn này để trả về dữ liệu từ bảng **khách hàng** của cơ sở dữ liệu **Chinook** :

SELECT customerid, city, country

FROM customers;

|  |
| --- |
| **SELECT** |

**SELECT**

|  |
| --- |
| The **SELECT** keyword indicates which columns to return. For example, you can return the **customerid** column from the **Chinook** database with |

Từ khóa **SELECT** cho biết cột nào cần trả về. Ví dụ: bạn có thể trả về cột **customerid** từ cơ sở dữ liệu **Chinook** với

|  |
| --- |
| **SELECT customerid** |

**SELECT customerid**

|  |
| --- |
| You can also select multiple columns by separating them with a comma. For example, if you want to return both the **customerid** and **city** columns, you should write **SELECT customerid, city**. |

Bạn cũng có thể chọn nhiều cột bằng cách phân tách chúng bằng dấu phẩy. Ví dụ: nếu bạn muốn trả về cả cột **customerid** và **city** , bạn nên viết **SELECT customerid, city** .

|  |
| --- |
| If you want to return all columns in a table, you can follow the **SELECT** keyword with an asterisk (**\***). The first line in the query will be **SELECT \***. |

Nếu bạn muốn trả về tất cả các cột trong một bảng, bạn có thể theo dõi từ khóa **SELECT** bằng dấu hoa thị ( **\*** ). Dòng đầu tiên trong truy vấn sẽ là **SELECT \*** .

|  |
| --- |
| **Note:** Although the tables you're querying in this course are relatively small, using **SELECT \*** may not be advisable when working with large databases and tables; in those cases, the final output may be difficult to understand and might be slow to run. |

**Lưu ý:** Mặc dù các bảng bạn đang truy vấn trong khóa học này tương đối nhỏ nhưng việc sử dụng **SELECT \*** có thể không được khuyến khích khi làm việc với các cơ sở dữ liệu và bảng lớn; trong những trường hợp đó, kết quả đầu ra cuối cùng có thể khó hiểu và có thể chạy chậm.

|  |
| --- |
| **FROM** |

**FROM**

|  |
| --- |
| The **SELECT** keyword always comes with the **FROM** keyword. **FROM** indicates which table to query. To use the **FROM** keyword, you should write it after the **SELECT** keyword, often on a new line, and follow it with the name of the table you’re querying. If you want to return all columns from the **customers** table, you can write: |

Từ khóa **SELECT** luôn đi kèm với từ khóa **FROM** . **FROM** cho biết bảng nào cần truy vấn. Để sử dụng từ khóa **FROM** , bạn nên viết nó sau từ khóa **SELECT** , thường là trên một dòng mới và theo sau là tên của bảng bạn đang truy vấn. Nếu bạn muốn trả về tất cả các cột từ bảng **khách hàng** , bạn có thể viết:

|  |
| --- |
| **SELECT \*** |

**SELECT \***

|  |
| --- |
| **FROM customers;** |

**FROM customers;**

|  |
| --- |
| When you want to end the query here, you put a semicolon (**;**) at the end to tell SQL that this is the entire query. |

Khi muốn kết thúc truy vấn tại đây, bạn đặt dấu chấm phẩy ( **;** ) ở cuối để cho SQL biết đây là toàn bộ truy vấn.

|  |
| --- |
| **Note:** Line breaks are not necessary in SQL queries, but are often used to make the query easier to understand. If you prefer, you can also write the previous query on one line as |

**Lưu ý:** Ngắt dòng không cần thiết trong truy vấn SQL nhưng thường được dùng để làm cho truy vấn dễ hiểu hơn. Nếu muốn, bạn cũng có thể viết truy vấn trước đó trên một dòng dưới dạng

|  |
| --- |
| **SELECT \* FROM customers;** |

**SELECT \* FROM customers;**

|  |
| --- |
| **ORDER BY** |

**ORDER BY**

|  |
| --- |
| Database tables are often very complicated, and this is where other SQL keywords come in handy. **ORDER BY** is an important keyword for organizing the data you extract from a table. |

Các bảng cơ sở dữ liệu thường rất phức tạp và đây là lúc các từ khóa SQL khác phát huy tác dụng. **ORDER BY** là một từ khóa quan trọng để sắp xếp dữ liệu bạn trích xuất từ ​​một bảng.

|  |
| --- |
| **ORDER BY** sequences the records returned by a query based on a specified column or columns. This can be in either ascending or descending order. |

**ORDER BY** sắp xếp các bản ghi được truy vấn trả về dựa trên một hoặc nhiều cột được chỉ định. Điều này có thể theo thứ tự tăng dần hoặc giảm dần.

|  |
| --- |
| **Sorting in ascending order** |

**Sắp xếp theo thứ tự tăng dần**

|  |
| --- |
| To use the **ORDER BY** keyword, write it at the end of the query and specify a column to base the sort on. In this example, SQL will return the **customerid**, **city**, and **country** columns from the **customers** table, and the records will be sequenced by the **city** column:  SELECT customerid, city, country  FROM customers  ORDER BY city; |

Để sử dụng từ khóa **ORDER BY** , hãy viết nó vào cuối truy vấn và chỉ định một cột để làm cơ sở sắp xếp. Trong ví dụ này, SQL sẽ trả về các cột **customerid** , **city** và **country** từ bảng **khách hàng** và các bản ghi sẽ được sắp xếp theo cột **thành phố** :

SELECT customerid, city, country

FROM customers

ORDER BY city;

|  |
| --- |
| The **ORDER BY** keyword sorts the records based on the column specified after this keyword. By default, as shown in this example, the sequence will be in ascending order. This means |

Từ khóa ORDER **BY** sắp xếp các bản ghi dựa trên cột được chỉ định sau từ khóa này. Theo mặc định, như trong ví dụ này, trình tự sẽ theo thứ tự tăng dần. Điều này có nghĩa là

|  |
| --- |
| * if you choose a column containing numeric data, it sorts the output from the smallest to largest. For example, if sorting on **customerid**, the ID numbers are sorted from smallest to largest. * if the column contains alphabetic characters, such as in the example with the **city** column, it orders the records from the beginning of the alphabet to the end. |

* nếu bạn chọn một cột chứa dữ liệu số, nó sẽ sắp xếp kết quả đầu ra từ nhỏ nhất đến lớn nhất. Ví dụ: nếu sắp xếp theo **customerid** thì số ID sẽ được sắp xếp từ nhỏ nhất đến lớn nhất.
* nếu cột chứa các ký tự chữ cái, chẳng hạn như trong ví dụ với  cột **thành phố** , nó sẽ sắp xếp các bản ghi từ đầu bảng chữ cái đến cuối.

|  |
| --- |
| **Sorting in descending order** |

**Sắp xếp theo thứ tự giảm dần**

|  |
| --- |
| You can also use the **ORDER BY** with the **DESC** keyword to sort in descending order. The **DESC** keyword is short for "descending" and tells SQL to sort numbers from largest to smallest, or alphabetically from Z to A. This can be done by following **ORDER BY** with the **DESC** keyword. For example, you can run this query to examine how the results differ when **DESC** is applied:  SELECT customerid, city, country  FROM customers  ORDER BY city DESC; |

Bạn cũng có thể sử dụng **ORDER BY** với từ khóa **DESC** để sắp xếp theo thứ tự giảm dần. Từ khóa **DESC** là viết tắt của "giảm dần" và yêu cầu SQL sắp xếp các số từ lớn nhất đến nhỏ nhất hoặc theo thứ tự bảng chữ cái từ Z đến A. Điều này có thể được thực hiện bằng cách làm theo **ORDER BY** với từ khóa **DESC** . Ví dụ: bạn có thể chạy truy vấn này để kiểm tra xem các kết quả khác nhau như thế nào khi áp dụng  **DESC :**

SELECT customerid, city, country

FROM customers

ORDER BY city DESC;

|  |
| --- |
| Now, cities at the end of the alphabet are listed first. |

Bây giờ, các thành phố ở cuối bảng chữ cái được liệt kê đầu tiên.

|  |
| --- |
| **Sorting based on multiple columns** |

**Sắp xếp dựa trên nhiều cột**

|  |
| --- |
| You can also choose multiple columns to order by. For example, you might first choose the **country** and then the **city** column. SQL then sorts the output by **country**, and for rows with the same **country**, it sorts them based on **city**. You can run this to explore how SQL displays this:  SELECT customerid, city, country  FROM customers  ORDER BY country, city; |

Bạn cũng có thể chọn nhiều cột để sắp xếp theo thứ tự. Ví dụ: trước tiên bạn có thể chọn quốc **gia** và sau đó là cột **thành phố** . Sau đó, SQL sắp xếp kết quả đầu ra theo **quốc gia** và đối với các hàng có cùng **quốc gia** , nó sẽ sắp xếp chúng dựa trên **thành phố** . Bạn có thể chạy cái này để khám phá cách SQL hiển thị cái này:

SELECT customerid, city, country

FROM customers

ORDER BY country, city;

|  |
| --- |
| **Key takeaways** |

**Bài học chính**

|  |
| --- |
| **SELECT** and **FROM** are important keywords in SQL queries. You use **SELECT** to indicate which columns to return and **FROM** to indicate which table to query. You can also include **ORDER BY** in your query to organize the output. These foundational SQL skills will support you as you move into more advanced queries. |

**CHỌN** và **TỪ** là những từ khóa quan trọng trong truy vấn SQL. Bạn sử dụng **SELECT** để cho biết cột nào cần trả về và **FROM** để cho biết bảng nào cần truy vấn. Bạn cũng có thể bao gồm **ORDER BY** trong truy vấn của mình để sắp xếp kết quả đầu ra. Những kỹ năng SQL cơ bản này sẽ hỗ trợ bạn khi bạn chuyển sang các truy vấn nâng cao hơn.

***2.3. Resources for completing SQL labs – Tài nguyên để hoàn thành các bài thí nghiệm SQL***

|  |
| --- |
| **Resources for completing SQL labs** |

**Tài nguyên để hoàn thành các bài thí nghiệm SQL**

|  |
| --- |
| This course features hands-on lab activities where you’ll have the opportunity to practice using SQL queries in the terminal. You’ll use a platform called Qwiklabs to complete these labs. In this reading, you’ll learn how to use Qwiklabs. |

Khóa học này có các hoạt động thực hành trong phòng thí nghiệm, nơi bạn sẽ có cơ hội thực hành sử dụng các truy vấn SQL trong thiết bị đầu cuối. Bạn sẽ sử dụng nền tảng có tên Qwiklabs để hoàn thành các phòng thí nghiệm này. Trong bài đọc này, bạn sẽ học cách sử dụng Qwiklabs.

|  |
| --- |
| This reading first provides a section on how to use Qwiklabs, which includes details on how to launch a lab, how to interact within the Qwiklabs environment, and how to end a lab. This is followed by another section on helpful navigation tips and keyboard shortcuts; these may be useful when working in the terminal. |

Bài đọc này trước tiên cung cấp phần về cách sử dụng Qwiklabs, bao gồm chi tiết về cách khởi chạy phòng thí nghiệm, cách tương tác trong môi trường Qwiklabs và cách kết thúc phòng thí nghiệm. Tiếp theo là phần khác về các mẹo điều hướng hữu ích và phím tắt; những điều này có thể hữu ích khi làm việc trong thiết bị đầu cuối.

|  |
| --- |
| **Note**: You will not launch Qwiklabs directly from this reading and instead will do this through lab activities and exemplars that you encounter throughout the course. |

**Lưu ý** : Bạn sẽ không khởi chạy Qwiklabs trực tiếp từ bài đọc này mà thay vào đó sẽ thực hiện việc này thông qua các hoạt động trong phòng thí nghiệm và các ví dụ mà bạn gặp trong suốt khóa học.

|  |
| --- |
| **How to use Qwiklabs** |

**Cách sử dụng Qwiklabs**

|  |
| --- |
| **Launching Qwiklabs** |

**Ra mắt Qwiklabs**

|  |
| --- |
| When you select a lab, you start from a Coursera page. You will need to click **Launch App** on that page. After you click **Launch App**, a new tab will open with a Qwiklabs page that contains instructions for that particular lab. |

Khi bạn chọn một phòng thí nghiệm, bạn bắt đầu từ trang Coursera. Bạn sẽ cần nhấp vào **Khởi chạy ứng dụng** trên trang đó. Sau khi bạn nhấp vào **Khởi chạy ứng dụng** , một tab mới sẽ mở ra với trang Qwiklabs chứa hướng dẫn cho phòng thí nghiệm cụ thể đó.

|  |
| --- |
| **Start Lab button** |

**Nút bắt đầu phòng thí nghiệm**

|  |
| --- |
| On the Qwiklabs page, you must click **Start Lab** to open a temporary terminal. The instructions for the lab will move to the right side of the screen. |

Trên trang Qwiklabs, bạn phải nhấp vào **Start Lab** để mở thiết bị đầu cuối tạm thời. Các hướng dẫn cho phòng thí nghiệm sẽ di chuyển sang phía bên phải của màn hình.



|  |
| --- |
| Read the instructions and complete all the tasks in the lab by entering commands in the terminal. |

Đọc hướng dẫn và hoàn thành tất cả các nhiệm vụ trong phòng thí nghiệm bằng cách nhập lệnh trong thiết bị đầu cuối.

|  |
| --- |
| **Note**: It may take a moment for the terminal to start. |

**Lưu ý** : Có thể mất một chút thời gian để thiết bị đầu cuối khởi động.

|  |
| --- |
| **Lab control dialog box** |

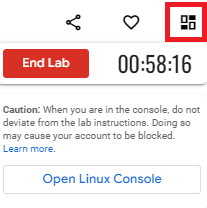
**Hộp thoại điều khiển phòng thí nghiệm**

|  |
| --- |
| After you click **Start Lab**, the lab control dialog box opens. It contains the **End Lab** button, the **timer**, and the **Open Linux Console** button. |

Sau khi bạn nhấn **Start Lab** , hộp thoại điều khiển lab sẽ mở ra. Nó chứa nút **End Lab**  , **bộ hẹn giờ** và nút **Open Linux Console** .

|  |
| --- |
| You can hide or unhide the dialog box by clicking the following icon in the red box: |

Bạn có thể ẩn hoặc hiện hộp thoại bằng cách nhấp vào biểu tượng sau trong hộp màu đỏ:



|  |
| --- |
| **The timer** |

**Đồng hồ bấm giờ**

|  |
| --- |
| The **timer** starts when the terminal has loaded. The timer keeps track of the amount of time you have left to complete a lab. The timer counts down until it reaches 00:00:00. When it does, your temporary terminal and resources are deleted. |

Bộ **đếm thời gian** bắt đầu khi thiết bị đầu cuối đã được tải. Bộ đếm thời gian theo dõi lượng thời gian bạn còn lại để hoàn thành phòng thí nghiệm. Đồng hồ đếm ngược cho đến khi về 00:00:00. Khi đó, thiết bị đầu cuối và tài nguyên tạm thời của bạn sẽ bị xóa.

|  |
| --- |
| You will have ample time to complete the labs. But, stay focused on completing the tasks to ensure you use your time well. |

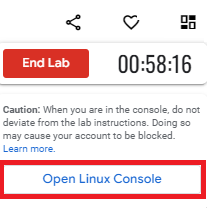
Bạn sẽ có nhiều thời gian để hoàn thành các bài thí nghiệm. Tuy nhiên, hãy tập trung hoàn thành nhiệm vụ để đảm bảo bạn sử dụng tốt thời gian của mình.

|  |
| --- |
| **Open Linux Console button** |

**Nút mở bảng điều khiển Linux**

|  |
| --- |
| When you click the button to **Open Linux Console**, the terminal opens in a new browser window: |

Khi bạn nhấp vào nút **Open Linux Console** , terminal sẽ mở trong cửa sổ trình duyệt mới:



|  |
| --- |
| Use this feature if you want a full-screen view of the terminal. You can close this window at any time. Closing the window does not end your lab, and you can continue working in the terminal in the original tab. |

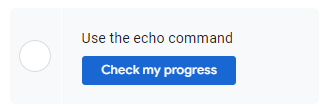
Sử dụng tính năng này nếu bạn muốn xem toàn màn hình của thiết bị đầu cuối. Bạn có thể đóng cửa sổ này bất cứ lúc nào. Việc đóng cửa sổ không kết thúc phòng thí nghiệm của bạn và bạn có thể tiếp tục làm việc trong thiết bị đầu cuối trong tab ban đầu.

|  |
| --- |
| **Check progress** |

**Kiểm tra tiến độ**

|  |
| --- |
| You can check your progress by clicking **Check my progress** at the end of each task. |

Bạn có thể kiểm tra tiến độ của mình bằng cách nhấp vào **Kiểm tra tiến độ của tôi** ở cuối mỗi nhiệm vụ.



|  |
| --- |
| If you haven’t yet completed a task, you’ll receive hints on what you must do to complete it. |

Nếu bạn chưa hoàn thành nhiệm vụ, bạn sẽ nhận được gợi ý về những gì bạn phải làm để hoàn thành nhiệm vụ đó.

|  |
| --- |
| You can click **Check my progress** whenever you want to check the completion status of a task or receive a hint. |

Bạn có thể nhấp vào **Kiểm tra tiến trình của tôi** bất cứ khi nào bạn muốn kiểm tra trạng thái hoàn thành của một nhiệm vụ hoặc nhận gợi ý.

|  |
| --- |
| **Using copy/paste commands** |

**Sử dụng lệnh sao chép/dán**

|  |
| --- |
| The first time you try to use copy or paste keyboard shortcuts (such as **CTRL + C**), you’ll receive a pop-up requesting permission to use your device’s clipboard:  “**googlecoursera.qwiklabs.com wants to see text and images copied to the clipboard.**” Please click **Allow** if you would like to be able to use these shortcuts in the Qwiklabs platform. If you choose not to allow Qwiklabs access to your clipboard, you cannot use keyboard shortcuts but you can still complete the lab. |

Lần đầu tiên bạn cố gắng sử dụng các phím tắt sao chép hoặc dán (chẳng hạn như **CTRL + C** ), bạn sẽ nhận được một cửa sổ bật lên yêu cầu quyền sử dụng bảng nhớ tạm của thiết bị: “ **googlecoursera.qwiklabs.com muốn xem văn bản và hình ảnh được sao chép sang bảng nhớ tạm.** ” Vui lòng nhấp vào **Cho phép** nếu bạn muốn có thể sử dụng các phím tắt này trong nền tảng Qwiklabs. Nếu bạn chọn không cho phép Qwiklabs truy cập vào khay nhớ tạm của mình, bạn không thể sử dụng phím tắt nhưng vẫn có thể hoàn thành bài thí nghiệm.

|  |
| --- |
| **Code block** |

**Khối mã**

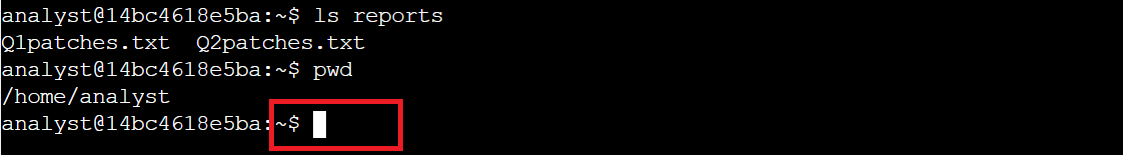
|  |
| --- |
| Certain steps may include a code block. Click the copy button to copy the code provided and then paste it into the terminal. |

Một số bước nhất định có thể bao gồm một khối mã. Nhấp vào nút sao chép để sao chép mã được cung cấp rồi dán vào thiết bị đầu cuối.



|  |
| --- |
| To paste code or other text content that you have copied from the instructions into the terminal, activate the terminal by clicking anywhere inside it. The terminal is active when the cursor in the terminal changes from a static empty outline to a flashing solid block. |

Để dán mã hoặc nội dung văn bản khác mà bạn đã sao chép từ hướng dẫn vào thiết bị đầu cuối, hãy kích hoạt thiết bị đầu cuối bằng cách nhấp vào bất kỳ đâu bên trong thiết bị đầu cuối. Thiết bị đầu cuối hoạt động khi con trỏ trong thiết bị đầu cuối thay đổi từ đường viền trống tĩnh sang khối rắn nhấp nháy.



|  |
| --- |
| Once the terminal is active, use the keyboard shortcut **CTRL + V** (hold down the **CTRL** key and press the **V** key) to insert the copied text into the terminal at the location of the flashing cursor. |

Khi thiết bị đầu cuối hoạt động, hãy sử dụng phím tắt **CTRL + V** (giữ phím **CTRL** và nhấn phím **V** ) để chèn văn bản đã sao chép vào thiết bị đầu cuối tại vị trí con trỏ nhấp nháy.

|  |
| --- |
| **Scrolling** |

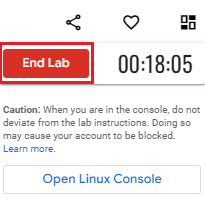
**Cuộn**

|  |
| --- |
| In certain situations, you may want to scroll within the terminal window. To do so, use the scroll wheel on your mouse or the touchpad of your computer. |

Trong một số trường hợp nhất định, bạn có thể muốn cuộn trong cửa sổ terminal. Để làm như vậy, hãy sử dụng con lăn trên chuột hoặc bàn di chuột của máy tính.

|  |
| --- |
| **End Lab button** |

**Nút kết thúc phòng thí nghiệm**



|  |
| --- |
| Finally, click **End Lab** when you’ve completed the tasks in the lab. |

Cuối cùng, nhấp vào **End Lab** khi bạn đã hoàn thành các nhiệm vụ trong lab.

|  |
| --- |
| **Note**: Don't click **End Lab** until you're finished; you'll lose access to the work you've done throughout the lab. |

**Lưu ý** : Đừng nhấp vào **End Lab** cho đến khi bạn hoàn thành; bạn sẽ mất quyền truy cập vào công việc bạn đã thực hiện trong phòng thí nghiệm.

|  |
| --- |
| **Tracking progress on Coursera** |

**Theo dõi tiến trình trên Coursera**

|  |
| --- |
| If you complete a lab but your progress hasn’t been tracked on Coursera, you may need to refresh the page for your progress to be registered. Once you complete the lab and refresh the page, the green check mark should appear. |

Nếu bạn hoàn thành bài thí nghiệm nhưng tiến trình của bạn chưa được theo dõi trên Coursera, bạn có thể cần phải làm mới trang để đăng ký tiến trình của mình. Sau khi bạn hoàn thành bài thực hành và làm mới trang, dấu kiểm màu xanh lục sẽ xuất hiện.

|  |
| --- |
| **Helpful navigation tips and keyboard shortcuts** |

**Mẹo điều hướng hữu ích và phím tắt**

|  |
| --- |
| The following contains a list of navigation tips and keyboard shortcuts you may find useful when completing your SQL labs. Your cursor must be in the terminal window to use these navigation tips and keyboard shortcuts. |

Phần sau đây chứa danh sách các mẹo điều hướng và phím tắt mà bạn có thể thấy hữu ích khi hoàn thành các bài thí nghiệm SQL của mình. Con trỏ của bạn phải ở trong cửa sổ terminal để sử dụng các mẹo điều hướng và phím tắt này.

|  |
| --- |
| * **CTRL + C**: Terminates a command that is currently running; from the instructions portion of Qwiklabs, you can use **CTRL + C** to copy, but within the terminal, it will only terminate a command and if one isn't running, it will exit out of the MariaDB shell; if you unintentionally exit, you can reconnect by running the **sudo mysql organization** command * **CTRL + V**: Pastes text * **CTRL + L**: Clears the terminal screen; within MariaDB, you must use **CTRL + L** and cannot use **clear** * **\c + Enter**: Clears the current input * **CTRL + A**: Sets your cursor at the beginning of a command * **CTRL + E**: Sets your cursor at the end of a command * **Left arrow key**: Moves left within a command * **Right arrow key**: Moves right within a command * **Up arrow** **key**: Provides the last command you entered into the command line; can be entered multiple times to go through multiple commands from the command history * **Down arrow key**: Provides the next command in the command history; must be after using the **up arrow** key * **Tab** **key**: Provides available suggestions for completing your text |

* **CTRL + C** : Chấm dứt lệnh hiện đang chạy; từ phần hướng dẫn của Qwiklabs, bạn có thể sử dụng **CTRL + C** để sao chép, nhưng trong thiết bị đầu cuối, nó sẽ chỉ chấm dứt một lệnh và nếu một lệnh không chạy, nó sẽ thoát ra khỏi trình bao MariaDB; nếu vô tình thoát ra, bạn có thể kết nối lại bằng cách chạy lệnh **tổ chức sudo mysql**
* **CTRL + V** : Dán văn bản
* **CTRL + L** : Xóa màn hình terminal; trong MariaDB, bạn phải sử dụng **CTRL + L** và không thể sử dụng **clear**
* **\c + Enter** : Xóa đầu vào hiện tại
* **CTRL + A** : Đặt con trỏ của bạn ở đầu lệnh
* **CTRL + E** : Đặt con trỏ của bạn ở cuối lệnh
* **Phím mũi tên trái** : Di ​​chuyển sang trái trong lệnh
* **Phím mũi tên phải** : Di ​​chuyển sang phải trong lệnh
* **Phím mũi tên lên** : Cung cấp lệnh cuối cùng bạn đã nhập vào dòng lệnh; có thể được nhập nhiều lần để đi qua nhiều lệnh từ lịch sử lệnh
* **Phím mũi tên xuống** : Cung cấp lệnh tiếp theo trong lịch sử lệnh; phải sau khi sử dụng phím **mũi tên lên**
* **Phím tab** : Cung cấp các gợi ý có sẵn để hoàn thành văn bản của bạn

|  |
| --- |
| **Note:** If you unintentionally exit the **organization** database in the MariaDB shell, you can reconnect by running the **sudo mysql organization** command. |

**Lưu ý:** Nếu vô tình thoát khỏi cơ sở dữ liệu **tổ chức** trong trình bao MariaDB, bạn có thể kết nối lại bằng cách chạy lệnh **tổ chức sudo mysql** .

|  |
| --- |
| **Key takeaways** |

**Bài học chính**

|  |
| --- |
| Knowing how to navigate Qwiklabs will be useful as you complete the labs throughout this course. These labs can help you practice what you’ve learned in an interactive environment. |

Biết cách điều hướng Qwiklabs sẽ hữu ích khi bạn hoàn thành các bài thí nghiệm trong suốt khóa học này. Những phòng thí nghiệm này có thể giúp bạn thực hành những gì bạn đã học trong môi trường tương tác.

***2.4. Activity: Perform a SQL query – Hoạt động: Thực hiện truy vấn SQL***

***2.5. Optional Exemplar: Perform a SQL query – Mẫu tùy chọn: Thực hiện truy vấn SQL***

***2.6. Basic filters on SQL queries – Bộ lọc cơ bản trên truy vấn SQL***

|  |
| --- |
| One of the most powerful features of SQL is its ability to filter. In this video, we're going to learn how this helps us make better queries and select more specific pieces of data from a database. |

Một trong những tính năng mạnh mẽ nhất của SQL là khả năng lọc.Trong video này, chúng ta sẽ tìm hiểu cách điều này giúp chúng ta thực hiện các truy vấn tốt hơn vàchọn các phần dữ liệu cụ thể hơn từ cơ sở dữ liệu.

|  |
| --- |
| Filtering is selecting data that match a certain condition. Think of filtering as a way of only choosing the data we want. Let's say we wanted to select apples from a fruit cart. Filtering allows us to specify what kind of apples we want to choose. When we go buy apples, we might explicitly say, "Choose only apples that are fresh." This removes apples that aren't fresh from the selection. This is a filter! As a security analyst, you might filter a log-in attempts table to find all attempts from a specific country. This could be done by applying a filter on the country column. For example, you could filter to just return records containing Canada. |

Lọc là chọn dữ liệu phù hợp với một điều kiện nhất định.Hãy nghĩ đến việc lọc như một cách chỉ chọn dữ liệu chúng ta muốn.Giả sử chúng ta muốn chọn táo từ xe bán trái cây.Việc lọc cho phép chúng ta chỉ định loại táo nào chúng ta muốn chọn.Khi đi mua táo, chúng ta có thể nói rõ ràng rằng: "Chỉ chọn những quả táo còn tươi".Thao tác này sẽ loại bỏ những quả táo không còn tươi khỏi vùng chọn.Đây là một bộ lọc!Là nhà phân tích bảo mật, bạn có thể lọc bảng số lần đăng nhập để tìm tất cả các lần thửtừ một quốc gia cụ thể.Điều này có thể được thực hiện bằng cách áp dụng bộ lọc trên cột quốc gia.Ví dụ: bạn có thể lọc để chỉ trả về các bản ghi có chứa Canada.

|  |
| --- |
| Before we get started, we need to focus on an important part of the syntax of SQL. Let's learn about operators. An operator is a symbol or keyword that represents an operation. An example of an operator would be the equal to operator. For example, if we wanted to find all records that have USA in the country column, we use country = 'USA' To filter a query in SQL, we simply add an extra line to the SELECT and FROM statement we used before. This extra line will use a WHERE clause. In SQL, WHERE indicates the condition for a filter. After the keyword WHERE, the specific condition is listed using operators. So if we wanted to find all of the login attempts made in the United States, we would create this filter. In this particular condition, we're indicating to return all records that have a value in the country column that is equal to USA. |

Trước khi bắt đầu, chúng ta cần tập trung vào một phần quan trọng trong cú pháp của SQL.Hãy cùng tìm hiểu về các toán tử.Toán tử là một ký hiệu hoặc từ khóa đại diện cho một thao tác.Một ví dụ về toán tử sẽ là toán tử bằng.Ví dụ: nếu chúng ta muốn tìm tất cả các bản ghicó USA trong cột quốc gia, chúng tôi sử dụng country = 'USA'Để lọc một truy vấn trong SQL, chúng ta chỉ cần thêm một dòng bổ sung vào SELECT và FROMtuyên bố chúng tôi đã sử dụng trước đây.Dòng bổ sung này sẽ sử dụng mệnh đề WHERE.Trong SQL, WHERE cho biết điều kiện của bộ lọc.Sau từ khóa WHERE, điều kiện cụ thể được liệt kê bằng các toán tử.Vì vậy, nếu chúng tôi muốn tìm tất cả các lần đăng nhập được thực hiện ở Hoa Kỳ,chúng tôi sẽ tạo bộ lọc này.Trong điều kiện cụ thể này, chúng tôi đang yêu cầu trả lại tất cả các bản ghicó giá trị trong cột quốc gia bằng với Hoa Kỳ.

|  |
| --- |
| Let's try putting it all together in SQL. We're going to start with selecting all the columns from the log\_in\_attempts table. And then add the WHERE filter. Don't forget the semicolon! This tells us we finished the SQL statement. Now, let's run this query! Because of our filter, only the rows where the country of the log-in attempt was USA are returned. |

Hãy thử kết hợp tất cả lại với nhau trong SQL.Chúng ta sẽ bắt đầu bằng việc chọn tất cả các cột từbảng log\_in\_attempts. Và sau đó thêm bộ lọc WHERE.Đừng quên dấu chấm phẩy!Điều này cho chúng ta biết chúng ta đã hoàn thành câu lệnh SQL.Bây giờ hãy chạy truy vấn này! Do bộ lọc của chúng tôi, chỉ có các hàngnơi quốc gia của lần đăng nhập là Hoa Kỳ được trả về.

|  |
| --- |
| In the previous example, the condition for our filter was based simply on returning records that are equal to a particular value. We can also make our conditions more complex by searching for a pattern instead of an exact word. For example, in the employees table, we have a column for office. We could search for records in this column that match a certain pattern. Perhaps we might want all offices in the East building. To search for a pattern, we used the percentage sign to act as a wildcard for unspecified characters. If we ran a filter for 'East%', this would return all records that start with East -- for example, the offices East-120, East-290, and East-435. |

Trong ví dụ trước, điều kiện cho bộ lọc của chúng tôi chỉ đơn giản dựa trên việc trả vềcác bản ghi tương đương với một giá trị cụ thể.Chúng ta cũng có thể làm cho điều kiện của mình phức tạp hơn bằng cách tìm kiếmmột khuôn mẫu thay vì một từ chính xác.Ví dụ, trong bảng nhân viên, chúng ta có một cột dành cho văn phòng.Chúng ta có thể tìm kiếm các bản ghi trong cột này khớp với một mẫu nhất định.Có lẽ chúng ta muốn có tất cả các văn phòng ở tòa nhà phía Đông.Để tìm kiếm một mẫu, chúng tôi đã sử dụng dấu phần trăm để đóng vai trò là ký tự đại diện choký tự không xác định.Nếu chúng tôi chạy bộ lọc cho 'East%', bộ lọc này sẽ trả về tất cả các bản ghi bắt đầu bằng East --ví dụ: các văn phòng East-120, East-290 và East-435.

|  |
| --- |
| When searching for patterns with the percentage sign, we cannot use the equals operator. Instead, we use another operator, LIKE. LIKE is an operator used with WHERE to search for a pattern in a column. |

Khi tìm kiếm các mẫu có dấu phần trăm,chúng ta không thể sử dụng toán tử bằng.Thay vào đó, chúng ta sử dụng một toán tử khác, THÍCH.THÍCH là toán tử được sử dụng với WHERE để tìm kiếm mẫu trong một cột.

|  |
| --- |
| Since LIKE is an operator, similar to the equal sign, we use it instead of the equal sign. So, when our goal is to return all values in the office column that start with the word East, LIKE would appear in a WHERE clause. |

Vì THÍCH là một toán tử, tương tự như dấu bằng,chúng tôi sử dụng nó thay vì dấu bằng.Vì vậy, khi mục tiêu của chúng ta là trả về tất cả các giá trị trong cột văn phòng bắt đầu bằng từEast, THÍCH sẽ xuất hiện trong mệnh đề WHERE.

|  |
| --- |
| Let's go back to the example in which we wanted to filter for log-in attempts made in the United States. Imagine that we realize that our database contains inconsistencies with how the United States is represented. Some entries use US while others use USA. Let's get into SQL and apply this new type of filter with LIKE. We're going to start with the same first two lines of code because we want to select all columns from the log-in attempts table. And we're going to add a filter with LIKE so that records will be returned if they contain a value in the country column beginning with the characters US. This includes both US and USA. Let's run this query to check if the output changes. This returns all the entries where the user location was in the United States. And now we can use the LIKE clause to filter columns based on a pattern! |

Hãy quay lại ví dụ mà chúng tôi muốn lọccác nỗ lực đăng nhập được thực hiện tại Hoa Kỳ.Hãy tưởng tượng rằng chúng ta nhận ra rằng cơ sở dữ liệu của chúng ta có những điểm không nhất quán với cách thứcHoa Kỳ được đại diện.Một số mục sử dụng Hoa Kỳ trong khi những mục khác sử dụng Hoa Kỳ.Hãy cùng truy cập SQL và áp dụng loại bộ lọc mới này với THÍCH.Chúng ta sẽ bắt đầu với hai dòng đầu tiên giống nhau củacode vì chúng tôi muốn chọn tất cả các cột từ bảng số lần đăng nhập.Và chúng tôi sẽ thêm bộ lọc với THÍCH để các bản ghi sẽ được trả về nếuchúng chứa một giá trị trong cột quốc gia bắt đầu bằng các ký tự US.Điều này bao gồm cả Hoa Kỳ và Hoa Kỳ.Hãy chạy truy vấn này để kiểm tra xem kết quả đầu ra có thay đổi không. Điều này trả về tất cảcác mục có vị trí của người dùng ở Hoa Kỳ.Và bây giờ chúng ta có thể sử dụng mệnh đề THÍCH để lọc các cột dựa trên mẫu!

|  |
| --- |
| Wow, we've already learned how to get very precise with our database and get exactly the data we need with one single query. I'm excited for what's next! |

Ồ, chúng ta đã học được cách sử dụng cơ sở dữ liệu một cách chính xác vàlấy chính xác dữ liệu chúng ta cần chỉ bằng một truy vấn.Tôi rất vui mừng cho những gì tiếp theo!

***2.7. The WHERE clause and basic operators – Mệnh đề WHERE và các toán tử cơ bản***

|  |
| --- |
| **The WHERE clause and basic operators** |

**Mệnh đề WHERE và các toán tử cơ bản**

|  |
| --- |
| Previously, you focused on how to refine your SQL queries by using the **WHERE** clause to filter results. In this reading, you’ll further explore how to use the **WHERE** clause, the **LIKE** operator and the percentage sign (**%**) wildcard. You’ll also be introduced to the underscore (**\_**), another wildcard that can help you filter queries. |

Trước đây, bạn đã tập trung vào cách tinh chỉnh các truy vấn SQL bằng cách sử dụng mệnh đề **WHERE** để lọc kết quả. Trong bài đọc này, bạn sẽ khám phá thêm cách sử dụng mệnh đề **WHERE** , toán tử **THÍCH** và ký tự đại diện dấu phần trăm ( **%** ). Bạn cũng sẽ được làm quen với dấu gạch dưới ( **\_** ), một ký tự đại diện khác có thể giúp bạn lọc truy vấn.

|  |
| --- |
| **How filtering helps** |

**Cách lọc giúp ích**

|  |
| --- |
| As a security analyst, you'll often be responsible for working with very large and complicated security logs. To find the information you need, you'll often need to use SQL to filter the logs. |

Là nhà phân tích bảo mật, bạn thường phải chịu trách nhiệm làm việc với các nhật ký bảo mật rất lớn và phức tạp. Để tìm thông tin bạn cần, bạn thường cần sử dụng SQL để lọc nhật ký.

|  |
| --- |
| In a cybersecurity context, you might use filters to find the login attempts of a specific user or all login attempts made at the time of a security issue. As another example, you might filter to find the devices that are running a specific version of an application. |

Trong bối cảnh an ninh mạng, bạn có thể sử dụng bộ lọc để tìm các lần đăng nhập của một người dùng cụ thể hoặc tất cả các lần đăng nhập được thực hiện tại thời điểm xảy ra sự cố bảo mật. Một ví dụ khác, bạn có thể lọc để tìm các thiết bị đang chạy một phiên bản cụ thể của ứng dụng.

|  |
| --- |
| **WHERE** |

**WHERE**

|  |
| --- |
| To create a filter in SQL, you need to use the keyword **WHERE**. **WHERE** indicates the condition for a filter. |

Để tạo bộ lọc trong SQL, bạn cần sử dụng từ khóa **WHERE** . **WHERE** cho biết điều kiện của bộ lọc.

|  |
| --- |
| If you needed to email employees with a title of IT Staff, you might use a query like the one in the following example. You can run this example to examine what it returns:  SELECT firstname, lastname, title, email  FROM employees  WHERE title = 'IT Staff'; |

Nếu bạn cần gửi email cho nhân viên với chức danh Nhân viên CNTT, bạn có thể sử dụng truy vấn giống như trong ví dụ sau. Bạn có thể chạy ví dụ này để kiểm tra xem nó trả về kết quả gì:

SELECT firstname, lastname, title, email

FROM employees

WHERE title = 'IT Staff';

|  |
| --- |
| Rather than returning all records in the **employees** table, this **WHERE** clause instructs SQL to return only those that contain **'IT Staff'** in the **title** column. It uses the equals sign (**=**) operator to set this condition. |

Thay vì trả về tất cả các bản ghi trong bảng **nhân viên , mệnh đề WHERE** này hướng dẫn SQL chỉ trả về những bản ghi có chứa **'Nhân viên CNTT'** trong cột **tiêu đề** . Nó sử dụng toán tử dấu bằng ( **=** ) để đặt điều kiện này.

|  |
| --- |
| **Note:** You should place the semicolon (**;**) where the query ends. When you add a filter to a basic query, the semicolon is after the filter. |

**Lưu ý:** Bạn nên đặt dấu chấm phẩy ( **;** ) ở vị trí kết thúc truy vấn. Khi bạn thêm bộ lọc vào truy vấn cơ bản, dấu chấm phẩy sẽ ở sau bộ lọc.

|  |
| --- |
| **Filtering for patterns** |

**Lọc các mẫu**

|  |
| --- |
| You can also filter based on a pattern. For example, you can identify entries that start or end with a certain character or characters. Filtering for a pattern requires incorporating two more elements into your **WHERE** clause: |

Bạn cũng có thể lọc dựa trên một mẫu. Ví dụ: bạn có thể xác định các mục bắt đầu hoặc kết thúc bằng một hoặc nhiều ký tự nhất định. Việc lọc một mẫu yêu cầu kết hợp thêm hai phần tử vào mệnh đề **WHERE** của bạn :

|  |
| --- |
| * a wildcard * the **LIKE** operator |

* một ký tự đại diện
* toán tử **THÍCH**

|  |
| --- |
| **Wildcards** |

**Ký tự đại diện**

|  |
| --- |
| A **wildcard** is a special character that can be substituted with any other character. Two of the most useful wildcards are the percentage sign (**%**) and the underscore (**\_**): |

Ký **tự đại diện** là một ký tự đặc biệt có thể được thay thế bằng bất kỳ ký tự nào khác. Hai trong số các ký tự đại diện hữu ích nhất là dấu phần trăm ( **%** ) và dấu gạch dưới ( **\_** ):

|  |
| --- |
| * The percentage sign substitutes for any number of other characters. * The underscore symbol only substitutes for one other character. |

* Ký hiệu phần trăm thay thế cho bất kỳ số lượng ký tự nào khác.
* Ký hiệu gạch dưới chỉ thay thế cho một ký tự khác.

|  |
| --- |
| These wildcards can be placed after a string, before a string, or in both locations depending on the pattern you’re filtering for. |

Các ký tự đại diện này có thể được đặt sau một chuỗi, trước một chuỗi hoặc ở cả hai vị trí tùy thuộc vào mẫu bạn đang lọc.

|  |
| --- |
| The following table includes these wildcards applied to the string **'a'** and examples of what each pattern would return. |

Bảng sau đây bao gồm các ký tự đại diện được áp dụng cho chuỗi **'a'** và ví dụ về kết quả mà mỗi mẫu sẽ trả về.

|  |  |
| --- | --- |
| **Pattern** | **Results that could be returned** |
| **'a%'** | **apple123, art, a** |
| **'a\_'** | **as, an, a7** |
| **'a\_\_'** | **ant, add, a1c** |
| **'%a'** | **pizza, Z6ra, a** |
| **'\_a'** | **ma, 1a, Ha** |
| **'%a%'** | **Again, back, a** |
| **'\_a\_'** | **Car, ban, ea7** |

|  |  |
| --- | --- |
| **Mẫu** | **Kết quả có thể được trả về** |
| **'a%'** | **apple123, art, a** |
| **'a\_'** | **as, an, a7** |
| **'a\_\_'** | **ant, add, a1c** |
| **'%a'** | **pizza, Z6ra, a** |
| **'\_a'** | **ma, 1a, Ha** |
| **'%a%'** | **Again, back, a** |
| **'\_a\_'** | **Car, ban, ea7** |

|  |
| --- |
| **LIKE** |

**LIKE**

|  |
| --- |
| To apply wildcards to the filter, you need to use the **LIKE** operator instead of an equals sign (**=**). **LIKE** is used with **WHERE** to search for a pattern in a column. |

Để áp dụng ký tự đại diện cho bộ lọc, bạn cần sử dụng toán tử **THÍCH** thay vì dấu bằng ( **=** ). **THÍCH** được sử dụng với **WHERE** để tìm kiếm mẫu trong một cột.

|  |
| --- |
| For instance, if you want to email employees with a title of either **'IT Staff'** or **'IT Manager'**, you can use **LIKE** operator combined with the **%** wildcard:  SELECT lastname, firstname, title, email  FROM employees  WHERE title LIKE 'IT%'; |

Ví dụ: nếu bạn muốn gửi email cho nhân viên với tiêu đề là **“Nhân viên CNTT”** hoặc **“Quản lý CNTT”** , bạn có thể sử dụng toán tử **THÍCH** kết hợp với ký tự đại diện **%** :

SELECT lastname, firstname, title, email

FROM employees

WHERE title LIKE 'IT%';

|  |
| --- |
| This query returns all records with values in the **title** column that start with the pattern of **'IT'**. This means both **'IT Staff'** and **'IT Manager'** are returned. |

Truy vấn này trả về tất cả các bản ghi có giá trị trong cột **tiêu đề** bắt đầu bằng mẫu **'IT'** . Điều này có nghĩa là cả **'Nhân viên CNTT'** và **'Quản lý CNTT'** đều được trả về.

|  |
| --- |
| As another example, if you want to search through the invoices table to find all customers located in states with an abbreviation of **'NY'**, **'NV'**, **'NS'** or **'NT'**, you can use the **'N\_'** pattern on the **state** column:  SELECT firstname,lastname, state, country  FROM customers  WHERE state LIKE 'N\_'; |

Một ví dụ khác, nếu bạn muốn tìm kiếm trong bảng hóa đơn để tìm tất cả khách hàng ở các tiểu bang có tên viết tắt là **'NY'** , **'NV'** , **'NS'** hoặc **'NT'** , bạn có thể sử dụng mẫu **'N\_'** trên cột **trạng thái** :

SELECT firstname,lastname, state, country

FROM customers

WHERE state LIKE 'N\_';

|  |
| --- |
| This returns all the records with state abbreviations that follow this pattern. |

Điều này trả về tất cả các bản ghi có chữ viết tắt trạng thái theo mẫu này.

|  |
| --- |
| **Key takeaways** |

**Bài học chính**

|  |
| --- |
| Filters are important when refining what your query returns. **WHERE** is an essential keyword for adding a filter to your query.  You can also filter for patterns by combining the **LIKE** operator with the percentage sign (**%**) and the underscore (**\_**) wildcards. |

Bộ lọc rất quan trọng khi tinh chỉnh kết quả truy vấn của bạn trả về. **WHERE** là từ khóa cần thiết để thêm bộ lọc vào truy vấn của bạn. Bạn cũng có thể lọc các mẫu bằng cách kết hợp toán **tử LIKE** với dấu phần trăm ( **%** ) và ký tự đại diện gạch dưới ( **\_** ).

***2.8. Activity: Filter a SQL query – Hoạt động: Lọc truy vấn SQL***

***2.9. Optional Exemplar: Filter a SQL query – Mẫu tùy chọn: Lọc truy vấn SQL***

***2.10. Test your knowledge: SQL queries – Kiểm tra kiến ​​thức của bạn: Truy vấn SQL***

**3. More SQL filters – Các bộ lọc SQL khác**

***3.1. Filter dates and numbers – Lọc ngày và số***

|  |
| --- |
| In this video, we're going to continue using SQL queries and filters, but now we're going to apply them to new data types. First, let's explore the three common data types that you will find in databases: string, numeric, and date and time. String data is data consisting of an ordered sequence of characters. These characters could be numbers, letters, or symbols. For example, you'll encounter string data in user names, such as a user name: analyst10. Numeric data is data consisting of numbers, such as a count of log-in attempts. Unlike strings, mathematical operations can be used on numeric data, like multiplication or addition. Date and time data refers to data representing a date and/or time. |

Trong video này, chúng ta sẽ tiếp tục sử dụng các truy vấn và bộ lọc SQL,nhưng bây giờ chúng ta sẽ áp dụng chúng cho các kiểu dữ liệu mới.Trước tiên, hãy khám phá ba loại dữ liệu phổ biến mà bạn sẽ tìm thấy trong cơ sở dữ liệu:chuỗi, số và ngày và giờ.Dữ liệu chuỗi là dữ liệu bao gồm một chuỗi ký tự được sắp xếp.Những ký tự này có thể là số, chữ cái hoặc ký hiệu.Ví dụ: bạn sẽ gặp dữ liệu chuỗi trong tên người dùng,chẳng hạn như tên người dùng: nhà phân tích10.Dữ liệu số là dữ liệu bao gồm các số,chẳng hạn như số lần đăng nhập.Không giống như chuỗi, các phép toán có thể được sử dụng trên dữ liệu số,như phép nhân hoặc phép cộng.Dữ liệu ngày và giờ đề cập đến dữ liệu biểu thị ngày và/hoặc thời gian.

|  |
| --- |
| Previously, we applied filters using string data, but now let's work with numeric and date and time data. As a security analyst, you'll often need to query numbers and dates. For example, we could filter patch dates to find machines that need an update, or we could filter log-in attempts to return only those made in a certain period of time. We learned about operators in the last video, and we're going to use them again for numbers and dates. |

Trước đây, chúng tôi đã áp dụng các bộ lọc sử dụng dữ liệu chuỗi, nhưngbây giờ hãy làm việc với dữ liệu số và ngày và giờ.Là một nhà phân tích bảo mật, bạn thường cần truy vấn các con số và ngày tháng.Ví dụ: chúng tôi có thể lọc ngày vá lỗi để tìm các máy cần cập nhật,hoặc chúng tôi có thể lọc các lần đăng nhập để chỉ trả lạinhững gì được thực hiện trong một khoảng thời gian nhất định.Chúng ta đã tìm hiểu về các toán tử trong video trước vàchúng ta sẽ sử dụng lại chúng cho số và ngày tháng.

|  |
| --- |
| Common operators for working with numeric or date and time data types include: equals, greater than, less than, not equal to, greater than or equal to, and less than or equal to. Let's say you want to find the log-in attempts made after 6 pm. Because this is past normal business hours, you want to look for suspicious patterns. You can identify these attempts by using the greater than operator in your filter. We'll start writing our query in SQL. We begin by indicating that we want to select all columns FROM the log\_in\_attempts table. Then we'll add our filter with WHERE. |

Các toán tử phổ biến để làm việc với số hoặc ngày vàCác kiểu dữ liệu thời gian bao gồm: bằng, lớn hơn, nhỏ hơn,không bằng, lớn hơn hoặc bằng và nhỏ hơn hoặc bằng.Giả sử bạn muốn tìm những lần đăng nhập được thực hiện sau 6 giờ chiều.Vì đã quá giờ làm việc bình thường nênbạn muốn tìm kiếm những mẫu hình đáng ngờ.Bạn có thể xác định những lần thử này bằng cách sử dụng toán tử lớn hơn trong bộ lọc của mình.Chúng ta sẽ bắt đầu viết truy vấn của mình bằng SQL.Chúng tôi bắt đầu bằng cách chỉ ra rằng chúng tôi muốn chọn tất cả các cột TỪbảng log\_in\_attempts.Sau đó, chúng tôi sẽ thêm bộ lọc của mình với WHERE.

|  |
| --- |
| Our condition indicates that the value in the time column must be greater than, or for dates and times, later than '18:00', which is how 6 pm is written in SQL. Let's run this and examine the output. Perfect! Now we have a list of log-in attempts made after 6 pm. |

Điều kiện của chúng tôi chỉ ra rằng giá trị trong cột thời gian phải lớn hơn hoặcđối với ngày và giờ, muộn hơn '18:00', đó là cách viết 6 giờ chiều trong SQL.Hãy chạy cái này và kiểm tra đầu ra.Hoàn hảo! Bây giờ chúng tôi có danh sách các lần đăng nhập được thực hiện sau 6 giờ chiều.

|  |
| --- |
| We can also filter for numbers and dates by using the BETWEEN operator. BETWEEN is an operator that filters for numbers or dates within a range. An example of this would be when looking for all patches installed within a certain range. Let's do this! Let's find all the patches installed between March 1st, 2021 and September 1st, 2021. In our query, we start with selecting all records FROM the machines table. |

Chúng ta cũng có thể lọc số và ngày bằng cách sử dụng toán tử GIỮA.GIỮA là toán tử lọc số hoặc ngày trong một phạm vi.Một ví dụ về điều này là khi tìm kiếmtất cả các bản vá được cài đặt trong một phạm vi nhất định.Làm thôi nào! Hãy tìm tất cả các bản vá được cài đặt từ ngày 1 tháng 3,2021 và ngày 1 tháng 9 năm 2021.Trong truy vấn của chúng tôi, chúng tôi bắt đầu bằng việc chọn tất cả các bản ghi TỪ bảng máy.

|  |
| --- |
| And we add the BETWEEN operator in the WHERE statement. |

Và chúng ta thêm toán tử BETWEEN vào câu lệnh WHERE.

|  |
| --- |
| Let's break down the statement. First, after WHERE, we indicate which column to filter, in our case, OS\_patch\_date. Next, comes our operator BETWEEN. We then add the beginning of our range, type AND, then finish by adding the end of our range and a semicolon. Now, let's run this and explore the output. And now we have a list of all machines patched between those two dates! |

Hãy chia nhỏ tuyên bố.Đầu tiên, sau WHERE, chúng tôi chỉ ra cột nào cần lọc,trong trường hợp của chúng tôi, OS\_patch\_date.Tiếp theo, đến toán tử GIỮA của chúng tôi.Sau đó, chúng tôi thêm phần đầu của phạm vi, nhập AND,sau đó kết thúc bằng cách thêm phần cuối của phạm vi của chúng tôi và dấu chấm phẩy.Bây giờ, hãy chạy cái này và khám phá kết quả.Và bây giờ chúng ta có danh sách tất cả các máy được vá giữa hai ngày đó!

|  |
| --- |
| Before we wrap up, an important thing to note is that when we filter for strings, dates, and times, we use quotation marks to specify what we're looking for. However, for numbers, we don't use quotation marks. With this new knowledge, you're now ready to work on all sorts of interesting filters for numbers and dates. In the next video, we'll be able to expand our filtering even further by using multiple conditions in one query. |

Trước khi kết thúc, điều quan trọng cần lưu ý là khi chúng tôi lọc chuỗi,ngày và giờ, chúng tôi sử dụng dấu ngoặc kép để chỉ rõ nội dung chúng tôi đang tìm kiếm.Tuy nhiên, đối với các con số, chúng ta không sử dụng dấu ngoặc kép.Với kiến ​​thức mới này,bây giờ bạn đã sẵn sàng làm việc với tất cả các loại bộ lọc thú vị về số và ngày tháng.Trong video tiếp theo, chúng tôi sẽ có thể mở rộng tính năng lọc hơn nữa bằng cáchsử dụng nhiều điều kiện trong một truy vấn.

***3.2. Operators for filtering dates and numbers – Toán tử lọc ngày và số***

|  |
| --- |
| **Operators for filtering dates and numbers** |

**Toán tử lọc ngày và số**

|  |
| --- |
| Previously, you examined operators like less than (**<**) or greater than (**>**) and explored how they can be used in filtering numeric and date and time data types. This reading summarizes what you learned and provides new examples of using operators in filters. |

Trước đây, bạn đã kiểm tra các toán tử như nhỏ hơn ( **<** ) hoặc lớn hơn ( **>** ) và khám phá cách chúng có thể được sử dụng trong việc lọc các kiểu dữ liệu số và ngày và giờ. Bài đọc này tóm tắt những gì bạn đã học và cung cấp các ví dụ mới về cách sử dụng toán tử trong bộ lọc.

|  |
| --- |
| **Numbers, dates, and times in cybersecurity** |

**Số, ngày và giờ trong an ninh mạng**

|  |
| --- |
| Security analysts work with more than just **string data**, or data consisting of an ordered sequence of characters. |

Các nhà phân tích bảo mật làm việc không chỉ với **dữ liệu chuỗi** hoặc dữ liệu bao gồm một chuỗi ký tự được sắp xếp.

|  |
| --- |
| They also frequently work with **numeric data**, or data consisting of numbers. A few examples of numeric data that you might encounter in your work as a security analyst include: |

Họ cũng thường xuyên làm việc với **dữ liệu số** hoặc dữ liệu bao gồm các con số. Một số ví dụ về dữ liệu số mà bạn có thể gặp trong công việc của mình với tư cách là nhà phân tích bảo mật bao gồm:

|  |
| --- |
| * the number of login attempts * the count of a specific type of log entry * the volume of data being sent from a source * the volume of data being sent to a destination |

* số lần đăng nhập
* số lượng của một loại mục nhật ký cụ thể
* khối lượng dữ liệu được gửi từ một nguồn
* khối lượng dữ liệu được gửi đến đích

|  |
| --- |
| You'll also encounter **date and time data**, or data representing a date and/or time. As a first example, logs will generally timestamp every record. Other time and date data might include: |

Bạn cũng sẽ gặp **dữ liệu ngày và giờ** hoặc dữ liệu biểu thị ngày và/hoặc giờ. Ví dụ đầu tiên, nhật ký thường sẽ đánh dấu thời gian cho mỗi bản ghi. Dữ liệu ngày và giờ khác có thể bao gồm:

|  |
| --- |
| * login dates * login times * dates for patches * the duration of a connection |

* ngày đăng nhập
* lần đăng nhập
* ngày cho các bản vá lỗi
* thời lượng kết nối

|  |
| --- |
| **Comparison operators** |

**Toán tử so sánh**

|  |
| --- |
| In SQL, filtering numeric and date and time data often involves operators. You can use the following operators in your filters to make sure you return only the rows you need: |

Trong SQL, việc lọc dữ liệu số, ngày và giờ thường liên quan đến các toán tử. Bạn có thể sử dụng các toán tử sau trong bộ lọc của mình để đảm bảo chỉ trả về những hàng bạn cần:

|  |  |
| --- | --- |
| **operator** | **use** |
| **<** | less than |
| **>** | greater than |
| **=** | equal to |
| **<=** | less than or equal to |
| **>=** | greater than or equal to |
| **<>** | not equal to |

|  |  |
| --- | --- |
| **Toán tử** | **sử dụng** |
| **<** | ít hơn |
| **>** | lớn hơn |
| **=** | tương đương với |
| **<=** | ít hơn hoặc bằng |
| **>=** | lớn hơn hoặc bằng |
| **<>** | không bằng |

|  |
| --- |
| **Note:** You can also use **!=** as an alternative operator for not equal to. |

**Lưu ý:** Bạn cũng có thể sử dụng **!=** làm toán tử thay thế cho không bằng.

|  |
| --- |
| **Incorporating operators into filters** |

**Kết hợp các toán tử vào bộ lọc**

|  |
| --- |
| These comparison operators are used in the **WHERE** clause at the end of a query. The following query uses the **>** operator to filter the **birthdate** column. You can run this query to explore its output:  SELECT firstname, lastname, birthdate  FROM employees  WHERE birthdate > '1970-01-01'; |

Các toán tử so sánh này được sử dụng trong mệnh đề **WHERE** ở cuối truy vấn. Truy vấn sau đây sử dụng toán tử **>** để lọc cột **ngày sinh** . Bạn có thể chạy truy vấn này để khám phá đầu ra của nó:

SELECT firstname, lastname, birthdate

FROM employees

WHERE birthdate > '1970-01-01';

|  |
| --- |
| This query returns the first and last names of employees born after, but not on, **'1970-01-01'** (or January 1, 1970). If you were to use the **>=** operator instead, the results would also include results on exactly **'1970-01-01'**. |

Truy vấn này trả về họ và tên của nhân viên sinh sau, nhưng không phải vào **ngày '1970-01-01'** (hoặc ngày 1 tháng 1 năm 1970). Thay vào đó, nếu bạn sử dụng toán tử **>=** thì kết quả cũng sẽ bao gồm kết quả chính xác là **'1970-01-01'** .

|  |
| --- |
| In other words, the **>** operator is exclusive and the **>=** operator is inclusive.  An **exclusive operator** is an operator that does not include the value of comparison.An **inclusive operator** is an operator that includes the value of comparison. |

Nói cách khác, toán tử **>** là độc quyền và toán tử **>=** là bao gồm. Toán **tử độc quyền** là toán tử không chứa giá trị so sánh. Toán **tử bao gồm** là toán tử bao gồm giá trị so sánh.

|  |
| --- |
| **BETWEEN** |

**BETWEEN**

|  |
| --- |
| Another operator used for numeric data as well as date and time data is the **BETWEEN** operator. **BETWEEN** filters for numbers or dates within a range. For example, if you want to find the first and last names of all employees hired between January 1, 2002 and January 1, 2003, you can use the **BETWEEN** operator as follows:  SELECT firstname, lastname, hiredate  FROM employees  WHERE hiredate BETWEEN '2002-01-01' AND '2003-01-01'; |

Một toán tử khác được sử dụng cho dữ liệu số cũng như dữ liệu ngày và giờ là toán tử **GIỮA** . **GIỮA** các bộ lọc cho số hoặc ngày trong một phạm vi. Ví dụ: nếu bạn muốn tìm họ và tên của tất cả nhân viên được thuê từ ngày 1 tháng 1 năm 2002 đến ngày 1 tháng 1 năm 2003, bạn có thể sử dụng toán tử **BETWEEN** như sau:

SELECT firstname, lastname, hiredate

FROM employees

WHERE hiredate BETWEEN '2002-01-01' AND '2003-01-01';

|  |
| --- |
| **Note:** The **BETWEEN** operator is inclusive. This means records with a **hiredate** of January 1, 2002 or January 1, 2003 are included in the results of the previous query. |

**Lưu ý:** Toán tử **BETWEEN** mang tính bao gồm. Điều này có nghĩa là các bản ghi có **ngày được thuê** là ngày 1 tháng 1 năm 2002 hoặc ngày 1 tháng 1 năm 2003 sẽ được đưa vào kết quả của truy vấn trước đó.

|  |
| --- |
| **Key takeaways** |

**Bài học chính**

|  |
| --- |
| Operators are important when filtering numeric and date and time data. These include exclusive operators such as **<** and inclusive operators such as  **<=**. The **BETWEEN** operator, another inclusive operator, helps you return the data you need within a range. |

Các toán tử rất quan trọng khi lọc dữ liệu số và ngày và giờ. Chúng bao gồm các toán tử độc quyền như **<** và các toán tử bao hàm như  **<=** . Toán tử **BETWEEN** , một toán tử bao gồm khác, giúp bạn trả về dữ liệu bạn cần trong một phạm vi.

***3.3. Activity: Apply more filters in SQL – Hoạt động: Áp dụng thêm bộ lọc trong SQL***

***3.4. Optional Exemplar: Apply more filters in SQL – Mẫu tùy chọn: Áp dụng nhiều bộ lọc hơn trong SQL***

***3.5. Filters with AND, OR, and NOT – Bộ lọc có AND, OR và NOT***

|  |
| --- |
| In the previous lesson, we learned about even more ways to filter queries in SQL to work with some typical security analyst tasks. However, when working with real security questions, we often have to filter for multiple conditions. Vulnerabilities, for instance, might depend on more than one factor. For example, a security vulnerability might be related to machines using a specific email client on a specific operating system. So, to find the possible vulnerabilities, we need to find machines using both the email client and the operating system. |

Ở bài học trước,chúng tôi đã tìm hiểu về nhiều cách hơn nữa để lọc truy vấn trongSQL để làm việc với một số nhiệm vụ phân tích bảo mật điển hình.Tuy nhiên, khi làm việc với các câu hỏi bảo mật thực sự,chúng ta thường phải lọc nhiều điều kiện.Ví dụ, các lỗ hổngcó thể phụ thuộc vào nhiều hơn một yếu tố.Ví dụ, mộtlỗ hổng bảo mật có thể liên quan đếnmáy sử dụng ứng dụng email cụ thểtrên một hệ điều hành cụ thể.Vì vậy, để tìm ra những lỗ hổng có thể xảy ra,chúng ta cần tìm máy sử dụngcả ứng dụng email và hệ điều hành.

|  |
| --- |
| To make a query with multiple conditions that must be met, we use the AND operator between two separate conditions. AND is an operator that specifies that both conditions must be met simultaneously. Bringing this back to our fruit and vegetable analogy, this is the same as asking someone to select apples from the big box where the apples are large and fresh. This means our results won't include any small apples even if they're fresh, or any rotten apples even if they're large. They'll only include large fresh apples. The apples must meet both conditions. |

Để thực hiện một truy vấn vớiphải đáp ứng nhiều điều kiện,chúng tôi sử dụng toán tử AND giữa hai điều kiện riêng biệt.AND là toán tử chỉ định rằngcả hai điều kiện phải được đáp ứng đồng thời.Đưa điều này trở lại với sự tương tự về trái cây và rau quả của chúng ta,điều này cũng giống như yêu cầu ai đó chọn táo từcái hộp lớn đựng những quả táo to và tươi.Điều này có nghĩa là kết quả của chúng tôi sẽ không bao gồm bất kỳ quả táo nhỏ nàongay cả khi chúng còn tươi, hoặcbất kỳ quả táo thối nào ngay cả khi chúng lớn.Chúng sẽ chỉ bao gồm những quả táo tươi lớn.Những quả táo phải đáp ứng cả hai điều kiện.

|  |
| --- |
| Going back to our database, the machines table lists all operating systems and email clients. We want a list of machines running Operating System 1 and a list of machines using Email Client 1. We'll use the left and right circles in the Venn diagram to represent these groups. We need SQL to select the machines that have both OS 1 and Email Client 1. The filled-in area at the intersection of these circles represents this condition. Let's take this and implement it in SQL. |

Quay trở lại cơ sở dữ liệu của chúng tôi,danh sách bảng máy móctất cả các hệ điều hành và ứng dụng email.Chúng tôi muốn có danh sách các máy chạy Hệ điều hành1 và danh sách các máy sử dụng Email Client 1.Chúng ta sẽ sử dụng vòng tròn bên trái và bên phải trongsơ đồ Venn để thể hiện các nhóm này.Chúng tôi cần SQL để chọn các máycó cả OS 1 và Email Client 1.Khu vực lấp đầy tại ngã tưnhững vòng tròn này đại diện cho tình trạng này.Hãy lấy cái này và triển khai nó trong SQL.

|  |
| --- |
| First, we're going to start by building the first lines of the query, telling SQL to SELECT\* all columns FROM the machines table. Then, we'll add the WHERE clause. |

Đầu tiên, chúng ta sẽ bắt đầu bằngxây dựng những dòng đầu tiên của truy vấn,yêu cầu SQL CHỌN\*tất cả các cột TỪ bảng máy.Sau đó, chúng ta sẽ thêm mệnh đề WHERE.

|  |
| --- |
| Let's examine this more closely. First, we indicate the first condition that it must meet, that the operating system column has a value of '0S 1' |

Hãy xem xét điều này chặt chẽ hơn.Đầu tiên, chúng tôi chỉ rađiều kiện đầu tiên nó phải đáp ứng,cột hệ điều hành có giá trị '0S 1'

|  |
| --- |
| Then, we use AND to join this to another condition. And finally, we enter the other condition, in this case that the email client column should have a value of 'Email Client 1' |

Sau đó, chúng ta sử dụng AND để nối điều kiện này với điều kiện khác.Và cuối cùng, chúng ta nhập điều kiện khác,trong trường hợp nàycột ứng dụng email nêncó giá trị 'Email Client 1'

|  |
| --- |
| And this is how you use the AND operator in SQL! Let's run this to get the query results. Perfect! All the results match both our conditions! |

Và đây là cách bạn sử dụng toán tử AND trong SQL!Hãy chạy cái này để có kết quả truy vấn.Hoàn hảo! Tất cả các kết quả phù hợp với cả hai điều kiện của chúng tôi!

|  |
| --- |
| Let's keep going and explore more ways to combine different conditions by working with the OR operator. The OR operator is an operator that specifies that either condition can be met. In a Venn diagram, let's say each circle represents a condition. When they are joined with OR, SQL would select all rows that satisfy one of the conditions. And it's also ok if it meets both conditions. |

Hãy tiếp tục và khám phá thêm nhiều cách kết hợpcác điều kiện khác nhau bằng cách làm việc với toán tử OR.Toán tử OR là toán tửchỉ định rằng một trong hai điều kiện có thể được đáp ứng.Trong sơ đồ Venn,giả sử mỗi vòng tròn đại diện cho một điều kiện.Khi chúng được nối với OR,SQL sẽ chọn tất cả các hàngthỏa mãn một trong các điều kiện.Và cũng không sao nếu đáp ứng được cả hai điều kiện.

|  |
| --- |
| Let's run another query and use the OR operator. Let's say that we wanted the filter to identify machines that have either OS 1 or OS 3 because both types need a patch. We'll type in these conditions. |

Hãy chạy một truy vấn khác và sử dụng toán tử OR.Hãy nói rằng chúng tôi muốnbộ lọc để xác định các máy cóOS 1 hoặc OS 3 vì cả hai loại đều cần một bản vá.Chúng ta sẽ gõ vào những điều kiện này.

|  |
| --- |
| Let's examine this more closely. After WHERE, our first condition indicates we want to filter, so that the query selects machines with 'OS 1' We use the OR operator because we also want to find records that match another condition. This additional condition is placed after OR and indicates to also select machines running 'OS 3' Executing the query, our results now include records that have a value of either OS 1 or OS 3 in the operating system column. Good job, we're running some complex queries. |

Hãy xem xét điều này chặt chẽ hơn.Sau WHERE, điều kiện đầu tiên cho biết chúng ta muốnbộ lọc để truy vấn chọn các máy có 'OS 1'Chúng tôi sử dụng toán tử OR vì chúng tôi cũng muốnđể tìm các bản ghi phù hợp với điều kiện khác.Điều kiện bổ sung này được đặt sau OR vàbiểu thị cũng chọn các máy chạy 'OS 3'Thực hiện truy vấn,kết quả của chúng tôi hiện bao gồm các bản ghi có giá trị làOS 1 hoặc OS 3 trong cột hệ điều hành.Làm tốt lắm, chúng tôi đang chạy một số truy vấn phức tạp.

|  |
| --- |
| The last operator we're going to go into is the NOT operator. NOT negates a condition. In a diagram, we can show this by selecting every entry that does not match our condition. The condition is represented by the circle. The filled-in portion outside the circle represents what gets returned. This is all data that does not match the condition. For example, when picking out fruit, you can be looking for any fruit that is not an apple. That is a lot more efficient than telling your friend you want a banana or an orange or a lime, and so on. |

Toán tử cuối cùng chúng ta sẽ sử dụngvào là toán tử NOT.NOT phủ nhận một điều kiện.Trong một sơ đồ,chúng ta có thể hiển thị điều này bằng cách chọnmọi mục không phù hợp với điều kiện của chúng tôi.Điều kiện được thể hiện bằng vòng tròn.Phần điền bên ngoàivòng tròn đại diện cho những gì được trả lại.Đây là tất cả dữ liệu không phù hợp với điều kiện.Ví dụ, khi hái trái cây,bạn có thể tìm kiếm bất kỳ loại trái cây nào không phải là táo.Điều đó hiệu quả hơn rất nhiềuhơn là nói với bạn của bạn rằng bạn muốnmột quả chuối hoặc một quả cam hoặc một quả chanh, v.v.

|  |
| --- |
| Suppose you wanted to update all of the devices in your company except for the ones using OS 3. Bringing this into SQL, we can write this query. |

Giả sử bạn muốn cập nhậttất cả các thiết bị trongcông ty của bạn ngoại trừ những công ty sử dụng OS 3.Đưa cái này vào SQL,chúng ta có thể viết truy vấn này.

|  |
| --- |
| We place NOT after WHERE and before the condition of the filter. Executing these queries gives us the list of all the machines that aren't running OS 3, and now we know which machines to update. |

Chúng tôi đặt KHÔNG sauWHERE và trước tình trạng của bộ lọc.Việc thực hiện các truy vấn này sẽ cho chúng ta danh sáchcủa tất cả các máy không chạy OS 3 vàbây giờ chúng tôi biết máy nào cần cập nhật.

|  |
| --- |
| That was a lot of new content that we just looked into, but you're learning more and more SQL that you can use on your journey to become an analyst! In the next video, we'll be learning how to combine and join two tables together to expand the kinds of queries we can run. I'll meet you there! |

Đó là rất nhiều nội dung mới mà chúng tôi vừa xem xét,nhưng bạn đang học ngày càng nhiều SQL hơn mà bạncó thể sử dụng trên hành trình trở thành nhà phân tích của bạn!Trong video tiếp theo,chúng ta sẽ học cách kết hợp vànối hai bảng lại với nhau đểmở rộng các loại truy vấn chúng tôi có thể chạy. Tôi sẽ gặp bạn ở đó!

***3.6. More on filters with AND, OR, and NOT – Thông tin thêm về các bộ lọc có AND, OR và NOT***

|  |
| --- |
| **More on filters with AND, OR, and NOT** |

**Thông tin thêm về các bộ lọc có AND, OR và NOT**

|  |
| --- |
| Previously, you explored how to add filters containing the **AND**, **OR**, and **NOT** operators to your SQL queries. In this reading, you'll continue to explore how these operators can help you refine your queries. |

Trước đây, bạn đã khám phá cách thêm các bộ lọc chứa các toán tử **AND** , **OR** và **NOT** vào các truy vấn SQL của mình. Trong bài đọc này, bạn sẽ tiếp tục khám phá cách các toán tử này có thể giúp bạn tinh chỉnh các truy vấn của mình.

|  |
| --- |
| **Logical operators** |

**Toán tử logic**

|  |
| --- |
| **AND**, **OR**, and **NOT** allow you to filter your queries to return the specific information that will help you in your work as a security analyst. They are all considered logical operators. |

**VÀ** , **HOẶC** và **KHÔNG** cho phép bạn lọc các truy vấn của mình để trả về thông tin cụ thể sẽ giúp bạn trong công việc của mình với tư cách là nhà phân tích bảo mật. Chúng đều được coi là toán tử logic.

|  |
| --- |
| **AND** |

**AND**

|  |
| --- |
| First, **AND** is used to filter on two conditions. **AND** specifies that both conditions must be met simultaneously. |

Đầu tiên, **AND** được sử dụng để lọc theo hai điều kiện. **AND** chỉ định rằng cả hai điều kiện phải được đáp ứng đồng thời.

|  |
| --- |
| As an example, a cybersecurity concern might affect only those customer accounts that meet both the condition of being handled by a support representative with an ID of 5 and the condition of being located in the USA. To find the names and emails of those specific customers, you should place the two conditions on either side of the **AND** operator in the **WHERE** clause:  SELECT firstname, lastname, email, country, supportrepid  FROM customers  WHERE supportrepid = 5 AND country = 'USA'; |

Ví dụ: mối lo ngại về an ninh mạng có thể chỉ ảnh hưởng đến những tài khoản khách hàng đáp ứng cả điều kiện được xử lý bởi đại diện hỗ trợ có ID là 5 và điều kiện phải ở Hoa Kỳ. Để tìm tên và email của những khách hàng cụ thể đó, bạn nên đặt 2 điều kiện ở hai bên toán tử **AND** trong mệnh đề **WHERE** :

SELECT firstname, lastname, email, country, supportrepid

FROM customers

WHERE supportrepid = 5 AND country = 'USA';

|  |
| --- |
| Running this query returns four rows of information about the customers. You can use this information to contact them about the security concern. |

Việc chạy truy vấn này trả về bốn hàng thông tin về khách hàng. Bạn có thể sử dụng thông tin này để liên hệ với họ về vấn đề bảo mật.

|  |
| --- |
| **OR** |

**OR**

|  |
| --- |
| The **OR** operator also connects two conditions, but **OR** specifies that either condition can be met. It returns results where the first condition, the second condition, or both are met. |

Toán tử **OR** cũng kết nối hai điều kiện, nhưng **OR** chỉ định rằng một trong hai điều kiện có thể được đáp ứng. Nó trả về kết quả khi điều kiện đầu tiên, điều kiện thứ hai hoặc cả hai đều được đáp ứng.

|  |
| --- |
| For example, if you are responsible for finding all customers who are either in the USA or Canada so that you can communicate information about a security update, you can use an **OR** operator to find all the needed records. As the following query demonstrates, you should place the two conditions on either side of the **OR** operator in the **WHERE** clause:  SELECT firstname, lastname, email, country  FROM customers  WHERE country = 'Canada' OR country = 'USA'; |

Ví dụ: nếu bạn chịu trách nhiệm tìm kiếm tất cả khách hàng ở Hoa Kỳ hoặc Canada để có thể truyền đạt thông tin về bản cập nhật bảo mật, bạn có thể sử dụng toán tử **OR** để tìm tất cả các bản ghi cần thiết. Như truy vấn sau đây minh họa, bạn nên đặt hai điều kiện ở hai bên của toán tử **OR** trong mệnh đề **WHERE** :

SELECT firstname, lastname, email, country

FROM customers

WHERE country = 'Canada' OR country = 'USA';

|  |
| --- |
| The query returns all customers in either the US or Canada. |

Truy vấn trả về tất cả khách hàng ở Hoa Kỳ hoặc Canada.

|  |
| --- |
| **Note:** Even if both conditions are based on the same column, you need to write out both full conditions. For instance, the query in the previous example contains the filter **WHERE country = 'Canada' OR country = 'USA'**. |

**Lưu ý:** Ngay cả khi cả hai điều kiện đều dựa trên cùng một cột, bạn vẫn cần phải viết ra cả hai điều kiện đầy đủ. Ví dụ: truy vấn trong ví dụ trước chứa bộ lọc **WHERE country = 'Canada' OR country = 'USA'** .

|  |
| --- |
| **NOT** |

**NOT**

|  |
| --- |
| Unlike the previous two operators, the **NOT** operator only works on a single condition, and not on multiple ones. The **NOT** operator negates a condition. This means that SQL returns all records that don’t match the condition specified in the query. |

Không giống như hai toán tử trước, toán tử **NOT** chỉ hoạt động trên một điều kiện duy nhất chứ không hoạt động trên nhiều điều kiện. Toán tử **NOT** phủ nhận một điều kiện. Điều này có nghĩa là SQL trả về tất cả các bản ghi không khớp với điều kiện được chỉ định trong truy vấn.

|  |
| --- |
| For example, if a cybersecurity issue doesn't affect customers in the USA but might affect those in other countries, you can return all customers who are not in the USA. This would be more efficient than creating individual conditions for all of the other countries. To use the **NOT** operator for this task, write the following query and place **NOT** directly after **WHERE**:  SELECT firstname, lastname, email, country  FROM customers  WHERE NOT country = 'USA'; |

Ví dụ: nếu sự cố an ninh mạng không ảnh hưởng đến khách hàng ở Hoa Kỳ nhưng có thể ảnh hưởng đến khách hàng ở các quốc gia khác, bạn có thể trả lại tất cả khách hàng không ở Hoa Kỳ. Điều này sẽ hiệu quả hơn việc tạo điều kiện riêng cho tất cả các quốc gia khác. Để sử dụng toán tử **NOT** cho tác vụ này, hãy viết truy vấn sau và đặt **NOT** ngay sau **WHERE** :

SELECT firstname, lastname, email, country

FROM customers

WHERE NOT country = 'USA';

|  |
| --- |
| SQL returns every entry where the customers are not from the USA. |

SQL trả về mọi mục nhập mà khách hàng không đến từ Hoa Kỳ.

|  |
| --- |
| **Pro tip:** Another way of finding values that are not equal to a certain value is by using the **<>** operator or the **!=** operator. For example, **WHERE country <> 'USA'** and **WHERE country != 'USA'** are the same filters as **WHERE NOT country = 'USA'**. |

**Mẹo chuyên nghiệp:** Một cách khác để tìm các giá trị không bằng một giá trị nhất định là sử dụng toán tử **<>** hoặc toán tử **!=** . Ví dụ: **WHERE country <> 'USA'** và **WHERE country != 'USA'** là các bộ lọc giống nhau như **WHERE NOT country = 'USA'** .

|  |
| --- |
| **Combining logical operators** |

**Kết hợp các toán tử logic**

|  |
| --- |
| Logical operators can be combined in filters. For example, if you know that both the USA and Canada are not affected by a cybersecurity issue, you can combine operators to return customers in all countries besides these two. In the following query, **NOT** is placed before the first condition, it's joined to a second condition with **AND**, and then **NOT** is also placed before that second condition. You can run it to explore what it returns:  SELECT firstname, lastname, email, country  FROM customers  WHERE NOT country = 'Canada' AND NOT country = 'USA'; |

Các toán tử logic có thể được kết hợp trong các bộ lọc. Ví dụ: nếu bạn biết rằng cả Hoa Kỳ và Canada đều không bị ảnh hưởng bởi vấn đề an ninh mạng, bạn có thể kết hợp các nhà khai thác để trả lại khách hàng ở tất cả các quốc gia ngoài hai quốc gia này. Trong truy vấn sau, **NOT** được đặt trước điều kiện đầu tiên, nó được nối với điều kiện thứ hai bằng **AND** và sau đó **NOT** cũng được đặt trước điều kiện thứ hai đó. Bạn có thể chạy nó để khám phá những gì nó trả về:

SELECT firstname, lastname, email, country

FROM customers

WHERE NOT country = 'Canada' AND NOT country = 'USA';

|  |
| --- |
| **Key takeaways** |

**Bài học chính**

|  |
| --- |
| Logical operators allow you to create more specific filters that target the security-related information you need. The **AND** operator requires two conditions to be true simultaneously, the **OR** operator requires either one or both conditions to be true, and the **NOT** operator negates a condition. Logical operators can be combined together to create even more specific queries. |

Toán tử logic cho phép bạn tạo các bộ lọc cụ thể hơn nhằm vào thông tin liên quan đến bảo mật mà bạn cần. Toán tử **AND** yêu cầu hai điều kiện phải đồng thời đúng, toán tử **OR** yêu cầu một hoặc cả hai điều kiện đều đúng và toán tử **NOT** phủ định một điều kiện. Các toán tử logic có thể được kết hợp với nhau để tạo ra các truy vấn cụ thể hơn nữa.

***3.7. Activity: Filter with AND, OR, and NOT – Hoạt động: Lọc bằng AND, OR và NOT***

***3.8. Optional Exemplar: Filter with AND, OR, and NOT – Mẫu tùy chọn: Lọc bằng AND, OR và NOT***

***3.9. Portfolio Activity: Apply filters to SQL queries – Hoạt động danh mục đầu tư: Áp dụng bộ lọc cho truy vấn SQL***

|  |
| --- |
| **Activity Overview**  In this activity, you will create a new portfolio document to demonstrate your experience using SQL. You can add this document to your cybersecurity portfolio, which you can share with prospective employers or recruiters. To review the importance of building a professional portfolio and options for creating your portfolio, read [Create a cybersecurity portfolio](https://www.coursera.org/learn/linux-and-sql/resources/wDFrc).  To create your portfolio document, you will review a scenario and follow a series of steps. This scenario is connected to [the lab](https://www.coursera.org/learn/linux-and-sql/ungradedLti/wVReS/activity-filter-with-and-or-and-not) you have just completed about using the AND, OR, and NOT operators in SQL to filter for information. You will explain the queries you performed in that lab, and this will help you prepare for future job interviews and other steps in the hiring process.  Be sure to complete this activity and answer the questions that follow before moving on. The next course item will provide you with a completed exemplar to compare to your own work. |

**Tổng quan về hoạt động**

Trong hoạt động này, bạn sẽ tạo một tài liệu danh mục đầu tư mới để thể hiện trải nghiệm sử dụng SQL của mình. Bạn có thể thêm tài liệu này vào danh mục an ninh mạng của mình để có thể chia sẻ với các nhà tuyển dụng hoặc nhà tuyển dụng tiềm năng. Để xem lại tầm quan trọng của việc xây dựng danh mục đầu tư chuyên nghiệp và các lựa chọn để tạo danh mục đầu tư của bạn, hãy đọc[Tạo danh mục đầu tư an ninh mạng](https://www.coursera.org/learn/linux-and-sql/resources/wDFrc).

Để tạo tài liệu portfolio, bạn sẽ xem xét một kịch bản và làm theo một loạt các bước. Kịch bản này được kết nối với[phòng thí nghiệm](https://www.coursera.org/learn/linux-and-sql/ungradedLti/wVReS/activity-filter-with-and-or-and-not)bạn vừa hoàn tất cách sử dụng các toán tử AND, OR và NOT trong SQL để lọc thông tin. Bạn sẽ giải thích các truy vấn bạn đã thực hiện trong phòng thí nghiệm đó và điều này sẽ giúp bạn chuẩn bị cho các cuộc phỏng vấn xin việc trong tương lai cũng như các bước khác trong quy trình tuyển dụng.

Hãy chắc chắn hoàn thành hoạt động này và trả lời các câu hỏi tiếp theo trước khi tiếp tục. Mục khóa học tiếp theo sẽ cung cấp cho bạn một ví dụ hoàn chỉnh để so sánh với công việc của chính bạn.

|  |
| --- |
| **Scenario**  Review the scenario below. Then complete the step-by-step instructions.  You are a security professional at a large organization. Part of your job is to investigate security issues to help keep the system secure. You recently discovered some potential security issues that involve login attempts and employee machines.  Your task is to examine the organization’s data in their **employees** and **log\_in\_attempts** tables. You’ll need to use SQL filters to retrieve records from different datasets and investigate the potential security issues.  **Note:** This scenario involves the same queries as the ones the [Filter with AND, OR, and NOT](https://www.coursera.org/learn/linux-and-sql/ungradedLti/wVReS/activity-filter-with-and-or-and-not) lab. You can revisit the lab to get screenshots to include in your portfolio document. If you choose, it's also possible to complete this activity without revisiting the lab by typing your queries in the template. |

**Kịch bản**

Xem lại kịch bản dưới đây. Sau đó hoàn thành các hướng dẫn từng bước.

Bạn là chuyên gia bảo mật tại một tổ chức lớn. Một phần công việc của bạn là điều tra các vấn đề bảo mật để giúp giữ an toàn cho hệ thống. Gần đây bạn đã phát hiện ra một số vấn đề bảo mật tiềm ẩn liên quan đến nỗ lực đăng nhập và máy của nhân viên.

Nhiệm vụ của bạn là kiểm tra dữ liệu của tổ chức trong bảng **nhân viên** và bảng **log\_in\_attempts** . Bạn sẽ cần sử dụng bộ lọc SQL để truy xuất bản ghi từ các bộ dữ liệu khác nhau và điều tra các vấn đề bảo mật tiềm ẩn.

**Lưu ý:** Kịch bản này bao gồm các truy vấn tương tự như các truy vấn[Lọc bằng AND, OR và NOT](https://www.coursera.org/learn/linux-and-sql/ungradedLti/wVReS/activity-filter-with-and-or-and-not)phòng thí nghiệm. Bạn có thể quay lại phòng thí nghiệm để lấy ảnh chụp màn hình để đưa vào tài liệu danh mục đầu tư của mình. Nếu bạn chọn, bạn cũng có thể hoàn thành hoạt động này mà không cần truy cập lại phòng thí nghiệm bằng cách nhập truy vấn của mình vào mẫu.

|  |
| --- |
| **Step-By-Step Instructions**  Follow the instructions to complete each step of the activity. Then, answer the 8 questions at the end of the activity before going to the next course item to compare your work to a completed exemplar. |

**Hướng dẫn từng bước một**

Làm theo hướng dẫn để hoàn thành từng bước của hoạt động. Sau đó, trả lời 8 câu hỏi ở cuối hoạt động trước khi chuyển sang mục khóa học tiếp theo để so sánh bài làm của bạn với một bài mẫu đã hoàn thành.

|  |
| --- |
| **Step 1: Access the template**  To use the template for this course item, click the following link and select *Use Template*. (In this step, you will just open the template. More instructions for how to use the template will be included in later steps.)  Link to template: [Apply filters to SQL queries](https://docs.google.com/document/d/1QLYj8sdBCYtcZv3ZF1RlcPft8Uh-fscWSZsiT_6QVy0/template/preview?usp=sharing) |

|  |
| --- |
| **Step 2: Access supporting materials**  The following supporting materials will help you complete this activity. Keep them open as you proceed to the next steps.  To use the supporting materials for this course item, click the links.  The **Instructions for including SQL queries** document provides instructions and best practices for including samples of SQL queries in your portfolio activity.  Link to supporting materials: [Instructions for including SQL queries](https://docs.google.com/document/d/1b06OpDP1RH8iE8phf0h5GRsMPPxoLZ92z86_OtESJp8/template/preview?usp=sharing&resourcekey=0-V4KE_W_sE-p9i3H7dpUppQ)  The **Table formats** document describes how the tables used for this portfolio activity are organized.  Link to supporting material: [Table formats](https://docs.google.com/document/d/10uIJTRVJEL9nM_cXgMTFZNNmxRKAYzjbwMFdjYgO2wQ/template/preview?usp=sharing&resourcekey=0-zYsLZ5L4jmKShdfZ8fccQg)  **Note**:  It is recommended that you use the **Filter with AND, OR, and NOT** lab to complete this portfolio activity. If you’re revisiting the lab, the **Table formats** document is optional. You will also be able to view the tables in the lab. |

**Bước 2: Truy cập tài liệu hỗ trợ**

Các tài liệu hỗ trợ sau đây sẽ giúp bạn hoàn thành hoạt động này. Giữ chúng mở khi bạn tiến hành các bước tiếp theo.

Để sử dụng các tài liệu hỗ trợ cho mục khóa học này, hãy nhấp vào liên kết.

Tài **liệu Hướng dẫn bao gồm truy vấn SQL** cung cấp hướng dẫn và cách thực hành tốt nhất để đưa các mẫu truy vấn SQL vào hoạt động danh mục đầu tư của bạn.

Link các tài liệu hỗ trợ:[Hướng dẫn thêm truy vấn SQL](https://docs.google.com/document/d/1b06OpDP1RH8iE8phf0h5GRsMPPxoLZ92z86_OtESJp8/template/preview?usp=sharing&resourcekey=0-V4KE_W_sE-p9i3H7dpUppQ)

Tài liệu **định dạng bảng** mô tả cách sắp xếp các bảng được sử dụng cho hoạt động danh mục đầu tư này.

Liên kết đến tài liệu hỗ trợ:[Định dạng bảng](https://docs.google.com/document/d/10uIJTRVJEL9nM_cXgMTFZNNmxRKAYzjbwMFdjYgO2wQ/template/preview?usp=sharing&resourcekey=0-zYsLZ5L4jmKShdfZ8fccQg)

**Lưu ý** : Bạn nên sử dụng phòng thí nghiệm **Bộ lọc với AND, OR và NOT** để hoàn thành hoạt động danh mục đầu tư này. Nếu bạn đang xem lại phòng thí nghiệm, tài liệu **Định dạng bảng** là tùy chọn. Bạn cũng sẽ có thể xem các bảng trong phòng thí nghiệm.

|  |
| --- |
| **Step 3: Retrieve after hours failed login attempts**  You recently discovered a potential security incident that occurred after business hours. To investigate this, you need to query the **log\_in\_attempts** table and review after hours login activity. Use filters in SQL to create a query that identifies all failed login attempts that occurred after 18:00. (The time of the login attempt is found in the **login\_time** column. The **success** column contains a value of **0** when a login attempt failed; you can use either a value of **0** or **FALSE** in your query to identify failed login attempts.)  Describe your query and how it works in the **Retrieve after hours failed login attempts** section of the **Apply filters to SQL queries** template.  In the **Filter with AND, OR, and NOT** lab, take a screenshot of the SQL query you used and copy it into the template. Or, type this query directly into the template. |

**Bước 3: Truy xuất sau nhiều giờ đăng nhập không thành công**

Gần đây bạn đã phát hiện ra một sự cố bảo mật tiềm ẩn xảy ra sau giờ làm việc. Để điều tra vấn đề này, bạn cần truy vấn bảng **log\_in\_attempts** và xem lại hoạt động đăng nhập sau giờ làm việc. Sử dụng các bộ lọc trong SQL để tạo truy vấn xác định tất cả các lần đăng nhập không thành công xảy ra sau 18:00. (Thời gian của lần thử đăng nhập được tìm thấy trong cột **login\_time** . Cột **thành công** chứa giá trị **0** khi lần thử đăng nhập không thành công; bạn có thể sử dụng giá trị **0** hoặc **FALSE** trong truy vấn của mình để xác định các lần thử đăng nhập không thành công.)

Mô tả truy vấn của bạn và cách truy vấn hoạt động trong phần **Truy xuất sau nhiều giờ đăng nhập không thành công** của mẫu **Áp dụng bộ lọc cho truy vấn SQL** .

Trong phòng **thí nghiệm Bộ lọc có AND, OR và NOT** , hãy chụp ảnh màn hình truy vấn SQL bạn đã sử dụng và sao chép nó vào mẫu. Hoặc, nhập truy vấn này trực tiếp vào mẫu.

|  |
| --- |
| **Step 4: Retrieve login attempts on specific dates**  A suspicious event occurred on 2022-05-09. To investigate this event, you want to review all login attempts which occurred on this day and the day before. Use filters in SQL to create a query that identifies all login attempts that occurred on 2022-05-09 or 2022-05-08. (The date of the login attempt is found in the **login\_date** column.)  Describe your query and how it works in the **Retrieve login attempts on specific dates** section of the **Apply filters to SQL queries** template.  In the **Filter with AND, OR, and NOT** lab, take a screenshot of the SQL query you used and copy it into the template. Or, type this query directly into the template. |

**Bước 4: Truy xuất các lần đăng nhập vào những ngày cụ thể**

Một sự kiện đáng ngờ đã xảy ra vào ngày 2022-05-09. Để điều tra sự kiện này, bạn muốn xem lại tất cả các lần đăng nhập đã xảy ra vào ngày này và ngày hôm trước. Sử dụng các bộ lọc trong SQL để tạo truy vấn xác định tất cả các lần đăng nhập xảy ra vào ngày 09/05/2022 hoặc 08/05/2022. (Ngày đăng nhập được tìm thấy trong cột **login\_date** .)

Mô tả truy vấn của bạn và cách truy vấn hoạt động trong phần **Truy xuất các lần đăng nhập vào các ngày cụ thể** của mẫu **Áp dụng bộ lọc cho truy vấn SQL** .

Trong phòng **thí nghiệm Bộ lọc có AND, OR và NOT** , hãy chụp ảnh màn hình truy vấn SQL bạn đã sử dụng và sao chép nó vào mẫu. Hoặc, nhập truy vấn này trực tiếp vào mẫu.

|  |
| --- |
| **Step 5: Retrieve login attempts outside of Mexico**  There’s been suspicious activity with login attempts, but the team has determined that this activity didn't originate in Mexico. Now, you need to investigate login attempts that occurred outside of Mexico. Use filters in SQL to create a query that identifies all login attempts that occurred outside of Mexico. (When referring to Mexico, the **country** column contains values of both **MEX** and **MEXICO**, and you need to use the **LIKE** keyword with **%** to make sure your query reflects this.)  Describe your query and how it works in the **Retrieve login attempts outside of Mexico** section of the **Apply filters to SQL queries** template.  In the **Filter with AND, OR, and NOT** lab, take a screenshot of the SQL query you used and copy it into the template. Or, type this query directly into the template. |

**Bước 5: Truy xuất các lần đăng nhập bên ngoài Mexico**

Đã có hoạt động đáng ngờ xảy ra với các lần thử đăng nhập nhưng nhóm đã xác định rằng hoạt động này không bắt nguồn từ Mexico. Bây giờ, bạn cần điều tra các lần đăng nhập xảy ra bên ngoài Mexico. Sử dụng các bộ lọc trong SQL để tạo truy vấn xác định tất cả các lần đăng nhập xảy ra bên ngoài Mexico. (Khi đề cập đến Mexico, cột **quốc gia** chứa các giá trị của cả **MEX** và **MEXICO** và bạn cần sử dụng từ khóa **THÍCH** với **%** để đảm bảo truy vấn của bạn phản ánh điều này.)

Mô tả truy vấn của bạn và cách truy vấn hoạt động trong phần **Truy xuất các lần đăng nhập bên ngoài Mexico** của mẫu **Áp dụng bộ lọc cho truy vấn SQL** .

Trong phòng **thí nghiệm Bộ lọc có AND, OR và NOT** , hãy chụp ảnh màn hình truy vấn SQL bạn đã sử dụng và sao chép nó vào mẫu. Hoặc, nhập truy vấn này trực tiếp vào mẫu.

|  |
| --- |
| **Step 6: Retrieve employees in Marketing**  Your team wants to perform security updates on specific employee machines in the Marketing department. You’re responsible for getting information on these employee machines and will need to query the **employees** table. Use filters in SQL to create a query that identifies all employees in the Marketing department for all offices in the East building.  (The department of the employee is found in the **department** column, which contains values that include **Marketing**. The office is found in the office column. Some examples of values in this column are **East-170**, **East-320**, and **North-434**. You’ll need to use the **LIKE** keyword with **%** to filter for the East building.)  Describe your query and how it works in the **Retrieve employees in Marketing** section of the **Apply filters to SQL queries** template.  In the **Filter with AND, OR, and NOT** lab, take a screenshot of the SQL query you used and copy it into the template. Or, type this query directly into the template. |

**Bước 6: Truy xuất nhân viên Marketing**

Nhóm của bạn muốn thực hiện cập nhật bảo mật trên các máy cụ thể của nhân viên trong bộ phận Tiếp thị. Bạn chịu trách nhiệm lấy thông tin về các máy của nhân viên này và sẽ cần truy vấn bảng **nhân viên** . Sử dụng các bộ lọc trong SQL để tạo truy vấn xác định tất cả nhân viên trong bộ phận Tiếp thị cho tất cả các văn phòng trong tòa nhà phía Đông.

(Bộ phận của nhân viên được tìm thấy trong cột **bộ phận** , chứa các giá trị bao gồm **Tiếp thị** . Văn phòng được tìm thấy trong cột văn phòng. Một số ví dụ về các giá trị trong cột này là **East-170** , **East-320** và **North-434** . Bạn sẽ cần sử dụng từ khóa **THÍCH** với **%** để lọc tòa nhà phía Đông.)

Mô tả truy vấn của bạn và cách truy vấn hoạt động trong phần **Truy xuất nhân viên trong Tiếp thị** của mẫu **Áp dụng bộ lọc cho truy vấn SQL** .

Trong phòng **thí nghiệm Bộ lọc có AND, OR và NOT** , hãy chụp ảnh màn hình truy vấn SQL bạn đã sử dụng và sao chép nó vào mẫu. Hoặc, nhập truy vấn này trực tiếp vào mẫu.

|  |
| --- |
| **Step 7: Retrieve employees in Finance or Sales**  Your team now needs to perform a different security update on machines for employees in the Sales and Finance departments. Use filters in SQL to create a query that identifies all employees in the Sales or Finance departments. (The department of the employee is found in the **department** column, which contains values that include **Sales** and **Finance**.)  Describe your query and how it works in the **Retrieve employees in Finance or Sales** section of the **Apply filters to SQL queries** template.  In the **Filter with AND, OR, and NOT** lab, take a screenshot of the SQL query you used and copy it into the template. Or, type this query directly into the template. |

**Bước 7: Truy xuất nhân viên bộ phận Tài chính hoặc Bán hàng**

Bây giờ, nhóm của bạn cần thực hiện một bản cập nhật bảo mật khác trên máy cho nhân viên trong bộ phận Bán hàng và Tài chính. Sử dụng các bộ lọc trong SQL để tạo truy vấn xác định tất cả nhân viên trong bộ phận Bán hàng hoặc Tài chính. (Bộ phận của nhân viên được tìm thấy trong cột **bộ phận** , chứa các giá trị bao gồm **Bán hàng** và **Tài chính** .)

Mô tả truy vấn của bạn và cách truy vấn hoạt động trong phần **Truy xuất nhân viên trong Tài chính hoặc Bán hàng** của mẫu **Áp dụng bộ lọc cho truy vấn SQL** .

Trong phòng **thí nghiệm Bộ lọc có AND, OR và NOT** , hãy chụp ảnh màn hình truy vấn SQL bạn đã sử dụng và sao chép nó vào mẫu. Hoặc, nhập truy vấn này trực tiếp vào mẫu.

|  |
| --- |
| **Step 8: Retrieve all employees not in IT**  Your team needs to make one more update to employee machines. The employees who are in the Information Technology department already had this update, but employees in all other departments need it. Use filters in SQL to create a query which identifies all employees not in the IT department. (The department of the employee is found in the **department** column, which contains values that include **Information Technology**.)  Describe your query and how it works in the **Retrieve all employees not in IT** section of the **Apply filters to SQL queries** template.  In the **Filter with AND, OR, and NOT** lab, take a screenshot of the SQL query you used and copy it into the template. Or, type this query directly into the template. |

**Bước 8: Truy xuất tất cả nhân viên không thuộc CNTT**

Nhóm của bạn cần thực hiện thêm một bản cập nhật cho máy của nhân viên. Các nhân viên ở bộ phận Công nghệ thông tin đã có bản cập nhật này, nhưng nhân viên ở tất cả các bộ phận khác đều cần nó. Sử dụng các bộ lọc trong SQL để tạo truy vấn xác định tất cả nhân viên không thuộc bộ phận CNTT. (Bộ phận của nhân viên được tìm thấy trong cột **bộ phận** , chứa các giá trị bao gồm **Công nghệ thông tin** .)

Mô tả truy vấn của bạn và cách thức hoạt động trong phần **Truy xuất tất cả nhân viên không thuộc CNTT** của mẫu **Áp dụng bộ lọc cho truy vấn SQL** .

Trong phòng **thí nghiệm Bộ lọc có AND, OR và NOT** , hãy chụp ảnh màn hình truy vấn SQL bạn đã sử dụng và sao chép nó vào mẫu. Hoặc, nhập truy vấn này trực tiếp vào mẫu.

|  |
| --- |
| **Step 9: Finalize your document**  To finalize the document and make its purpose clear to potential employers, be sure to complete the **Project description** and **Summary** sections of the **Apply filters to SQL queries** template.  In the Project description section, give a general overview of the scenario and what you accomplish through SQL. Write two to four sentences.  In the Summary section, provide a short summary of the previous tasks and connect them to the scenario. Write approximately two to four sentences. |

**Bước 9: Hoàn thiện tài liệu của bạn**

Để hoàn thiện tài liệu và làm rõ mục đích của tài liệu với các nhà tuyển dụng tiềm năng, hãy nhớ hoàn thành phần **Mô tả dự án** và **Tóm tắt** của mẫu **Áp dụng bộ lọc cho truy vấn SQL** .

Trong phần Mô tả dự án, hãy đưa ra cái nhìn tổng quan chung về kịch bản và những gì bạn đạt được thông qua SQL. Viết hai đến bốn câu.

Trong phần Tóm tắt, hãy cung cấp bản tóm tắt ngắn gọn về các nhiệm vụ trước đó và kết nối chúng với kịch bản. Viết khoảng hai đến bốn câu.

|  |
| --- |
| **What to Include in Your Response**  Be sure to include the following in your completed activity:   * Screenshots of your queries or typed versions of the queries * Explanations of your queries * A project description at the beginning * A summary at the end * Details on using **LIKE** to search for a pattern * Details on filtering for dates and times * Details on using **AND** and **OR** to filter on multiple conditions * Details on using **NOT** in filters |

**Những gì cần bao gồm trong phản hồi của bạn**

Hãy chắc chắn bao gồm những điều sau đây trong hoạt động đã hoàn thành của bạn:

* Ảnh chụp màn hình truy vấn của bạn hoặc phiên bản đã nhập của truy vấn
* Giải thích về truy vấn của bạn
* Mô tả dự án ở phần đầu
* Tóm tắt ở cuối
* Chi tiết về cách sử dụng **THÍCH** để tìm kiếm mẫu
* Chi tiết về lọc ngày và giờ
* Chi tiết về cách sử dụng **AND** và **OR** để lọc theo nhiều điều kiện
* Chi tiết về việc sử dụng **NOT** trong bộ lọc

***3.10. Portfolio Activity Exemplar: Apply filters to SQL queries – Ví dụ về hoạt động danh mục đầu tư: Áp dụng bộ lọc cho truy vấn SQL***

|  |
| --- |
| **Portfolio Activity Exemplar: Apply filters to SQL queries** |

**Ví dụ về hoạt động danh mục đầu tư: Áp dụng bộ lọc cho truy vấn SQL**

|  |
| --- |
| **Completed Exemplar**  To review the exemplar for this course item, click the following link and select *Use Template*.  Link to exemplar: [Apply filters to SQL queries](https://docs.google.com/document/d/1R-wz2DrsddIlst5iWVKa8-_j8sROgKAWvtITmy-o2dk/template/preview?usp=sharing&resourcekey=0-VW7ZQ-CAPGe9JIbBSjZJjg) |

**Mẫu đã hoàn thành**

Để xem lại ví dụ mẫu cho mục khóa học này, hãy nhấp vào liên kết sau và chọn *Sử dụng Mẫu* .

Liên kết đến ví dụ:[Áp dụng bộ lọc cho truy vấn SQL](https://docs.google.com/document/d/1R-wz2DrsddIlst5iWVKa8-_j8sROgKAWvtITmy-o2dk/template/preview?usp=sharing&resourcekey=0-VW7ZQ-CAPGe9JIbBSjZJjg)

|  |
| --- |
| **Assessment of Exemplar**  Compare the exemplar to your completed activity. Review your work using each of the criteria in the exemplar. What did you do well? Where can you improve? Use your answers to these questions to revise your project as needed and guide you as you continue to progress through the certificate program.  ***Note:*** *The exemplar represents one possible way to complete the* ***Apply filters to SQL queries*** *portfolio activity. Yours will likely differ in certain ways. What’s important is that you understand how to use SQL queries to apply filters.*  The exemplar uses details from the given scenario and includes the following:   * Screenshots of queries or typed versions of the queries * Explanations of queries * A project description at the beginning * A summary at the end * Details on using **LIKE** to search for a pattern * Details on filtering for dates and times * Details on using **AND** and **OR** to filter on multiple conditions * Details on using **NOT** in filters |

**Đánh giá mẫu mực**

So sánh ví dụ với hoạt động đã hoàn thành của bạn. Xem lại công việc của bạn bằng cách sử dụng từng tiêu chí trong ví dụ. Bạn đã làm tốt điều gì? Bạn có thể cải thiện ở đâu? Sử dụng câu trả lời của bạn cho những câu hỏi này để sửa đổi dự án của bạn nếu cần và hướng dẫn bạn khi bạn tiếp tục tiến bộ thông qua chương trình chứng chỉ.

***Lưu ý:*** *Mẫu này thể hiện một cách có thể để hoàn thành hoạt động* ***Áp dụng bộ lọc cho danh mục truy vấn SQL*** *. Của bạn có thể sẽ khác nhau theo những cách nhất định. Điều quan trọng là bạn hiểu cách sử dụng truy vấn SQL để áp dụng bộ lọc.*

Ví dụ mẫu sử dụng các chi tiết từ tình huống đã cho và bao gồm những thông tin sau:

* Ảnh chụp màn hình của truy vấn hoặc phiên bản đã nhập của truy vấn
* Giải thích các truy vấn
* Mô tả dự án ở phần đầu
* Tóm tắt ở cuối
* Chi tiết về cách sử dụng **LIKE** để tìm kiếm mẫu
* Chi tiết về lọc ngày và giờ
* Chi tiết về cách sử dụng **AND** và **OR** để lọc theo nhiều điều kiện
* Chi tiết về việc sử dụng **NOT** trong bộ lọc

***3.11. Test your knowledge: More SQL filters – Kiểm tra kiến ​​thức của bạn: Thêm bộ lọc SQL***

**4. SQL joins – SQL joins**

***4.1. Join tables in SQL – Nối các bảng trong SQL***

|  |
| --- |
| You've already learned a lot about SQL queries and filters. Nice work! The last concept we're introducing in this section is joining tables when querying a database. This is helpful when you need information from two different tables in a database. Let's say we have two tables: one that tells us about security vulnerabilities of different operating systems, and one about different machines in our company, including their operating systems. Having the ability to combine them gives us a list of vulnerable machines. That's pretty cool, right? |

Bạn đã học được rất nhiều vềTruy vấn và bộ lọc SQL. Công việc tốt đẹp!Khái niệm cuối cùng chúng tôi giới thiệu trongphần này đang nối các bảng khi truy vấn cơ sở dữ liệu.Điều này rất hữu ích khi bạn cầnthông tin từ hai bảng khác nhau trong cơ sở dữ liệu.Giả sử chúng ta có hai bảng:một thông tin cho chúng ta biết về các lỗ hổng bảo mật củacác hệ điều hành khác nhau và mộtvề các loại máy khác nhau trong công ty chúng tôi,bao gồm cả hệ điều hành của họ.Có khả năng kết hợp chúngcung cấp cho chúng tôi danh sách các máy dễ bị tấn công.Điều đó khá tuyệt phải không?

|  |
| --- |
| First, let's start talking about the syntax of joins. Since we're working with two tables now, we need a way to tell SQL what table we're picking columns from. In our example database, we have an employee\_id column in both the employees table and the machines table. In SQL statements that contain two columns, SQL needs to know which column we're referring to. The way to resolve this is by writing the name of the table first, then a period, and then the name of a column. So, we would have employees followed by a period, followed by the column name. This is the employee\_id column for the employees table. Similarly, this is the employee\_id column for the machines table. Now that we understand this syntax, let's apply it to a join! |

Đầu tiên, hãy bắt đầu nói về cú pháp của các phép nối.Vì hiện tại chúng ta đang làm việc với hai bảng,chúng ta cần một cách để nói với SQLchúng tôi đang chọn cột từ bảng nào.Trong cơ sở dữ liệu mẫu của chúng tôi,chúng tôi có cột nhan viên\_idtrong cả bảng nhân viên và bảng máy móc.Trong câu lệnh SQL có chứa hai cột,SQL cần biết chúng ta đang đề cập đến cột nào.Cách để giải quyết điều này là bằng cáchviết tên bảng trước,sau đó là dấu chấm và sau đó là tên của một cột.Vì vậy, chúng ta sẽ có nhân viên theo sau bởi một khoảng thời gian,theo sau là tên cột.Đây là cột member\_id cho bảng nhân viên.Tương tự, đây là cột member\_idcho bảng máy.Bây giờ chúng ta đã hiểu cú pháp này,hãy áp dụng nó để tham gia!

|  |
| --- |
| Imagine that we want to get a deeper understanding of the employees accessing the machines in our company. By joining the employees and the machines tables, we can do this! We first need to identify the shared column that we'll use to connect the two tables. In this case, we'll use a primary key and one table to connect to another table where it's a foreign key. The primary key of the employees table is employee\_id, which is a foreign key in the machines table. employee\_id is a primary key in the employees table because it has a unique value for every row in the employees table, and no empty values. We don't have a guarantee that the employee\_id column in the machines table follows the same criteria since it's a foreign key and not a primary key. |

Hãy tưởng tượng rằng chúng ta muốn có đượcsự hiểu biết sâu sắc hơn vềcác nhân viên truy cập vào máy móc trong công ty chúng tôi.Bằng cách tham gia cùng các nhân viên vàbàn máy, chúng ta có thể làm được điều này!Đầu tiên chúng ta cần xác địnhcột được chia sẻ mà chúng tôi sẽdùng để kết nối hai bảng.Trong trường hợp này, chúng tôi sẽ sử dụng khóa chính vàmột bảng để kết nối vớimột bảng khác nơi đó là khóa ngoại.Khóa chính của bảng nhân viên là worker\_id,đó là khóa ngoại trong bảng máy.nhân viên\_id là khóa chínhtrong bảng nhân viên vì nó cómột giá trị duy nhất cho mỗi hàng trongbảng nhân viên và không có giá trị trống.Chúng tôi không đảm bảo rằng cột member\_id trongbảng máy saucùng tiêu chí vì nókhóa ngoại chứ không phải khóa chính.

|  |
| --- |
| Next, we'll use a type of join called an INNER JOIN. An INNER JOIN returns rows matching on a specified column that exists in more than one table. Tables usually contain many more rows, but to further explain what we mean by INNER JOIN, let's focus on just four rows from the employees table and four rows from the machines table. We'll also look at just a few columns of each table for this example. Let's say we choose employee\_id in both tables to perform an INNER JOIN. Let's look at the two rows where there is a match. Both tables have 1188 and 1189 in their respective employee\_id columns, so they are considered a match. The results of the join is the two rows that have 1188 and 1189 and all columns from both tables. |

Tiếp theo, chúng ta sẽ sử dụng một loại liên kết được gọi là INNER JOIN.INNER JOIN trả về các hàng khớp trênmột cột được chỉ định tồn tại trong nhiều bảng.Các bảng thường chứa nhiều hàng hơn,nhưng để giải thích thêm ý nghĩa của INNER JOIN,hãy tập trung vào bốn hàng từbảng nhân viên và bốn hàng từ bảng máy móc.Chúng ta cũng sẽ xem xétchỉ một vài cột của mỗi bảng cho ví dụ này.Giả sử chúng ta chọnnhân viên\_id trong cả hai bảng để thực hiện THAM GIA INNER.Chúng ta hãy nhìn vào hai hàng có sự trùng khớp.Cả hai bảng đều có 1188 và1189 trong cột nhan viên\_id tương ứng của họ,vì vậy chúng được coi là một trận đấu.Kết quả của phép nối là hai hàng có 1188và 1189 và tất cả các cột từ cả hai bảng.

|  |
| --- |
| Before we move on to the queries, we have to talk about the NULL values in the tables. In SQL, NULL represents a missing value due to any reason. In this case, this might be machines that are not assigned to any employee. Now, let's bring this into SQL and do an INNER JOIN on the full tables. Let's imagine we want to join these tables in order to get a list of users and their office location that also shows what operating system they use on their machines. employee\_id is a common column between these tables, and we can use this to join them. But we won't need to show this column in the results. First, let's start with a basic query that indicates we want to select the username, office, and operating\_system columns. We want employees to be our first or left table, so we'll use that in our FROM statement. Now, we write the part of the query that tells SQL to join the machines table with the employees table. |

Trước khi chúng ta chuyển sang các truy vấn,chúng ta phải nói về các giá trị NULL trong các bảng.Trong SQL, NULL đại diện cho một giá trị bị thiếu vì bất kỳ lý do gì.Trong trường hợp này, đây có thể làmáy móc không được giao cho bất kỳ nhân viên nào.Bây giờ, hãy đưa cái này vào SQLvà thực hiện INNER JOIN trên các bảng đầy đủ.Hãy tưởng tượng chúng ta muốn tham giacác bảng này để có được danh sách người dùng vàvị trí văn phòng của họ cũng hiển thịhọ sử dụng hệ điều hành nào trên máy của họ.nhân viên\_id là một cột chung giữa các bảng này vàchúng ta có thể sử dụng điều này để tham gia cùng họ.Nhưng chúng ta sẽ không cần hiển thị cột này trong kết quả.Trước tiên, hãy bắt đầu với một truy vấn cơ bảnđiều đó cho biết chúng tôi muốn chọn tên người dùng,cột văn phòng và hệ điều hành.Chúng tôi muốn nhân viên là bàn đầu tiên hoặc bên trái của chúng tôi, vì vậychúng tôi sẽ sử dụng điều đó trong câu lệnh FROM của chúng tôi.Bây giờ, chúng ta viết phần truy vấn thông báo cho SQLđể nối bảng máy với bảng nhân viên.

|  |
| --- |
| Let's break down this query. INNER JOIN tells SQL to perform the INNER JOIN. Then, we name the second table we want to combine with the first. This is called the right table. In this case, we want to join machines with the employees table that was already identified after FROM. Lastly, we tell SQL what column to base the join on. In our case, we're using the employee\_id column. Since we're using two tables, we have to identify the table and follow that with the column name. So, we have employees.employee\_id. And machines.employee\_id. |

Hãy chia nhỏ truy vấn này.INNER JOIN yêu cầu SQL thực hiện INNER JOIN.Sau đó, chúng tôi đặt tên cho bảng thứ haichúng tôi muốn kết hợp với cái đầu tiên.Đây được gọi là bảng bên phải.Trong trường hợp này, chúng tôi muốn kết nối các máy vớibảng nhân viên đó làđã được xác định sau FROM.Cuối cùng, chúng tôi cho SQL biết cột nào sẽ làm cơ sở cho phép nối.Trong trường hợp của chúng tôi, chúng tôi đang sử dụng cột worker\_id.Vì chúng ta đang sử dụng hai bảng,chúng ta phải xác định bảngvà làm theo đó với tên cột.Vì vậy, chúng ta có nhan viên.employee\_id. Và máy móc.employee\_id.

|  |
| --- |
| Let's review the output. Perfect! We have now joined two tables. The results of our query displays the records that match on the employee\_id column. Notice that these records contain columns from both tables, but only the ones we've indicated through our SELECT statement. There are other types of joins that don't require a match to join two tables, and we're going to discuss those in the next video. I'll meet you there! |

Hãy xem lại kết quả đầu ra.Hoàn hảo! Bây giờ chúng ta đã nối hai bảng.Kết quả truy vấn của chúng tôi hiển thịcác bản ghi khớp với cột member\_id.Chú ý rằng những hồ sơ nàychứa các cột từ cả hai bảng,nhưng chỉ những cái chúng tôi cóđược chỉ định thông qua câu lệnh SELECT của chúng tôi.Có những kiểu kết nối khác khôngyêu cầu một trận đấu để tham gia hai bảng vàchúng ta sẽ thảo luận về những điều đó trongvideo tiếp theo. Tôi sẽ gặp bạn ở đó!

***4.2. Types of joins – Các loại kết nối***

|  |
| --- |
| Welcome back. I hope you enjoyed working on inner joins. In the previous video and exercises, we saw how inner joins can be useful by only returning records that share a value in specify columns. However, in some situations, we might need all of the entries from one or both of our tables. This is where we need to use outer joins. |

Chào mừng trở lại. Tôi hy vọng bạn thích làm việc với các kết nối bên trong.Trong video trước vàbài tập, chúng ta đã thấy các phép nối bên trong có thể hoạt động như thế nàohữu ích bằng cách chỉ trả lại hồ sơchia sẻ một giá trị trong các cột được chỉ định.Tuy nhiên, trong một số trường hợp, chúng ta có thể cầntất cả các mục từ một hoặc cả hai bảng của chúng tôi.Đây là nơi chúng ta cần sử dụng các phép nối ngoài.

|  |
| --- |
| There are three types of outer joins: LEFT JOIN, RIGHT JOIN, and FULL OUTER JOIN. Similar to inner joins, outer joins combine two tables together; however, they don't necessarily need a match between columns to return a row. Which rows are returned depends on the type of join. |

Có ba loại liên kết ngoài: LEFT JOIN,RIGHT JOIN và THAM GIA ĐẦY ĐỦ.Tương tự như các phép nối bên trong,các phép nối ngoài kết hợp hai bảng lại với nhau;tuy nhiên, họ không nhất thiết cầnkhớp giữa các cột để trả về một hàng.Những hàng nào được trả về tùy thuộc vào kiểu nối.

|  |
| --- |
| LEFT JOIN returns all of the records of the first table, but only returns rows of the second table that match on a specified column. Like we did in the previous video, let's examine this type of join by looking at just four rows of two tables with a small number of columns. Employees is the left table, or the first table, and machines is the right table, or the second table. Let's join on employee\_id. There's a matching value in this column for two of the four records. When we execute the join, SQL returns these rows with the matching value, all other rows from the left table, and all columns from both tables. Records from the employees table that didn't match but were returned through the LEFT JOIN contain NULL values in columns that came from the machines table. Next, let's talk about right joins. |

LEFT JOIN trả về tất cả các bản ghi của bảng đầu tiên,nhưng chỉ trả về hàngbảng thứ hai khớp với một cột được chỉ định.Giống như chúng ta đã làm trong video trước, chúng ta hãykiểm tra kiểu tham gia này bằng cáchchỉ nhìn vào bốn hànghai bảng có số lượng cột nhỏ.Nhân viên là bàn bên trái, hoặc bàn đầu tiên,và máy móc là bảng bên phải, hoặc bảng thứ hai.Hãy tham gia vào nhân viên\_id.Có một giá trị phù hợp trongcột này cho hai trong số bốn bản ghi.Khi chúng tôi thực hiện phép nối,SQL trả về các hàng này với giá trị phù hợp,tất cả các hàng khác từbảng bên trái và tất cả các cột từ cả hai bảng.Các bản ghi từ bảng nhân viênkhông khớp nhưng được trả về qua TRÁITHAM GIA chứa giá trị NULLtrong các cột đến từ bảng máy.Tiếp theo, hãy nói về phép nối phải.

|  |
| --- |
| RIGHT JOIN returns all of the records of the second table but only returns rows from the first table that match on a specified column. With a RIGHT JOIN on the previous example, the full result returns matching rows from both, all the rows from the second table, and all the columns in both tables. For the values that don't exist in either table, we are left with a NULL value. Last, we'll discuss full outer joins. |

RIGHT THAM GIA trả về tất cảcủa các bản ghi của bảng thứ hainhưng chỉ trả về các hàng từbảng đầu tiên khớp với một cột được chỉ định.Với RIGHT JOIN ở ví dụ trước,kết quả đầy đủ trả về các hàng khớp từ cả hai,tất cả các hàng từbảng thứ hai và tất cả các cột trong cả hai bảng.Đối với các giá trị không tồn tại trong cả hai bảng,chúng ta còn lại một giá trị NULL.Cuối cùng, chúng ta sẽ thảo luận về phép nối ngoài đầy đủ.

|  |
| --- |
| FULL OUTER JOIN returns all records from both tables. Using our same example, a FULL OUTER JOIN returns all columns from all tables. If a row doesn't have a value for a particular column, it returns NULL. For example, the machines table do not have any rows with employee\_id 1190, so the values for that row and the columns that came from the machines table is NULL. To implement left joins, right joins, and full outer joins in SQL, you use the same syntax structure as the INNER JOIN but use these keywords: LEFT JOIN, RIGHT JOIN, and FULL OUTER JOIN. |

FULL OUTER JOIN trả về tất cả các bản ghitừ cả hai bảng. Sử dụng ví dụ tương tự của chúng tôi,FULL OUTER JOIN trả về tất cả các cột từ tất cả các bảng.Nếu một hàng không có giá trị chomột cột cụ thể, nó trả về NULL.Ví dụ, bảng máykhông có bất kỳ hàng nào với worker\_id1190, do đó các giá trị cho hàng đó vàcác cột đến từ bảng máy là NULL.Để thực hiện các phép nối trái, nối phải,và các phép nối ngoài đầy đủ trong SQL, bạn sử dụngcấu trúc cú pháp tương tự như INNER JOINnhưng hãy sử dụng những từ khóa sau:THAM GIA TRÁI, THAM GIA PHẢI,và THAM GIA ĐẦY ĐỦ.

|  |
| --- |
| As a security analyst, you're not required to know all of these from memory. Once you understand the type of join you need, you can quickly search and find all the information you need to execute these queries. With this information on joins, we've now covered some very important information you'll need as a security analyst using SQL. Thank you for joining me in this video. |

Là một nhà phân tích chứng khoán,bạn không bắt buộc phải biết tất cả những điều này từ trí nhớ.Khi bạn hiểu loại hình tham gia bạn cần,bạn có thể nhanh chóng tìm kiếm và tìm thấytất cả thông tin bạn cần để thực hiện các truy vấn này.Với thông tin này về các phép nối,bây giờ chúng ta đã đề cập đến một số thông tin rất quan trọngbạn sẽ cần với tư cách là một nhà phân tích bảo mật sử dụng SQL.Cảm ơn bạn đã tham gia cùng tôi trong video này.

***4.3. Compare types of joins – So sánh các loại liên kết***

|  |
| --- |
| **Compare types of joins** |

**So sánh các loại liên kết**

|  |
| --- |
| Previously, you explored SQL joins and how to use them to join data from multiple tables when these tables share a common column. You also examined how there are different types of joins, and each of them returns different rows from the tables being joined. In this reading, you'll review these concepts and more closely analyze the syntax needed for each type of join. |

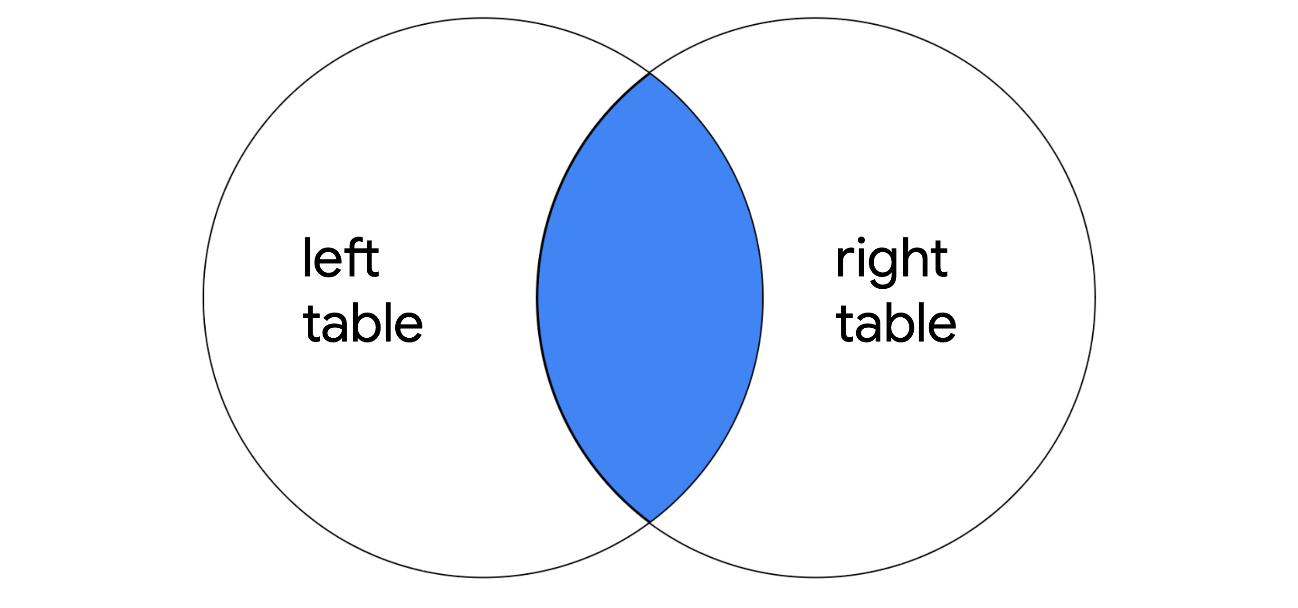
Trước đây, bạn đã khám phá các phép nối SQL và cách sử dụng chúng để nối dữ liệu từ nhiều bảng khi các bảng này có chung một cột. Bạn cũng đã kiểm tra xem có các loại liên kết khác nhau như thế nào và mỗi loại liên kết đó trả về các hàng khác nhau từ các bảng được nối. Trong bài đọc này, bạn sẽ xem lại các khái niệm này và phân tích kỹ hơn cú pháp cần thiết cho từng kiểu nối.

|  |
| --- |
| **Inner joins** |

**Kết nối bên trong**

|  |
| --- |
| The first type of join that you might perform is an inner join. **INNER JOIN** returns rows matching on a specified column that exists in more than one table. |

Kiểu liên kết đầu tiên mà bạn có thể thực hiện là liên kết bên trong. **INNER JOIN** trả về các hàng khớp trên một cột được chỉ định tồn tại trong nhiều bảng.



|  |
| --- |
| It only returns the rows where there is a match, but like other types of joins, it returns all specified columns from all joined tables. For example, if the query joins two tables with **SELECT \***, all columns in both of the tables are returned. |

Nó chỉ trả về các hàng có kết quả khớp, nhưng giống như các kiểu nối khác, nó trả về tất cả các cột được chỉ định từ tất cả các bảng đã nối. Ví dụ: nếu truy vấn nối hai bảng với **SELECT \*** , tất cả các cột trong cả hai bảng đều được trả về.

|  |
| --- |
| **Note:** If a column exists in both of the tables, it is returned twice when **SELECT \*** is used. |

**Lưu ý:** Nếu một cột tồn tại trong cả hai bảng, cột đó sẽ được trả về hai lần khi sử dụng **SELECT \* .**

|  |
| --- |
| **The syntax of an inner join** |

**Cú pháp của phép nối bên trong**

|  |
| --- |
| To write a query using **INNER JOIN**, you can use the following syntax:  **SELECT \***  **FROM employees**  **INNER JOIN machines ON employees.device\_id = machines.device\_id;** |

Để viết truy vấn bằng **INNER JOIN** , bạn có thể sử dụng cú pháp sau:

**SELECT \***

**FROM employees**

**INNER JOIN machines ON employees.device\_id = machines.device\_id;**

|  |
| --- |
| You must specify the two tables to join by including the first or left table after **FROM** and the second or right table after **INNER JOIN**. |

Bạn phải chỉ định hai bảng để nối bằng cách bao gồm bảng đầu tiên hoặc bảng bên trái sau **FROM** và bảng thứ hai hoặc bảng bên phải sau **INNER JOIN** .

|  |
| --- |
| After the name of the right table, use the **ON** keyword and the **=** operator to indicate the column you are joining the tables on. It's important that you specify both the table and column names in this portion of the join by placing a period (**.**) between the table and the column. |

Sau tên của bảng bên phải, hãy sử dụng từ khóa **ON** và toán tử **=** để chỉ ra cột mà bạn đang nối các bảng trên đó. Điều quan trọng là bạn phải chỉ định cả tên bảng và tên cột trong phần nối này bằng cách đặt dấu chấm ( **.** ) giữa bảng và cột.

|  |
| --- |
| In addition to selecting all columns, you can select only certain columns.  For example, if you only want the join to return the **username**, **operating\_system** and **device\_id** columns, you can write this query:  **SELECT username, operating\_system, employees.device\_id**  **FROM  employees**  **INNER JOIN machines ON employees.device\_id = machines.device\_id;** |

Ngoài việc chọn tất cả các cột, bạn chỉ có thể chọn một số cột nhất định. Ví dụ: nếu bạn chỉ muốn phép nối trả về các **username**, **operating\_system** và **device\_id**, bạn có thể viết truy vấn này:

**SELECT username, operating\_system, employees.device\_id**

**FROM  employees**

**INNER JOIN machines ON employees.device\_id = machines.device\_id;**

|  |
| --- |
| **Note**: In the example query, **username** and **operating\_system** only appear in one of the two tables, so they are written with just the column name. On the other hand, because **device\_id** appears in both tables, it's necessary to indicate which one to return by specifying both the table and column name (**employees.device\_id**). |

**Lưu ý** : Trong truy vấn ví dụ, **tên người dùng** và **hệ điều hành** chỉ xuất hiện ở một trong hai bảng nên chúng chỉ được viết bằng tên cột. Mặt khác, vì **device\_id** xuất hiện trong cả hai bảng, nên cần phải chỉ ra bảng nào sẽ trả về bằng cách chỉ định cả tên bảng và tên cột ( **nhân viên.device\_id** ).

|  |
| --- |
| **Outer joins** |

**Kết nối bên ngoài**

|  |
| --- |
| Outer joins expand what is returned from a join. Each type of outer join returns all rows from either one table or both tables. |

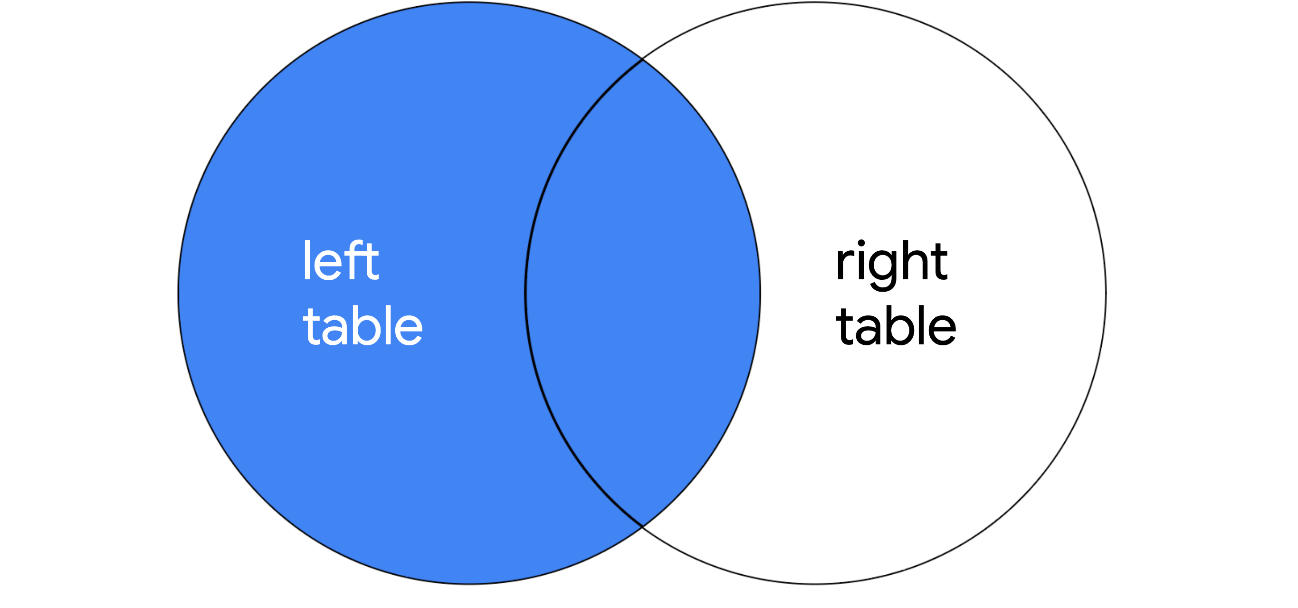
Các phép nối bên ngoài mở rộng những gì được trả về từ một phép nối. Mỗi kiểu nối ngoài trả về tất cả các hàng từ một bảng hoặc cả hai bảng.

|  |
| --- |
| **Left joins** |

**Left joins**

|  |
| --- |
| When joining two tables, **LEFT JOIN** returns all the records of the first table, but only returns rows of the second table that match on a specified column. |

Khi nối hai bảng, **LEFT JOIN** trả về tất cả các bản ghi của bảng đầu tiên nhưng chỉ trả về các hàng của bảng thứ hai khớp với một cột được chỉ định. 



|  |
| --- |
| The syntax for using **LEFT JOIN** is demonstrated in the following query:  **SELECT \***  **FROM employees**  **LEFT JOIN machines ON employees.device\_id = machines.device\_id;** |

Cú pháp sử dụng **LEFT JOIN** được thể hiện trong truy vấn sau:

**SELECT \***

**FROM employees**

**LEFT JOIN machines ON employees.device\_id = machines.device\_id;**

|  |
| --- |
| As with all joins, you should specify the first or left table as the table that comes after **FROM** and the second or right table as the table that comes after **LEFT JOIN**. In the example query, because **employees** is the left table, all of its records are returned. Only records that match on the **device\_id** column are returned from the right table, **machines**. |

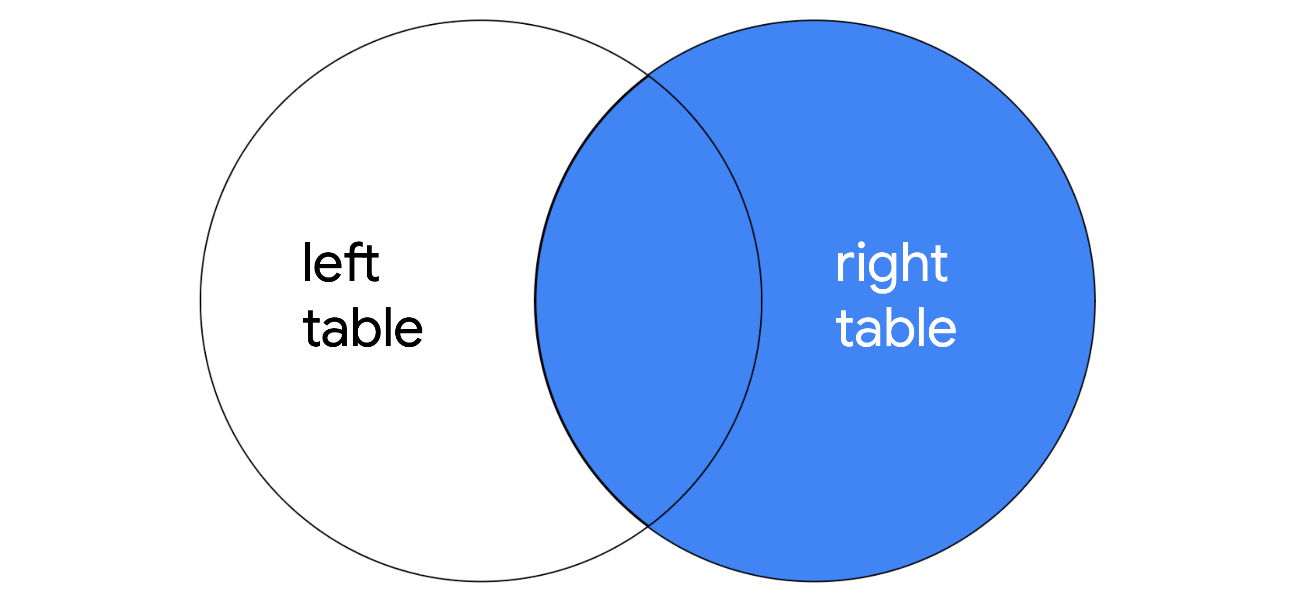
Giống như tất cả các phép nối, bạn nên chỉ định bảng đầu tiên hoặc bảng bên trái làm bảng sau **FROM** và bảng thứ hai hoặc bảng bên phải làm bảng sau **LEFT JOIN** . Trong truy vấn ví dụ, vì **nhân viên** là bảng bên trái nên tất cả các bản ghi của nó đều được trả về. Chỉ các bản ghi khớp với cột **device\_id** mới được trả về từ bảng bên phải, **máy móc** .

|  |
| --- |
| **Right joins** |

**Right joins**

|  |
| --- |
| When joining two tables, **RIGHT JOIN** returns all of the records of the second table, but only returns rows from the first table that match on a specified column. |

Khi nối hai bảng, **RIGHT JOIN** trả về tất cả các bản ghi của bảng thứ hai, nhưng chỉ trả về các hàng từ bảng đầu tiên khớp với một cột được chỉ định.



|  |
| --- |
| The following query demonstrates the syntax for **RIGHT JOIN**:  **SELECT \***  **FROM employees**  **RIGHT JOIN machines ON employees.device\_id = machines.device\_id;** |

Truy vấn sau đây thể hiện cú pháp của **RIGHT JOIN** :

**SELECT \***

**FROM employees**

**RIGHT JOIN machines ON employees.device\_id = machines.device\_id;**

|  |
| --- |
| **RIGHT JOIN** has the same syntax as **LEFT JOIN**, with the only difference being the keyword **RIGHT JOIN** instructs SQL to produce different output. The query returns all records from **machines**, which is the second or right table. Only matching records are returned from **employees**, which is the first or left table. |

**RIGHT JOIN** có cú pháp tương tự như **LEFT JOIN** , với điểm khác biệt duy nhất là từ khóa **RIGHT JOIN** hướng dẫn SQL tạo ra kết quả đầu ra khác nhau. Truy vấn trả về tất cả các bản ghi từ **máy** , là bảng thứ hai hoặc bảng bên phải. Chỉ các bản ghi phù hợp mới được trả về từ **bảng nhân viên** , là bảng đầu tiên hoặc bảng bên trái.

|  |
| --- |
| **Note:**  You can use **LEFT JOIN** and **RIGHT JOIN** and return the exact same results if you use the tables in reverse order. The following **RIGHT JOIN** query returns the exact same result as the **LEFT JOIN** query demonstrated in the previous section:  **SELECT \***  **FROM machines**  **RIGHT JOIN employees ON employees.device\_id = machines.device\_id;** |

**Lưu ý:**   Bạn có thể sử dụng **LEFT JOIN** và **RIGHT JOIN** và trả về kết quả tương tự nếu bạn sử dụng các bảng theo thứ tự ngược lại. Truy vấn **RIGHT JOIN** sau đây trả về kết quả giống hệt như truy vấn **LEFT JOIN** được trình bày trong phần trước:

**SELECT \***

**FROM machines**

**RIGHT JOIN employees ON employees.device\_id = machines.device\_id;**

|  |
| --- |
| All that you have to do is switch the order of the tables that appear before and after the keyword used for the join, and you will have swapped the left and right tables. |

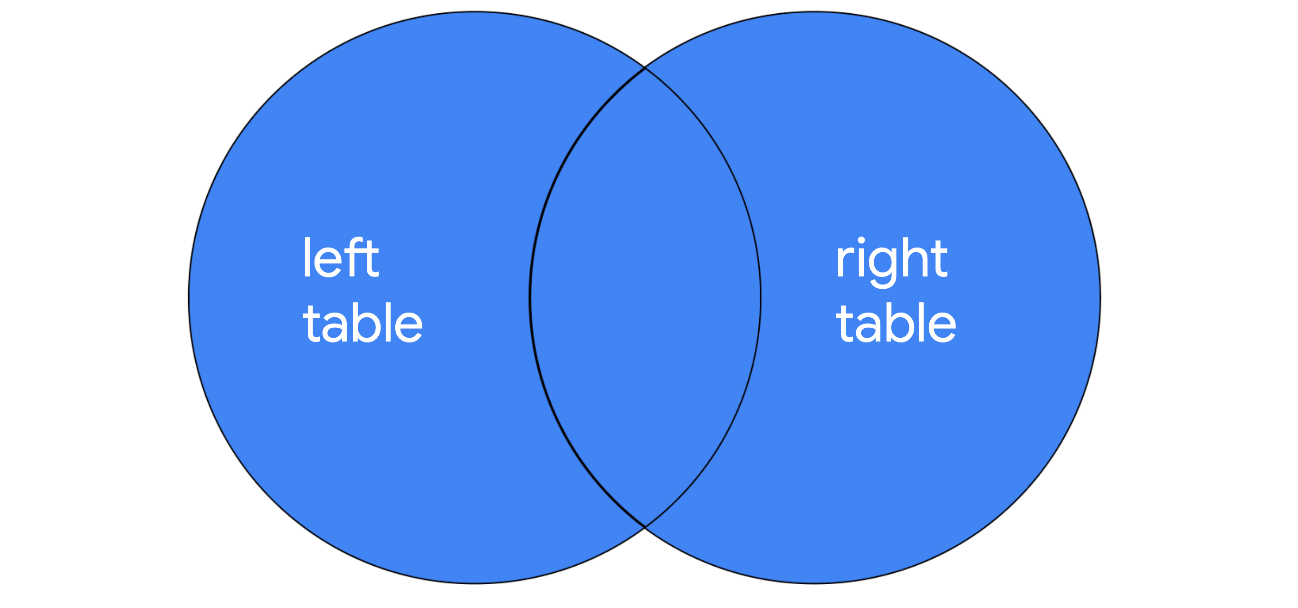
Tất cả những gì bạn phải làm là chuyển đổi thứ tự của các bảng xuất hiện trước và sau từ khóa được sử dụng để nối và bạn sẽ hoán đổi các bảng bên trái và bên phải.

|  |
| --- |
| **Full outer joins** |

**Full outer joins**

|  |
| --- |
| **FULL OUTER JOIN** returns all records from both tables. You can think of it as a way of completely merging two tables. |

**FULL OUTER JOIN** trả về tất cả bản ghi từ cả hai bảng. Bạn có thể coi nó như một cách hợp nhất hoàn toàn hai bảng.



|  |
| --- |
| You can review the syntax for using **FULL OUTER JOIN** in the following query:  **SELECT \***  **FROM employees**  **FULL OUTER JOIN machines ON employees.device\_id = machines.device\_id;** |

Bạn có thể xem lại cú pháp sử dụng **FULL OUTER JOIN** trong truy vấn sau:

**SELECT \***

**FROM employees**

**FULL OUTER JOIN machines ON employees.device\_id = machines.device\_id;**

|  |
| --- |
| The results of a **FULL OUTER JOIN** query include all records from both tables. Similar to **INNER JOIN**, the order of tables does not change the results of the query. |

Kết quả của truy vấn **FULL OUTER JOIN** bao gồm tất cả các bản ghi từ cả hai bảng. Tương tự như **INNER JOIN** , thứ tự các bảng không làm thay đổi kết quả truy vấn.

|  |
| --- |
| **Key takeaways** |

**Bài học chính**

|  |
| --- |
| When working in SQL, there are multiple ways to join tables.  All joins return the records that match on a specified column. **INNER JOIN** will return only these records. Outer joins also return all other records from one or both of the tables. **LEFT JOIN** returns all records from the first or left table, **RIGHT JOIN** returns all records from the second or right table, and **FULL OUTER JOIN** returns all records from both tables. |

Khi làm việc trong SQL, có nhiều cách để nối các bảng. Tất cả các phép nối trả về các bản ghi khớp với một cột được chỉ định. **INNER JOIN** sẽ chỉ trả về những bản ghi này. Các phép nối ngoài cũng trả về tất cả các bản ghi khác từ một hoặc cả hai bảng. **LEFT JOIN** trả về tất cả các bản ghi từ bảng đầu tiên hoặc bên trái, **RIGHT JOIN** trả về tất cả các bản ghi từ bảng thứ hai hoặc bên phải và **FULL OUTER JOIN** trả về tất cả các bản ghi từ cả hai bảng.

***4.4. Identify: Choose the appropriate type of join – Xác định: Chọn kiểu nối thích hợp***

|  |  |
| --- | --- |
| INNER JOIN |  |

|  |  |
| --- | --- |
| INNER JOIN |  |

|  |  |
| --- | --- |
| LEFT JOIN |  |

|  |  |
| --- | --- |
| LEFT JOIN |  |

|  |  |
| --- | --- |
| RIGHT JOIN |  |

|  |  |
| --- | --- |
| RIGHT JOIN |  |

|  |  |
| --- | --- |
| FULL OUTER JOIN |  |

|  |  |
| --- | --- |
| FULL OUTER JOIN |  |

***4.5. Activity: Complete a join – Hoạt động: Hoàn thành việc tham gia***

***4.6. Optional Exemplar: Complete a join – Mẫu tùy chọn: Hoàn thành việc tham gia***

***4.7. Test your knowledge: SQL joins – Kiểm tra kiến ​​thức của bạn: SQL tham gia***

***4.8. Continuous learning in SQL – Học tập liên tục trong SQL***

|  |
| --- |
| **Continuous learning in SQL** |

**Học tập liên tục trong SQL**

|  |
| --- |
| You've explored a lot about SQL, including applying filters to SQL queries and joining multiple tables together in a query.  There's still more that you can do with SQL. This reading will explore an example of something new you can add to your SQL toolbox: aggregate functions. You'll then focus on how you can continue learning about this and other SQL topics on your own. |

Bạn đã khám phá nhiều điều về SQL, bao gồm việc áp dụng các bộ lọc cho truy vấn SQL và nối nhiều bảng lại với nhau trong một truy vấn. Vẫn còn nhiều điều bạn có thể làm với SQL. Bài đọc này sẽ khám phá một ví dụ về một điều gì đó mới mà bạn có thể thêm vào hộp công cụ SQL của mình: các hàm tổng hợp. Sau đó, bạn sẽ tập trung vào cách bạn có thể tiếp tục tự mình tìm hiểu về chủ đề này và các chủ đề SQL khác.

|  |
| --- |
| **Aggregate functions** |

**Chức năng tổng hợp**

|  |
| --- |
| In SQL, **aggregate functions** are functions that perform a calculation over multiple data points and return the result of the calculation. The actual data is not returned. |

Trong SQL, **hàm tổng hợp** là các hàm thực hiện phép tính trên nhiều điểm dữ liệu và trả về kết quả của phép tính. Dữ liệu thực tế không được trả về.

|  |
| --- |
| There are various aggregate functions that perform different calculations:   * **COUNT** returns a single number that represents the number of rows returned from your query. * **AVG** returns a single number that represents the average of the numerical data in a column. * **SUM** returns a single number that represents the sum of the numerical data in a column. |

Có nhiều hàm tổng hợp khác nhau thực hiện các phép tính khác nhau:

* **COUNT** trả về một số đại diện cho số hàng được trả về từ truy vấn của bạn.
* **AVG** trả về một số duy nhất biểu thị mức trung bình của dữ liệu số trong một cột.
* **SUM** trả về một số duy nhất biểu thị tổng dữ liệu số trong một cột.

|  |
| --- |
| **Aggregate function syntax** |

**Cú pháp hàm tổng hợp**

|  |
| --- |
| To use an aggregate function, place the keyword for it after the **SELECT** keyword, and then in parentheses, indicate the column you want to perform the calculation on. |

Để sử dụng hàm tổng hợp, hãy đặt từ khóa cho hàm đó sau từ khóa **SELECT** , sau đó trong ngoặc đơn, cho biết cột bạn muốn thực hiện phép tính.

|  |
| --- |
| For example, when working with the **customers** table, you can use aggregate functions to summarize important information about the table. If you want to find out how many customers there are in total, you can use the **COUNT** function on any column, and SQL will return the total number of records, excluding **NULL** values. You can run this query and explore its output:  SELECT COUNT(firstname)  FROM customers; |

Ví dụ: khi làm việc với bảng **khách hàng** , bạn có thể sử dụng các hàm tổng hợp để tóm tắt thông tin quan trọng về bảng. Nếu bạn muốn biết tổng cộng có bao nhiêu khách hàng, bạn có thể sử dụng hàm **COUNT** trên bất kỳ cột nào và SQL sẽ trả về tổng số bản ghi, không bao gồm giá trị **NULL** . Bạn có thể chạy truy vấn này và khám phá đầu ra của nó:

SELECT COUNT(firstname)

FROM customers;

|  |
| --- |
| The result is a table with one column titled **COUNT(firstname)** and one row that indicates the count. |

Kết quả là một bảng có một cột có tiêu đề **COUNT(firstname)** và một hàng cho biết số lượng.

+-------------------+

| COUNT(firstname)|

+-------------------+

| 59 |

+-------------------+

|  |
| --- |
| If you want to find the number of customers from a specific country, you can add a filter to your query:  SELECT COUNT(firstname)  FROM customers  WHERE country = 'USA'; |

Nếu bạn muốn tìm số lượng khách hàng từ một quốc gia cụ thể, bạn có thể thêm bộ lọc vào truy vấn của mình:

SELECT COUNT(firstname)

FROM customers

WHERE country = 'USA';

|  |
| --- |
| With this filter, the count is lower because it only includes the records where the **country** column contains a value of **'USA'**. |

Với bộ lọc này, số lượng sẽ thấp hơn vì nó chỉ bao gồm các bản ghi trong đó cột **quốc gia** chứa giá trị **'USA'** .

+-------------------+

| COUNT(firstname)|

+-------------------+

| 59 |

+-------------------+

|  |
| --- |
| There are a lot of other aggregate functions in SQL. The syntax of placing them after **SELECT** is exactly the same as the **COUNT** function. |

Có rất nhiều hàm tổng hợp khác trong SQL. Cú pháp đặt chúng sau **SELECT** hoàn toàn giống với hàm **COUNT** .

|  |
| --- |
| **Continuing to learn SQL** |

**Tiếp tục học SQL**

|  |
| --- |
| SQL is a widely used querying language, with many more keywords and applications. You can continue to learn more about aggregate functions and other aspects of using SQL on your own. |

SQL là ngôn ngữ truy vấn được sử dụng rộng rãi với nhiều từ khóa và ứng dụng hơn. Bạn có thể tiếp tục tìm hiểu thêm về các hàm tổng hợp và các khía cạnh khác của việc tự mình sử dụng SQL.

|  |
| --- |
| Most importantly, approach new tasks with curiosity and a willingness to find new ways to apply SQL to your work as a security analyst. Identify the data results that you need and try to use SQL to obtain these results. |

Quan trọng nhất, hãy tiếp cận các nhiệm vụ mới với sự tò mò và sẵn sàng tìm ra những cách mới để áp dụng SQL vào công việc của bạn với tư cách là nhà phân tích bảo mật. Xác định các kết quả dữ liệu mà bạn cần và cố gắng sử dụng SQL để có được những kết quả này.

|  |
| --- |
| Fortunately, SQL is one of the most important tools for working with databases and analyzing data, so you'll find a lot of support in trying to learn SQL online. First, try searching for the concepts you've already learned and practiced to find resources that have accurate easy-to-follow explanations. When you identify these resources, you can use them to extend your knowledge. |

May mắn thay, SQL là một trong những công cụ quan trọng nhất để làm việc với cơ sở dữ liệu và phân tích dữ liệu, vì vậy bạn sẽ tìm thấy rất nhiều sự hỗ trợ khi cố gắng học SQL trực tuyến. Trước tiên, hãy thử tìm kiếm các khái niệm bạn đã học và thực hành để tìm các tài nguyên có giải thích chính xác, dễ hiểu. Khi bạn xác định được những nguồn tài nguyên này, bạn có thể sử dụng chúng để mở rộng kiến ​​thức của mình.

|  |
| --- |
| Continuing your practical experience with SQL is also important. You can also search for new databases that allow you to perform SQL queries using what you've learned. |

Việc tiếp tục trải nghiệm thực tế với SQL cũng rất quan trọng. Bạn cũng có thể tìm kiếm cơ sở dữ liệu mới cho phép bạn thực hiện các truy vấn SQL bằng những gì bạn đã học.

|  |
| --- |
| **Key takeaways** |

**Bài học chính**

|  |
| --- |
| Aggregate functions like **COUNT**, **SUM**, and **AVG** allow you to work with SQL in new ways. There are many other additional aspects of SQL that could be useful to you as an analyst. By continuing to explore SQL on your own, you can expand the ways you can apply SQL in a cybersecurity context. |

Các hàm tổng hợp như **COUNT** , **SUM** và **AVG** cho phép bạn làm việc với SQL theo những cách mới. Có nhiều khía cạnh bổ sung khác của SQL có thể hữu ích cho bạn với tư cách là nhà phân tích. Bằng cách tiếp tục tự mình khám phá SQL, bạn có thể mở rộng các cách áp dụng SQL trong bối cảnh an ninh mạng.

***4.9. SQL and the security analyst – SQL và nhà phân tích bảo mật***

**5. Review: Databases and SQL – Đánh giá: Cơ sở dữ liệu và SQL**

***5.1. Wrap-up – Gói lại***

|  |
| --- |
| Congratulations! We've made it together through the end of our focus on SQL. You've put in a lot of work and learned an important tool that will help you on your journey as a security analyst. Let's take a moment to go through all of the topics you learned in this section. |

Chúc mừng! Chúng tôi đã làm đượccùng nhau cho đến khi kết thúc quá trình tập trung vào SQL.Bạn đã đưa vào rất nhiềulàm việc và học được một công cụ quan trọngsẽ giúp bạn trên hành trình trở thành nhà phân tích bảo mật.Chúng ta hãy dành một chút thời gian để đi qua tất cảvề các chủ đề bạn đã học trong phần này.

|  |
| --- |
| We started by learning about the structure of relational databases and how we can access them by using the query language SQL. We then got hands-on practice with writing our own SQL queries. We used SQL to bring up information you might need on the job when working as an analyst. We then focused on SQL filters. We started with simple conditions with strings, and by the end, we learned how to use multiple filters in one query. We concluded the unit with SQL joins and learned how to join multiple tables, giving us even more information at once. |

Chúng tôi bắt đầu bằng việc tìm hiểu vềcấu trúc của cơ sở dữ liệu quan hệvà cách chúng ta có thể truy cập chúng bằng cáchsử dụng ngôn ngữ truy vấn SQL.Sau đó chúng tôi thực hành thực hànhbằng cách viết các truy vấn SQL của riêng chúng ta.Chúng tôi đã sử dụng SQL để đưa ra thông tin mà bạn có thểcần thiết trong công việc khi làm nhà phân tích.Sau đó chúng tôi tập trung vào các bộ lọc SQL.Chúng tôi bắt đầu với các điều kiện đơn giản với chuỗi,và cuối cùng, chúng tôi đã học được cách sử dụngnhiều bộ lọc trong một truy vấn.Chúng tôi đã kết thúc bài học bằng SQLtham gia và học cách tham gia nhiều bảng,cung cấp cho chúng tôi nhiều thông tin hơn cùng một lúc.

|  |
| --- |
| By completing this course, you just took a very big step in your future career as a security analyst. You have been introduced to a powerful tool that can help you in your work. Whenever you need to, I encourage you to revisit the materials in this course. Learning a querying language like SQL takes time. Thank you again for joining me in this journey. I hope you'll enjoy using SQL as much as I do. |

Bằng cách hoàn thành khóa học này,bạn vừa thực hiện một bước rất lớn trongsự nghiệp tương lai của bạn với tư cách là một nhà phân tích bảo mật.Bạn đã được giới thiệumột công cụ mạnh mẽ có thể giúp ích cho bạn trong công việc.Bất cứ khi nào bạn cần,Tôi khuyến khích bạn xem lại các tài liệu trong khóa học này.Học một ngôn ngữ truy vấn như SQL cần có thời gian.Cảm ơn bạn một lần nữa vì đã tham gia cùng tôi trong cuộc hành trình này.Tôi hy vọng bạn sẽ thích sử dụng SQL nhiều như tôi.

***5.2. Reference guide: SQL – Hướng dẫn tham khảo: SQL***

|  |
| --- |
| **Reference guide: SQL** |

**Hướng dẫn tham khảo: SQL**

|  |
| --- |
| The SQL reference guide contains keywords for SQL queries. Security analysts can use these keywords to query databases and find data to support security-related decisions. The reference guide is divided into four different categories of SQL keywords for security-related tasks: |

Hướng dẫn tham khảo SQL chứa các từ khóa cho truy vấn SQL. Các nhà phân tích bảo mật có thể sử dụng những từ khóa này để truy vấn cơ sở dữ liệu và tìm dữ liệu để hỗ trợ các quyết định liên quan đến bảo mật. Hướng dẫn tham khảo được chia thành bốn loại từ khóa SQL khác nhau cho các tác vụ liên quan đến bảo mật:

|  |
| --- |
| * Query a database * Apply filters to SQL queries * Join tables * Perform calculations |

tham khảo được chia thành bốn loại từ khóa SQL khác nhau cho các tác vụ liên quan đến bảo mật:

* Truy vấn cơ sở dữ liệu
* Áp dụng bộ lọc cho truy vấn SQL
* Tham gia các bảng
* Thực hiện tính toán

|  |
| --- |
| Within each category, commands are organized alphabetically. |

Trong mỗi danh mục, các lệnh được sắp xếp theo thứ tự bảng chữ cái.

|  |
| --- |
| **Access and save the guide** |

**Truy cập và lưu hướng dẫn**

|  |
| --- |
| You can save a copy of this guide for future reference. You can use it as a resource for additional practice or in your future professional projects. |

Bạn có thể lưu một bản sao của hướng dẫn này để tham khảo sau này. Bạn có thể sử dụng nó như một nguồn tài liệu để thực hành bổ sung hoặc cho các dự án chuyên môn trong tương lai của mình.

|  |
| --- |
| To access a downloadable version of this course item, click the following link and select *Use Template*.  [Reference guide: SQL](https://docs.google.com/document/d/1QVfrtp4QywbvQ5ALupN7-gKNrXI9yrYDv6PyCwWVAYg/template/preview) |

Để truy cập phiên bản có thể tải xuống của mục khóa học này, hãy nhấp vào liên kết sau và chọn *Sử dụng Mẫu* .

[Hướng dẫn tham khảo: SQL](https://docs.google.com/document/d/1QVfrtp4QywbvQ5ALupN7-gKNrXI9yrYDv6PyCwWVAYg/template/preview)

***5.3. Glossary terms from module 4 – Thuật ngữ trong học phần 4***

|  |
| --- |
| **Glossary terms from module 4** |

**Thuật ngữ trong học phần 4**

|  |
| --- |
| **Terms and definitions from Course 4, Module 4** |

**Các thuật ngữ và định nghĩa trong Khóa 4, Học phần 4**

|  |
| --- |
| **Database**: An organized collection of information or data |

**Cơ sở dữ liệu** : Một tập hợp thông tin hoặc dữ liệu có tổ chức

|  |
| --- |
| **Date and time data:** Data representing a date and/or time |

**Dữ liệu ngày và giờ:** Dữ liệu biểu thị ngày và/hoặc thời gian

|  |
| --- |
| **Exclusive operator**: An operator that does not include the value of comparison |

**Toán tử độc quyền** : Toán tử không chứa giá trị so sánh

|  |
| --- |
| **Filtering:** Selecting data that match a certain condition |

**Lọc:** Chọn dữ liệu phù hợp với một điều kiện nhất định

|  |
| --- |
| **Foreign key:** A column in a table that is a primary key in another table |

**Khóa ngoại:** Một cột trong bảng là khóa chính trong bảng khác

|  |
| --- |
| **Inclusive operator:** An operator that includes the value of comparison |

**Toán tử bao gồm:** Toán tử bao gồm giá trị so sánh

|  |
| --- |
| **Log:** A record of events that occur within an organization's systems |

**Nhật ký:** Bản ghi các sự kiện xảy ra trong hệ thống của tổ chức

|  |
| --- |
| **Numeric data:** Data consisting of numbers |

**Dữ liệu số:** Dữ liệu bao gồm các số

|  |
| --- |
| **Operator:** A symbol or keyword that represents an operation |

**Toán tử:** Một ký hiệu hoặc từ khóa đại diện cho một thao tác

|  |
| --- |
| **Primary key:** A column where every row has a unique entry |

**Khóa chính:** Một cột trong đó mỗi hàng có một mục nhập duy nhất

|  |
| --- |
| **Query:** A request for data from a database table or a combination of tables |

**Truy vấn:** Yêu cầu dữ liệu từ bảng cơ sở dữ liệu hoặc kết hợp các bảng

|  |
| --- |
| **Relational database:** A structured database containing tables that are related to each other |

**Cơ sở dữ liệu quan hệ:** Cơ sở dữ liệu có cấu trúc chứa các bảng có liên quan với nhau

|  |
| --- |
| **String data**: Data consisting of an ordered sequence of characters |

**Dữ liệu chuỗi** : Dữ liệu bao gồm một chuỗi ký tự được sắp xếp

|  |
| --- |
| **SQL (Structured Query Language):** A programming language used to create, interact with, and request information from a database |

**SQL (Ngôn ngữ truy vấn có cấu trúc):** Ngôn ngữ lập trình được sử dụng để tạo, tương tác và yêu cầu thông tin từ cơ sở dữ liệu

|  |
| --- |
| **Syntax:** The rules that determine what is correctly structured in a computing language |

**Cú pháp:** Các quy tắc xác định những gì được cấu trúc chính xác trong ngôn ngữ máy tính

|  |
| --- |
| **Wildcard**: A special character that can be substituted with any other character |

**Ký tự đại diện** : Ký tự đặc biệt có thể thay thế bằng bất kỳ ký tự nào khác

***5.4. Module 4 challenge – Thử thách mô-đun 4***

**6. Congratulations on completing Course 4! – Chúc mừng bạn đã hoàn thành Khóa 4!**

***6.1. Course wrap-up – Tóm tắt khóa học***

|  |
| --- |
| You made it to the end of this course! Congratulations—you did it! I hope you are proud of all you learned. The focus of this course was computing basics. Understanding the basics of computing is a valuable skill as you transition into your career as a security analyst. |

Bạn đã hoàn thành khóa học này!Xin chúc mừng—bạn đã làm được!Tôi hy vọng bạn tự hào về tất cả những gì bạn đã học được.Trọng tâm của khóa học này là kiến ​​thức cơ bản về máy tính.Hiểu biết cơ bản vềtính toán là một kỹ năng có giá trị vìbạn chuyển sang sự nghiệp của mình với tư cách là nhà phân tích bảo mật.

|  |
| --- |
| Let's recap what you learned in this course. We first focused on operating systems and how they relate to applications and hardware. Understanding how the system you're protecting works is essential for doing your job effectively. That brings us to the Linux operating system. When working in the security profession, familiarity with Linux is important. We first discussed this architecture and various distributions. Then, we used a Linux command line to carry out tasks you might encounter as a security analyst. Finally, we looked at another useful tool and used SQL to query databases. |

Hãy tóm tắt lại những gì bạn đã học được trong khóa học này.Đầu tiên chúng tôi tập trung vào hệ điều hànhvà cách chúng liên quan đến các ứng dụng và phần cứng.Hiểu cách hệ thống bạn đang bảo vệcông việc là điều cần thiết để thực hiện công việc của bạn một cách hiệu quả.Điều đó đưa chúng ta đến với hệ điều hành Linux.Khi làm việc trong ngành bảo vệ,sự quen thuộc với Linux là quan trọng.Lần đầu tiên chúng tôi thảo luận về kiến ​​trúc nàyvà phân phối khác nhau.Sau đó, chúng tôi sử dụng dòng lệnh Linux để thực hiệnra các nhiệm vụ bạn có thể gặp phải với tư cách là nhà phân tích bảo mật.Cuối cùng, chúng tôi đã xem xétmột công cụ hữu ích khác và sử dụng SQL để truy vấn cơ sở dữ liệu.

|  |
| --- |
| After this course, I hope you have a better understanding of how these foundations of computing support a security analyst in their daily work. I also hope you continue your path with this program. There are a lot of other useful and exciting topics ahead. Once again, congratulations. You've finished another course. Building skills is something you should be proud of. Keep it up as you progress through this program. |

Sau khóa học này, tôihy vọng bạn hiểu rõ hơn vềnhững nền tảng máy tính này hỗ trợ như thế nàomột nhà phân tích bảo mật trong công việc hàng ngày của họ.Tôi cũng hy vọng bạn tiếp tục con đường của mình với chương trình này.Còn rất nhiều điều hữu ích khácvà các chủ đề thú vị phía trước.Một lần nữa xin chúc mừng.Bạn đã hoàn thành một khóa học khác.Xây dựng kỹ năng là điều bạn nên tự hào.Hãy duy trì nó khi bạn tiến bộ thông qua chương trình này.

***6.2. Course 4 glossary – Thuật ngữ khóa 4***

|  |
| --- |
| **Course 4 glossary** |

**Thuật ngữ khóa 4**

|  |
| --- |
| We’ve covered a lot of terms—some of which you may have already known, and some of which are new. To make it easy to remember what a word means, we created this glossary of terms and definitions. |

Chúng tôi đã đề cập đến rất nhiều thuật ngữ—một số thuật ngữ có thể bạn đã biết và một số thuật ngữ mới. Để giúp bạn dễ dàng nhớ nghĩa của một từ, chúng tôi đã tạo ra bảng chú giải các thuật ngữ và định nghĩa này.

|  |
| --- |
| To use the glossary for this course item, click the link below and select “Use Template.”  Link to glossary: [Course 4 Glossary](https://docs.google.com/document/d/1ki6X7Q792RGNK8w0ltKIoB3So-8lqUx4Rdb7V94MdyM/template/preview?usp=sharing&resourcekey=0-z6oHYq011xfRKtaw-qXDMA) |

Để sử dụng bảng thuật ngữ cho mục khóa học này, hãy nhấp vào liên kết bên dưới và chọn “Sử dụng mẫu”.

Liên kết đến bảng thuật ngữ:[Thuật ngữ khóa 4](https://docs.google.com/document/d/1ki6X7Q792RGNK8w0ltKIoB3So-8lqUx4Rdb7V94MdyM/template/preview?usp=sharing&resourcekey=0-z6oHYq011xfRKtaw-qXDMA)

***6.3. Your Course 4 learning journey – Hành trình học tập Khóa 4 của bạn***

***6.4. Get started on the next course – Bắt đầu khóa học tiếp theo***

|  |
| --- |
| **Get started on the next course** |

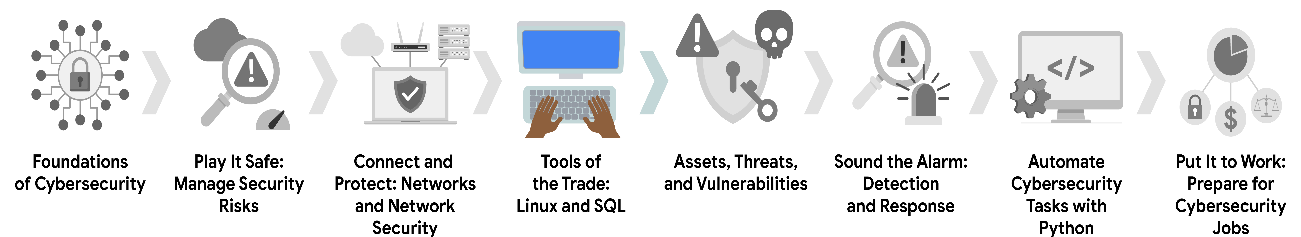
**Bắt đầu khóa học tiếp theo**

|  |
| --- |
| Congratulations on completing Course 4 of the Google Cybersecurity Certificate:**Tools of the Trade: Linux and SQL**! In this part of the program, you learned about computing skills that will support your work as an analyst. First, you learned about operating systems. Then, you communicated with the Linux operating system through the Bash shell in order to complete security-related tasks. Finally, you performed SQL queries that returned information to support security-related decisions. |

Chúc mừng bạn đã hoàn thành Khóa 4 của Chứng chỉ An ninh mạng của Google: **Công cụ thương mại: Linux và SQL** ! Trong phần này của chương trình, bạn đã tìm hiểu về các kỹ năng tính toán sẽ hỗ trợ công việc của bạn với tư cách là nhà phân tích. Đầu tiên bạn đã tìm hiểu về hệ điều hành. Sau đó, bạn giao tiếp với hệ điều hành Linux thông qua shell Bash để hoàn thành các tác vụ liên quan đến bảo mật. Cuối cùng, bạn đã thực hiện các truy vấn SQL trả về thông tin nhằm hỗ trợ các quyết định liên quan đến bảo mật.

|  |
| --- |
| The Google Cybersecurity Certificate has eight courses: |

Chứng chỉ An ninh mạng của Google có tám khóa học:



|  |
| --- |
| 1. **Foundations of Cybersecurity** — Explore the cybersecurity profession, including significant events that led to the development of the cybersecurity field and its continued importance to organizational operations. Learn about entry-level cybersecurity roles and responsibilities. 2. **Play It Safe: Manage Security Risks** — Identify how cybersecurity professionals use frameworks and controls to protect business operations, and explore common cybersecurity tools. 3. **Connect and Protect: Networks and Network Security** — Gain an understanding of network-level vulnerabilities and how to secure networks. 4. **Tools of the Trade: Linux and SQL** — Explore foundational computing skills, including communicating with the Linux operating system through the command line and querying databases with SQL. *(This is the course you just completed. Well done!)* 5. **Assets, Threats, and Vulnerabilities** — Learn about the importance of security controls and developing a threat actor mindset to protect and defend an organization’s assets from various threats, risks, and vulnerabilities. 6. **Sound the Alarm: Detection and Response** — Understand the incident response lifecycle and practice using tools to detect and respond to cybersecurity incidents. 7. **Automate Cybersecurity Tasks with Python** — Explore the Python programming language and write code to automate cybersecurity tasks. 8. **Put It to Work: Prepare for Cybersecurity Jobs** — Learn about incident classification, escalation, and ways to communicate with stakeholders. This course closes out the program with tips on how to engage with the cybersecurity community and prepare for your job search. |

1. **Nền tảng của an ninh mạng** - Khám phá nghề an ninh mạng, bao gồm các sự kiện quan trọng dẫn đến sự phát triển của lĩnh vực an ninh mạng và tầm quan trọng liên tục của nó đối với hoạt động của tổ chức. Tìm hiểu về vai trò và trách nhiệm an ninh mạng cấp cơ bản.
2. **Chơi an toàn: Quản lý rủi ro bảo mật** — Xác định cách các chuyên gia an ninh mạng sử dụng khuôn khổ và biện pháp kiểm soát để bảo vệ hoạt động kinh doanh cũng như khám phá các công cụ an ninh mạng phổ biến.
3. **Kết nối và bảo vệ: Mạng và bảo mật mạng** - Hiểu biết về các lỗ hổng cấp độ mạng và cách bảo mật mạng.
4. **Công cụ giao dịch: Linux và SQL** - Khám phá các kỹ năng tính toán cơ bản, bao gồm giao tiếp với hệ điều hành Linux thông qua dòng lệnh và truy vấn cơ sở dữ liệu bằng SQL. *(Đây là khóa học bạn vừa hoàn thành. Làm tốt lắm!)*
5. **Tài sản, mối đe dọa và lỗ hổng bảo mật** - Tìm hiểu về tầm quan trọng của kiểm soát bảo mật và phát triển tư duy của tác nhân đe dọa để bảo vệ và bảo vệ tài sản của tổ chức khỏi các mối đe dọa, rủi ro và lỗ hổng khác nhau.
6. **Báo động: Phát hiện và ứng phó** - Hiểu vòng đời ứng phó sự cố và thực hành sử dụng các công cụ để phát hiện và ứng phó với sự cố an ninh mạng.
7. **Tự động hóa các tác vụ an ninh mạng bằng Python** — Khám phá ngôn ngữ lập trình Python và viết mã để tự động hóa các tác vụ an ninh mạng.
8. **Đưa nó vào hoạt động: Chuẩn bị cho các công việc về an ninh mạng** — Tìm hiểu về phân loại sự cố, trình báo và cách liên lạc với các bên liên quan. Khóa học này kết thúc chương trình với các mẹo về cách tương tác với cộng đồng an ninh mạng và chuẩn bị cho quá trình tìm kiếm việc làm của bạn.

|  |
| --- |
|  |

|  |
| --- |
|  |

|  |
| --- |
|  |

|  |
| --- |
|  |

|  |
| --- |
|  |

|  |
| --- |
|  |

|  |
| --- |
|  |

|  |
| --- |
|  |

|  |
| --- |
|  |

|  |
| --- |
|  |

|  |
| --- |
|  |

|  |
| --- |
|  |

|  |
| --- |
|  |

|  |
| --- |
|  |