**Module 1: Network architecture – Kiến trúc mạng**

|  |
| --- |
| You'll be introduced to network security and explain how it relates to ongoing security threats and vulnerabilities. You will learn about network architecture and mechanisms to secure a network. |

Bạn sẽ được giới thiệu về bảo mật mạng và giải thích nó liên quan như thế nào đến các mối đe dọa và lỗ hổng bảo mật đang diễn ra. Bạn sẽ tìm hiểu về kiến ​​trúc mạng và cơ chế bảo mật mạng.

|  |
| --- |
| **Learning Objectives**   * Define types of networks * Describe physical components of a network * Understand how the TCP/IP model provides a framework for network communication * Explain how data is sent and received over a network * Explain network architecture |

**Mục tiêu học tập**

* Xác định các loại mạng
* Mô tả các thành phần vật lý của mạng
* Hiểu cách mô hình TCP/IP cung cấp một khuôn khổ cho giao tiếp mạng
* Giải thích cách gửi và nhận dữ liệu qua mạng
* Giải thích kiến ​​trúc mạng

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

***1.1. Introduction to Course 3 – Giới thiệu khóa học 3***

|  |
| --- |
| You've learned about security domains in previous courses. Now we'll explore one of those domains further: networks. It's important to secure networks because network-based attacks are growing in both frequency and complexity. |

Bạn đã học về miền bảo mật trong các khóa học trước.Bây giờ chúng ta sẽ khám phá thêm một trong những miền đó: mạng.Điều quan trọng là phải bảo mật mạng vì các cuộc tấn công dựa trên mạng đang gia tăng ở cảtần suất và độ phức tạp.

|  |
| --- |
| Hi there! My name is Chris, and I'm the Chief Information Security Officer for Google Fiber. I'm excited to be your instructor for this course! I've been working in network security and engineering for over 20 years, and I'm looking forward to sharing some of my knowledge and experience with you. |

Chào bạn! Tên tôi là Chris và tôi là Giám đốc An ninh Thông tin củaGoogle Fiber.Tôi rất vui được trở thành người hướng dẫn bạn cho khóa học này!Tôi đã làm việc trong lĩnh vực kỹ thuật và an ninh mạng hơn 20 năm vàTôi rất mong được chia sẻ một số kiến ​​thức và kinh nghiệm của mình với bạn.

|  |
| --- |
| This course will help you understand the basic structure of a network (also referred to as network architecture) and commonly used network tools. You'll also learn about network operations and explore some basic network protocols. Next, you'll learn about common network attacks and how network intrusion tactics can prevent a threat to a network. Finally, the course will provide an overview of security hardening practices and how you might use them to help secure a network. |

Khóa học này sẽ giúp bạn hiểu cấu trúc cơ bản của mạng (cũng nhưđược gọi là kiến ​​trúc mạng) và các công cụ mạng thường được sử dụng.Bạn cũng sẽ tìm hiểu về hoạt động mạng và khám phá một số giao thức mạng cơ bản.Tiếp theo, bạn sẽ tìm hiểu về các cuộc tấn công mạng phổ biến vàchiến thuật xâm nhập mạng có thể ngăn chặn mối đe dọa đối với mạng như thế nào.Cuối cùng, khóa học sẽ cung cấp cái nhìn tổng quan về các phương pháp tăng cường bảo mậtvà cách bạn có thể sử dụng chúng để giúp bảo mật mạng.

|  |
| --- |
| There's a lot to learn in securing networks, and I'm excited to go on this journey with you. Ready to get started? Let's go! |

Có rất nhiều điều cần tìm hiểu về việc bảo mật mạng vàTôi rất vui được đi cùng bạn trên cuộc hành trình này.Sẵn sàng để bắt đầu?Đi nào!

***1.2. Course 3 overview – Tổng quan khóa 3***

|  |
| --- |
| **Course 3 overview** |

**Tổng quan khóa học 3**



|  |
| --- |
| Hello and welcome to **Connect and Protect: Networks and Network Security**, the third course in the Google Cybersecurity Certificate. You’re on an exciting journey! |

Xin chào và chào mừng bạn đến với **Connect and Protect: Networks and Network Security** , khóa học thứ ba 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 network architecture, operations, intrusion tactics, common types of network vulnerabilities and attacks, and how to secure networks. You’ll also be introduced to common network protocols, firewalls, virtual private networks (VPNs), and system hardening practices. |

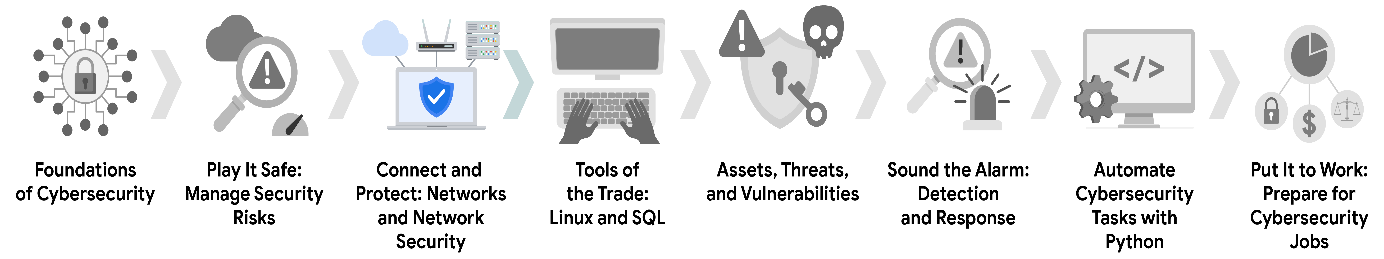
Khi kết thúc khóa học này, bạn sẽ hiểu rõ hơn về kiến ​​trúc mạng, hoạt động, chiến thuật xâm nhập, các loại lỗ hổng và tấn công mạng phổ biến cũng như cách bảo mật mạng. Bạn cũng sẽ được giới thiệu các giao thức mạng phổ biến, tường lửa, mạng riêng ảo (VPN) và các phương pháp tăng cường hệ thống.

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

**Tiến độ chương trình chứng chỉ**

|  |
| --- |
| The Google Cybersecurity Certificate program has eight courses. **Connect and Protect: Networks and Network Security** is the third course. |

Chương trình Chứng chỉ An ninh mạng của Google có tám khóa học. **Kết nối và Bảo vệ: Mạng và An ninh Mạng** là khóa học thứ ba.



|  |
| --- |
| 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)— *(current course)* 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)— 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)— *(khóa học hiện tại)* 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)- 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 3 content** |

**Nội dung khóa 3**

|  |
| --- |
| 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. |

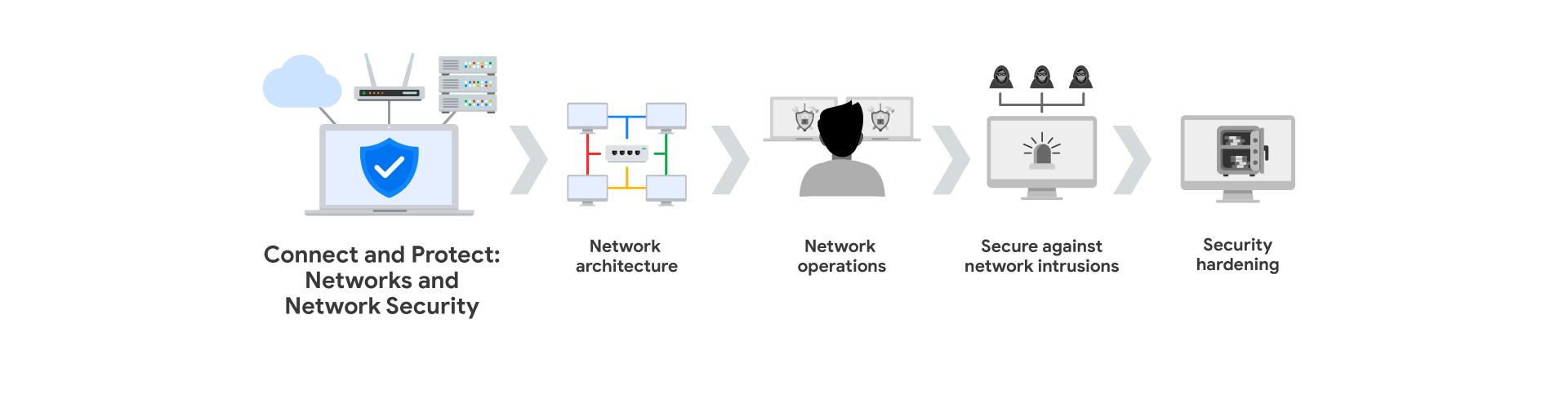
Mỗi khóa học của chương trình chứng chỉ này được chia thành các mô-đun. Bạn có thể hoàn thành các khóa học theo tốc độ của riêng mình nhưng phần phân tích mô-đun được thiết kế để giúp bạn hoàn thành toàn bộ Chứng chỉ an ninh mạng của Google trong khoảng sáu tháng.

|  |
| --- |
| 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: Network architecture** |

**Mô-đun 1: Kiến trúc mạng**

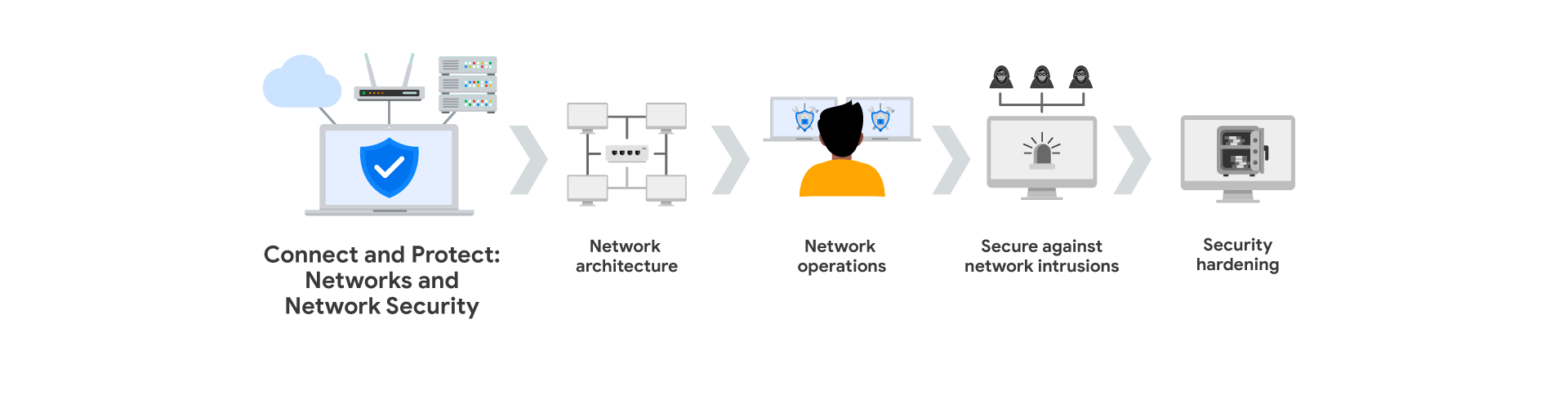


|  |
| --- |
| You'll be introduced to network security and explain how it relates to ongoing security threats and vulnerabilities. You will learn about network architecture and mechanisms to secure a network. |

Bạn sẽ được giới thiệu về bảo mật mạng và giải thích nó liên quan như thế nào đến các mối đe dọa và lỗ hổng bảo mật đang diễn ra. Bạn sẽ tìm hiểu về kiến ​​trúc mạng và cơ chế bảo mật mạng.

|  |
| --- |
| **Module 2: Network operations** |

**Mô-đun 2: Hoạt động mạng**

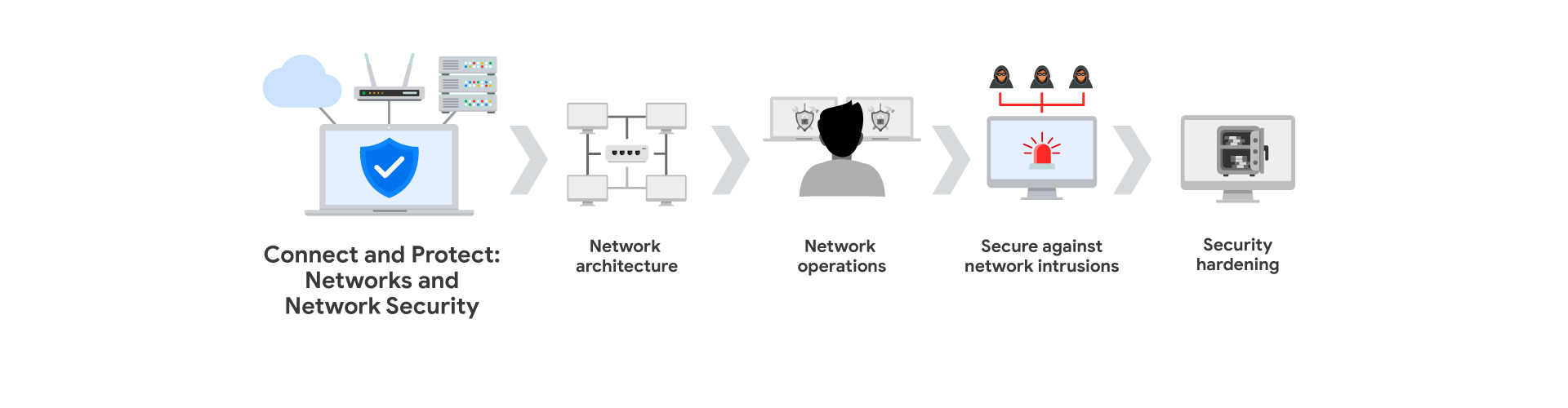


|  |
| --- |
| You will explore network protocols and how network communication can introduce vulnerabilities. In addition, you'll learn about common security measures, like firewalls, that help network operations remain safe and reliable. |

Bạn sẽ khám phá các giao thức mạng và cách giao tiếp mạng có thể gây ra các lỗ hổng. Ngoài ra, bạn sẽ tìm hiểu về các biện pháp bảo mật phổ biến, như tường lửa, giúp hoạt động mạng luôn an toàn và đáng tin cậy.

|  |
| --- |
| **Module 3: Secure against network intrusions** |

**Mô-đun 3: Bảo mật chống xâm nhập mạng**

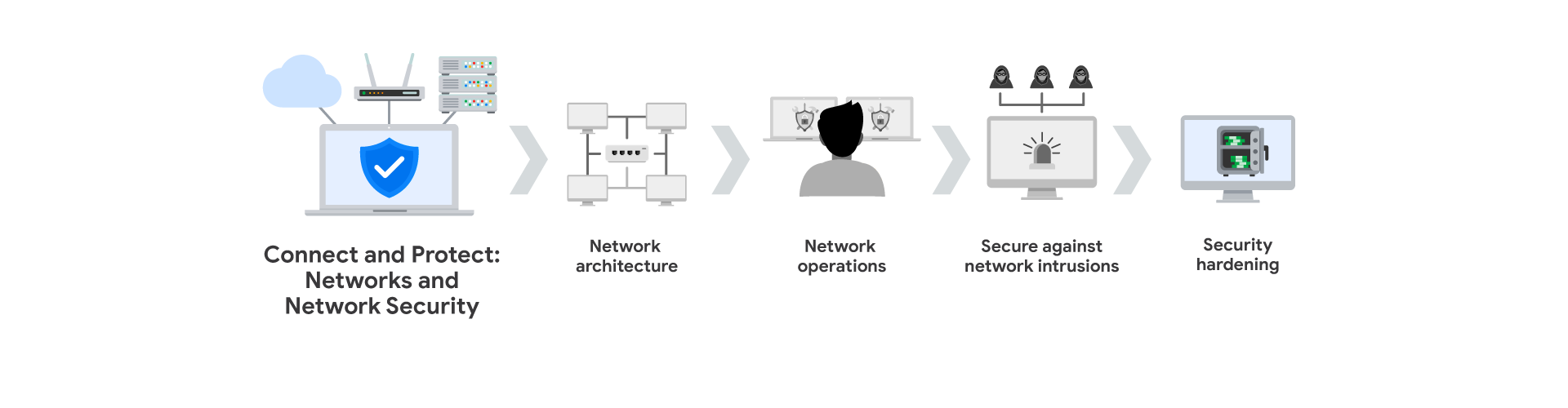


|  |
| --- |
| You will understand types of network attacks and techniques used to secure compromised network systems and devices. You'll explore the many ways that malicious actors exploit vulnerabilities in network infrastructure and how cybersecurity professionals identify and close potential loopholes. |

Bạn sẽ hiểu các loại tấn công mạng và kỹ thuật được sử dụng để bảo mật các hệ thống và thiết bị mạng bị xâm phạm. Bạn sẽ khám phá nhiều cách mà các tác nhân độc hại khai thác lỗ hổng trong cơ sở hạ tầng mạng cũng như cách các chuyên gia an ninh mạng xác định và đóng các lỗ hổng tiềm ẩn.

|  |
| --- |
| **Module 4: Security hardening** |

**Mô-đun 4: Tăng cường bảo mật**



|  |
| --- |
| You will become familiar with network hardening practices that strengthen network systems. You'll learn how security hardening helps defend against malicious actors and intrusion methods. You'll also learn how to use security hardening to address the unique security challenges posed by cloud infrastructures. |

Bạn sẽ làm quen với các phương pháp tăng cường mạng nhằm củng cố hệ thống mạng. Bạn sẽ tìm hiểu cách tăng cường bảo mật giúp bảo vệ chống lại các tác nhân độc hại và các phương pháp xâm nhập. Bạn cũng sẽ tìm hiểu cách sử dụng biện pháp tăng cường bảo mật để giải quyết các thách thức bảo mật đặc biệt do cơ sở hạ tầng đám mây đặt ra.

|  |
| --- |
| **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/networks-and-network-security/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 hướng dẫn 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/networks-and-network-security/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/networks-and-network-security/resources/Cd90m) 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/networks-and-network-security/resources/Cd90m)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.

|  |
| --- |
| **Obtain the Google Cybersecurity Certificate** |

**Nhận Chứng chỉ an ninh mạng của Google**

|  |
| --- |
| To receive your official Google Cybersecurity Certificate, you must:   * Pass all graded assignments in all 8 courses of the certificate program. Each graded assignment is part of a cumulative graded score for the course, and the passing grade for each course is 80%. |

Để nhận Chứng chỉ an ninh mạng chính thức của Google, bạn phải:

* Đạt tất cả các bài tập được chấm điểm trong tất cả 8 khóa học của chương trình cấp chứng chỉ. Mỗi bài tập được chấm điểm là một phần của điểm chấm điểm tích lũy cho khóa học và điểm đậu cho mỗi khóa học là 80%.

|  |
| --- |
| AND **one**of the following:   * Pay the [course certificate fee](https://www.coursera.support/s/article/209818963-Payments-on-Coursera?language=en_US), * Be approved for [Coursera Financial Aid](https://www.coursera.support/s/article/209819033-Apply-for-Financial-Aid-or-a-Scholarship?language=en_US), **or** * Complete the certificate through an educational institution, employer, or agency that's sponsoring your participation. |

VÀ  **một** trong những điều sau đây:

* Tra[lệ phí cấp chứng chỉ khóa học](https://www.coursera.support/s/article/209818963-Payments-on-Coursera?language=en_US),
* Được chấp thuận cho[Hỗ trợ tài chính Coursera](https://www.coursera.support/s/article/209819033-Apply-for-Financial-Aid-or-a-Scholarship?language=en_US),  **hoặc**
* Hoàn thành chứng chỉ thông qua tổ chức giáo dục, người sử dụng lao động hoặc cơ quan tài trợ cho sự tham gia của bạn.

|  |
| --- |
| **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/networks-and-network-security/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. 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 được 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 nhiệm vụ 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/networks-and-network-security/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. 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/networks-and-network-security/supplement/lFqNR/course-3-glossary) 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 thuật ngữ 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/networks-and-network-security/supplement/lFqNR/course-3-glossary)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.   * Click **thumbs-up** for materials that are helpful. * Click **thumbs-down** for materials that are not helpful. |

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.

* Hãy **nhấp vào biểu tượng** thích để xem các 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. Introduction to networks – Giới thiệu về mạng**

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

|  |
| --- |
| Before securing a network, you need to understand the basic design of a network and how it functions. |

Trước khi bảo mật mạng,bạn cần hiểu thiết kế cơ bản của mạng và cách thức hoạt động của mạng.

|  |
| --- |
| In this section of the course, you will learn about the structure of a network, standard networking tools, cloud networks, and the basic framework for organizing communications across a network called the TCP/IP model. |

Trong phần này của khóa học, bạn sẽ tìm hiểu về cấu trúc của mạng,công cụ mạng tiêu chuẩn, mạng đám mây,và khuôn khổ cơ bản chotổ chức thông tin liên lạc qua mạng được gọi là mô hình TCP/IP.

|  |
| --- |
| Securing networks is a big part of a security analyst's responsibilities, so I'm excited to help you understand how to secure your organization's network from threats, risks, and vulnerabilities. |

Bảo mật mạng là một phần trách nhiệm quan trọng của nhà phân tích bảo mật,vì vậy tôi rất vui được giúp bạn hiểu cách bảo mật mạng của tổ chức bạnkhỏi các mối đe dọa, rủi ro và điểm yếu.

|  |
| --- |
| Let's get going! |

Hãy bắt đầu đi!

***2.2. Chris: My path to cybersecurity – Chris: Con đường đến với an ninh mạng của tôi***

|  |
| --- |
| My name is Chris and I'm the Chief Information Security Officer at Google Fiber. We provide high speed Internet to customers across the United States. As the chief information security officer, I'm responsible for making sure that the network stays safe, our customers' data stays safe and that we are supporting law enforcement and others as required. The career path was a long and winding one. My actual first job was working as a butcher at the family grocery store. I eventually ended up with a job in the computer center at college, which is where I learned a lot of my initial computer skills. Then when I graduated from college, I started off as a software developer, designing accounting software for a consulting company supporting the Department of Agriculture. Then I moved on from that to other roles, eventually ending up in one of the first Internet over cable companies. I ran several of their services, email, web services, etc. My stuff kept getting attacked. I fell into cybersecurity because I had to defend the things that I was building. I realized it was fun. I realized that it was a great career opportunity. I've just stuck with that ever since then. When I got into this field, other than a couple of books, there wasn't a lot of training material out there. There were some other people out there that I could ask questions of, and I could get some mentoring from. But as a general rule of thumb, I was on my own. Despite this being a fairly technical field, the most important thing you're going to learn are the connections you're going to make to other people. I made a conscious decision to become actively involved in some of the outside work organizations, the trade associations, the non profits, the meet ups, and other cybersecurity organizations. This enabled me to build the reputation and the relationships so that as my career moved along, people were reaching out to me saying, hey Chris, we have this opportunity, are you interested? Because the cybersecurity industry is so varied, it can seem like there is a tremendous amount you have to learn that there is this huge step that you have to take in order to get into the industry. That can be daunting. But the thing to remember is, once you have that fundamental level of skills and fundamental level of background, there are so many different directions you can go and there's so much opportunity out there. There's this continuous education and curiosity aspect of the job that is so much fun. It means that you are always having the opportunity to learn something new, to change directions and go in new ways because cybersecurity is going to be constantly changing. And that's part of the fun. |

Tên tôi là Chris và tôi làGiám đốc An ninh Thông tin tại Google Fiber.Chúng tôi cung cấp Internet tốc độ caocho khách hàng trên khắp Hoa Kỳ.Với tư cách là giám đốc an ninh thông tin,Tôi chịu trách nhiệm làmchắc chắn rằng mạng vẫn an toàn,dữ liệu của khách hàng luôn được an toàn và chúng tôiđang hỗ trợ việc thực thi pháp luật và những người khác theo yêu cầu.Con đường sự nghiệp là một con đường dài và quanh co.Công việc thực sự đầu tiên của tôi là làm việc nhưmột người bán thịt ở cửa hàng tạp hóa của gia đình.Cuối cùng tôi đã kết thúc vớimột công việc ở trung tâm máy tính ở trường đại học,đó là nơi tôi đã họcrất nhiều kỹ năng máy tính ban đầu của tôi.Rồi khi tôi tốt nghiệp đại học,Tôi khởi đầu là một nhà phát triển phần mềm,thiết kế phần mềm kế toán chomột công ty tư vấn hỗ trợSở Nông nghiệp.Sau đó tôi chuyển từ vai trò đó sang vai trò khác,cuối cùng kết thúc ở một trongInternet qua cáp đầu tiên của các công ty.Tôi đã điều hành một số dịch vụ của họ,email, dịch vụ web, v.v.Đồ của tôi liên tục bị tấn công.Tôi rơi vào tình trạng an ninh mạngbởi vì tôi phải bảo vệ những thứ tôi đang xây dựng.Tôi nhận ra điều đó thật vui.Tôi nhận ra rằng đó là một cơ hội nghề nghiệp tuyệt vời.Tôi đã bị mắc kẹt với điều đó kể từ đó.Khi tôi bước vào lĩnh vực này,ngoài vài cuốn sách,không có nhiều tài liệu đào tạo ở đó.Ngoài kia có một số người khác mà tôicó thể đặt câu hỏi và tôi có thể nhận được một số lời khuyên từ.Nhưng theo nguyên tắc chung, tôi chỉ có một mình.Mặc dù đây là một lĩnh vực khá kỹ thuật,điều quan trọng nhất bạn sẽ làmhọc là những kết nốibạn sẽ làm cho người khác.Tôi đã đưa ra một quyết định có ý thức để trở nên tích cựctham gia vào một số tổ chức công việc bên ngoài,các hiệp hội thương mại, các tổ chức phi lợi nhuận,những cuộc gặp gỡ,và các tổ chức an ninh mạng khác.Điều này đã giúp tôi xây dựng được danh tiếng vàcác mối quan hệ để khi sự nghiệp của tôi tiến triển,mọi người liên hệ với tôi và nói, này Chris,chúng tôi có cơ hội này, bạn có quan tâm không?Bởi vì ngành an ninh mạng rất đa dạng,có vẻ như cóbạn phải học rất nhiều rằng cóbước tiến lớn này mà bạn cóphải thực hiện để có thể gia nhập ngành.Điều đó có thể gây khó khăn.Nhưng điều cần nhớ là,một khi bạn có trình độ cơ bản đóvề kỹ năng và trình độ nền tảng cơ bản,có rất nhiều hướng khác nhau mà bạn có thểđi và có rất nhiều cơ hội ngoài kia.Có sự giáo dục liên tục này vàkhía cạnh tò mò của công việc đó là rất nhiều niềm vui.Nó có nghĩa là bạn luôn luôncó cơ hội học hỏi điều gì đó mới mẻ,để thay đổi hướng đi và đi theo những con đường mới bởi vìan ninh mạng sẽthay đổi liên tục. Và đó là một phần của niềm vui.

***2.3. What are networks? – Mạng là gì?***

|  |
| --- |
| Welcome! Before you can understand the importance of securing a network, you need to know what a network is. |

Chào mừng! Trước khi bạn có thể hiểu được tầm quan trọng của việc bảo mật mạng,bạn cần biết mạng là gì.

|  |
| --- |
| A network is a group of connected devices. At home, the devices connected to your network might be your laptop, cell phones, and smart devices, like your refrigerator or air conditioner. In an office, devices like workstations, printers, and servers all connect to the network. The devices on a network can communicate with each other over network cables, or wireless connections. Networks in your home and office can communicate with networks in other locations, and the devices on them. |

Mạng là một nhóm các thiết bị được kết nối.Ở nhà, các thiết bị kết nối với mạng của bạn có thể là máy tính xách tay,điện thoại di động và các thiết bị thông minh, như tủ lạnh hoặc máy điều hòa không khí.Trong văn phòng, các thiết bị như máy trạm, máy in vàtất cả các máy chủ đều kết nối với mạng.Các thiết bị trên mạng có thể liên lạc với nhau qua cáp mạng hoặckết nối không dây.Mạng ở nhà và văn phòng của bạn có thể giao tiếp với mạng ở các địa điểm khác,và các thiết bị trên đó.

|  |
| --- |
| Devices need to find each other on a network to establish communications. These devices will use unique addresses, or identifiers, to locate each other. The addresses will ensure that communications happens with the right device. These are called the IP and MAC addresses. |

Các thiết bị cần tìm thấy nhau trên mạng để thiết lập liên lạc.Các thiết bị này sẽ sử dụng địa chỉ hoặc số nhận dạng duy nhất để xác định vị trí của nhau.Các địa chỉ sẽ đảm bảo rằng việc liên lạc diễn ra vớithiết bị phù hợp.Chúng được gọi là địa chỉ IP và MAC.

|  |
| --- |
| Devices can communicate on two types of networks: a local area network, also known as a LAN, and a wide area network, also known as a WAN. |

Các thiết bị có thể giao tiếp trên hai loại mạng:mạng cục bộ hay còn gọi là mạng LAN,và mạng diện rộng, còn được gọi là WAN.

|  |
| --- |
| A local area network, or LAN, spans a small area like an office building, a school, or a home. For example, when a personal device like your cell phone or tablet connects to the WIFI in your house, they form a LAN. The LAN then connects to the internet. |

Mạng cục bộ hoặc mạng LAN,trải rộng trên một khu vực nhỏ như tòa nhà văn phòng, trường học hoặc nhà riêng.Ví dụ: khi một thiết bị cá nhân như điện thoại di động hoặc máy tính bảng của bạnkết nối với WIFI trong nhà bạn, chúng tạo thành mạng LAN.Mạng LAN sau đó kết nối với internet.

|  |
| --- |
| A wide area network or WAN spans a large geographical area like a city, state, or country. You can think of the internet as one big WAN. An employee of a company in San Francisco can communicate and share resources with another employee in Dublin, Ireland over the WAN. |

Mạng diện rộng hoặc WAN trải rộng trên một khu vực địa lý rộng lớn như thành phố, tiểu bang,hoặc quốc gia.Bạn có thể coi Internet như một mạng WAN lớn.Một nhân viên của một công ty ở San Francisco có thể giao tiếp vàchia sẻ tài nguyên với một nhân viên khác ở Dublin, Ireland qua mạng WAN.

|  |
| --- |
| Now that you've learned about the structure and types of networks, meet me in an upcoming video to learn about the devices that connect to them. |

Bây giờ bạn đã tìm hiểu về cấu trúc và các loại mạng,gặp tôi trong video sắp tới để tìm hiểu về các thiết bị kết nối với chúng.

***2.4. Tina: Working in network security – Tina: Làm việc trong lĩnh vực an ninh mạng***

|  |
| --- |
| My name is Tina and I'm a software engineer at Google. As a software engineer, I work on an internal tool that serves the security engineers and network engineers at Google. Network security is important because we want to make sure that our network systems are safe and resilient to be able to defend against malicious hackers, and that we have the ability to protect our user data. Working with network security allows to see the overview of the whole company's network systems, which is super cool. My favorite part of my job is the impact I get to have on the community that I serve at Google. I would say most of my day is a lot of coding, design, talking to security teams and network teams on their priorities and their blockers and being able to come up with a solution. There are often going to be requests that come from network teams and security teams that have specific requirements on certain platforms or on a feature that they need in one of the network policies, and usually we would escalate that and try to work on a fix for that. One piece of advice I would give for someone who wants to take on the cybersecurity journey is to be able to always keep learning and be curious about how things work. Because security is an ever changing field, cybersecurity is definitely a team sport. Everybody has something to contribute, and especially on cybersecurity problems, there can be a lot of possibilities and a lot of different solutions to one problem. It's always great to be able to have people to brainstorm with and to track down issues together because things can get very complex sometimes, but it's also a fun process to be able to work on things together. |

Tên tôi là Tina và tôi là kỹ sư phần mềm tại Google.Là một kỹ sư phần mềm,Tôi làm việc trên một công cụ nội bộphục vụ các kỹ sư bảo mậtvà các kỹ sư mạng tại Google.An ninh mạng rất quan trọng vì chúng tamuốn đảm bảo rằng hệ thống mạng của chúng tôian toàn và kiên cường để có thểđể bảo vệ chống lại các tin tặc nguy hiểm,và rằng chúng tôi có khả năng bảo vệ dữ liệu người dùng của mình.Làm việc với an ninh mạng cho phép xemtổng quan về hệ thống mạng toàn công ty,đó là siêu mát mẻ.Phần yêu thích nhất trong công việc của tôi là tác động mà tôi nhận đượccó mặt trong cộng đồng mà tôi phục vụ tại Google.Tôi có thể nói rằng phần lớn thời gian trong ngày của tôi dành cho việc viết mã, thiết kế,nói chuyện với các nhóm bảo mật và nhóm mạng trênnhững ưu tiên của họ và những rào cản của họvà có khả năng đưa ra giải pháp.Thường sẽ cóyêu cầu đến từ các nhóm mạng vàcác nhóm bảo mật có yêu cầu cụ thể vềnền tảng nhất định hoặc trênmột tính năng mà họ cần ở một trong các chính sách mạng,và thông thường chúng tôi sẽ báo cáo điều đóvà cố gắng tìm cách khắc phục điều đó.Một lời khuyên tôi sẽ đưa radành cho ai đó muốn đảm nhậnhành trình an ninh mạng là để có thểluôn luôn học hỏi vàtò mò về cách mọi thứ hoạt động.Bởi vì bảo mật là một lĩnh vực luôn thay đổi,an ninh mạng chắc chắn là một môn thể thao đồng đội.Mọi người đều có điều gì đó để đóng góp,và đặc biệt là về các vấn đề an ninh mạng,có thể có rất nhiều khả năngvà rất nhiều giải pháp khác nhau cho một vấn đề.Thật tuyệt vời khi có thểđể mọi người động não cùng và đểcùng nhau theo dõi các vấn đề vì mọi thứđôi khi có thể trở nên rất phức tạp,nhưng đó cũng là một quá trình thú vịcó thể làm việc cùng nhau.

***2.5. Emmanuel: Useful skills for network security – Emmanuel: Những kỹ năng hữu ích cho an ninh mạng***

|  |
| --- |
| My name is Emmanuel and I am an offensive security engineer at Google. For offensive security, my job is to simulate adversaries and threats that are targeting various companies and I look at defending how we can protect Google's infrastructure. I make it harder to hack Google by actually hacking Google. The technical skills that I use is a lot of programming, as well as learning about operational and platform security. Knowing how these computers work, what is under the hood, and understanding the components that create this infrastructure. An entry-level cybersecurity analyst would look at using command lines, log parsing, and network traffic analysis in their everyday scope of work. Command line allows you to interact with various levels of your operating system, whether it's the low-level things like the memory and the kernel, or if it's high-level things like the applications and the programs that you're running on your computer. With log parsing, they're going to be times where you may need to figure out and debug what is going on in your program or application and these logs are there to help you and support you in finding the root issue and then resolve it from there. With this network traffic analysis, there may be times where you need to figure out why is my Internet going slow? Why is traffic not being routed to the appropriate destination? What can I do to ensure that my network is up and running? Network traffic analysis is looking at network across various application and network layers and seeing what that traffic is doing, how we can secure that traffic, as well as identify any vulnerabilities and concerns. In the contexts for me, for security, I look at: are passwords being leaked in the traffic that's being sent across the network? Are infrastructures being secured? Are firewalls being readily configured and configured safely? One skill that has continued to grow with me in my current role has been communicating effectively to product teams, engineers, and identifying an issue that is influencing or affecting the business, and communicating to those teams effectively to fix it. Being able to take on these many hats and explain things with the right business approach to things to ensure that the issues that I do find in my work are identified but they are also fixed. My advice to folks who are taking this certificate would take things apart, feel uncomfortable, learn and grow and find opportunities to learn and understand how things work and that skill set will benefit you for the remainder of your journey. |

Tên tôi là Emmanuel và tôi làmột kỹ sư bảo mật tấn công tại Google.Để đảm bảo an ninh tấn công,công việc của tôi là mô phỏng kẻ thù và các mối đe dọađang nhắm mục tiêu vào nhiều công ty khác nhau và tôinhìn cách phòng thủ thế nàochúng tôi có thể bảo vệ cơ sở hạ tầng của Google.Tôi làm cho việc hack khó khăn hơnGoogle bằng cách thực sự hack Google.Kỹ năng kỹ thuật mà tôi sử dụng chủ yếu là lập trình,cũng như tìm hiểu vềbảo mật hoạt động và nền tảng.Biết cách các máy tính này hoạt động,bên dưới mui xe có gì,và tìm hiểu các thành phầntạo ra cơ sở hạ tầng này.Một nhà phân tích an ninh mạng cấp độ đầu vào sẽnhìn vào việc sử dụng dòng lệnh,phân tích nhật ký và lưu lượng mạngphân tích trong phạm vi công việc hàng ngày của họ.Dòng lệnh cho phép bạn tương tácvới nhiều cấp độ khác nhau của hệ điều hành của bạn,cho dù đó là những thứ cấp thấpnhư bộ nhớ và kernel,hoặc nếu đó là những thứ cấp cao nhưcác ứng dụng và chương trìnhmà bạn đang chạy trên máy tính của mình.Với việc phân tích cú pháp nhật ký, chúng sẽnhững thời điểm mà bạn có thể cần phải tính toánout và gỡ lỗi những gì đang diễn ra trong chương trình của bạnhoặc ứng dụng và những nhật ký này làở đó để giúp đỡ bạn và hỗ trợ bạn trongtìm ra vấn đề gốc rễ và sau đó giải quyết nó từ đó.Với phân tích lưu lượng mạng này,có thể có những lúc bạn cần phải tìm hiểutại sao Internet của tôi lại chậm?Tại sao giao thông khôngđược chuyển đến đích thích hợp?Tôi có thể làm gì đểđảm bảo rằng mạng của tôi đang hoạt động?Phân tích lưu lượng mạng đang xem xét mạng trêncác lớp ứng dụng và mạng khác nhauvà xem lưu lượng truy cập đó đang làm gì,cách chúng tôi có thể đảm bảo lưu lượng truy cập đó,cũng như xác định bất kỳ lỗ hổng và mối lo ngại nào.Trong bối cảnh đối với tôi, vì sự an toàn,Tôi nhìn vào: mật khẩu đang đượcbị rò rỉ trong giao thông đóđược gửi qua mạng?Cơ sở hạ tầng có được đảm bảo không?Tường lửa có sẵn sàng khôngđược cấu hình và cấu hình an toàn?Một kỹ năng đã tiếp tụccùng tôi phát triển trong vai trò hiện tại của tôiđã giao tiếp hiệu quảtới các nhóm sản phẩm, kỹ sư,và xác định một vấn đề đang ảnh hưởng hoặcảnh hưởng đến hoạt động kinh doanh vàliên lạc với các nhóm đó một cách hiệu quả để khắc phục nó.Có thể đội nhiều chiếc mũ nàyvà giải thích mọi việc bằng cách tiếp cận kinh doanh phù hợp vớinhững điều để đảm bảo rằng những vấn đề mà tôitìm thấy trong công việc của tôi làđược xác định nhưng chúng cũng được cố định.Lời khuyên của tôi dành cho những người đang dùngchứng chỉ này sẽ mấtmọi thứ xa cách, cảm thấy không thoải mái,học hỏi và phát triển và tìm thấycơ hội để học hỏi và hiểu cáchmọi thứ hoạt động và bộ kỹ năng đó sẽmang lại lợi ích cho bạn trong suốt chặng đường còn lại.

***2.6. Network tools – Công cụ mạng***

|  |
| --- |
| In this video, you'll learn about the common devices that make up a network. Let's get started. |

Trong video này, bạn sẽ tìm hiểu vềcác thiết bị phổ biến tạo nênmột mạng lưới. Bắt đầu nào.

|  |
| --- |
| A hub is a network device that broadcasts information to every device on the network. Think of a hub like a radio tower that broadcasts a signal to any radio tuned to the correct frequency. |

Hub là một thiết bị mạngphát thông tin tới mọi thiết bị trên mạng.Hãy nghĩ về một trung tâm giống như một tháp radio phát sóngmột tín hiệu tới bất kỳ đài phát thanh nào được điều chỉnh theo tần số chính xác.

|  |
| --- |
| Another network device is a switch. A switch makes connections between specific devices on a network by sending and receiving data between them. A switch is more intelligent than a hub. It only passes data to the intended destination. This makes switches more secure than hubs, and enables them to control the flow of traffic and improve network performance. |

Một thiết bị mạng khác là switch.Một switch tạo kết nối giữacác thiết bị cụ thể trên mạng bằng cách gửivà nhận dữ liệu giữa chúng.Switch thông minh hơn hub.Nó chỉ truyền dữ liệu đến đích dự định.Điều này làm cho thiết bị chuyển mạch an toàn hơn trung tâm,và cho phép họ kiểm soát luồng giao thôngvà cải thiện hiệu suất mạng.

|  |
| --- |
| Another device that we'll discuss is a router. A router is a network device that connects multiple networks together. |

Một thiết bị khác mà chúng ta sẽ thảo luận là bộ định tuyến.Bộ định tuyến là một thiết bị mạng cókết nối nhiều mạng với nhau.

|  |
| --- |
| For example, if a computer in one network wants to send information to a tablet on another network, then the information will be transferred as follows: First, the information travels from the computer to the router. Then, the router reads the destination address, and forwards the data to the intended network's router. Finally, the receiving router directs that information to the tablet. |

Ví dụ: nếu một máy tính trong một mạngmuốn gửi thông tin đến máy tính bảng trên mạng khác,thì thông tin sẽ được chuyển như sau:Đầu tiên, thông tin được truyền đitừ máy tính đến bộ định tuyến.Sau đó, bộ định tuyến đọc địa chỉ đích,và chuyển tiếp dữ liệu đến bộ định tuyến của mạng dự định.Cuối cùng, bộ định tuyến nhậnhướng thông tin đó đến máy tính bảng.

|  |
| --- |
| Finally, let's discuss modems. A modem is a device that connects your router to the internet, and brings internet access to the LAN. |

Cuối cùng, hãy thảo luận về modem.Modem là thiết bị kết nốibộ định tuyến của bạn với internet,và mang lại khả năng truy cập internet vào mạng LAN.

|  |
| --- |
| For example, if a computer from one network wants to send information to a device on a network in a different geographic location, it would be transferred as follows: The computer would send information to the router, and the router would then transfer the information through the modem to the internet. The intended recipient's modem receives the information, and transfers it to the router. Finally, the recipient's router forwards that information to the destination device. |

Ví dụ: nếu một máy tính từ một mạng muốn gửithông tin tới một thiết bị trên mạngở một vị trí địa lý khác,nó sẽ được chuyển như sau:Máy tính sẽ gửi thông tin đến bộ định tuyến,và bộ định tuyến sau đó sẽ chuyểnthông tin qua modem tới internet.Modem của người nhận sẽ nhận được thông tin,và chuyển nó đến bộ định tuyến.Cuối cùng, bộ định tuyến của người nhận sẽ chuyển tiếpthông tin đó đến thiết bị đích.

|  |
| --- |
| Network tools such as hubs, switches, routers, and modems are physical devices. However, many functions performed by these physical devices can be completed by virtualization tools. |

Các công cụ mạng như hub, switch,bộ định tuyến và modem là các thiết bị vật lý.Tuy nhiên, nhiều chức năng được thực hiện bởinhững thiết bị vật lý này có thểhoàn thành bằng các công cụ ảo hóa.

|  |
| --- |
| Virtualization tools are pieces of software that perform network operations. Virtualization tools carry out operations that would normally be completed by a hub, switch, router, or modem, and they are offered by Cloud service providers. These tools provide opportunities for cost savings and scalability. You'll learn more about them later in the certificate program. |

Các công cụ ảo hóa là một phần củaphần mềm thực hiện các hoạt động mạng.Công cụ ảo hóa thực hiện các hoạt độngviệc đó thường được hoàn thành bởi một hub, switch,bộ định tuyến hoặc modem,và chúng được cung cấp bởi các nhà cung cấp dịch vụ Đám mây.Những công cụ này tạo cơ hội chotiết kiệm chi phí và khả năng mở rộng.Bạn sẽ tìm hiểu thêm về họ sautrong chương trình chứng chỉ.

|  |
| --- |
| Now you've explored some common devices that make up a network. Coming up, you're going to learn more about cloud computing, and how networks can be designed using cloud services. |

Bây giờ bạn đã khám phá một số thiết bị phổ biếntạo nên một mạng lưới. Sắp diễn ra,bạn sẽ tìm hiểu thêm về điện toán đám mây,và cách mạng có thể được thiết kế bằng dịch vụ đám mây.

***2.7. Network components, devices, and diagrams – Các thành phần, thiết bị và sơ đồ mạng***

|  |
| --- |
| **Network components, devices, and diagrams** |

**Các thành phần, thiết bị và sơ đồ mạng**

|  |
| --- |
| In this reading, you will review network devices and connections and investigate a simple network diagram similar to those used every day by network security professionals. |

Trong bài đọc này, bạn sẽ xem xét các thiết bị và kết nối mạng cũng như khảo sát một sơ đồ mạng đơn giản tương tự như sơ đồ được các chuyên gia an ninh mạng sử dụng hàng ngày.

|  |
| --- |
| A foundational understanding of network architecture, sometimes referred to as network design, will help you as you learn about security vulnerabilities inherent in all networks and how malicious actors attempt to exploit them. Let’s get started! |

Sự hiểu biết cơ bản về kiến ​​trúc mạng, đôi khi được gọi là thiết kế mạng, sẽ giúp bạn khi bạn tìm hiểu về các lỗ hổng bảo mật vốn có trong tất cả các mạng và cách các tác nhân độc hại cố gắng khai thác chúng. Bắt đầu nào!

|  |
| --- |
| **Network devices** |

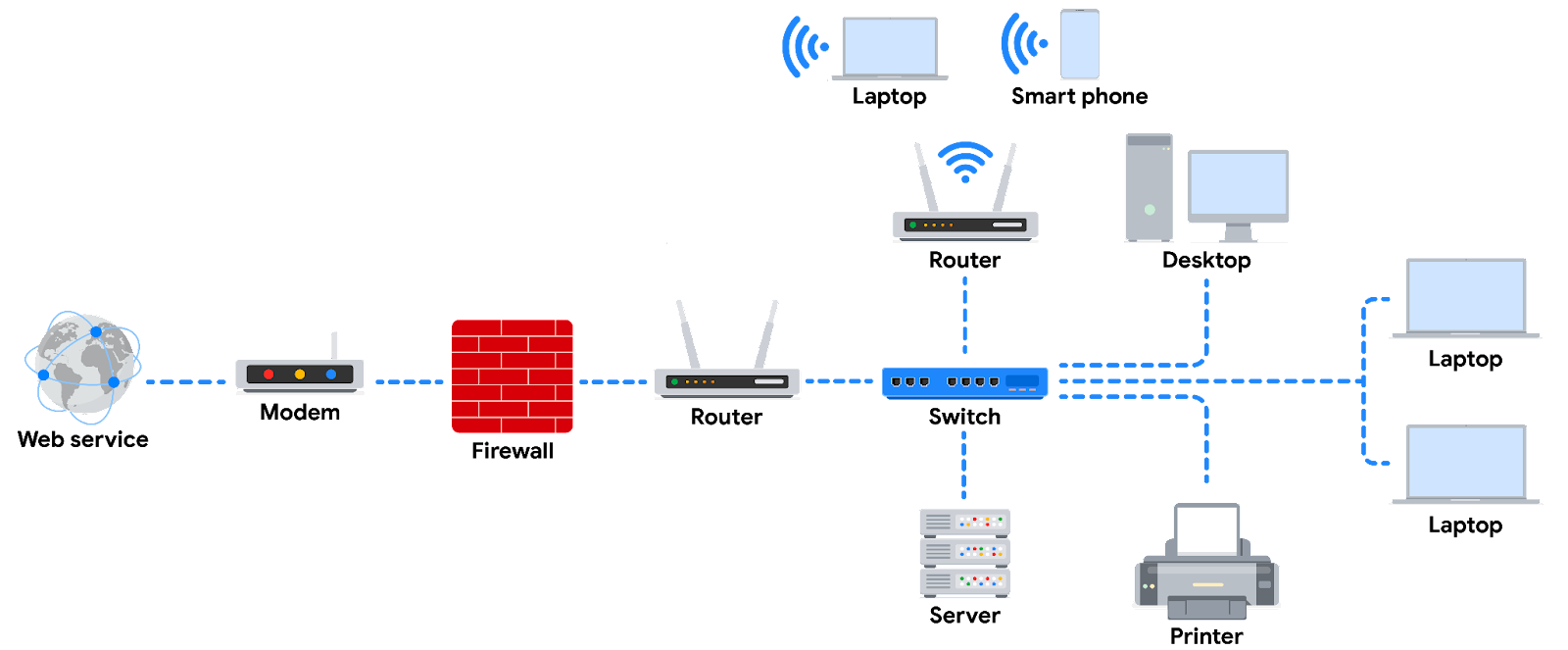
**Thiết bị mạng**

|  |
| --- |
| Network devices maintain information and services for users of a network. These devices connect over wired and wireless connections. After establishing a connection to the network, the devices send data packets. The data packets provide information about the source and the destination of the data.  This is how the information is sent and received via different devices on a network. |

Các thiết bị mạng duy trì thông tin và dịch vụ cho người dùng mạng. Các thiết bị này kết nối qua kết nối có dây và không dây. Sau khi thiết lập kết nối với mạng, các thiết bị sẽ gửi các gói dữ liệu. Các gói dữ liệu cung cấp thông tin về nguồn và đích của dữ liệu. Đây là cách thông tin được gửi và nhận qua các thiết bị khác nhau trên mạng.

|  |
| --- |
| The network is the overall infrastructure that allows devices to communicate with each other. Network devices are specialized vehicles like routers and switches that manage what is being sent and received over the network. Additionally, devices like computers and phones connect to the network via network devices. |

Mạng là cơ sở hạ tầng tổng thể cho phép các thiết bị giao tiếp với nhau. Thiết bị mạng là phương tiện chuyên dụng như bộ định tuyến và bộ chuyển mạch quản lý những gì được gửi và nhận qua mạng. Ngoài ra, các thiết bị như máy tính và điện thoại kết nối với mạng thông qua các thiết bị mạng.



|  |
| --- |
| **Note:** In this diagram, a **router** connects to the internet through a **modem**, which is provided by your internet service provider (ISP). The firewall is a security device that monitors incoming and outgoing traffic on your network. The router then directs traffic to the devices on your home network, which can include computers, laptops, smartphones, tablets, printers, and other devices. You can imagine here that the server is a file server. All devices on this network can access the files in this **server**. This diagram also includes a **switch** which is an optional device that can be used to connect more devices to your network by providing additional ports and Ethernet connections. Additionally, there are 2 routers connected to the switch here for load balancing purposes which will improve the performance of the network. |

**Lưu ý:** Trong sơ đồ này, **bộ định tuyến** kết nối với Internet thông qua **modem** do nhà cung cấp dịch vụ Internet (ISP) của bạn cung cấp. Tường lửa là một thiết bị bảo mật giám sát lưu lượng truy cập vào và ra trên mạng của bạn. Sau đó, bộ định tuyến sẽ hướng lưu lượng truy cập đến các thiết bị trên mạng gia đình của bạn, có thể bao gồm máy tính, máy tính xách tay, điện thoại thông minh, máy tính bảng, máy in và các thiết bị khác. Bạn có thể tưởng tượng ở đây máy chủ là một máy chủ tập tin. Tất cả các thiết bị trên mạng này có thể truy cập các tập tin trong **máy chủ** này . Sơ đồ này cũng bao gồm một **bộ chuyển mạch** là một thiết bị tùy chọn có thể được sử dụng để kết nối nhiều thiết bị hơn với mạng của bạn bằng cách cung cấp thêm cổng và kết nối Ethernet. Ngoài ra, có 2 bộ định tuyến được kết nối với bộ chuyển mạch ở đây nhằm mục đích cân bằng tải, giúp cải thiện hiệu suất của mạng.

|  |
| --- |
| **Devices and desktop computers** |

**Thiết bị và máy tính để bàn**

|  |
| --- |
| Most internet users are familiar with everyday devices, such as personal computers, laptops, mobile phones, and tablets. Each device and desktop computer has a unique MAC address and IP address, which identify it on the network. They also have a network interface that sends and receives data packets. These devices can connect to the network via a hard wire or a wireless connection. |

Hầu hết người dùng internet đều quen thuộc với các thiết bị hàng ngày, chẳng hạn như máy tính cá nhân, máy tính xách tay, điện thoại di động và máy tính bảng. Mỗi thiết bị và máy tính để bàn có một địa chỉ MAC và địa chỉ IP duy nhất xác định nó trên mạng. Họ cũng có giao diện mạng để gửi và nhận các gói dữ liệu. Các thiết bị này có thể kết nối với mạng thông qua dây cứng hoặc kết nối không dây.

|  |
| --- |
| **Firewalls** |

**Tường lửa**

|  |
| --- |
| A **firewall** is a network security device that monitors traffic to or from your network. It is like your first line of defense. Firewalls can also restrict specific incoming and outgoing network traffic. The organization configures the security rules of the firewall. Firewalls often reside between the secured and controlled internal network and the untrusted network resources outside the organization, such as the internet. Remember, though, firewalls are just one line of defense in the cybersecurity landscape. |

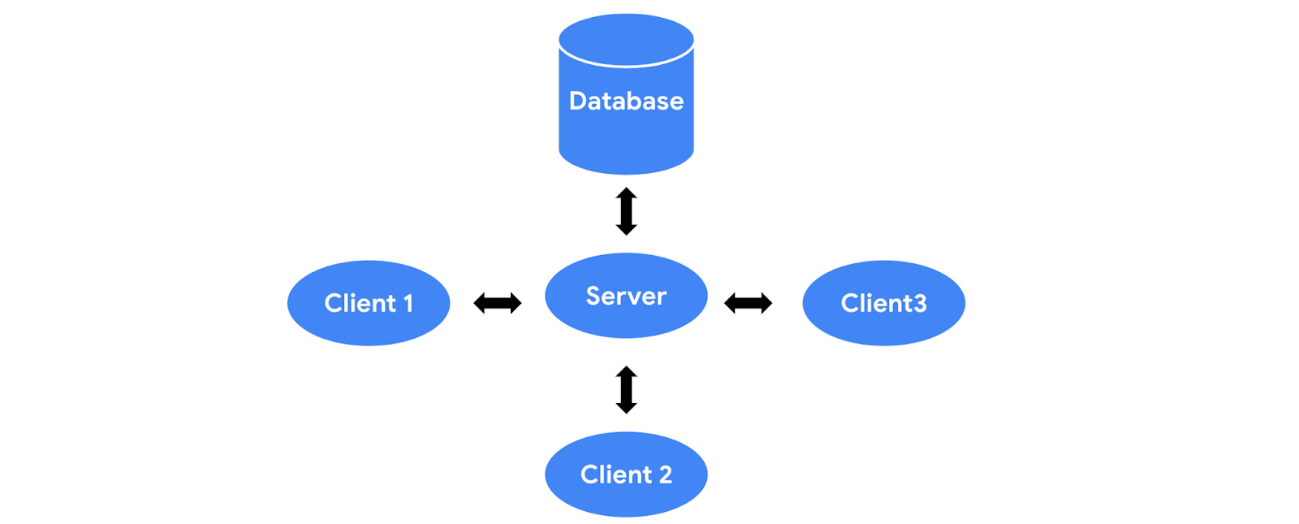
**Tường** **lửa** là một thiết bị bảo mật mạng giám sát lưu lượng đến hoặc đi từ mạng của bạn. Nó giống như tuyến phòng thủ đầu tiên của bạn. Tường lửa cũng có thể hạn chế lưu lượng mạng đến và đi cụ thể. Tổ chức cấu hình các quy tắc bảo mật của tường lửa. Tường lửa thường nằm giữa mạng nội bộ được bảo mật và kiểm soát cũng như các tài nguyên mạng không đáng tin cậy bên ngoài tổ chức, chẳng hạn như internet. Tuy nhiên, hãy nhớ rằng tường lửa chỉ là một tuyến phòng thủ trong bối cảnh an ninh mạng.

|  |
| --- |
| **Servers** |

**Máy chủ**

|  |
| --- |
| **Servers** provide information and services for devices like computers, smart home devices, and smartphones on the network. The devices that connect to a server are called clients. The following graphic outlines this model, which is called the client-server model. In this model, clients send requests to the server for information and services. The server performs the requests for the clients. Common examples include DNS servers that perform domain name lookups for internet sites, file servers that store and retrieve files from a database, and corporate mail servers that organize mail for a company. |

**Máy chủ** cung cấp thông tin và dịch vụ cho các thiết bị như máy tính, thiết bị nhà thông minh và điện thoại thông minh trên mạng. Các thiết bị kết nối với máy chủ được gọi là máy khách. Đồ họa sau đây phác thảo mô hình này, được gọi là mô hình máy khách-máy chủ. Trong mô hình này, khách hàng gửi yêu cầu đến máy chủ để lấy thông tin và dịch vụ. Server thực hiện các yêu cầu cho client. Các ví dụ phổ biến bao gồm máy chủ DNS thực hiện tra cứu tên miền cho các trang internet, máy chủ tệp lưu trữ và truy xuất tệp từ cơ sở dữ liệu và máy chủ thư công ty sắp xếp thư cho một công ty.



|  |
| --- |
| **Hubs and switches** |

**Hub và switch**

|  |
| --- |
| Hubs and switches both direct traffic on a local network. A **hub** is a device that provides a common point of connection for all devices directly connected to it. Hubs additionally repeat all information out to all ports. From a security perspective, this makes hubs vulnerable to eavesdropping. For this reason, hubs are not used as often on modern networks; most organizations use switches instead. Hubs are more commonly used for a limited network setup like a home office. |

Hub và switch đều có lưu lượng truy cập trực tiếp trên mạng cục bộ. Hub là một **thiết** bị cung cấp điểm kết nối chung cho tất cả các thiết bị được kết nối trực tiếp với nó. Các trung tâm cũng lặp lại tất cả thông tin tới tất cả các cổng. Từ góc độ bảo mật, điều này làm cho các trung tâm dễ bị nghe lén. Vì lý do này, các hub không được sử dụng thường xuyên trên các mạng hiện đại; thay vào đó hầu hết các tổ chức đều sử dụng thiết bị chuyển mạch. Hub được sử dụng phổ biến hơn để thiết lập mạng hạn chế như văn phòng tại nhà.

|  |
| --- |
| Switches are the preferred choice for most networks. A **switch** forwards packets between devices directly connected to it. They analyze the destination address of each data packet and send it to the intended device. Switches maintain a MAC address table that matches MAC addresses of devices on the network to port numbers on the switch and forwards incoming data packets according to the destination MAC address. Switches are a part of the data link layer in the TCP/IP model. Overall, switches improve performance and security. |

Switch là lựa chọn ưu tiên cho hầu hết các mạng. Một **switch** chuyển tiếp các gói tin giữa các thiết bị được kết nối trực tiếp với nó. Họ phân tích địa chỉ đích của từng gói dữ liệu và gửi nó đến thiết bị dự định. Bộ chuyển mạch duy trì bảng địa chỉ MAC khớp địa chỉ MAC của thiết bị trên mạng với số cổng trên bộ chuyển mạch và chuyển tiếp các gói dữ liệu đến theo địa chỉ MAC đích. Switch là một phần của lớp liên kết dữ liệu trong mô hình TCP/IP. Nhìn chung, các thiết bị chuyển mạch cải thiện hiệu suất và tính bảo mật.

|  |
| --- |
| **Routers** |

**Bộ định tuyến**

|  |
| --- |
| **Routers** connect networks and direct traffic, based on the IP address of the destination network. Routers allow devices on different networks to communicate with each other. In the TCP/IP model, routers are a part of the network layer. The IP address of the destination network is contained in the IP header. The router reads the IP header information and forwards the packet to the next router on the path to the destination. This continues until the packet reaches the destination network. Routers can also include a firewall feature that allows or blocks incoming traffic based on information in the transmission. This stops malicious traffic from entering the private network and damaging the local area network. |

**Bộ định tuyến** kết nối các mạng và lưu lượng truy cập trực tiếp, dựa trên địa chỉ IP của mạng đích. Bộ định tuyến cho phép các thiết bị trên các mạng khác nhau liên lạc với nhau. Trong mô hình TCP/IP, bộ định tuyến là một phần của lớp mạng. Địa chỉ IP của mạng đích được chứa trong tiêu đề IP. Bộ định tuyến đọc thông tin tiêu đề IP và chuyển tiếp gói đến bộ định tuyến tiếp theo trên đường dẫn đến đích. Điều này tiếp tục cho đến khi gói đến mạng đích. Bộ định tuyến cũng có thể bao gồm tính năng tường lửa cho phép hoặc chặn lưu lượng truy cập đến dựa trên thông tin trong đường truyền. Điều này ngăn chặn lưu lượng truy cập độc hại xâm nhập vào mạng riêng và làm hỏng mạng cục bộ.

|  |
| --- |
| **Modems and wireless access points** |

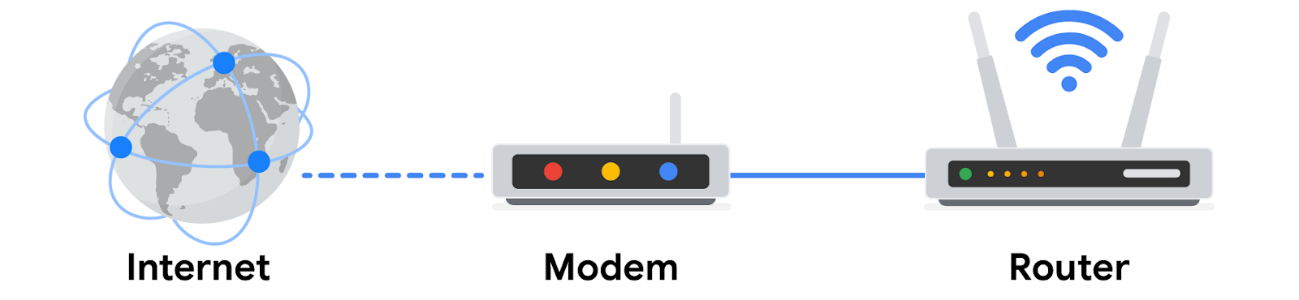
**Modem và điểm truy cập không dây**

|  |
| --- |
| **Modems** usually connect your home or office with an internet service provider (ISP). ISPs provide internet connectivity via telephone lines or coaxial cables. Modems receive transmissions or digital signals from the internet and translate them into analog signals that can travel through the physical connection provided by your ISP. Usually, modems connect to a router that takes the decoded transmissions and sends them on to the local network. |

**Modem** thường kết nối nhà hoặc văn phòng của bạn với nhà cung cấp dịch vụ internet (ISP). ISP cung cấp kết nối internet thông qua đường dây điện thoại hoặc cáp đồng trục. Modem nhận tín hiệu truyền hoặc tín hiệu số từ internet và chuyển chúng thành tín hiệu tương tự có thể truyền qua kết nối vật lý do ISP của bạn cung cấp. Thông thường, modem kết nối với bộ định tuyến để nhận các đường truyền được giải mã và gửi chúng tới mạng cục bộ.

|  |
| --- |
| **Note:** Enterprise networks used by large organizations to connect their users and devices often use other broadband technologies to handle high-volume traffic, instead of using a modem. |

**Lưu ý:** Mạng doanh nghiệp được các tổ chức lớn sử dụng để kết nối người dùng và thiết bị của họ thường sử dụng các công nghệ băng thông rộng khác để xử lý lưu lượng truy cập lớn thay vì sử dụng modem.

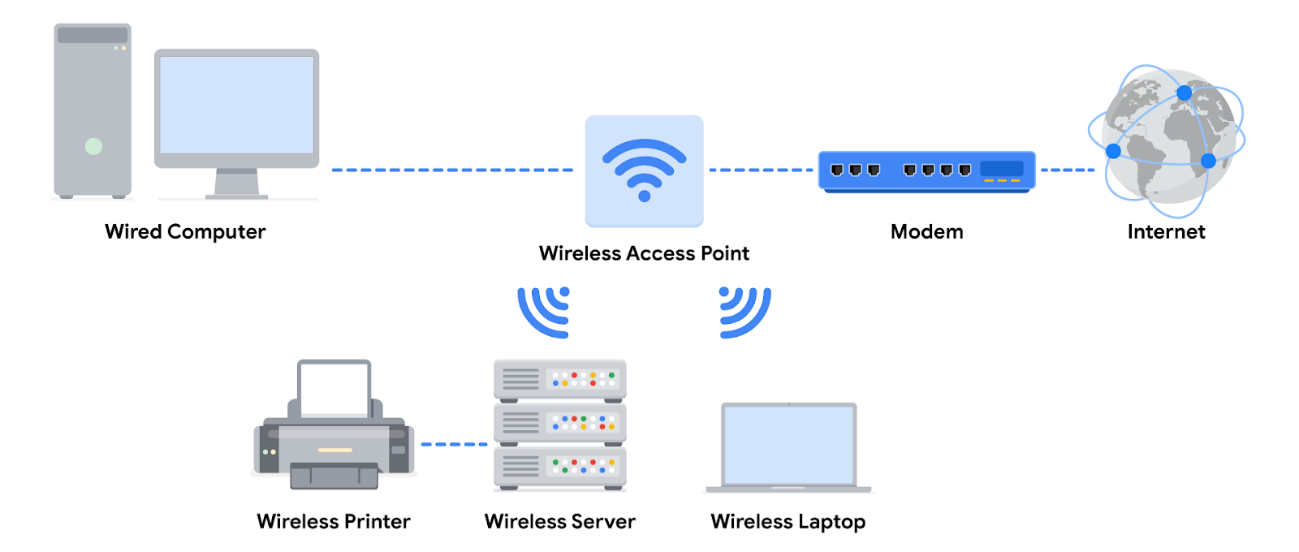


|  |
| --- |
| **Wireless access point** |

**Điểm truy cập không dây**

|  |
| --- |
| A **wireless access point** sends and receives digital signals over radio waves creating a wireless network. Devices with wireless adapters connect to the access point using Wi-Fi. **Wi-Fi** refers to a set of standards that are used by network devices to communicate wirelessly. Wireless access points and the devices connected to them use Wi-Fi protocols to send data through radio waves where they are sent to routers and switches and directed along the path to their final destination. |

**Điểm** **truy cập không dây** gửi và nhận tín hiệu số qua sóng vô tuyến tạo ra mạng không dây. Các thiết bị có bộ điều hợp không dây kết nối với điểm truy cập bằng Wi-Fi. **Wi-Fi** đề cập đến một bộ tiêu chuẩn được các thiết bị mạng sử dụng để liên lạc không dây. Các điểm truy cập không dây và các thiết bị được kết nối với chúng sử dụng giao thức Wi-Fi để gửi dữ liệu qua sóng vô tuyến, nơi chúng được gửi đến bộ định tuyến và bộ chuyển mạch và được dẫn dọc theo đường dẫn đến đích cuối cùng.



|  |
| --- |
| **Using network diagrams as a security analyst** |

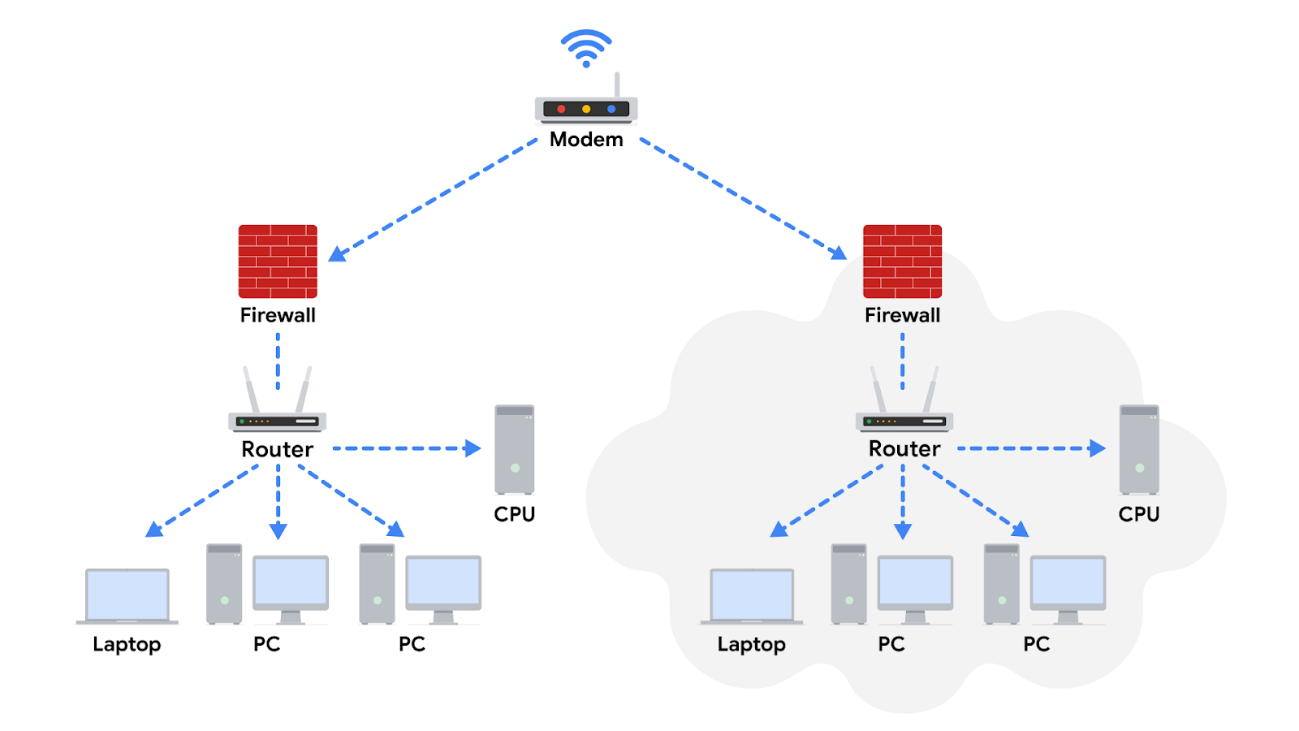
**Sử dụng sơ đồ mạng làm nhà phân tích bảo mật**

|  |
| --- |
| Network diagrams allow network administrators and security personnel to imagine the architecture and design of their organization’s private network. |

Sơ đồ mạng cho phép quản trị viên mạng và nhân viên an ninh tưởng tượng kiến ​​trúc và thiết kế mạng riêng của tổ chức họ.

|  |
| --- |
| **Network diagrams** are maps that show the devices on the network and how they connect. Network diagrams use small representative graphics to portray each network device and dotted lines to show how each device connects to the other. By studying network diagrams, security analysts develop and refine their strategies for securing network architectures. |

**Sơ đồ mạng** là bản đồ hiển thị các thiết bị trên mạng và cách chúng kết nối. Sơ đồ mạng sử dụng đồ họa đại diện nhỏ để mô tả từng thiết bị mạng và các đường chấm để hiển thị cách mỗi thiết bị kết nối với thiết bị kia. Bằng cách nghiên cứu sơ đồ mạng, các nhà phân tích bảo mật phát triển và cải tiến các chiến lược của họ để bảo mật kiến ​​trúc mạng.



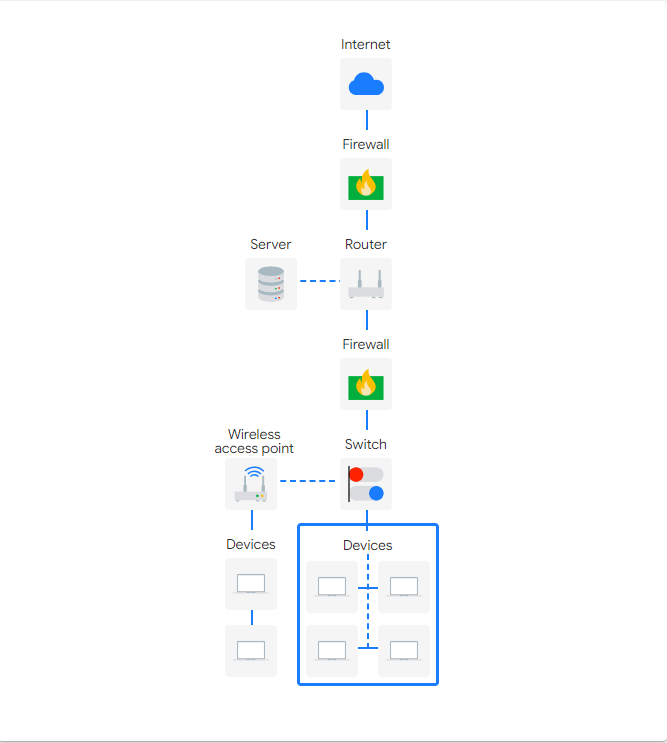
|  |
| --- |
| **Key takeaways** |

**Bài học chính**

|  |
| --- |
| In the client-server model, the client requests information and services from the server, and the server performs the requests for the clients. Network devices include routers, workstations, servers, hubs, switches, and modems. Security analysts use network diagrams to visualize network architecture. |

Trong mô hình máy khách-máy chủ, máy khách yêu cầu thông tin và dịch vụ từ máy chủ và máy chủ thực hiện các yêu cầu đó cho máy khách. Các thiết bị mạng bao gồm bộ định tuyến, máy trạm, máy chủ, trung tâm, bộ chuyển mạch và modem. Các nhà phân tích bảo mật sử dụng sơ đồ mạng để trực quan hóa kiến ​​trúc mạng.

***2.8. Practice: Design a local area network – Thực hành: Thiết kế mạng cục bộ***



***2.9. Cloud networks – Mạng đám mây***

|  |
| --- |
| Companies have traditionally owned their network devices, and kept them in their own office buildings. But now, a lot of companies are using third-party providers to manage their networks. |

Các công ty có truyền thống sở hữu các thiết bị mạng của họ vàgiữ họ trong tòa nhà văn phòng riêng của họ.Nhưng hiện nay, rất nhiều công ty đang sử dụng các nhà cung cấp bên thứ ba để quản lý mạng của họ.

|  |
| --- |
| Why? Well, this model helps companies save money while giving them access to more network resources. The growth of cloud computing is helping many companies reduce costs and streamline their network operations. |

Tại sao?Chà, mô hình này giúp các công ty tiết kiệm tiền trong khi cho phép họ truy cập vào nhiều mạng hơntài nguyên.Sự phát triển của điện toán đám mây đang giúp nhiều công ty giảm chi phí vàhợp lý hóa các hoạt động mạng của họ.

|  |
| --- |
| Cloud computing is the practice of using remote servers, applications, and network services that are hosted on the internet instead of on local physical devices. |

Điện toán đám mây là việc sử dụng các máy chủ, ứng dụng và mạng từ xadịch vụ được lưu trữ trên internet thay vì trên các thiết bị vật lý cục bộ.

|  |
| --- |
| Today, the number of businesses that use cloud computing is increasing every year, so it's important to understand how cloud networks function and how to secure them. |

Ngày nay, số lượng doanh nghiệp sử dụng điện toán đám mây ngày càng tăng lên hàng năm,vì vậy điều quan trọng là phải hiểu cách hoạt động của mạng đám mây và cách bảo mật chúng.

|  |
| --- |
| Cloud providers offer an alternative to traditional on-premise networks, and allow organizations to have the benefits of the traditional network without storing the devices and managing the network on their own. |

Các nhà cung cấp đám mây cung cấp giải pháp thay thế cho mạng tại chỗ truyền thống vàcho phép các tổ chức có được những lợi ích của mạng truyền thống mà không cần lưu trữcác thiết bị và tự quản lý mạng.

|  |
| --- |
| A cloud network is a collection of servers or computers that stores resources and data in a remote data center that can be accessed via the internet. Because companies don't house the servers at their physical location, these servers are referred to as being "in the cloud". |

Mạng đám mây là một tập hợp các máy chủ hoặc máy tính lưu trữ tài nguyên vàdữ liệu trong một trung tâm dữ liệu từ xa có thể được truy cập qua internet.Bởi vì các công ty không đặt máy chủ ở vị trí thực tế của họ,những máy chủ này được coi là "trên đám mây".

|  |
| --- |
| Traditional networks host web servers from a business in its physical location. However, cloud networks are different from traditional networks because they use remote servers, which allow online services and web applications to be used from any geographic location. Cloud security will become increasingly relevant to many security professionals as more organizations migrate to cloud services. |

Mạng truyền thống lưu trữ các máy chủ web từ một doanh nghiệp ở vị trí thực tế của nó.Tuy nhiên, mạng đám mây khác với mạng truyền thống vì chúng sử dụng máy chủ từ xa,cho phép các dịch vụ trực tuyến và ứng dụng webđược sử dụng từ bất kỳ vị trí địa lý nào.Bảo mật đám mây sẽ ngày càng trở nên phù hợp với nhiều chuyên gia bảo mật vìnhiều tổ chức hơn chuyển sang dịch vụ đám mây.

|  |
| --- |
| Cloud service providers offer cloud computing to maintain applications. For example, they provide on-demand storage and processing power that their customers only pay as needed. They also provide business and web analytics that organizations can use to monitor their web traffic and sales. |

Các nhà cung cấp dịch vụ đám mây cung cấp điện toán đám mây để duy trì các ứng dụng.Ví dụ: họ cung cấp dịch vụ lưu trữ theo yêu cầu vàsức mạnh xử lý mà khách hàng của họ chỉ phải trả khi cần thiết.Họ cũng cung cấp kinh doanh vàphân tích trang web mà các tổ chức có thể sử dụng để giám sát lưu lượng truy cập trang web và doanh số bán hàng của họ.

|  |
| --- |
| With the transition to cloud networking, I have witnessed an overlap of identity-based security on top of the more traditional network-based solutions. This meant that my focus needed to be on verifying both where the traffic is coming from and the identity that is coming with it. |

Với việc chuyển đổi sang mạng đám mây, tôi đã chứng kiến ​​sự chồng chéo của các giải pháp dựa trên danh tínhbảo mật trên các giải pháp dựa trên mạng truyền thống hơn.Điều này có nghĩa là tôi cần tập trung vào việc xác minh cả lưu lượng truy cập đến từ đâuvà danh tính đi kèm với nó.

|  |
| --- |
| More organizations are moving their network services to the cloud to save money and simplify their operations. As this trend has grown, cloud security has become a significant aspect of network security. |

Ngày càng có nhiều tổ chức chuyển dịch vụ mạng của họ sang đám mây để tiết kiệm tiền và đơn giản hóahoạt động của họ.Khi xu hướng này phát triển,Bảo mật đám mây đã trở thành một khía cạnh quan trọng của an ninh mạng.

***2.10. Cloud computing and software-defined networks – Điện toán đám mây và mạng được xác định bằng phần mềm***

|  |
| --- |
| **Cloud computing and software-defined networks** |

**Điện toán đám mây và mạng được xác định bằng phần mềm**

|  |
| --- |
| In this section of the course, you’ve been learning the basic architecture of networks. You’ve learned about how physical network devices like workstations, servers, routers, and switches connect to each other to create a network. Networks may cover small geographical areas, as is the case in a local area network (LAN). Or they may span a large geographic area, like a city, state, or country, as is the case in a wide area network (WAN). You also learned about cloud networks and how cloud computing has grown in recent years. |

Trong phần này của khóa học, bạn đã học về kiến ​​trúc cơ bản của mạng. Bạn đã tìm hiểu về cách các thiết bị mạng vật lý như máy trạm, máy chủ, bộ định tuyến và bộ chuyển mạch kết nối với nhau để tạo thành mạng. Mạng có thể bao phủ các khu vực địa lý nhỏ, như trường hợp của mạng cục bộ (LAN). Hoặc chúng có thể trải rộng trên một khu vực địa lý rộng lớn, như thành phố, tiểu bang hoặc quốc gia, như trường hợp của mạng diện rộng (WAN). Bạn cũng đã tìm hiểu về mạng đám mây và điện toán đám mây đã phát triển như thế nào trong những năm gần đây.

|  |
| --- |
| In this reading, you will further examine the concepts of cloud computing and cloud networking. You’ll also learn about hybrid networks and software-defined networks, as well as the benefits they offer. This reading will also cover the benefits of hosting networks in the cloud and why cloud-hosting is beneficial for large organizations. |

Trong bài đọc này, bạn sẽ xem xét sâu hơn các khái niệm về điện toán đám mây và mạng đám mây. Bạn cũng sẽ tìm hiểu về mạng kết hợp và mạng được xác định bằng phần mềm cũng như những lợi ích mà chúng mang lại. Bài đọc này cũng sẽ đề cập đến các lợi ích của việc lưu trữ mạng trên đám mây và tại sao lưu trữ trên đám mây lại mang lại lợi ích cho các tổ chức lớn.

|  |
| --- |
| **Computing processes in the cloud** |

**Quy trình tính toán trên đám mây**

|  |
| --- |
| Traditional networks are called on-premise networks, which means that all of the devices used for network operations are kept at a physical location owned by the company, like in an office building, for example. **Cloud computing**, however, refers to the practice of using remote servers, applications, and network services that are hosted on the internet instead of at a physical location owned by the company. |

Mạng truyền thống được gọi là mạng tại chỗ, có nghĩa là tất cả các thiết bị được sử dụng cho hoạt động mạng đều được lưu giữ tại một vị trí thực tế thuộc sở hữu của công ty, chẳng hạn như trong một tòa nhà văn phòng. Tuy nhiên, **điện toán đám mây** đề cập đến hoạt động sử dụng máy chủ, ứng dụng và dịch vụ mạng từ xa được lưu trữ trên internet thay vì tại một địa điểm thực tế do công ty sở hữu.

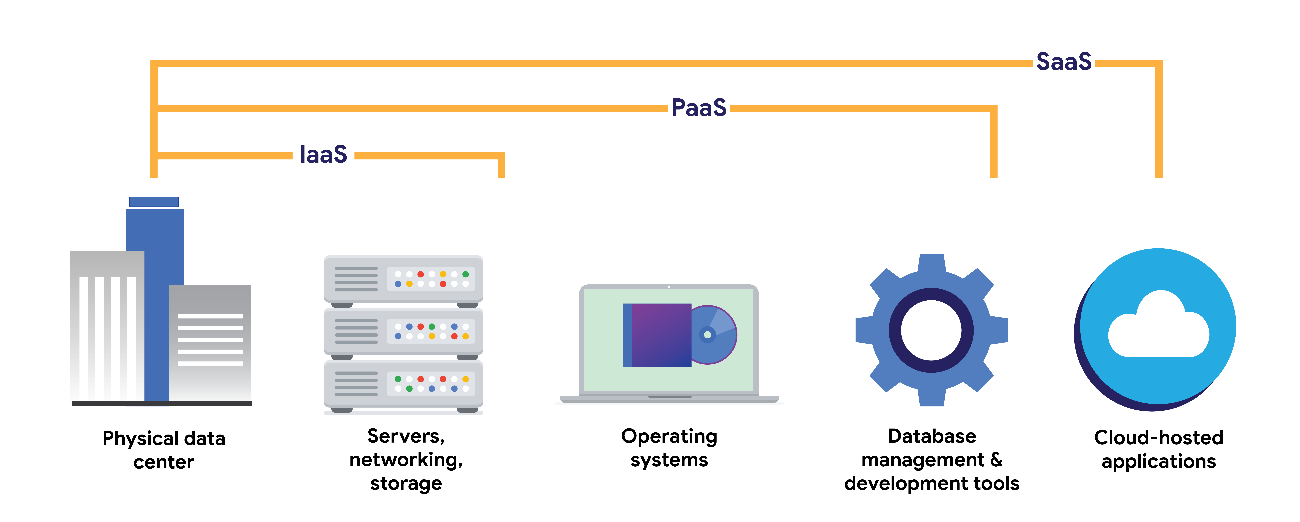
|  |
| --- |
| A cloud service provider (CSP) is a company that offers cloud computing services. These companies own large data centers in locations around the globe that house millions of servers. Data centers provide technology services, such as storage, and compute at such a large scale that they can sell their services to other companies for a fee. Companies can pay for the storage and services they need and consume them through the CSP’s application programming interface (API) or web console. |

Nhà cung cấp dịch vụ đám mây (CSP) là một công ty cung cấp dịch vụ điện toán đám mây. Các công ty này sở hữu các trung tâm dữ liệu lớn ở các địa điểm trên toàn cầu, nơi chứa hàng triệu máy chủ. Các trung tâm dữ liệu cung cấp các dịch vụ công nghệ, chẳng hạn như lưu trữ và tính toán ở quy mô lớn đến mức họ có thể bán dịch vụ của mình cho các công ty khác với một khoản phí. Các công ty có thể trả tiền cho dung lượng lưu trữ và dịch vụ họ cần và sử dụng chúng thông qua giao diện lập trình ứng dụng (API) hoặc bảng điều khiển web của CSP.

|  |
| --- |
| CSPs provide three main categories of services:   * **Software as a service (SaaS)** refers to software suites operated by the CSP that a company can use remotely without hosting the software. * **Infrastructure as a service** **(IaaS)** refers to the use of virtual computer components offered by the CSP. These include virtual containers and storage that are configured remotely through the CSP’s API or web console. Cloud-compute and storage services can be used to operate existing applications and other technology workloads without significant modifications. Existing applications can be modified to take advantage of the availability, performance, and security features that are unique to cloud provider services. * **Platform as a service (PaaS)** refers to tools that application developers can use to design custom applications for their company. Custom applications are designed and accessed in the cloud and used for a company’s specific business needs. |

CSP cung cấp ba loại dịch vụ chính:

* **Phần mềm dưới dạng dịch vụ (SaaS)** đề cập đến các bộ phần mềm do CSP vận hành mà công ty có thể sử dụng từ xa mà không cần lưu trữ phần mềm.
* **Cơ sở hạ tầng dưới dạng dịch vụ (IaaS)** đề cập đến việc sử dụng các thành phần máy tính ảo do CSP cung cấp. Chúng bao gồm các bộ chứa và bộ lưu trữ ảo được định cấu hình từ xa thông qua API hoặc bảng điều khiển web của CSP. Dịch vụ lưu trữ và điện toán đám mây có thể được sử dụng để vận hành các ứng dụng hiện có và khối lượng công việc công nghệ khác mà không cần sửa đổi đáng kể. Các ứng dụng hiện có có thể được sửa đổi để tận dụng tính khả dụng, hiệu suất và tính năng bảo mật dành riêng cho các dịch vụ của nhà cung cấp đám mây.
* **Nền tảng dưới dạng dịch vụ (PaaS)** đề cập đến các công cụ mà nhà phát triển ứng dụng có thể sử dụng để thiết kế các ứng dụng tùy chỉnh cho công ty của họ. Các ứng dụng tùy chỉnh được thiết kế và truy cập trên đám mây và được sử dụng cho các nhu cầu kinh doanh cụ thể của công ty.



|  |
| --- |
| **Hybrid cloud environments** |

**Môi trường đám mây lai**

|  |
| --- |
| When organizations use a CSP’s services in addition to their on-premise computers, networks, and storage, it is referred to as a hybrid cloud environment. When organizations use more than one CSP, it is called a multi-cloud environment. The vast majority of organizations use hybrid cloud environments to reduce costs and maintain control over network resources. |

Khi các tổ chức sử dụng dịch vụ của CSP ngoài máy tính, mạng và bộ lưu trữ tại chỗ của họ, thì môi trường đó được gọi là môi trường đám mây lai. Khi các tổ chức sử dụng nhiều CSP, nó được gọi là môi trường nhiều đám mây. Phần lớn các tổ chức sử dụng môi trường đám mây lai để giảm chi phí và duy trì quyền kiểm soát tài nguyên mạng.

|  |
| --- |
| **Software-defined networks** |

**Mạng được xác định bằng phần mềm**

|  |
| --- |
| CSPs offer networking tools similar to the physical devices that you have learned about in this section of the course. Next, you’ll review  software-defined networking in the cloud. Software-defined networks (SDNs) are made up of virtual network devices and services. Just like CSPs provide virtual computers, many SDNs also provide virtual switches, routers, firewalls, and more. Most modern network hardware devices also support network virtualization and software-defined networking. This means that physical switches and routers use software to perform packet routing. In the case of cloud networking, the SDN tools are hosted on servers located at the CSP’s data center. |

CSP cung cấp các công cụ mạng tương tự như các thiết bị vật lý mà bạn đã tìm hiểu trong phần này của khóa học. Tiếp theo, bạn sẽ xem xét kết nối mạng được xác định bằng phần mềm trên đám mây. Mạng được xác định bằng phần mềm (SDN) được tạo thành từ các thiết bị và dịch vụ mạng ảo. Giống như CSP cung cấp máy tính ảo, nhiều SDN cũng cung cấp bộ chuyển mạch ảo, bộ định tuyến, tường lửa, v.v. Hầu hết các thiết bị phần cứng mạng hiện đại cũng hỗ trợ ảo hóa mạng và kết nối mạng được xác định bằng phần mềm. Điều này có nghĩa là các bộ chuyển mạch và bộ định tuyến vật lý sử dụng phần mềm để thực hiện định tuyến gói. Trong trường hợp kết nối mạng đám mây, các công cụ SDN được lưu trữ trên các máy chủ đặt tại trung tâm dữ liệu của CSP.

|  |
| --- |
| **Benefits of cloud computing and software-defined networks** |

**Lợi ích của điện toán đám mây và mạng được xác định bằng phần mềm**

|  |
| --- |
| Three of the main reasons that cloud computing is so attractive to businesses are reliability, decreased cost, and increased scalability. |

Ba trong số những lý do chính khiến điện toán đám mây hấp dẫn doanh nghiệp là độ tin cậy, giảm chi phí và tăng khả năng mở rộng.

|  |
| --- |
| **Reliability** |

**độ tin cậy**

|  |
| --- |
| Reliability in cloud computing is based on how available cloud services and resources are, how secure connections are, and how often the services are effectively running. Cloud computing allows employees and customers to access the resources they need consistently and with minimal interruption. |

Độ tin cậy trong điện toán đám mây dựa trên mức độ sẵn có của các dịch vụ và tài nguyên đám mây, mức độ kết nối an toàn và tần suất các dịch vụ hoạt động hiệu quả. Điện toán đám mây cho phép nhân viên và khách hàng truy cập các tài nguyên họ cần một cách nhất quán và ít bị gián đoạn nhất.

|  |
| --- |
| **Cost** |

**Trị giá**

|  |
| --- |
| Traditionally, companies have had to provide their own network infrastructure, at least for internet connections. This meant there could be potentially significant upfront costs for companies. However, because CSPs have such large data centers, they are able to offer virtual devices and services at a fraction of the cost required for companies to install, patch, upgrade, and manage the components and software themselves. |

Theo truyền thống, các công ty phải cung cấp cơ sở hạ tầng mạng riêng, ít nhất là cho kết nối internet. Điều này có nghĩa là các công ty có thể phải chịu những chi phí trả trước đáng kể. Tuy nhiên, vì CSP có các trung tâm dữ liệu lớn như vậy nên họ có thể cung cấp các thiết bị và dịch vụ ảo với một phần chi phí cần thiết để các công ty tự cài đặt, vá lỗi, nâng cấp và quản lý các thành phần và phần mềm.

|  |
| --- |
| **Scalability** |

**Khả năng mở rộng**

|  |
| --- |
| Another challenge that companies face with traditional computing is scalability. When organizations experience an increase in their business needs, they might be forced to buy more equipment and software to keep up. But what if business decreases shortly after? They might no longer have the business to justify the cost incurred by the upgraded components. CSPs reduce this risk by making it easy to consume services in an elastic utility model as needed. This means that companies only pay for what they need when they need it. |

Một thách thức khác mà các công ty phải đối mặt với điện toán truyền thống là khả năng mở rộng. Khi các tổ chức nhận thấy nhu cầu kinh doanh ngày càng tăng, họ có thể buộc phải mua thêm thiết bị và phần mềm để theo kịp. Nhưng nếu việc kinh doanh giảm sút ngay sau đó thì sao? Họ có thể không còn khả năng kinh doanh để biện minh cho chi phí phát sinh từ các thành phần được nâng cấp. CSP giảm thiểu rủi ro này bằng cách giúp dễ dàng sử dụng dịch vụ trong mô hình tiện ích linh hoạt khi cần thiết. Điều này có nghĩa là các công ty chỉ trả tiền cho những gì họ cần khi họ cần.

|  |
| --- |
| Changes can be made quickly through the CSPs, APIs, or web console—much more quickly than if network technicians had to purchase their own hardware and set it up. For example, if a company needs to protect against a threat to their network, web application firewalls (WAFs), intrusion detection/protection systems (IDS/IPS), or L3/L4 firewalls can be configured quickly whenever necessary, leading to better network performance and security. |

Các thay đổi có thể được thực hiện nhanh chóng thông qua CSP, API hoặc bảng điều khiển web—nhanh hơn nhiều so với việc các kỹ thuật viên mạng phải mua phần cứng của riêng họ và thiết lập nó. Ví dụ: nếu một công ty cần bảo vệ khỏi mối đe dọa đối với mạng của họ, tường lửa ứng dụng web (WAF), hệ thống phát hiện/bảo vệ xâm nhập (IDS/IPS) hoặc tường lửa L3/L4 có thể được cấu hình nhanh chóng bất cứ khi nào cần thiết, dẫn đến mạng tốt hơn hiệu suất và bảo mật.

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

**Bài học chính**

|  |
| --- |
| In this reading, you learned more about cloud computing and cloud networking. You learned that CSPs are companies that own large data centers that house millions of servers in locations all over the globe and then provide modern technology services, including compute, storage, and networking, through the internet. SDNs are an approach to network management. SDNs enable dynamic, programmatically efficient network configurations to improve network performance and monitoring. This makes it more like cloud computing than traditional network management. Organizations can improve reliability, save costs, and scale quickly by using CSPs to provide networking services instead of building and maintaining their own network infrastructure. |

Trong bài đọc này, bạn đã tìm hiểu thêm về điện toán đám mây và mạng đám mây. Bạn đã biết rằng CSP là những công ty sở hữu các trung tâm dữ liệu lớn có hàng triệu máy chủ đặt tại các địa điểm trên toàn cầu và sau đó cung cấp các dịch vụ công nghệ hiện đại, bao gồm điện toán, lưu trữ và kết nối mạng thông qua internet. SDN là một cách tiếp cận để quản lý mạng. SDN cho phép cấu hình mạng động, hiệu quả theo chương trình để cải thiện hiệu suất và giám sát mạng. Điều này làm cho nó giống điện toán đám mây hơn là quản lý mạng truyền thống. Các tổ chức có thể cải thiện độ tin cậy, tiết kiệm chi phí và mở rộng quy mô nhanh chóng bằng cách sử dụng CSP để cung cấp dịch vụ mạng thay vì xây dựng và duy trì cơ sở hạ tầng mạng của riêng họ.

|  |
| --- |
| **Resources for more information** |

**Tài nguyên để biết thêm thông tin**

|  |
| --- |
| For more information about cloud computing and the services offered, you can review [Google Cloud (GC)](https://cloud.google.com/). |

Để biết thêm thông tin về điện toán đám mây và các dịch vụ được cung cấp, bạn có thể xem lại[Đám mây của Google (GC)](https://cloud.google.com/).

***2.11. Identify: Functions of network tools – Xác định: Chức năng của các công cụ mạng***

|  |  |
| --- | --- |
| Definition | Term |
| A network device that connects multiple networks together. | Router |
| A network device that broadcasts information to every device on the network. | Hub |
| A network security device that monitors traffic to or from your network. | Firewall |
| A device that sends and receives data between devices on a network. | Switch |
| Connects a router to the internet and enables LAN internet access. | Modem |

|  |  |
| --- | --- |
| Định nghĩa | Thuật ngữ |
| Một thiết bị mạng kết nối nhiều mạng với nhau. | Router |
| Một thiết bị mạng phát thông tin tới mọi thiết bị trên mạng. | Hub |
| Một thiết bị bảo mật mạng giám sát lưu lượng đến hoặc đi từ mạng của bạn. | Firewall |
| Một thiết bị gửi và nhận dữ liệu giữa các thiết bị trên mạng. | Switch |
| Kết nối bộ định tuyến với internet và cho phép truy cập internet LAN. | Modem |

***2.12. Test your knowledge: Introduction to networks – Kiểm tra kiến ​​thức của bạn: Giới thiệu về mạng***

**3. Network communication – Truyền thông mạng**

***3.1. Introduction to network communication – Giới thiệu về truyền thông mạng***

|  |
| --- |
| Networks help organizations communicate and connect. But communication makes network attacks more likely because it gives a malicious actor an opportunity to take advantage of vulnerable devices and unprotected networks. |

Mạng giúp các tổ chức giao tiếp và kết nối.Nhưng giao tiếp làm cho các cuộc tấn công mạng có nhiều khả năng xảy ra hơn vì nó mang lại một mối đe dọa độc hạitạo cơ hội để tận dụng các thiết bị dễ bị tấn công vàmạng không được bảo vệ.

|  |
| --- |
| Communication over a network happens when data is transferred from one point to another. Pieces of data are typically referred to as data packets. |

Truyền thông qua mạng xảy ra khi dữ liệu được truyền từ điểm này tới điểm kháckhác. Các phần dữ liệu thường được gọi là gói dữ liệu.

|  |
| --- |
| A data packet is a basic unit of information that travels from one device to another within a network. When data is sent from one device to another across a network, it is sent as a packet that contains information about where the packet is going, where it's coming from, and the content of the message. |

Gói dữ liệu là một đơn vị thông tin cơ bản được truyền từ mộtthiết bị này sang thiết bị khác trong mạng.Khi dữ liệu được gửi từ thiết bị này sang thiết bị khác qua mạng, nó sẽ được gửi dưới dạngmột gói chứa thông tin về nơi gói sẽ đi, nó ở đâuđến từ đâu và nội dung của tin nhắn.

|  |
| --- |
| Think about data packets like a piece of physical mail. Imagine you want to send a letter to a friend. The envelope will need to have the address where you want the letter to go and your return address. Inside the envelope is a letter that contains the message that you want your friend to read. |

Hãy nghĩ về các gói dữ liệu giống như một mẩu thư vật lý.Hãy tưởng tượng bạn muốn gửi một lá thư cho một người bạn.Phong bì cần có địa chỉ nơi bạn muốn gửi thưvà địa chỉ trả lại của bạn. Bên trong phong bì là một lá thư có chứatin nhắn mà bạn muốn bạn bè của bạn đọc.

|  |
| --- |
| A data packet is very similar to a physical letter. It contains a header that includes the internet protocol address, the IP address, and the media access control, or MAC, address of the destination device. It also includes a protocol number that tells the receiving device what to do with the information in the packet. Then there's the body of the packet, which contains the message that needs to be transmitted to the receiving device. Finally, at the end of the packet, there's a footer, similar to a signature on a letter, the footer signals to the receiving device that the packet is finished. |

Một gói dữ liệu rất giống với một lá thư vật lý.Nó chứa một tiêu đề bao gồm địa chỉ giao thức internet, địa chỉ IPđịa chỉ và điều khiển truy cập phương tiện hoặc địa chỉ MAC của thiết bị đích.Nó cũng bao gồm một số giao thức cho thiết bị nhận biết phải làm gì vớithông tin trong gói tin.Sau đó là phần thân của gói chứa thông điệp cầnđược truyền đến thiết bị nhận.Cuối cùng, ở cuối gói có phần chân trang,tương tự như chữ ký trên một lá thư,chân trang báo hiệu cho thiết bị nhận rằng gói đã hoàn tất.

|  |
| --- |
| The movement of data packets across a network can provide an indication of how well the network is performing. Network performance can be measured by bandwidth. |

Sự di chuyển của các gói dữ liệu trên mạng có thể cung cấp một dấu hiệu về cáchmạng đang hoạt động tốt. Hiệu suất mạng có thể được đo bằng băng thông.

|  |
| --- |
| Bandwidth refers to the amount of data a device receives every second. You can calculate bandwidth by dividing the quantity of data by the time in seconds. Speed refers to the rate at which data packets are received or downloaded. Security personnel are interested in network bandwidth and speed because if either are irregular, it could be an indication of an attack. Packet sniffing is the practice of capturing and inspecting data packets across the network. |

Băng thông đề cập đến lượng dữ liệu mà thiết bị nhận được mỗi giây.Bạn có thể tính toán băng thông bằng cách chia số lượng dữ liệu cho thời gian tronggiây.Tốc độ đề cập đến tốc độ nhận hoặc tải xuống các gói dữ liệu.Nhân viên an ninh quan tâm đến băng thông và tốc độ mạngbởi vì nếu một trong hai điều đó không đều, nó có thể là dấu hiệu của một cuộc tấn công.Đánh hơi gói tin là thực hành thu thập vàkiểm tra các gói dữ liệu trên mạng.

|  |
| --- |
| Communication on the network is important for sharing resources and data because it allows organizations to function effectively. Coming up, you'll learn more about the protocols to support network communication. |

Truyền thông trên mạng rất quan trọng để chia sẻ tài nguyên vàdữ liệu vì nó cho phép các tổ chức hoạt động hiệu quả.Sắp diễn ra,bạn sẽ tìm hiểu thêm về các giao thức hỗ trợ giao tiếp mạng.

***3.2. The TCP/IP model – Mô hình TCP/IP***

|  |
| --- |
| Hello again. In this video, you'll learn more about communication protocols and devices used to communicate with each other across the internet. This is called the TCP/IP model. |

Xin chào lần nữa. Trong video này,bạn sẽ tìm hiểu thêm về các giao thức truyền thông vàthiết bị dùng để liên lạcvới nhau qua internet.Đây được gọi là mô hình TCP/IP.

|  |
| --- |
| TCP/IP stands for Transmission Control Protocol and Internet Protocol. TCP/IP is the standard model used for network communication. Let's take a closer look at this model by defining TCP and IP separately. |

TCP/IP là viết tắt củaGiao thức điều khiển truyền dẫn và Giao thức Internet.TCP/IP là mô hình chuẩnđược sử dụng cho truyền thông mạng.Chúng ta hãy xem xét kỹ hơn về mô hình này bằng cáchđịnh nghĩa TCP và IP riêng biệt.

|  |
| --- |
| First, TCP, or Transmission Control Protocol, is an internet communication protocol that allows two devices to form a connection and stream data. The protocol includes a set of instructions to organize data, so it can be sent across a network. It also establishes a connection between two devices and makes sure that packets reach their appropriate destination. |

Đầu tiên, TCP hoặc Giao thức điều khiển truyền dẫn,là một giao thức truyền thông internet cho phéphai thiết bị để tạo thành kết nối và truyền dữ liệu.Giao thức bao gồm một tập hợp các hướng dẫn đểtổ chức dữ liệu để nó có thể được gửi qua mạng.Nó cũng thiết lập kết nối giữa hai thiết bịvà đảm bảo rằng các góiđến đích thích hợp của họ.

|  |
| --- |
| The IP in TCP/IP stands for Internet Protocol. IP has a set of standards used for routing and addressing data packets as they travel between devices on a network. Included in the Internet Protocol (IP) is the IP address that functions as an address for each private network. You'll learn more about IP addresses a bit later. |

IP trong TCP/IP là viết tắt của Giao thức Internet.IP có một bộ tiêu chuẩn được sử dụng để định tuyến và đánh địa chỉgói dữ liệu khi chúng di chuyểngiữa các thiết bị trên mạng.Bao gồm trong Giao thức Internet (IP) là địa chỉ IPcó chức năng như một địa chỉ cho mỗi mạng riêng.Bạn sẽ tìm hiểu thêm về địa chỉ IP sau.

|  |
| --- |
| When data packets are sent and received across a network, they are assigned a port. |

Khi các gói dữ liệu được gửi và nhận qua mạng,họ được chỉ định một cổng.

|  |
| --- |
| Within the operating system of a network device, a port is a software-based location that organizes the sending and receiving of data between devices on a network. Ports divide network traffic into segments based on the service they will perform between two devices. The computers sending and receiving these data segments know how to prioritize and process these segments based on their port number. |

Trong hệ điều hành của một thiết bị mạng,một cổng là một vị trí dựa trên phần mềm để tổ chứcviệc gửi và nhận dữ liệugiữa các thiết bị trên mạng.Cổng chia lưu lượng mạng thành các phân đoạndựa trên dịch vụ họ sẽ thực hiệngiữa hai thiết bị.Các máy tính gửi vànhận được các phân đoạn dữ liệu này biết cáchưu tiên và xử lý các phân khúc nàydựa trên số cổng của họ.

|  |
| --- |
| This is like sending a letter to a friend who lives in an apartment building. The mail delivery person not only knows how to find the building, but they also know exactly where to go in the building to find the apartment number where your friend lives. |

Việc này giống như gửi một lá thư tớimột người bạn sống trong một tòa nhà chung cư.Người đưa thưkhông chỉ biết cách tìm ra tòa nhà,nhưng họ cũng biết chính xác nơi cần đi trong tòa nhàđể tìm số căn hộ nơi bạn của bạn sống.

|  |
| --- |
| Data packets include instructions that tell the receiving device what to do with the information. These instructions come in the form of a port number. Port numbers allow computers to split the network traffic and prioritize the operations they will perform with the data. Some common port numbers are: port 25, which is used for e-mail, port 443, which is used for secure internet communication, and port 20, for large file transfers. |

Các gói dữ liệu bao gồm các hướng dẫn cho biếtthiết bị nhận phải làm gì với thông tin.Các hướng dẫn này có dạng số cổng.Số cổng cho phép máy tínhđể phân chia lưu lượng mạng vàưu tiên các hoạt động mà họsẽ thực hiện với dữ liệu.Một số số cổng phổ biến là:cổng 25, được sử dụng cho e-mail,cổng 443, đó làđược sử dụng để liên lạc internet an toàn,và cổng 20, để truyền tệp lớn.

|  |
| --- |
| As you've learned in this video, a lot of information and instructions are contained in data packets as they travel across a network. Coming up, you'll learn more about the TCP/IP model. |

Như bạn đã học trong video này,rất nhiều thông tin và hướng dẫnchứa trong các gói dữ liệu nhưhọ đi qua một mạng.Tiếp theo, bạn sẽ tìm hiểu thêm về mô hình TCP/IP.

***3.3. The four layers of the TCP/IP model – Bốn lớp của mô hình TCP/IP***

|  |
| --- |
| Now that we've discussed the structure of a network and how communications takes place, it's important for you to know how the security professionals identify problems that might arise. |

Bây giờ chúng ta đã thảo luận về cấu trúc củamột mạng lưới và cách thức truyền thông diễn ra,điều quan trọng là bạn phải biết cáchcác chuyên gia bảo mật xác địnhnhững vấn đề có thể phát sinh.

|  |
| --- |
| The TCP/IP model is a framework that is used to visualize how data is organized and transmitted across the network. The TCP/IP model has four layers. The four layers are: the network access layer, the internet layer, the transport layer, and the application layer. |

Mô hình TCP/IP là một khuôn khổ được sử dụng đểhình dung dữ liệu như thế nàođược tổ chức và truyền tải trên mạng.Mô hình TCP/IP có bốn lớp.Bốn lớp đó là: lớp truy cập mạng,lớp internet, lớp vận chuyển,và lớp ứng dụng.

|  |
| --- |
| Knowing how the TCP/IP model organizes network activity allows security professionals to monitor and secure against risks. |

Biết cách mô hình TCP/IP tổ chức hoạt động mạngcho phép các chuyên gia bảo mậtgiám sát và đảm bảo an toàn trước các rủi ro.

|  |
| --- |
| Let's examine these layers one at a time. |

Chúng ta hãy kiểm tra các lớp này cùng một lúc.

|  |
| --- |
| Layer one is the network access layer. The network access layer deals with creation of data packets and their transmission across a network. This includes hardware devices connected to physical cables and switches that direct data to its destination. |

Lớp một là lớp truy cập mạng.Lớp truy cập mạng xử lý việc tạo racác gói dữ liệu và việc truyền tải chúng qua mạng.Điều này bao gồm các thiết bị phần cứng được kết nối vớicáp và công tắc vật lýdữ liệu trực tiếp đến đích của nó.

|  |
| --- |
| Layer two is the internet layer. The internet layer is where IP addresses are attached to data packets to indicate the location of the sender and receiver. The internet layer also focuses on how networks connect to each other. For example, data packets containing information that determine whether they will stay on the LAN or will be sent to a remote network, like the internet. |

Lớp hai là lớp internet.Lớp Internet là nơi gắn địa chỉ IP vàogói dữ liệu để chỉ ravị trí của người gửi và người nhận.Lớp internet cũng tập trungvề cách các mạng kết nối với nhau.Ví dụ, gói dữ liệuchứa thông tin xác định liệuhọ sẽ ở lại mạng LAN hoặc sẽ được gửiđến một mạng từ xa, như internet.

|  |
| --- |
| The transport layer includes protocols to control the flow of traffic across a network. These protocols permit or deny communication with other devices and include information about the status of the connection. Activities of this layer include error control, which ensures data is flowing smoothly across the network. |

Lớp vận chuyển bao gồm các giao thức đểkiểm soát luồng lưu lượng trên mạng.Các giao thức này cho phép hoặc từ chối liên lạc vớicác thiết bị khác và bao gồmthông tin về trạng thái của kết nối.Các hoạt động của lớp này bao gồm kiểm soát lỗi,đảm bảo dữ liệu đang chảythông suốt trên mạng.

|  |
| --- |
| Finally, at the application layer, protocols determine how the data packets will interact with receiving devices. Functions that are organized at application layer include file transfers and email services. |

Cuối cùng, ở lớp ứng dụng,các giao thức xác định cách thức các gói dữ liệusẽ tương tác với các thiết bị nhận.Các chức năng được tổ chức ở lớp ứng dụngbao gồm chuyển tập tin và dịch vụ email.

|  |
| --- |
| Now you have an understanding of the TCP/IP model and its four layers. Meet you in the next video. |

Bây giờ bạn đã hiểu vềmô hình TCP/IP vàbốn lớp. Hẹn gặp lại các bạn ở video tiếp theo.

***3.4. Learn more about the TCP/IP model – Tìm hiểu thêm về mô hình TCP/IP***

|  |
| --- |
| **Learn more about the TCP/IP model** |

**Tìm hiểu thêm về mô hình TCP/IP**

|  |
| --- |
| In this reading, you will build on what you have learned about the Transmission Control Protocol/Internet Protocol (TCP/IP) model, consider the differences between the Open Systems Interconnection (OSI) model and TCP/IP model, and learn how they’re related. Then, you’ll review each layer of the TCP/IP model and go over common protocols used in each layer. |

Trong bài đọc này, bạn sẽ dựa trên những gì đã học về mô hình Giao thức điều khiển truyền tải/Giao thức Internet (TCP/IP), xem xét sự khác biệt giữa mô hình Kết nối hệ thống mở (OSI) và mô hình TCP/IP, đồng thời tìm hiểu chúng ' lại liên quan. Sau đó, bạn sẽ xem xét từng lớp của mô hình TCP/IP và xem xét các giao thức phổ biến được sử dụng trong mỗi lớp.

|  |
| --- |
| As a security professional, it's important that you understand the TCP/IP model because it describes the functions of various network protocols. The TCP/IP model is based on the TCP/IP protocols suite that includes all network protocols that support the main TCP/IP protocol. To reiterate from previous lessons, a network protocol, also known as an internet protocol, is a set of standards used for routing and addressing data packets as they travel between devices on a network. In this reading, you will learn which network protocols operate on which communication layers of the TCP/IP model. The two most common models available are the TCP/IP and the OSI model. These models are a representative guideline of how hosts communicate across a network. The examples provided in this course will follow the TCP/IP model. |

Là một chuyên gia bảo mật, điều quan trọng là bạn phải hiểu mô hình TCP/IP vì nó mô tả chức năng của các giao thức mạng khác nhau. Mô hình TCP/IP dựa trên bộ giao thức TCP/IP bao gồm tất cả các giao thức mạng hỗ trợ giao thức TCP/IP chính. Nhắc lại từ các bài học trước, giao thức mạng, còn được gọi là giao thức internet, là một bộ tiêu chuẩn được sử dụng để định tuyến và đánh địa chỉ các gói dữ liệu khi chúng di chuyển giữa các thiết bị trên mạng. Trong bài đọc này, bạn sẽ tìm hiểu các giao thức mạng nào hoạt động trên các lớp giao tiếp nào của mô hình TCP/IP. Hai mô hình phổ biến nhất hiện có là mô hình TCP/IP và mô hình OSI. Những mô hình này là hướng dẫn tiêu biểu về cách các máy chủ giao tiếp qua mạng. Các ví dụ được cung cấp trong khóa học này sẽ tuân theo mô hình TCP/IP.

|  |
| --- |
| **The TCP/IP model** |

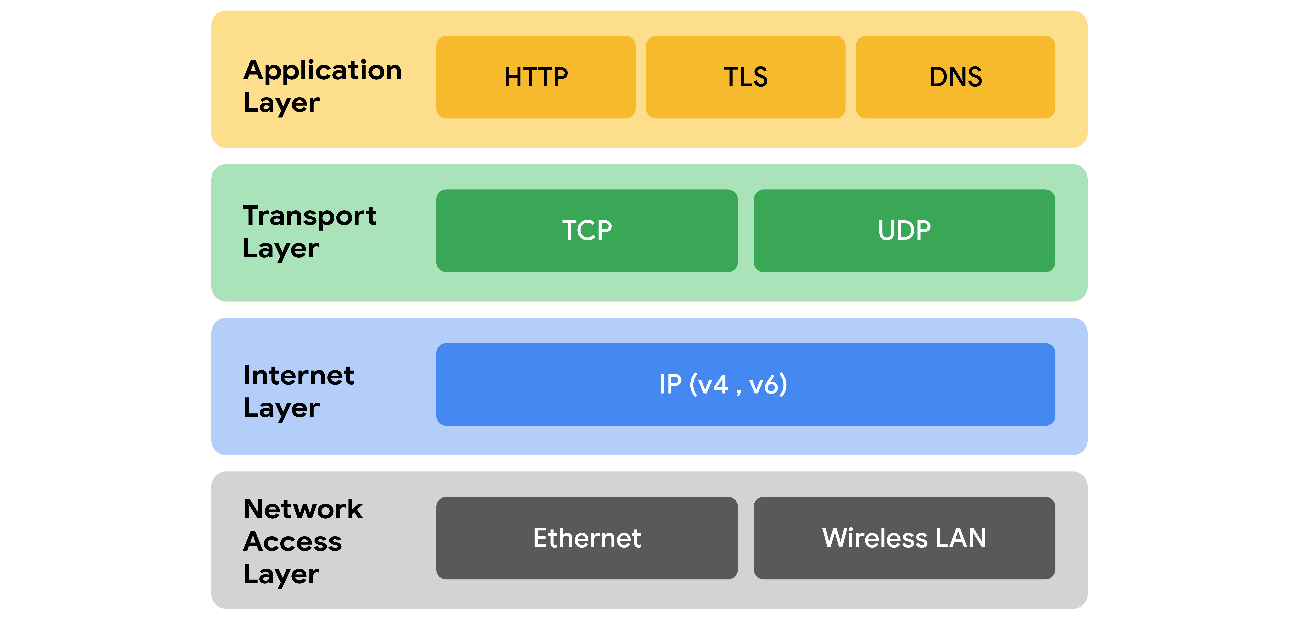
**Mô hình TCP/IP**

|  |
| --- |
| The **TCP/IP model** is a framework used to visualize how data is organized and transmitted across a network. This model helps network engineers and network security analysts conceptualize processes on the network and communicate where disruptions or security threats occur. |

Mô **hình TCP/IP** là một khung được sử dụng để trực quan hóa cách tổ chức và truyền dữ liệu qua mạng. Mô hình này giúp các kỹ sư mạng và nhà phân tích an ninh mạng khái niệm hóa các quy trình trên mạng và liên lạc khi xảy ra sự gián đoạn hoặc mối đe dọa bảo mật.

|  |
| --- |
| The TCP/IP model has four layers: the network access layer, internet layer, transport layer, and application layer. When troubleshooting issues on the network, security professionals can analyze which layers were impacted by an attack based on what processes were involved in an incident. |

Mô hình TCP/IP có bốn lớp: lớp truy cập mạng, lớp internet, lớp vận chuyển và lớp ứng dụng. Khi khắc phục sự cố trên mạng, các chuyên gia bảo mật có thể phân tích lớp nào bị ảnh hưởng bởi cuộc tấn công dựa trên những quy trình liên quan đến sự cố.



|  |
| --- |
| **Network access layer** |

**Lớp truy cập mạng**

|  |
| --- |
| The network access layer, sometimes called the data link layer, deals with the creation of data packets and their transmission across a network. This layer corresponds to the physical hardware involved in network transmission. Hubs, modems, cables, and wiring are all considered part of this layer. The address resolution protocol (ARP) is part of the network access layer. Since MAC addresses are used to identify hosts on the same physical network, ARP is needed to map IP addresses to MAC addresses for local network communication. |

Lớp truy cập mạng, đôi khi được gọi là lớp liên kết dữ liệu, xử lý việc tạo các gói dữ liệu và truyền chúng qua mạng. Lớp này tương ứng với phần cứng vật lý liên quan đến việc truyền tải mạng. Hub, modem, cáp và hệ thống dây điện đều được coi là một phần của lớp này. Giao thức phân giải địa chỉ (ARP) là một phần của lớp truy cập mạng. Vì địa chỉ MAC được sử dụng để xác định các máy chủ trên cùng một mạng vật lý, nên cần có ARP để ánh xạ địa chỉ IP thành địa chỉ MAC để liên lạc mạng cục bộ.

|  |
| --- |
| **Internet layer** |

**Lớp Internet**

|  |
| --- |
| The internet layer, sometimes referred to as the network layer, is responsible for ensuring the delivery to the destination host, which potentially resides on a different network. It ensures IP addresses are attached to data packets to indicate the location of the sender and receiver. The internet layer also determines which protocol is responsible for delivering the data packets and ensures the delivery to the destination host. Here are some of the common protocols that operate at the internet layer:   * **Internet Protocol (IP)**. IP sends the data packets to the correct destination and relies on the Transmission Control Protocol/User Datagram Protocol (TCP/UDP) to deliver them to the corresponding service. IP packets allow communication between two networks. They are routed from the sending network to the receiving network. TCP in particular retransmits any data that is lost or corrupt. * **Internet Control Message Protocol (ICMP)**. The ICMP shares error information and status updates of data packets. This is useful for detecting and troubleshooting network errors. The ICMP reports information about packets that were dropped or that disappeared in transit, issues with network connectivity, and packets redirected to other routers. |

Lớp internet, đôi khi được gọi là lớp mạng, chịu trách nhiệm đảm bảo việc phân phối đến máy chủ đích, có khả năng nằm trên một mạng khác. Nó đảm bảo địa chỉ IP được gắn vào các gói dữ liệu để cho biết vị trí của người gửi và người nhận. Lớp internet cũng xác định giao thức nào chịu trách nhiệm phân phối các gói dữ liệu và đảm bảo việc phân phối đến máy chủ đích. Dưới đây là một số giao thức phổ biến hoạt động ở lớp internet:

* **Giao thức Internet (IP)** . IP gửi các gói dữ liệu đến đúng đích và dựa vào Giao thức điều khiển truyền tải/Giao thức gói dữ liệu người dùng (TCP/UDP) để phân phối chúng đến dịch vụ tương ứng. Các gói IP cho phép liên lạc giữa hai mạng. Chúng được định tuyến từ mạng gửi đến mạng nhận. TCP đặc biệt truyền lại bất kỳ dữ liệu nào bị mất hoặc bị hỏng.
* **Giao thức tin nhắn điều khiển Internet (ICMP)** . ICMP chia sẻ thông tin lỗi và cập nhật trạng thái của gói dữ liệu. Điều này rất hữu ích để phát hiện và khắc phục sự cố lỗi mạng. ICMP báo cáo thông tin về các gói bị rớt hoặc biến mất trong quá trình truyền, các sự cố về kết nối mạng và các gói được chuyển hướng đến các bộ định tuyến khác.

|  |
| --- |
| **Transport layer** |

**Lớp vận chuyển**

|  |
| --- |
| The transport layer is responsible for delivering data between two systems or networks and includes protocols to control the flow of traffic across a network. TCP and UDP are the two transport protocols that occur at this layer. |

Lớp vận chuyển chịu trách nhiệm phân phối dữ liệu giữa hai hệ thống hoặc mạng và bao gồm các giao thức để kiểm soát luồng lưu lượng trên mạng. TCP và UDP là hai giao thức vận chuyển xảy ra ở lớp này.

|  |
| --- |
| **Transmission Control Protocol** |

**Giao thức điều khiển truyền dẫn**

|  |
| --- |
| The **Transmission Control Protocol (TCP)** is an internet communication protocol that allows two devices to form a connection and stream data. It ensures that data is reliably transmitted to the destination service. TCP contains the port number of the intended destination service, which resides in the TCP header of a TCP/IP packet. |

Giao **thức điều khiển truyền dẫn (TCP)** là giao thức truyền thông internet cho phép hai thiết bị tạo thành kết nối và truyền dữ liệu. Nó đảm bảo rằng dữ liệu được truyền đến dịch vụ đích một cách đáng tin cậy. TCP chứa số cổng của dịch vụ đích dự kiến, nằm trong tiêu đề TCP của gói TCP/IP.

|  |
| --- |
| **User Datagram Protocol** |

**Giao thức gói dữ liệu người dùng**

|  |
| --- |
| The **User Datagram Protocol (UDP)** is a connectionless protocol that does not establish a connection between devices before transmissions. It is used by applications that are not concerned with the reliability of the transmission. Data sent over UDP is not tracked as extensively as data sent using TCP. Because UDP does not establish network connections, it is used mostly for performance sensitive applications that operate in real time, such as video streaming. |

Giao **thức gói dữ liệu người dùng (UDP)** là giao thức không kết nối, không thiết lập kết nối giữa các thiết bị trước khi truyền. Nó được sử dụng bởi các ứng dụng không quan tâm đến độ tin cậy của việc truyền tải. Dữ liệu được gửi qua UDP không được theo dõi rộng rãi như dữ liệu được gửi bằng TCP. Vì UDP không thiết lập kết nối mạng nên nó được sử dụng chủ yếu cho các ứng dụng nhạy cảm về hiệu suất hoạt động trong thời gian thực, chẳng hạn như truyền phát video.

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

**Lớp ứng dụng**

|  |
| --- |
| The application layer in the TCP/IP model is similar to the application, presentation, and session layers of the OSI model. The application layer is responsible for making network requests or responding to requests. This layer defines which internet services and applications any user can access. Protocols in the application layer determine how the data packets will interact with receiving devices. Some common protocols used on this layer are:   * Hypertext transfer protocol (HTTP) * Simple mail transfer protocol (SMTP) * Secure shell (SSH) * File transfer protocol (FTP) * Domain name system (DNS) |

Lớp ứng dụng trong mô hình TCP/IP tương tự như lớp ứng dụng, lớp trình bày và lớp phiên của mô hình OSI. Lớp ứng dụng chịu trách nhiệm thực hiện các yêu cầu mạng hoặc phản hồi các yêu cầu. Lớp này xác định những dịch vụ và ứng dụng internet nào mà bất kỳ người dùng nào cũng có thể truy cập. Các giao thức trong lớp ứng dụng xác định cách các gói dữ liệu sẽ tương tác với các thiết bị nhận. Một số giao thức phổ biến được sử dụng trên lớp này là:

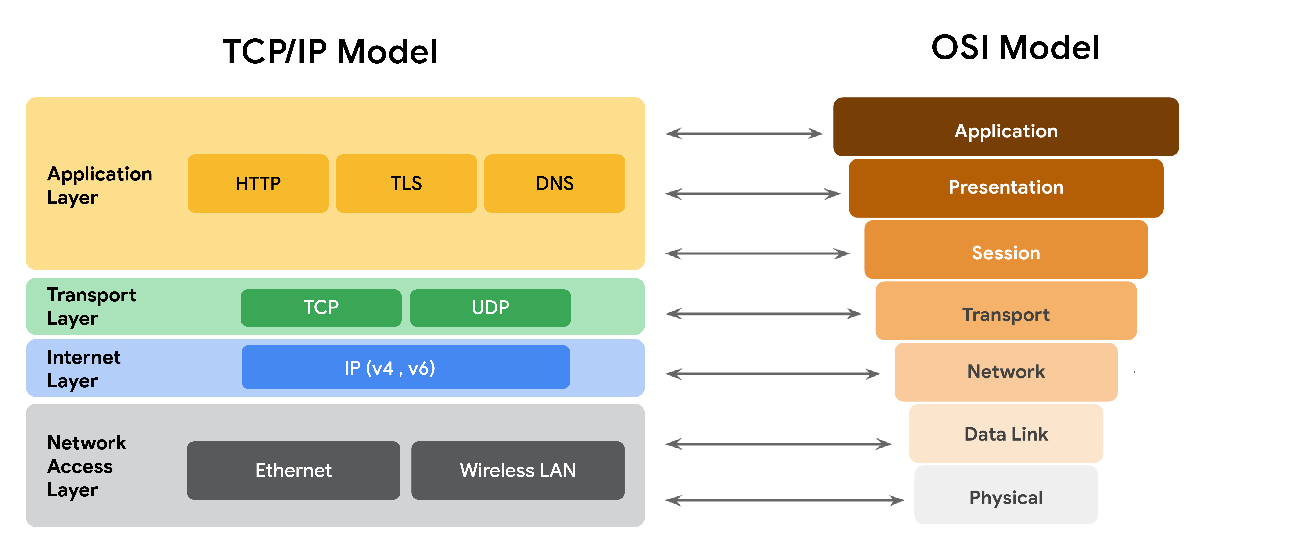
* Giao thức truyền siêu văn bản (HTTP)
* Giao thức truyền thư đơn giản (SMTP)
* Vỏ bảo mật (SSH)
* Giao thức truyền tệp (FTP)
* Hệ thống tên miền (DNS)

|  |
| --- |
| Application layer protocols rely on underlying layers to transfer the data across the network. |

Các giao thức lớp ứng dụng dựa vào các lớp bên dưới để truyền dữ liệu qua mạng.

|  |
| --- |
| **TCP/IP model versus OSI model** |

**Mô hình TCP/IP so với mô hình OSI**



|  |
| --- |
| The **OSI** visually organizes network protocols into different layers. Network professionals often use this model to communicate with each other about potential sources of problems or security threats when they occur. |

OSI tổ **chức** trực quan các giao thức mạng thành các lớp khác nhau. Các chuyên gia mạng thường sử dụng mô hình này để liên lạc với nhau về các nguồn gốc của sự cố hoặc mối đe dọa bảo mật tiềm ẩn khi chúng xảy ra.

|  |
| --- |
| The TCP/IP model combines multiple layers of the OSI model. There are many similarities between the two models. Both models define standards for networking and divide the network communication process into different layers. The TCP/IP model is a simplified version of the OSI model. |

Mô hình TCP/IP kết hợp nhiều lớp của mô hình OSI. Có nhiều điểm tương đồng giữa hai mô hình. Cả hai mô hình đều xác định các tiêu chuẩn cho mạng và chia quá trình giao tiếp mạng thành các lớp khác nhau. Mô hình TCP/IP là phiên bản đơn giản hóa của mô hình OSI.

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

**Bài học chính**

|  |
| --- |
| Both the TCP/IP and OSI models are conceptual models that help network professionals visualize network processes and protocols in regards to data transmission between two or more systems. The TCP/IP model contains four layers, and the OSI model contains seven layers. |

Cả hai mô hình TCP/IP và OSI đều là các mô hình khái niệm giúp các chuyên gia mạng trực quan hóa các quy trình và giao thức mạng liên quan đến việc truyền dữ liệu giữa hai hoặc nhiều hệ thống. Mô hình TCP/IP chứa bốn lớp và mô hình OSI chứa bảy lớp.

***3.5. The OSI model – Mô hình OSI***

|  |
| --- |
| **The OSI model** |

**Mô hình OSI**

|  |
| --- |
| So far in this section of the course, you learned about the components of a network, network devices, and how communication occurs across a network. You also studied the TCP/IP model to understand how network communication is organized across different layers of the internet. |

Cho đến nay trong phần này của khóa học, bạn đã tìm hiểu về các thành phần của mạng, thiết bị mạng và cách giao tiếp diễn ra trên mạng. Bạn cũng đã nghiên cứu mô hình TCP/IP để hiểu cách tổ chức giao tiếp mạng giữa các lớp khác nhau của Internet.

|  |
| --- |
| All communication on a network is organized using network protocols. Previously, you learned about the Transmission Control Protocol (TCP), which establishes connections between two devices, and the Internet Protocol (IP), which is used for routing and addressing data packets as they travel between devices on a network. These protocols are used on specific internet layers in the TCP/IP model. The 4-layer TCP/IP model is a condensed form of the OSI (open Systems Interconnection) model, which is made up of 7 layers. The OSI model will provide a more in depth understanding of the processes that occur at each layer. We will work backwards from layer seven to layer one, going from the processes that involve direct user interaction with the network to those that involve the physical connection to the internet via network components like cables and switches. This reading will also review the main differences between the TCP/IP and OSI models. |

Tất cả thông tin liên lạc trên mạng được tổ chức bằng các giao thức mạng. Trước đây, bạn đã tìm hiểu về Giao thức điều khiển truyền dẫn (TCP), thiết lập kết nối giữa hai thiết bị và Giao thức Internet (IP), được sử dụng để định tuyến và đánh địa chỉ các gói dữ liệu khi chúng di chuyển giữa các thiết bị trên mạng. Các giao thức này được sử dụng trên các lớp internet cụ thể trong mô hình TCP/IP. Mô hình TCP/IP 4 lớp là dạng rút gọn của mô hình OSI (Kết nối hệ thống mở), được tạo thành từ 7 lớp. Mô hình OSI sẽ cung cấp sự hiểu biết sâu sắc hơn về các quá trình xảy ra ở mỗi lớp. Chúng tôi sẽ làm việc ngược lại từ lớp bảy đến lớp một, đi từ các quy trình liên quan đến tương tác trực tiếp của người dùng với mạng đến các quy trình liên quan đến kết nối vật lý với Internet thông qua các thành phần mạng như cáp và bộ chuyển mạch. Bài đọc này cũng sẽ xem xét những khác biệt chính giữa mô hình TCP/IP và OSI.

|  |
| --- |
| **The TCP/IP model vs. the OSI model** |

**Mô hình TCP/IP so với mô hình OSI**

|  |
| --- |
| The **TCP/IP model** is a framework used to visualize how data is organized and transmitted across a network. This model helps network engineers and security analysts conceptualize processes on the network and communicate where disruptions or security threats occur. |

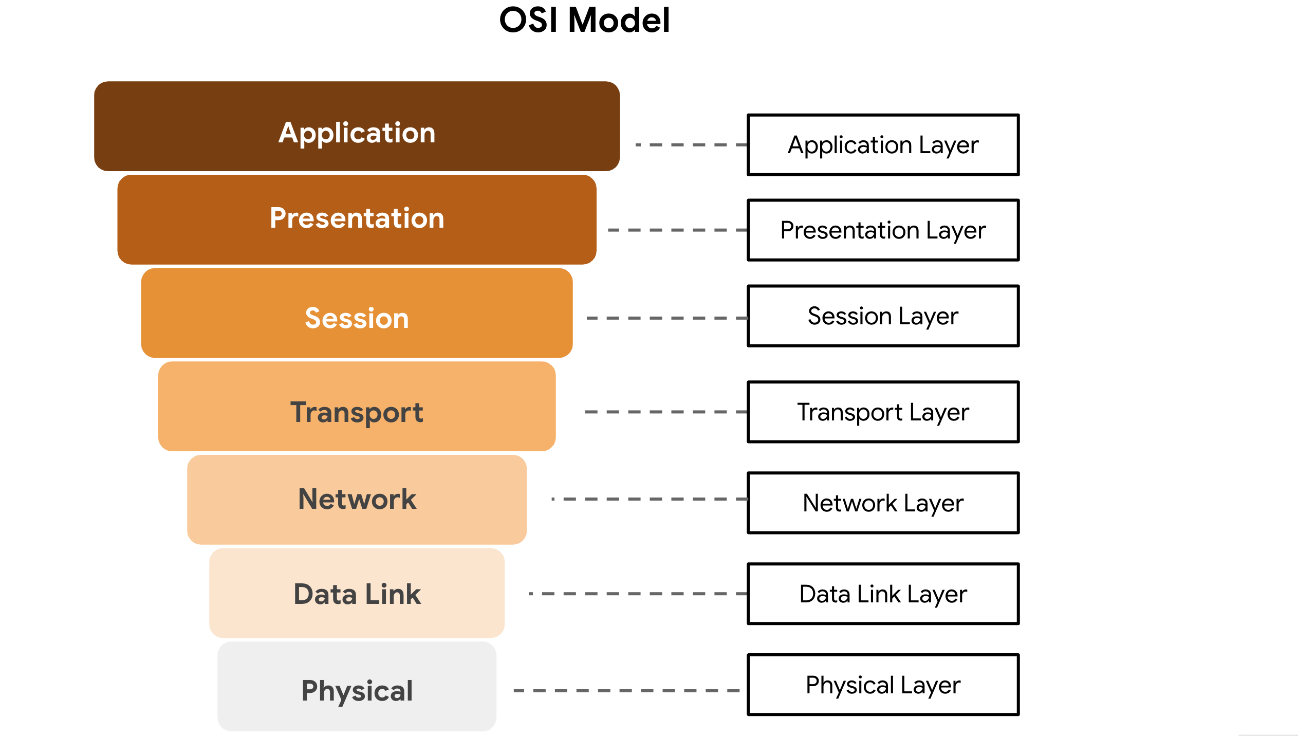
Mô **hình TCP/IP** là một khung được sử dụng để trực quan hóa cách tổ chức và truyền dữ liệu qua mạng. Mô hình này giúp các kỹ sư mạng và nhà phân tích bảo mật khái niệm hóa các quy trình trên mạng và liên lạc khi xảy ra sự gián đoạn hoặc mối đe dọa bảo mật.

|  |
| --- |
| The TCP/IP model has four layers: the network access layer, internet layer, transport layer, and application layer. When analyzing network events, security professionals can determine what layer or layers an attack occurred in based on what processes were involved in the incident. |

Mô hình TCP/IP có bốn lớp: lớp truy cập mạng, lớp internet, lớp vận chuyển và lớp ứng dụng. Khi phân tích các sự kiện mạng, các chuyên gia bảo mật có thể xác định cuộc tấn công đã xảy ra ở lớp nào hoặc nhiều lớp hơn dựa trên những quy trình liên quan đến vụ việc.

|  |
| --- |
| The **OSI model** is a standardized concept that describes the seven layers computers use to communicate and send data over the network. Network and security professionals often use this model to communicate with each other about potential sources of problems or security threats when they occur. |

Mô **hình OSI** là một khái niệm được tiêu chuẩn hóa mô tả bảy lớp máy tính sử dụng để giao tiếp và gửi dữ liệu qua mạng. Các chuyên gia mạng và bảo mật thường sử dụng mô hình này để liên lạc với nhau về các nguồn gốc của sự cố hoặc mối đe dọa bảo mật tiềm ẩn khi chúng xảy ra.



|  |
| --- |
| Some organizations rely heavily on the TCP/IP model, while others prefer to use the OSI model. As a security analyst, it’s important to be familiar with both models. Both the TCP/IP and OSI models are useful for understanding how networks work. |

Một số tổ chức phụ thuộc nhiều vào mô hình TCP/IP, trong khi những tổ chức khác thích sử dụng mô hình OSI hơn. Là một nhà phân tích bảo mật, điều quan trọng là phải làm quen với cả hai mô hình. Cả hai mô hình TCP/IP và OSI đều hữu ích để hiểu cách hoạt động của mạng.

|  |
| --- |
| **Layer 7: Application layer** |

**Lớp 7: Lớp ứng dụng**

|  |
| --- |
| The application layer includes processes that directly involve the everyday user. This layer includes all of the networking protocols that software applications use to connect a user to the internet. This characteristic is the identifying feature of the application layer—user connection to the internet via applications and requests. |

Lớp ứng dụng bao gồm các quy trình liên quan trực tiếp đến người dùng hàng ngày. Lớp này bao gồm tất cả các giao thức mạng mà các ứng dụng phần mềm sử dụng để kết nối người dùng với internet. Đặc điểm này là đặc điểm nhận dạng của lớp ứng dụng—kết nối người dùng với internet thông qua các ứng dụng và yêu cầu.

|  |
| --- |
| An example of a type of communication that happens at the application layer is using a web browser. The internet browser uses HTTP or HTTPS to send and receive information from the website server. The email application uses simple mail transfer protocol (SMTP) to send and receive email information. Also, web browsers use the domain name system (DNS) protocol to translate website domain names into IP addresses which identify the web server that hosts the information for the website. |

Một ví dụ về loại giao tiếp xảy ra ở lớp ứng dụng là sử dụng trình duyệt web. Trình duyệt internet sử dụng HTTP hoặc HTTPS để gửi và nhận thông tin từ máy chủ trang web. Ứng dụng email sử dụng giao thức truyền thư đơn giản (SMTP) để gửi và nhận thông tin email. Ngoài ra, các trình duyệt web sử dụng giao thức hệ thống tên miền (DNS) để dịch tên miền của trang web thành địa chỉ IP xác định máy chủ web lưu trữ thông tin cho trang web.

|  |
| --- |
| **Layer 6: Presentation layer** |

**Lớp 6: Lớp trình bày**

|  |
| --- |
| Functions at the presentation layer involve data translation and encryption for the network. This layer adds to and replaces data with formats that can be understood by applications (layer 7) on both sending and receiving systems. Formats at the user end may be different from those of the receiving system. Processes at the presentation layer require the use of a standardized format. |

Các chức năng ở lớp trình bày liên quan đến việc dịch dữ liệu và mã hóa mạng. Lớp này bổ sung và thay thế dữ liệu bằng các định dạng mà các ứng dụng (lớp 7) có thể hiểu được trên cả hệ thống gửi và nhận. Các định dạng ở cuối người dùng có thể khác với định dạng của hệ thống nhận. Các quy trình ở lớp trình bày yêu cầu sử dụng định dạng chuẩn hóa.

|  |
| --- |
| Some formatting functions that occur at layer 6 include encryption, compression, and confirmation that the character code set can be interpreted on the receiving system. One example of encryption that takes place at this layer is SSL, which encrypts data between web servers and browsers as part of websites with HTTPS. |

Một số chức năng định dạng xảy ra ở lớp 6 bao gồm mã hóa, nén và xác nhận rằng bộ mã ký tự có thể được giải thích trên hệ thống nhận. Một ví dụ về mã hóa diễn ra ở lớp này là SSL, mã hóa dữ liệu giữa máy chủ web và trình duyệt như một phần của trang web có HTTPS.

|  |
| --- |
| **Layer 5: Session layer** |

**Lớp 5: Lớp phiên**

|  |
| --- |
| A session describes when a connection is established between two devices. An open session allows the devices to communicate with each other. Session layer protocols keep the session open while data is being transferred and terminate the session once the transmission is complete. |

Phiên mô tả thời điểm kết nối được thiết lập giữa hai thiết bị. Phiên mở cho phép các thiết bị giao tiếp với nhau. Các giao thức lớp phiên giữ cho phiên mở trong khi dữ liệu đang được truyền và kết thúc phiên sau khi quá trình truyền hoàn tất.

|  |
| --- |
| The session layer is also responsible for activities such as authentication, reconnection, and setting checkpoints during a data transfer. If a session is interrupted, checkpoints ensure that the transmission picks up at the last session checkpoint when the connection resumes. Sessions include a request and response between applications. Functions in the session layer respond to requests for service from processes in the presentation layer (layer 6) and send requests for services to the transport layer (layer 4). |

Lớp phiên cũng chịu trách nhiệm về các hoạt động như xác thực, kết nối lại và thiết lập các điểm kiểm tra trong quá trình truyền dữ liệu. Nếu một phiên bị gián đoạn, các điểm kiểm tra sẽ đảm bảo rằng quá trình truyền sẽ được bắt đầu ở điểm kiểm tra phiên cuối cùng khi kết nối tiếp tục. Phiên bao gồm một yêu cầu và phản hồi giữa các ứng dụng. Các chức năng trong lớp phiên đáp ứng các yêu cầu dịch vụ từ các tiến trình trong lớp trình bày (lớp 6) và gửi yêu cầu dịch vụ đến lớp vận chuyển (lớp 4).

|  |
| --- |
| **Layer 4: Transport layer** |

**Lớp 4: Lớp vận chuyển**

|  |
| --- |
| The transport layer is responsible for delivering data between devices. This layer also handles the speed of data transfer, flow of the transfer, and breaking data down into smaller segments to make them easier to transport. Segmentation is the process of dividing up a large data transmission into smaller pieces that can be processed by the receiving system. These segments need to be reassembled at their destination so they can be processed at the session layer (layer 5). The speed and rate of the transmission also has to match the connection speed of the destination system. TCP and UDP are transport layer protocols. |

Lớp vận chuyển chịu trách nhiệm phân phối dữ liệu giữa các thiết bị. Lớp này cũng xử lý tốc độ truyền dữ liệu, luồng truyền và chia dữ liệu thành các phân đoạn nhỏ hơn để giúp chúng dễ vận chuyển hơn. Phân đoạn là quá trình chia việc truyền dữ liệu lớn thành các phần nhỏ hơn để hệ thống nhận có thể xử lý. Các phân đoạn này cần được tập hợp lại tại đích để chúng có thể được xử lý ở lớp phiên (lớp 5). Tốc độ và tốc độ truyền cũng phải phù hợp với tốc độ kết nối của hệ thống đích. TCP và UDP là các giao thức lớp vận chuyển.

|  |
| --- |
| **Layer 3: Network layer** |

**Lớp 3: Lớp mạng**

|  |
| --- |
| The network layer oversees receiving the frames from the data link layer (layer 2) and delivers them to the intended destination. The intended destination can be found based on the address that resides in the frame of the data packets. Data packets allow communication between two networks. These packets include IP addresses that tell routers where to send them. They are routed from the sending network to the receiving network. |

Lớp mạng giám sát việc nhận các khung từ lớp liên kết dữ liệu (lớp 2) và đưa chúng đến đích đã định. Điểm đến dự định có thể được tìm thấy dựa trên địa chỉ nằm trong khung của gói dữ liệu. Gói dữ liệu cho phép liên lạc giữa hai mạng. Các gói này bao gồm các địa chỉ IP cho bộ định tuyến biết nơi gửi chúng. Chúng được định tuyến từ mạng gửi đến mạng nhận.

|  |
| --- |
| **Layer 2: Data link layer** |

**Lớp 2: Lớp liên kết dữ liệu**

|  |
| --- |
| The data link layer organizes sending and receiving data packets within a single network. The data link layer is home to switches on the local network and network interface cards on local devices. |

Lớp liên kết dữ liệu tổ chức việc gửi và nhận các gói dữ liệu trong một mạng duy nhất. Lớp liên kết dữ liệu là nơi chuyển mạch mạng cục bộ và các card giao diện mạng trên các thiết bị cục bộ.

|  |
| --- |
| Protocols like network control protocol (NCP), high-level data link control (HDLC), and synchronous data link control protocol (SDLC) are used at the data link layer. |

Các giao thức như giao thức điều khiển mạng (NCP), điều khiển liên kết dữ liệu cấp cao (HDLC) và giao thức điều khiển liên kết dữ liệu đồng bộ (SDLC) được sử dụng ở lớp liên kết dữ liệu.

|  |
| --- |
| **Layer 1: Physical layer** |

**Lớp 1: Lớp vật lý**

|  |
| --- |
| As the name suggests, the physical layer corresponds to the physical hardware involved in network transmission. Hubs, modems, and the cables and wiring that connect them are all considered part of the physical layer. To travel across an ethernet or coaxial cable, a data packet needs to be translated into a stream of 0s and 1s. The stream of 0s and 1s are sent across the physical wiring and cables, received, and then passed on to higher levels of the OSI model. |

Như tên cho thấy, lớp vật lý tương ứng với phần cứng vật lý liên quan đến việc truyền tải mạng. Hub, modem, cáp và hệ thống dây điện kết nối chúng đều được coi là một phần của lớp vật lý. Để truyền qua cáp ethernet hoặc cáp đồng trục, gói dữ liệu cần được dịch thành luồng 0 và 1. Luồng 0 và 1 được gửi qua hệ thống dây và cáp vật lý, được nhận và sau đó được chuyển lên các cấp độ cao hơn của mô hình OSI.

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

**Bài học chính**

|  |
| --- |
| Both the TCP/IP and OSI models are conceptual models that help network professionals design network processes and protocols with regards to data transmission between two or more systems. The OSI model contains seven communication layers. Network and security professionals use the OSI model to communicate with each other about potential sources of problems or security threats when they occur.  Network engineers and network security analysts use the TCP/IP and OSI models to conceptualize network processes and communicate the location of disruptions or threats. |

Cả hai mô hình TCP/IP và OSI đều là các mô hình khái niệm giúp các chuyên gia mạng thiết kế các quy trình và giao thức mạng liên quan đến việc truyền dữ liệu giữa hai hoặc nhiều hệ thống. Mô hình OSI chứa bảy lớp truyền thông. Các chuyên gia mạng và bảo mật sử dụng mô hình OSI để liên lạc với nhau về các nguồn gốc tiềm ẩn của sự cố hoặc các mối đe dọa bảo mật khi chúng xảy ra. Các kỹ sư mạng và nhà phân tích bảo mật mạng sử dụng mô hình TCP/IP và OSI để khái niệm hóa các quy trình mạng và thông báo vị trí của sự gián đoạn hoặc mối đe dọa.

***3.6. Test your knowledge: Network communication – Kiểm tra kiến ​​thức của bạn: Truyền thông mạng***

**4. Local and wide network communication – Truyền thông mạng cục bộ và mạng rộng**

***4.1. IP addresses and network communication – Địa chỉ IP và truyền thông mạng***

|  |
| --- |
| Let's learn about how IP addresses are used to communicate over a network. IP stands for internet protocol. An internet protocol address, or IP address, is a unique string of characters that identifies a location of a device on the internet. Each device on the internet has a unique IP address, just like every house on a street has its own mailing address. |

Chúng ta hãy tìm hiểu về cáchĐịa chỉ IP được sử dụng để liên lạc qua mạng.IP là viết tắt của giao thức internet.Địa chỉ giao thức internet hoặc địa chỉ IP làmột chuỗi ký tự duy nhất xác địnhvị trí của một thiết bị trên internet.Mỗi thiết bị trên internet có một địa chỉ IP duy nhất,giống như mọi ngôi nhà trên phốcó địa chỉ gửi thư riêng.

|  |
| --- |
| There are two types of IP addresses: IP version 4, or IPv4, and IP version 6, or IPv6. Let's look at examples of an IPv4 address. |

Có hai loại địa chỉ IP:IP phiên bản 4 hoặc IPv4,và IP phiên bản 6 hoặc IPv6.Hãy xem các ví dụ về địa chỉ IPv4.

|  |
| --- |
| IPv4 addresses are written as four, 1, 2, or 3-digit numbers separated by a decimal point. In the early days of the internet, IP addresses were all IPV4. But as the use of the internet grew, all the IPv4 addresses started to get used up, so IPv6 was developed. |

Địa chỉ IPv4 được viết dưới dạng bốn ,Các số có 1, 2 hoặc 3 chữ số cách nhau bằng dấu thập phân.Trong những ngày đầu của Internet,Địa chỉ IP đều làIPV4. Nhưng khi việc sử dụng Internet ngày càng tăng,tất cả các địa chỉ IPv4 bắt đầu nhận đượcđã cạn kiệt nên IPv6 được phát triển.

|  |
| --- |
| IPv6 addresses are made up of 32 characters. The length of the IPv6 address will allow for more devices to be connected to the internet without running out of addresses as quickly as IPv4. |

Địa chỉ IPv6 được tạo thành từ 32 ký tự.Độ dài của địa chỉ IPv6sẽ cho phép kết nối nhiều thiết bị hơnvào internet mà không hếtđịa chỉ nhanh như IPv4.

|  |
| --- |
| IP addresses can be either public or private. Your internet service provider assigns a public IP address that is connected to your geographic location. When network communications goes out from your device on the internet, they all have the same public-facing address. Just like all the roommates in one home share the same mailing address, all the devices on a network share the same public-facing IP address. |

Địa chỉ IP có thể là công khai hoặc riêng tư.Nhà cung cấp dịch vụ internet của bạn chỉ địnhmột địa chỉ IP công cộng đượcđược kết nối với vị trí địa lý của bạn.Khi truyền thông mạng đitừ thiết bị của bạn trên internet,tất cả họ đều có cùng một địa chỉ công khai.Giống như tất cả bạn cùng phòng trongmột ngôi nhà có chung địa chỉ gửi thư,tất cả các thiết bị trên mạng chia sẻcùng một địa chỉ IP công khai.

|  |
| --- |
| Private IP addresses are only seen by other devices on the same local network. This means that all the devices on your home network can communicate with each other using unique IP addresses that the rest of the internet can't see. |

Địa chỉ IP riêng tư chỉ được nhìn thấybởi các thiết bị khác trên cùng một mạng cục bộ.Điều này có nghĩa là tất cả các thiết bị trênmạng gia đình của bạn có thể liên lạc với nhausử dụng địa chỉ IP duy nhấtmà phần còn lại của Internet không thể nhìn thấy.

|  |
| --- |
| Another kind of address used in network communications is called a MAC address. A MAC address is a unique alphanumeric identifier that is assigned to each physical device on a network. When a switch receives a data packet, it reads the MAC address of the destination device and maps it to a port. It then keeps this information in a MAC address table. Think of the MAC address table like an address book that the switch uses to direct data packets to the appropriate device. |

Một loại địa chỉ khác được sử dụng trongthông tin liên lạc mạng được gọi là địa chỉ MAC.Một địa chỉ MAC làmột mã định danh chữ và số duy nhất đó làđược gán cho mỗi thiết bị vật lý trên mạng.Khi một switch nhận được một gói dữ liệu,nó đọc địa chỉ MAC củathiết bị đích và ánh xạ nó tới một cổng.Sau đó nó giữ thông tin này trong bảng địa chỉ MAC.Hãy nghĩ đến bảng địa chỉ MACgiống như một sổ địa chỉ mà switchsử dụng để hướng các gói dữ liệu đến thiết bị thích hợp.

|  |
| --- |
| In this video, you learned about IP version 4 and IP version 6 addresses. You learned how IP and MAC addresses are used in network communication and the difference between a public and a private IP address. |

Trong video này, bạn đã tìm hiểu vềĐịa chỉ IP phiên bản 4 và IP phiên bản 6.Bạn đã tìm hiểu cách sử dụng địa chỉ IP và MAC trongtruyền thông mạng và sự khác biệtgiữa địa chỉ IP công cộng và địa chỉ IP riêng.

***4.2. Components of network layer communication – Các thành phần của giao tiếp lớp mạng***

|  |
| --- |
| **Components of network layer communication** |

**Các thành phần của giao tiếp lớp mạng**

|  |
| --- |
| In the reading about the [OSI model](https://www.coursera.org/learn/networks-and-network-security/supplement/YbKL0/the-osi-model-explained), you learned about the seven layers of the OSI model that are used to conceptualize the way data is transmitted across the internet. In this reading, you will learn more about operations that take place at layer 3 of the OSI model: the network layer. |

Trong bài đọc về[mô hình OSI](https://www.coursera.org/learn/networks-and-network-security/supplement/YbKL0/the-osi-model-explained), bạn đã tìm hiểu về bảy lớp của mô hình OSI được sử dụng để khái niệm hóa cách truyền dữ liệu qua internet. Trong bài đọc này, bạn sẽ tìm hiểu thêm về các hoạt động diễn ra ở lớp 3 của mô hình OSI: lớp mạng.

|  |
| --- |
| **Operations at the network layer** |

**Hoạt động ở lớp mạng**

|  |
| --- |
| Functions at the network layer organize the addressing and delivery of data packets across the network from the host device to the destination device. This includes directing the packets from one router to another router across the internet, till it reaches the internet protocol (IP) address of the destination network. The destination IP address is contained within the header of each data packet. This address will be stored for future routing purposes in  routing tables along the packet’s path to its destination. |

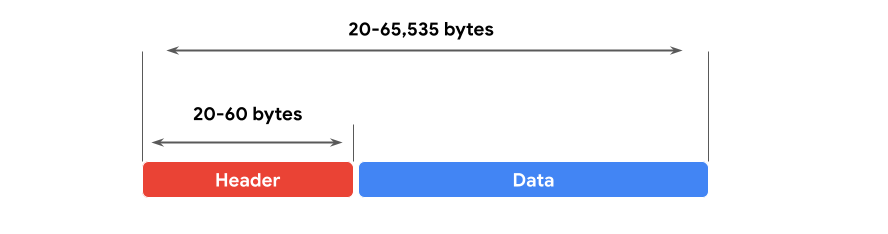
Các chức năng ở lớp mạng tổ chức việc đánh địa chỉ và phân phối các gói dữ liệu trên mạng từ thiết bị chủ đến thiết bị đích. Điều này bao gồm việc chuyển hướng các gói từ bộ định tuyến này sang bộ định tuyến khác trên internet cho đến khi nó đến được địa chỉ giao thức internet (IP) của mạng đích. Địa chỉ IP đích được chứa trong tiêu đề của mỗi gói dữ liệu. Địa chỉ này sẽ được lưu trữ cho mục đích định tuyến trong tương lai trong bảng định tuyến dọc theo đường dẫn của gói đến đích.

|  |
| --- |
| All data packets include an IP address. A data packet is also referred to as an IP packet for TCP connections or a datagram for UDP connections. A router uses the IP address to route packets from network to network based on information contained in the IP header of a data packet. Header information communicates more than just the address of the destination. It also includes information such as the source IP address, the size of the packet, and which protocol will be used for the data portion of the packet. |

Tất cả các gói dữ liệu bao gồm một địa chỉ IP. Gói dữ liệu còn được gọi là gói IP cho kết nối TCP hoặc gói dữ liệu cho kết nối UDP. Bộ định tuyến sử dụng địa chỉ IP để định tuyến các gói từ mạng này sang mạng khác dựa trên thông tin có trong tiêu đề IP của gói dữ liệu. Thông tin tiêu đề không chỉ truyền tải thông tin về địa chỉ đích. Nó cũng bao gồm các thông tin như địa chỉ IP nguồn, kích thước của gói và giao thức nào sẽ được sử dụng cho phần dữ liệu của gói.

|  |
| --- |
| **Format of an IPv4 packet** |

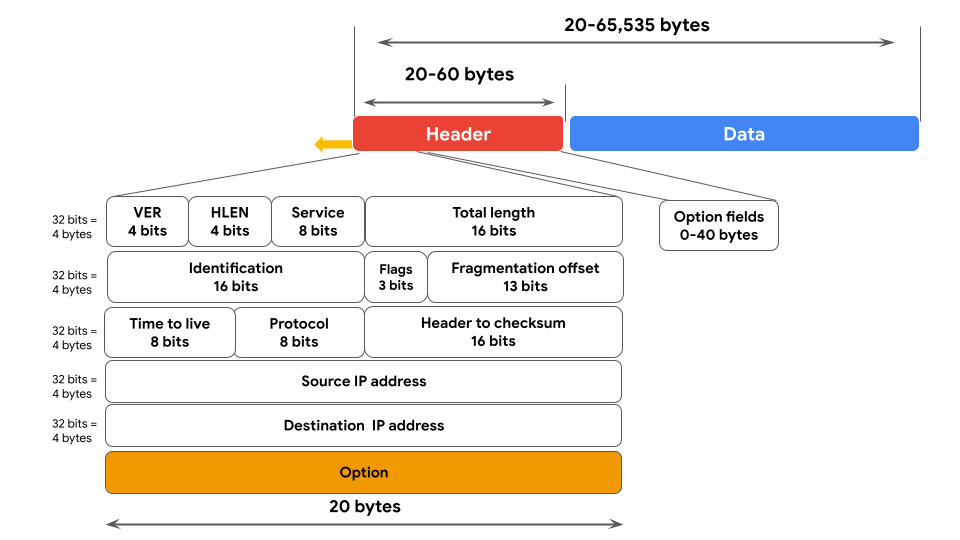
**Định dạng của gói IPv4**



|  |
| --- |
| Next, you can review the format of an IP version 4 (Ipv4) packet and review a detailed graphic of the packet header. An IPv4 packet is made up of two sections, the header and the data:   * An IPv4 header format is determined by the IPv4 protocol and includes the IP routing information that devices use to direct the packet. The size of the IPv4 header ranges from 20 to 60 bytes. The first 20 bytes are a fixed set of information containing data such as the source and destination IP address, header length, and total length of the packet. The last set of bytes can range from 0 to 40 and consists of the options field. * The length of the data section of an IPv4 packet can vary greatly in size. However, the maximum possible size of an IPv4 packet is 65,535 bytes. It contains the message being transferred over the internet, like website information or email text. |

Tiếp theo, bạn có thể xem lại định dạng của gói IP phiên bản 4 (IPv4) và xem lại hình ảnh chi tiết của tiêu đề gói. Một gói IPv4 được tạo thành từ hai phần, tiêu đề và dữ liệu:

* Định dạng tiêu đề IPv4 được xác định bởi giao thức IPv4 và bao gồm thông tin định tuyến IP mà thiết bị sử dụng để định hướng gói. Kích thước của tiêu đề IPv4 dao động từ 20 đến 60 byte. 20 byte đầu tiên là một tập hợp thông tin cố định chứa dữ liệu như địa chỉ IP nguồn và đích, độ dài tiêu đề và tổng chiều dài của gói. Tập byte cuối cùng có thể nằm trong khoảng từ 0 đến 40 và bao gồm trường tùy chọn.
* Độ dài của phần dữ liệu của gói IPv4 có thể khác nhau rất nhiều về kích thước. Tuy nhiên, kích thước tối đa có thể có của gói IPv4 là 65.535 byte. Nó chứa tin nhắn được chuyển qua internet, như thông tin trang web hoặc văn bản email.



|  |
| --- |
| There are 13 fields within the header of an IPv4 packet:   * **Version (VER):** This 4 bit component tells receiving devices what protocol the packet is using. The packet used in the illustration above is an IPv4 packet. * **IP Header Length (HLEN or IHL):** HLEN is the packet’s header length. This value indicates where the packet header ends and the data segment begins. * **Type of Service (ToS):** Routers prioritize packets for delivery to maintain quality of service on the network. The ToS field provides the router with this information. * **Total Length:** This field communicates the total length of the entire IP packet, including the header and data. The maximum size of an IPv4 packet is 65,535 bytes. * **Identification:** IPv4 packets can be up to 65, 535 bytes, but most networks have a smaller limit. In these cases, the packets are divided, or fragmented, into smaller IP packets. The identification field provides a unique identifier for all the fragments of the original IP packet so that they can be reassembled once they reach their destination. * **Flags:** This field provides the routing device with more information about whether the original packet has been fragmented and if there are more fragments in transit. * **Fragmentation Offset:** The fragment offset field tells routing devices where in the original packet the fragment belongs. * **Time to Live (TTL):** TTL prevents data packets from being forwarded by routers indefinitely. It contains a counter that is set by the source. The counter is decremented by one as it passes through each router along its path. When the TTL counter reaches zero, the router currently holding the packet will discard the packet and return an ICMP Time Exceeded error message to the sender. * **Protocol:** The protocol field tells the receiving device which protocol will be used for the data portion of the packet. * **Header Checksum:** The header checksum field contains a checksum that can be used to detect corruption of the IP header in transit. Corrupted packets are discarded. * **Source IP Address:** The source IP address is the IPv4 address of the sending device. * **Destination IP Address:** The destination IP address is the IPv4 address of the destination device. * **Options:** The options field allows for security options to be applied to the packet if the HLEN value is greater than five. The field communicates these options to the routing devices. |

Có 13 trường trong tiêu đề của gói IPv4:

* **Phiên bản (VER):** Thành phần 4 bit này cho thiết bị nhận biết gói đang sử dụng giao thức nào. Gói được sử dụng trong hình minh họa ở trên là gói IPv4.
* **Độ dài tiêu đề IP (HLEN hoặc IHL):** HLEN là độ dài tiêu đề của gói. Giá trị này cho biết nơi tiêu đề gói kết thúc và phân đoạn dữ liệu bắt đầu.
* **Loại dịch vụ (ToS):** Bộ định tuyến ưu tiên phân phối các gói để duy trì chất lượng dịch vụ trên mạng. Trường ToS cung cấp cho bộ định tuyến thông tin này.
* **Tổng chiều dài:** Trường này cho biết tổng chiều dài của toàn bộ gói IP, bao gồm tiêu đề và dữ liệu. Kích thước tối đa của gói IPv4 là 65.535 byte.
* **Nhận dạng:** Các gói IPv4 có thể lên tới 65, 535 byte, nhưng hầu hết các mạng đều có giới hạn nhỏ hơn. Trong những trường hợp này, các gói được chia hoặc phân mảnh thành các gói IP nhỏ hơn. Trường nhận dạng cung cấp một mã định danh duy nhất cho tất cả các phân đoạn của gói IP gốc để chúng có thể được tập hợp lại sau khi đến đích.
* **Cờ:** Trường này cung cấp cho thiết bị định tuyến nhiều thông tin hơn về việc liệu gói gốc có bị phân mảnh hay không và liệu có nhiều phân mảnh hơn trong quá trình truyền hay không.
* **Độ lệch phân mảnh:** Trường bù phân mảnh cho các thiết bị định tuyến biết phân đoạn đó thuộc về đâu trong gói gốc.
* **Thời gian tồn tại (TTL):** TTL ngăn các gói dữ liệu được chuyển tiếp vô thời hạn bởi các bộ định tuyến. Nó chứa một bộ đếm được thiết lập bởi nguồn. Bộ đếm giảm đi một khi nó đi qua mỗi bộ định tuyến dọc theo đường dẫn của nó. Khi bộ đếm TTL về 0, bộ định tuyến hiện đang giữ gói sẽ loại bỏ gói và trả về thông báo lỗi ICMP Time Exceeded cho người gửi.
* **Giao thức:** Trường giao thức cho thiết bị nhận biết giao thức nào sẽ được sử dụng cho phần dữ liệu của gói.
* **Tổng kiểm tra tiêu đề:** Trường tổng kiểm tra tiêu đề chứa tổng kiểm tra có thể được sử dụng để phát hiện lỗi tiêu đề IP trong quá trình truyền. Các gói bị hỏng sẽ bị loại bỏ.
* **Địa chỉ IP nguồn:** Địa chỉ IP nguồn là địa chỉ IPv4 của thiết bị gửi.
* **Địa chỉ IP đích:** Địa chỉ IP đích là địa chỉ IPv4 của thiết bị đích.
* **Tùy chọn:** Trường tùy chọn cho phép áp dụng các tùy chọn bảo mật cho gói nếu giá trị HLEN lớn hơn năm. Trường truyền đạt các tùy chọn này đến các thiết bị định tuyến.

|  |
| --- |
| **Difference between IPv4 and IPv6** |

**Sự khác biệt giữa IPv4 và IPv6**

|  |
| --- |
| In an earlier part of this course, you learned about the history of IP addressing. As the internet grew, it became clear that all of the IPv4 addresses would eventually be depleted; this is called IPv4 address exhaustion. At the time, no one had anticipated how many computing devices would need an IP address. IPv6 was developed to mitigate IPv4 address exhaustion and other related concerns. |

Trong phần trước của khóa học này, bạn đã tìm hiểu về lịch sử của địa chỉ IP. Khi Internet phát triển, rõ ràng là tất cả các địa chỉ IPv4 cuối cùng sẽ cạn kiệt; điều này được gọi là cạn kiệt địa chỉ IPv4. Vào thời điểm đó, không ai lường trước được có bao nhiêu thiết bị máy tính sẽ cần địa chỉ IP. IPv6 được phát triển để giảm thiểu tình trạng cạn kiệt địa chỉ IPv4 và các vấn đề liên quan khác.

|  |
| --- |
| Some of the key differences between IPv4 and IPv6 include the length and the format of the addresses. IPv4 addresses are made up of four decimal numbers separated by periods, each number ranging from 0 to 255. Together the numbers span 4 bytes, and allow for up to 4.3 billion possible addresses. An example of an IPv4 address would be: 198.51.100.0. IPv6 addresses are made of eight hexadecimal numbers separated by colons, each number consisting of up to four hexadecimal digits. Together, all numbers span 16 bytes, and allow for up to 340 undecillion addresses (340 followed by 36 zeros). An example of an IPv6 address would be: 2002:0db8:0000:0000:0000:ff21:0023:1234. |

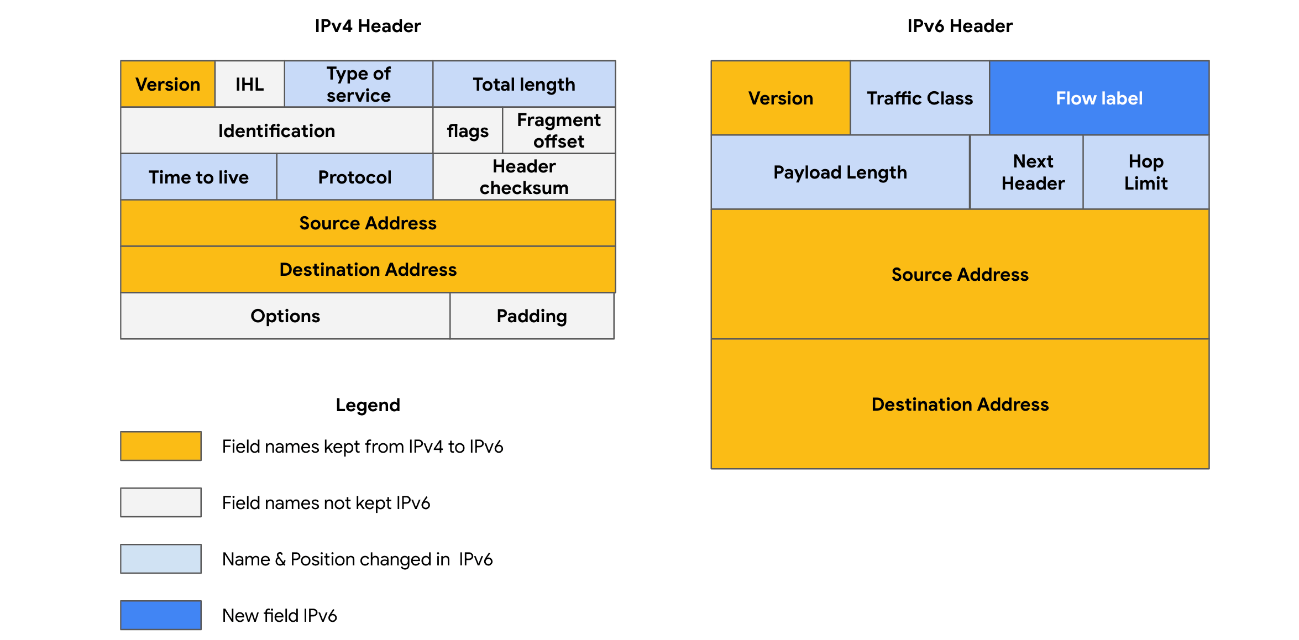
Một số khác biệt chính giữa IPv4 và IPv6 bao gồm độ dài và định dạng của địa chỉ. Địa chỉ IPv4 được tạo thành từ bốn số thập phân cách nhau bằng dấu chấm, mỗi số nằm trong khoảng từ 0 đến 255. Các số này có tổng chiều dài 4 byte và cho phép có thể có tới 4,3 tỷ địa chỉ. Một ví dụ về địa chỉ IPv4 sẽ là: 198.51.100.0. Địa chỉ IPv6 được tạo thành từ tám số thập lục phân cách nhau bằng dấu hai chấm, mỗi số bao gồm tối đa bốn chữ số thập lục phân. Cùng với nhau, tất cả các số đều trải dài 16 byte và cho phép tối đa 340 địa chỉ không có số thập phân (340 theo sau là 36 số 0). Một ví dụ về địa chỉ IPv6 sẽ là: 2002:0db8:0000:0000:0000:ff21:0023:1234.

|  |
| --- |
| ***Note:*** *to represent one or more consecutive sets of all zeros, you can replace the zeros with a double colon "::", so the above IPv6 address would be "*2002:0db8::ff21:0023:1234." |

***Lưu ý:*** *để thể hiện một hoặc nhiều bộ số 0 liên tiếp, bạn có thể thay thế các số 0 bằng dấu hai chấm kép "::", do đó địa chỉ IPv6 ở trên sẽ là "* 2002:0db8::ff21:0023:1234."

|  |
| --- |
| There are also some differences in the layout of an IPv6 packet header. The IPv6 header format is much simpler than IPv4. For example, the IPv4 Header includes the IHL, Identification, and Flags fields, whereas the IPv6 does not. The IPv6 header only introduces the Flow Label field, where the Flow Label identifies a packet as requiring special handling by other IPv6 routers. |

Ngoài ra còn có một số khác biệt trong cách bố trí tiêu đề gói IPv6. Định dạng tiêu đề IPv6 đơn giản hơn nhiều so với IPv4. Ví dụ: Tiêu đề IPv4 bao gồm các trường IHL, Nhận dạng và Cờ, trong khi IPv6 thì không. Tiêu đề IPv6 chỉ giới thiệu trường Nhãn luồng, trong đó Nhãn luồng xác định một gói yêu cầu xử lý đặc biệt bởi các bộ định tuyến IPv6 khác.



|  |
| --- |
| There are some important security differences between IPv4 and IPv6. IPv6 offers more efficient routing and eliminates private address collisions that can occur on IPv4 when two devices on the same network are attempting to use the same address. |

Có một số khác biệt quan trọng về bảo mật giữa IPv4 và IPv6. IPv6 cung cấp khả năng định tuyến hiệu quả hơn và loại bỏ xung đột địa chỉ riêng có thể xảy ra trên IPv4 khi hai thiết bị trên cùng một mạng đang cố gắng sử dụng cùng một địa chỉ.

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

**Bài học chính**

|  |
| --- |
| Analyzing the different fields in an IP data packet can be used to find out important security information about the packet. Some examples of security-related information found in IP address packets are: where the packet is coming from, where it’s going, and which protocol it’s using. Understanding the data in an IP data packet will allow you to make critical decisions about the security implications of packets that you inspect. |

Việc phân tích các trường khác nhau trong gói dữ liệu IP có thể được sử dụng để tìm hiểu thông tin bảo mật quan trọng về gói. Một số ví dụ về thông tin liên quan đến bảo mật được tìm thấy trong các gói địa chỉ IP là: gói đến từ đâu, nó sẽ đi đâu và nó đang sử dụng giao thức nào. Hiểu dữ liệu trong gói dữ liệu IP sẽ cho phép bạn đưa ra quyết định quan trọng về ý nghĩa bảo mật của gói mà bạn kiểm tra.

***4.3. Test your knowledge: Local and wide network communication – Kiểm tra kiến ​​thức của bạn: Giao tiếp mạng cục bộ và mạng rộng***

**5. Review: Network architecture – Đánh giá: Kiến trúc mạng**

***5.1. Wrap-up – Gói lại***

|  |
| --- |
| Hey, you made it! Well done! Let's wrap up what you've learned in this section of the course. |

Này, bạn đã làm được rồi!Làm tốt!Hãy tóm tắt những gì bạn đã học được trong phần này của khóa học.

|  |
| --- |
| We explored the structure of a network, including WANs and LANs. We also discussed standard networking tools like hubs, switches, routers, and modems. We briefly introduced cloud networks, and we discussed their benefits. We also spent some time on the TCP/IP model. As a reminder, technicians and security analysts often use this framework when communicating where network problems have occurred. |

Chúng tôi đã khám phá cấu trúc của mạng, bao gồm mạng WAN và mạng LAN.Chúng tôi cũng thảo luận về các công cụ mạng tiêu chuẩn như hub, switch,bộ định tuyến và modem.Chúng tôi đã giới thiệu ngắn gọn về mạng đám mây và thảo luận về lợi ích của chúng.Chúng tôi cũng đã dành chút thời gian cho mô hình TCP/IP.Xin nhắc lại, các kỹ thuật viên và nhà phân tích bảo mật thường sử dụng khuôn khổ này khiliên lạc ở nơi xảy ra sự cố mạng.

|  |
| --- |
| That wraps up this section. Next, you'll learn more about network operations and how data is transmitted over wireless networks. |

Thế là kết thúc phần này.Tiếp theo, bạn sẽ tìm hiểu thêm về hoạt động mạng vàdữ liệu được truyền qua mạng không dây như thế nào.

***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 3, Module 1** |

**Các thuật ngữ và định nghĩa trong Khóa 3, Học phần 1**

|  |
| --- |
| **Bandwidth:** The maximum data transmission capacity over a network, measured by bits per second |

**Băng thông:** Dung lượng truyền dữ liệu tối đa qua mạng, được đo bằng bit trên giây

|  |
| --- |
| **Cloud computing:** The practice of using remote servers, application, and network services that are hosted on the internet instead of on local physical devices |

**Điện toán đám mây:** Việc sử dụng các máy chủ, ứng dụng và dịch vụ mạng từ xa được lưu trữ trên internet thay vì trên các thiết bị vật lý cục bộ

|  |
| --- |
| **Cloud network:** A collection of servers or computers that stores resources and data in remote data centers that can be accessed via the internet |

**Mạng đám mây:** Tập hợp các máy chủ hoặc máy tính lưu trữ tài nguyên và dữ liệu trong các trung tâm dữ liệu từ xa có thể truy cập qua internet

|  |
| --- |
| **Data packet:** A basic unit of information that travels from one device to another within a network |

**Gói dữ liệu:** Một đơn vị thông tin cơ bản truyền từ thiết bị này sang thiết bị khác trong mạng

|  |
| --- |
| **Hub:** A network device that broadcasts information to every device on the network |

**Hub:** Một thiết bị mạng phát thông tin tới mọi thiết bị trên mạng

|  |
| --- |
| **Internet Protocol (IP):** A set of standards used for routing and addressing data packets as they travel between devices on a network |

**Giao thức Internet (IP):** Một bộ tiêu chuẩn được sử dụng để định tuyến và đánh địa chỉ các gói dữ liệu khi chúng di chuyển giữa các thiết bị trên mạng

|  |
| --- |
| **Internet Protocol (IP) address:** A unique string of characters that identifies the location of a device on the internet |

**Địa chỉ Giao thức Internet (IP):** Một chuỗi ký tự duy nhất xác định vị trí của thiết bị trên internet

|  |
| --- |
| **Local Area Network (LAN):** A network that spans small areas like an office building, a school, or a home |

**Mạng cục bộ (LAN):** Mạng trải rộng trên các khu vực nhỏ như tòa nhà văn phòng, trường học hoặc nhà riêng

|  |
| --- |
| **Media Access Control (MAC) address:** A unique alphanumeric identifier that is assigned to each physical device on a network |

**Địa chỉ Kiểm soát truy cập phương tiện (MAC):** Mã định danh chữ và số duy nhất được gán cho từng thiết bị vật lý trên mạng

|  |
| --- |
| **Modem:** A device that connects your router to the internet and brings internet access to the LAN |

**Modem:** Một thiết bị kết nối bộ định tuyến của bạn với internet và đưa truy cập internet vào mạng LAN

|  |
| --- |
| **Network:** A group of connected devices |

**Mạng:** Một nhóm các thiết bị được kết nối

|  |
| --- |
| **Open systems interconnection (OSI) model:** A standardized concept that describes the seven layers computers use to communicate and send data over the network |

**Mô hình kết nối hệ thống mở (OSI):** Một khái niệm được tiêu chuẩn hóa mô tả bảy lớp máy tính sử dụng để giao tiếp và gửi dữ liệu qua mạng

|  |
| --- |
| **Packet sniffing:** The practice of capturing and inspecting data packets across a network |

**Đánh hơi gói:** Thực hành thu thập và kiểm tra các gói dữ liệu trên mạng

|  |
| --- |
| **Port:** A software-based location that organizes the sending and receiving of data between devices on a network |

**Cổng:** Vị trí dựa trên phần mềm tổ chức việc gửi và nhận dữ liệu giữa các thiết bị trên mạng

|  |
| --- |
| **Router:** A network device that connects multiple networks together |

**Router:** Là thiết bị mạng kết nối nhiều mạng với nhau

|  |
| --- |
| **Speed:** The rate at which a device sends and receives data, measured by bits per second |

**Tốc độ:** Tốc độ thiết bị gửi và nhận dữ liệu, được đo bằng bit trên giây

|  |
| --- |
| **Switch:** A device that makes connections between specific devices on a network by sending and receiving data between them |

**Switch:** Một thiết bị tạo kết nối giữa các thiết bị cụ thể trên mạng bằng cách gửi và nhận dữ liệu giữa chúng

|  |
| --- |
| **TCP/IP model:** A framework used to visualize how data is organized and transmitted across a network |

**Mô hình TCP/IP:** Một khung được sử dụng để trực quan hóa cách tổ chức và truyền dữ liệu qua mạng

|  |
| --- |
| **Transmission Control Protocol (TCP):** An internet communication protocol that allows two devices to form a connection and stream data |

**Giao thức điều khiển truyền dẫn (TCP):** Giao thức truyền thông internet cho phép hai thiết bị tạo thành kết nối và truyền dữ liệu

|  |
| --- |
| **User Datagram Protocol (UDP):** A connectionless protocol that does not establish a connection between devices before transmissions |

**Giao thức gói dữ liệu người dùng (UDP):** Giao thức không kết nối không thiết lập kết nối giữa các thiết bị trước khi truyền

|  |
| --- |
| **Wide Area Network (WAN):** A network that spans a large geographic area like a city, state, or country |

**Mạng diện rộng (WAN):** Mạng trải rộng trên một khu vực địa lý rộng lớn như thành phố, tiểu bang hoặc quốc gia

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

**Module 2: Network operations – Điều hành mạng**

|  |
| --- |
| You will explore network protocols and how network communication can introduce vulnerabilities. In addition, you'll learn about common security measures, like firewalls, that help network operations remain safe and reliable. |

Bạn sẽ khám phá các giao thức mạng và cách giao tiếp mạng có thể gây ra các lỗ hổng. Ngoài ra, bạn sẽ tìm hiểu về các biện pháp bảo mật phổ biến, như tường lửa, giúp hoạt động mạng luôn an toàn và đáng tin cậy.

|  |
| --- |
| **Learning Objectives**   * Recognize network protocols * Describe the protocol(s) used to transmit and access data over wireless networks * Describe a firewall * Identify common network security measures and protocols |

**Mục tiêu học tập**

* Nhận biết các giao thức mạng
* Mô tả (các) giao thức được sử dụng để truyền và truy cập dữ liệu qua mạng không dây
* Mô tả tường lửa
* Xác định các biện pháp và giao thức bảo mật mạng phổ biến

**1. Introduction to network protocols – Giới thiệu các giao thức mạng**

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

|  |
| --- |
| Congratulations on the progress you've made so far! In this section, you'll learn about how networks operate using tools and protocols. These are the concepts that you'll use every day in your work as a security analyst. The tools and protocols you'll learn in this section of the program will help you protect your organization's network from attacks. Did you know that malicious actors can take advantage of data moving from one device to another on a network? Thankfully, there are tools and protocols to ensure the network stays protected against this type of threat. |

Xin chúc mừng những tiến bộ bạn đã đạt được cho đến nay!Trong phần này, bạn sẽ tìm hiểu về cáchmạng hoạt động bằng cách sử dụng các công cụ và giao thức.Đây là những khái niệm mà bạn sẽ sử dụng mọingày làm việc của bạn với tư cách là nhà phân tích chứng khoán.Các công cụ và giao thức bạn sẽ học trong phần này củachương trình sẽ giúp bạn bảo vệmạng của tổ chức bạn khỏi các cuộc tấn công.Bạn có biết rằng những kẻ độc hại có thể lợi dụngdữ liệu di chuyển từ thiết bị này sang thiết bị khác trên mạng?May mắn thay, có những công cụ vàcác giao thức để đảm bảo mạngvẫn được bảo vệ chống lại loại mối đe dọa này.

|  |
| --- |
| As an example, I once identified an attack based solely on the fact they were using the wrong protocol. The network traffic volumes were right, and it was coming from a trusted IP, but it was on the wrong protocol, which tipped us off enough to shut down the attack before they caused real damage. |

Ví dụ, tôi từng xác định một cuộc tấn côngchỉ dựa trên thực tế là họ đãsử dụng giao thức sai.Lưu lượng truy cập mạng ở mức phù hợp và nóđến từ một IP đáng tin cậy,nhưng nó sai giao thức,điều đó khiến chúng tôi đủ khó khăn để đóng cửacuộc tấn công trước khi chúng gây ra thiệt hại thực sự.

|  |
| --- |
| First, we'll discuss some common network protocols. Then we'll discuss virtual private networks, or VPNs. And finally, we'll learn about firewalls, security zones, and proxy servers. Now that you have an idea of where we're headed, let's get started. |

Đầu tiên, chúng ta sẽ thảo luận về một số giao thức mạng phổ biến.Sau đó chúng ta sẽ thảo luận về mạng riêng ảo hoặc VPN.Và cuối cùng, chúng ta sẽ tìm hiểu vềtường lửa, vùng bảo mật và máy chủ proxy.Bây giờ bạn đã biết chúng tôi đang ở đâuđầu, chúng ta hãy bắt đầu.

***1.2. Network protocols – Giao thức mạng***

|  |
| --- |
| Networks benefit from having rules. Rules ensure that data sent over the network gets to the right place. These rules are known as network protocols. Network protocols are a set of rules used by two or more devices on a network to describe the order of delivery and the structure of the data. |

Mạng được hưởng lợi từ việc có các quy tắc.Các quy tắc đảm bảo rằng dữ liệu được gửi quamạng đến đúng nơi.Những quy tắc này được gọi là giao thức mạng.Các giao thức mạng là một tập hợp cácquy tắc được sử dụng bởi hai hoặc nhiều thiết bị trênmột mạng lưới để mô tả thứ tự củaphân phối và cấu trúc của dữ liệu.

|  |
| --- |
| Let's use a scenario to demonstrate a few different types of network protocols and how they work together on a network. Say you want to access your favorite recipe website. You go to the address bar at the top of your browser and type in the website's address. For example: www.yummyrecipesforme.org. Before you gain access to the website, your device will establish communications with a web server. That communication uses a protocol called the Transmission Control Protocol, or TCP. TCP is an internet communications protocol that allows two devices to form a connection and stream data. |

Hãy sử dụng một kịch bản để chứng minhmột số loại giao thức mạng khác nhauvà cách chúng làm việc cùng nhau trên mạng.Giả sử bạn muốn truy cập trang web công thức nấu ăn yêu thích của mình.Bạn vào thanh địa chỉ ở trên cùngtrình duyệt của bạn và nhập địa chỉ của trang web.Ví dụ: www.yummyrecipesforme.org.Trước khi bạn có quyền truy cập vào trang web,thiết bị của bạn sẽ thiết lậpgiao tiếp với một máy chủ web.Giao tiếp đó sử dụng một giao thức gọi làGiao thức điều khiển truyền dẫn hoặc TCP.TCP là một giao thức truyền thông internet cho phéphai thiết bị để tạo thành kết nối và truyền dữ liệu.

|  |
| --- |
| TCP also verifies both devices before allowing any further communications to take place. This is often referred to as a handshake. Once communication is established using a TCP handshake, a request is made to the network. Using our example, we have requested data from the Yummy Recipes For Me server. Their servers will respond to that request and send data packets back to your device so that you can view the web page. |

TCP cũng xác minh cả hai thiết bịtrước khi cho phép thực hiện thêm bất kỳ thông tin liên lạc nào.Điều này thường được gọi là một cái bắt tay.Khi giao tiếp được thiết lập bằng cách sử dụng bắt tay TCP,một yêu cầu được gửi tới mạng.Sử dụng ví dụ của chúng tôi, chúng tôi đã yêu cầudữ liệu từ máy chủ Yummy Recipes For Me.Máy chủ của họ sẽ đáp ứng yêu cầu đó và gửigói dữ liệu quay trở lạithiết bị của bạn để bạn có thể xem trang web.

|  |
| --- |
| As data packets move across the network, they move between network devices such as routers. The Address Resolution Protocol, or ARP, is used to determine the MAC address of the next router or device on the path. This ensures that the data gets to the right place. Now the communication has been established and the destination device is known, it's time to access the Yummy Recipes For Me website. |

Khi các gói dữ liệu di chuyển trên mạng,chúng di chuyển giữa các thiết bị mạng như bộ định tuyến.Giao thức phân giải địa chỉ, hay ARP, được sử dụng đểxác định địa chỉ MAC củabộ định tuyến hoặc thiết bị tiếp theo trên đường dẫn.Điều này đảm bảo rằng dữ liệu được đến đúng nơi.Bây giờ việc giao tiếp đã đượcđược thiết lập và thiết bị đích đã được biết,đã đến lúc truy cập trang web Công thức nấu ăn ngon cho tôi.

|  |
| --- |
| The Hypertext Transfer Protocol Secure, or HTTPS, is a network protocol that provides a secure method of communication between client and website servers. It allows your web browser to securely send a request for a webpage to the Yummy Recipes For Me server and receive a webpage as a response. |

Giao thức truyền siêu văn bản an toàn hay HTTPS làmột giao thức mạng cung cấp một phương pháp an toàn đểgiao tiếp giữa máy khách và máy chủ trang web.Nó cho phép trình duyệt web của bạn gửi yêu cầu một cách an toàncho một trang web đến máy chủ Yummy Recipes For Mevà nhận được một trang web dưới dạng phản hồi.

|  |
| --- |
| Next comes a protocol called the Domain Name System, or DNS, which is a network protocol that translate internet domain names into IP addresses. The DNS protocol sends the domain name and the web address to a DNS server that retrieves the IP address of the website you were trying to access, in this case, Yummy Recipes For Me. The IP address is included as a destination address for the data packets traveling to the Yummy Recipes For Me web server. So just by visiting one website, the device on your networks are using four different protocols: TCP, ARP, HTTPS, and DNS. |

Tiếp theo là một giao thức được gọi làHệ thống tên miền hoặc DNS,đó là một giao thức mạng dịchtên miền internet thành địa chỉ IP.Giao thức DNS gửitên miền và địa chỉ web đểmột máy chủ DNS truy xuấtđịa chỉ IP của trang web bạn đang cố truy cập,trong trường hợp này là Công thức nấu ăn ngon cho tôi.Địa chỉ IP được đưa vào làm địa chỉ đích chocác gói dữ liệu di chuyển đếnmáy chủ web Công thức nấu ăn ngon cho tôi.Vì vậy, chỉ cần truy cập một trang web,thiết bị trên mạng của bạn làsử dụng bốn giao thức khác nhau:TCP, ARP, HTTPS và DNS.

|  |
| --- |
| These are just some of the protocols used in network communications. To help you learn more about the different protocols, we'll discuss them further in an upcoming course material. |

Đây chỉ là một số giao thứcđược sử dụng trong truyền thông mạng.Để giúp bạn tìm hiểu thêm về các giao thức khác nhau,chúng ta sẽ thảo luận thêm về chúngtrong tài liệu khóa học sắp tới.

|  |
| --- |
| But how do these protocols relate to security? Well, on the Yummy Recipes For Me website example, we used HTTPS, which is a secure protocol that requests a webpage from a web server. HTTPS encrypts data using the Secure Sockets Layer and Transport Layer Security, otherwise known as SSL/TLS. This helps keep the information secure from malicious actors who want to steal valuable information. |

Nhưng các giao thức này liên quan đến bảo mật như thế nào?Chà, trên ví dụ về trang web Công thức nấu ăn ngon cho tôi,chúng tôi đã sử dụng HTTPS, đó làmột giao thức an toàn màyêu cầu một trang web từ một máy chủ web.HTTPS mã hóa dữ liệu bằng cách sử dụngBảo mật lớp cổng bảo mật và lớp truyền tải,còn được gọi là SSL/TLS.Điều này giúp bảo mật thông tin khỏi bịnhững kẻ độc hại muốn đánh cắp thông tin có giá trị.

|  |
| --- |
| That's a lot of information and a lot of protocols to remember. Throughout your career as a security analyst, you'll become more familiar with network protocols and use them in your daily activities. |

Đó là rất nhiều thông tin vàrất nhiều giao thức cần nhớ.Trong suốt sự nghiệp của bạn với tư cách là nhà phân tích bảo mật,bạn sẽ trở nên quen thuộc hơn vớigiao thức mạng và sử dụng chúng trong hoạt động hàng ngày của bạn.

***1.3. Common network protocols – Các giao thức mạng phổ biến***

|  |
| --- |
| **Common network protocols** |

**Các giao thức mạng phổ biến**

|  |
| --- |
| In this section of the course, you learned about network protocols and how they organize communication over a network. This reading will discuss network protocols in more depth and review some basic protocols that you have learned previously. You will also learn new protocols and discuss some of the ways protocols are involved in network security. |

Trong phần này của khóa học, bạn đã tìm hiểu về các giao thức mạng và cách chúng tổ chức giao tiếp qua mạng. Bài đọc này sẽ thảo luận sâu hơn về các giao thức mạng và xem xét một số giao thức cơ bản mà bạn đã học trước đây. Bạn cũng sẽ tìm hiểu các giao thức mới và thảo luận về một số cách liên quan đến giao thức trong bảo mật mạng.

|  |
| --- |
| **Overview of network protocols** |

**Tổng quan về các giao thức mạng**

|  |
| --- |
| A **network protocol** is a set of rules used by two or more devices on a network to describe the order of delivery and the structure of data. Network protocols serve as instructions that come with the information in the data packet. These instructions tell the receiving device what to do with the data. Protocols are like a common language that allows devices all across the world to communicate with and understand each other. |

Giao **thức mạng** là một bộ quy tắc được sử dụng bởi hai hoặc nhiều thiết bị trên mạng để mô tả thứ tự phân phối và cấu trúc dữ liệu. Các giao thức mạng đóng vai trò là hướng dẫn đi kèm với thông tin trong gói dữ liệu. Những hướng dẫn này cho thiết bị nhận biết phải làm gì với dữ liệu. Các giao thức giống như một ngôn ngữ chung cho phép các thiết bị trên toàn thế giới giao tiếp và hiểu nhau.

|  |
| --- |
| Even though network protocols perform an essential function in network communication, security analysts should still understand their associated security implications. Some protocols have vulnerabilities that malicious actors exploit. For example, a nefarious actor could use the Domain Name System (DNS) protocol, which resolves web addresses to IP addresses, to divert traffic from a legitimate website to a malicious website containing malware. You’ll learn more about this topic in upcoming course materials. |

Mặc dù các giao thức mạng thực hiện một chức năng thiết yếu trong giao tiếp mạng, các nhà phân tích bảo mật vẫn phải hiểu ý nghĩa bảo mật liên quan của chúng. Một số giao thức có lỗ hổng mà các tác nhân độc hại khai thác. Ví dụ: kẻ xấu có thể sử dụng giao thức Hệ thống tên miền (DNS), giao thức này phân giải địa chỉ web thành địa chỉ IP, để chuyển hướng lưu lượng truy cập từ một trang web hợp pháp sang một trang web độc hại có chứa phần mềm độc hại. Bạn sẽ tìm hiểu thêm về chủ đề này trong các tài liệu khóa học sắp tới.

|  |
| --- |
| **Three categories of network protocols** |

**Ba loại giao thức mạng**

|  |
| --- |
| Network protocols can be divided into three main categories: communication protocols, management protocols, and security protocols. There are dozens of different network protocols, but you don’t need to memorize all of them for an entry-level security analyst role. However, it’s important for you to know the ones listed in this reading. |

Các giao thức mạng có thể được chia thành ba loại chính: giao thức truyền thông, giao thức quản lý và giao thức bảo mật. Có hàng tá giao thức mạng khác nhau, nhưng bạn không cần phải ghi nhớ tất cả chúng để có vai trò phân tích bảo mật cấp cơ bản. Tuy nhiên, điều quan trọng là bạn phải biết những điều được liệt kê trong bài đọc này.

|  |
| --- |
| **Communication protocols** |

**Giao thức truyền thông**

|  |
| --- |
| Communication protocols govern the exchange of information in network transmission. They dictate how the data is transmitted between devices and the timing of the communication. They also include methods to recover data lost in transit. Here are a few of them. |

Các giao thức truyền thông chi phối việc trao đổi thông tin trong truyền dẫn mạng. Chúng quy định cách dữ liệu được truyền giữa các thiết bị và thời gian liên lạc. Chúng cũng bao gồm các phương pháp khôi phục dữ liệu bị mất trong quá trình vận chuyển. Dưới đây là một vài trong số họ.

|  |
| --- |
| * **Transmission Control Protocol (TCP)** is an internet communication protocol that allows two devices to form a connection and stream data. TCP uses a three-way handshake process. First, the device sends a synchronize (SYN) request to a server. Then the server responds with a SYN/ACK packet to acknowledge receipt of the device's request. Once the server receives the final ACK packet from the device, a TCP connection is established. In the TCP/IP model, TCP occurs at the transport layer. * **User Datagram Protocol (UDP)** is a connectionless protocol that does not establish a connection between devices before a transmission. This makes it less reliable than TCP. But it also means that it works well for transmissions that need to get to their destination quickly. For example, one use of UDP is for sending DNS requests to local DNS servers. In the TCP/IP model, UDP occurs at the transport layer. * **Hypertext Transfer Protocol (HTTP)** is an application layer protocol that provides a method of communication between clients and website servers. HTTP uses port 80. HTTP is considered insecure, so it is being replaced on most websites by a secure version, called HTTPS that uses encryption from SSL/TLS for communication. However, there are still many websites that use the insecure HTTP protocol. In the TCP/IP model, HTTP occurs at the application layer. * **Domain Name System (DNS)** is a protocol that translates internet domain names into IP addresses. When a client computer wishes to access a website domain using their internet browser, a query is sent to a dedicated DNS server. The DNS server then looks up the IP address that corresponds to the website domain. DNS normally uses UDP on port 53. However, if the DNS reply to a request is large, it will switch to using the TCP protocol. In the TCP/IP model, DNS occurs at the application layer. |

* **Giao thức điều khiển truyền dẫn (TCP)** là giao thức truyền thông internet cho phép hai thiết bị tạo thành kết nối và truyền dữ liệu. TCP sử dụng quy trình bắt tay ba bước. Đầu tiên, thiết bị gửi yêu cầu đồng bộ hóa (SYN) đến máy chủ. Sau đó, máy chủ phản hồi bằng gói SYN/ACK để xác nhận đã nhận được yêu cầu của thiết bị. Khi máy chủ nhận được gói ACK cuối cùng từ thiết bị, kết nối TCP sẽ được thiết lập. Trong mô hình TCP/IP, TCP xảy ra ở lớp vận chuyển.
* **Giao thức gói dữ liệu người dùng (UDP)** là giao thức không kết nối, không thiết lập kết nối giữa các thiết bị trước khi truyền. Điều này làm cho nó kém tin cậy hơn TCP. Nhưng điều đó cũng có nghĩa là nó hoạt động tốt đối với các đường truyền cần đến đích nhanh chóng. Ví dụ: một cách sử dụng UDP là gửi yêu cầu DNS đến máy chủ DNS cục bộ. Trong mô hình TCP/IP, UDP xảy ra ở lớp vận chuyển.
* **Giao thức truyền siêu văn bản (HTTP)** là giao thức lớp ứng dụng cung cấp phương thức liên lạc giữa máy khách và máy chủ trang web. HTTP sử dụng cổng 80. HTTP được coi là không an toàn nên nó đang được thay thế trên hầu hết các trang web bằng một phiên bản bảo mật, được gọi là HTTPS sử dụng mã hóa từ SSL/TLS để liên lạc. Tuy nhiên, vẫn còn nhiều trang web sử dụng giao thức HTTP không an toàn. Trong mô hình TCP/IP, HTTP xảy ra ở lớp ứng dụng.
* **Hệ thống tên miền (DNS)** là một giao thức dịch tên miền internet thành địa chỉ IP. Khi máy khách muốn truy cập miền trang web bằng trình duyệt internet của họ, một truy vấn sẽ được gửi đến máy chủ DNS chuyên dụng. Sau đó, máy chủ DNS sẽ tra cứu địa chỉ IP tương ứng với tên miền của trang web. DNS thường sử dụng UDP trên cổng 53. Tuy nhiên, nếu DNS trả lời yêu cầu lớn, nó sẽ chuyển sang sử dụng giao thức TCP. Trong mô hình TCP/IP, DNS xuất hiện ở lớp ứng dụng.

|  |
| --- |
| **Management Protocols** |

**Giao thức quản lý**

|  |
| --- |
| The next category of network protocols is management protocols. Management protocols are used for monitoring and managing activity on a network. They include protocols for error reporting and optimizing performance on the network. |

Loại giao thức mạng tiếp theo là giao thức quản lý. Các giao thức quản lý được sử dụng để giám sát và quản lý hoạt động trên mạng. Chúng bao gồm các giao thức báo cáo lỗi và tối ưu hóa hiệu suất trên mạng.

|  |
| --- |
| * **Simple Network Management Protocol (SNMP)** is a network protocol used for monitoring and managing devices on a network. SNMP can reset a password on a network device or change its baseline configuration. It can also send requests to network devices for a report on how much of the network’s bandwidth is being used up. In the TCP/IP model, SNMP occurs at the application layer. * **Internet Control Message Protocol (ICMP)** is an internet protocol used by devices to tell each other about data transmission errors across the network. ICMP is used by a receiving device to send a report to the sending device about the data transmission. ICMP is commonly used as a quick way to troubleshoot network connectivity and latency by issuing the “ping” command on a Linux operating system. In the TCP/IP model, ICMP occurs at the internet layer. |

* **Giao thức quản lý mạng đơn giản (SNMP)** là giao thức mạng được sử dụng để giám sát và quản lý các thiết bị trên mạng. SNMP có thể đặt lại mật khẩu trên thiết bị mạng hoặc thay đổi cấu hình cơ bản của thiết bị đó. Nó cũng có thể gửi yêu cầu tới các thiết bị mạng để báo cáo về lượng băng thông của mạng đang được sử dụng hết. Trong mô hình TCP/IP, SNMP xảy ra ở lớp ứng dụng.
* **Giao thức tin nhắn điều khiển Internet (ICMP)** là giao thức internet được các thiết bị sử dụng để thông báo cho nhau về các lỗi truyền dữ liệu qua mạng. ICMP được thiết bị nhận sử dụng để gửi báo cáo đến thiết bị gửi về việc truyền dữ liệu. ICMP thường được sử dụng như một cách nhanh chóng để khắc phục sự cố kết nối và độ trễ mạng bằng cách đưa ra lệnh “ping” trên hệ điều hành Linux. Trong mô hình TCP/IP, ICMP xảy ra ở lớp internet.

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

**Giao thức bảo mật**

|  |
| --- |
| Security protocols are network protocols that ensure that data is sent and received securely across a network. Security protocols use encryption algorithms to protect data in transit. Below are some common security protocols. |

Giao thức bảo mật là các giao thức mạng đảm bảo rằng dữ liệu được gửi và nhận một cách an toàn trên mạng. Các giao thức bảo mật sử dụng thuật toán mã hóa để bảo vệ dữ liệu trong quá trình truyền. Dưới đây là một số giao thức bảo mật phổ biến.

|  |
| --- |
| * **Hypertext Transfer Protocol Secure (HTTPS)** is a network protocol that provides a secure method of communication between clients and website servers. HTTPS is a secure version of HTTP that uses secure sockets layer/transport layer security (SSL/TLS) encryption on all transmissions so that malicious actors cannot read the information contained. HTTPS uses port 443. In the TCP/IP model, HTTPS occurs at the application layer. * **Secure File Transfer Protocol (SFTP)** is a secure protocol used to transfer files from one device to another over a network. SFTP uses secure shell (SSH), typically through TCP port 22. SSH uses Advanced Encryption Standard (AES) and other types of encryption to ensure that unintended recipients cannot intercept the transmissions. In the TCP/IP model, SFTP occurs at the application layer. SFTP is used often with cloud storage. Every time a user uploads or downloads a file from cloud storage, the file is transferred using the SFTP protocol. |

* **Bảo mật Giao thức Truyền Siêu văn bản (HTTPS)** là giao thức mạng cung cấp phương thức liên lạc an toàn giữa máy khách và máy chủ trang web. HTTPS là phiên bản bảo mật của HTTP sử dụng mã hóa bảo mật lớp ổ cắm/lớp truyền tải (SSL/TLS) an toàn trên tất cả các đường truyền để tác nhân độc hại không thể đọc được thông tin chứa trong đó. HTTPS sử dụng cổng 443. Trong mô hình TCP/IP, HTTPS xảy ra ở lớp ứng dụng.
* **Giao thức truyền tệp an toàn (SFTP)** là giao thức an toàn được sử dụng để truyền tệp từ thiết bị này sang thiết bị khác qua mạng. SFTP sử dụng shell bảo mật (SSH), thường thông qua cổng TCP 22. SSH sử dụng Tiêu chuẩn mã hóa nâng cao (AES) và các loại mã hóa khác để đảm bảo rằng những người nhận ngoài ý muốn không thể chặn quá trình truyền. Trong mô hình TCP/IP, SFTP xảy ra ở lớp ứng dụng. SFTP được sử dụng thường xuyên với lưu trữ đám mây. Mỗi khi người dùng tải lên hoặc tải xuống một tệp từ bộ lưu trữ đám mây, tệp đó sẽ được truyền bằng giao thức SFTP.

|  |
| --- |
| **Note:** The encryption protocols mentioned do not conceal the source or destination IP address of network traffic. This means a malicious actor can still learn some basic information about the network traffic if they intercept it. |

**Lưu ý:** Các giao thức mã hóa được đề cập không che giấu địa chỉ IP nguồn hoặc đích của lưu lượng mạng. Điều này có nghĩa là kẻ tấn công độc hại vẫn có thể tìm hiểu một số thông tin cơ bản về lưu lượng mạng nếu chúng chặn nó.

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

**Bài học chính**

|  |
| --- |
| The protocols you learned about in this reading are basic networking protocols that entry-level cybersecurity analysts should know. Understanding how protocols function on a network is essential. Cybersecurity analysts can leverage their knowledge of protocols to successfully mitigate vulnerabilities on a network and potentially prevent future attacks. |

Các giao thức bạn đã tìm hiểu trong bài đọc này là các giao thức mạng cơ bản mà các nhà phân tích an ninh mạng cấp cơ bản nên biết. Hiểu cách các giao thức hoạt động trên mạng là điều cần thiết. Các nhà phân tích an ninh mạng có thể tận dụng kiến ​​thức của họ về các giao thức để giảm thiểu thành công các lỗ hổng trên mạng và có khả năng ngăn chặn các cuộc tấn công trong tương lai.

***1.4. Additional network protocols – Các giao thức mạng bổ sung***

|  |
| --- |
| **Additional network protocols** |

**Các giao thức mạng bổ sung**

|  |
| --- |
| In previous readings and videos, you learned how network protocols organize the sending and receiving of data across a network. You also learned that protocols can be divided into three categories: communication protocols, management protocols, and security protocols. |

Trong các bài đọc và video trước, bạn đã tìm hiểu cách các giao thức mạng tổ chức việc gửi và nhận dữ liệu qua mạng. Bạn cũng đã biết rằng các giao thức có thể được chia thành ba loại: giao thức truyền thông, giao thức quản lý và giao thức bảo mật.

|  |
| --- |
| This reading will introduce you to a few additional concepts and protocols that will come up regularly in your work as a security analyst. Some protocols are assigned port numbers by the Internet Assigned Numbers Authority (IANA). These port numbers are included in the description of each protocol, if assigned. |

Bài đọc này sẽ giới thiệu cho bạn một số khái niệm và giao thức bổ sung sẽ xuất hiện thường xuyên trong công việc của bạn với tư cách là nhà phân tích bảo mật. Một số giao thức được Cơ quan cấp số hiệu Internet (IANA) gán số cổng. Các số cổng này được bao gồm trong phần mô tả của từng giao thức, nếu được chỉ định.

|  |
| --- |
| **Network Address Translation** |

**Dịch địa chỉ mạng**

|  |
| --- |
| The devices on your local home or office network each have a private IP address that they use to communicate directly with each other. However, in order for the devices with private IP addresses to communicate with the public internet, they need to have a single public IP address that represents all devices on the LAN to the public. For outgoing messages, the router can replace a private source IP address with its public IP address and perform the reverse operation for responses. This process is known as Network Address Translation (NAT) and it generally requires a router or firewall to be specifically configured to perform NAT. NAT is a part of layer 2 (internet layer) and layer 3 (transport layer) of the TCP/IP model. |

Mỗi thiết bị trên mạng gia đình hoặc văn phòng địa phương của bạn đều có một địa chỉ IP riêng mà chúng sử dụng để liên lạc trực tiếp với nhau. Tuy nhiên, để các thiết bị có địa chỉ IP riêng có thể giao tiếp với Internet công cộng, chúng cần có một địa chỉ IP công cộng duy nhất đại diện cho tất cả các thiết bị trên mạng LAN với công chúng. Đối với các tin nhắn gửi đi, bộ định tuyến có thể thay thế địa chỉ IP nguồn riêng bằng địa chỉ IP công cộng và thực hiện thao tác ngược lại để phản hồi. Quá trình này được gọi là Dịch địa chỉ mạng (NAT) và thường yêu cầu bộ định tuyến hoặc tường lửa phải được cấu hình cụ thể để thực hiện NAT. NAT là một phần của lớp 2 (lớp internet) và lớp 3 (lớp truyền tải) của mô hình TCP/IP.

|  |  |
| --- | --- |
| **Private IP Addresses** | **Public IP Addresses** |
| * Assigned by the router * Unique only within private network * No cost to use * Address ranges:   + 10.0.0.0-10.255.255.255   + 172.16.0.0-172.31.255.255   + 192.168.0.0-192.168.255.255 | * Assigned by ISP and IANA * Unique address in global internet * Costs to lease a public IP address * Assignable address ranges:   + 1.0.0.0-9.255.255.255   + 11.0.0.0-126.255.255.255   + 128.0.0.0-172.15.255.255   + 172.32.0.0-192.167.255.255   + 192.169.0.0-233.255.255.255 |

|  |  |
| --- | --- |
| **Địa chỉ IP riêng** | **Địa chỉ IP công cộng** |
| * Được chỉ định bởi bộ định tuyến * Duy nhất chỉ trong mạng riêng * Không mất phí sử dụng * Phạm vi địa chỉ:   + 10.0.0.0-10.255.255.255   + 172.16.0.0-172.31.255.255   + 192.168.0.0-192.168.255.255 | * Được chỉ định bởi ISP và IANA * Địa chỉ duy nhất trên Internet toàn cầu * Chi phí thuê địa chỉ IP công cộng * Phạm vi địa chỉ có thể gán:   + 1.0.0.0-9.255.255.255   + 11.0.0.0-126.255.255.255   + 128.0.0.0-172.15.255.255   + 172.32.0.0-192.167.255.255   + 192.169.0.0-233.255.255.255 |

|  |
| --- |
| **Dynamic Host Configuration Protocol** |

**Giao thức cấu hình máy chủ động**

|  |
| --- |
| Dynamic Host Configuration Protocol (DHCP) is in the management family of network protocols. DHCP is an application layer protocol used on a network to configure devices. It works with the router to assign a unique IP address to each device and provide the addresses of the appropriate DNS server and default gateway for each device. DHCP servers operate on UDP port 67 while DHCP clients operate on UDP port 68. |

Giao thức cấu hình máy chủ động (DHCP) nằm trong nhóm giao thức mạng quản lý. DHCP là giao thức lớp ứng dụng được sử dụng trên mạng để định cấu hình thiết bị. Nó hoạt động với bộ định tuyến để gán một địa chỉ IP duy nhất cho từng thiết bị và cung cấp địa chỉ của máy chủ DNS và cổng mặc định thích hợp cho từng thiết bị. Máy chủ DHCP hoạt động trên cổng UDP 67 trong khi máy khách DHCP hoạt động trên cổng UDP 68.

|  |
| --- |
| **Address Resolution Protocol** |

**Địa chỉ Nghị quyết Nghị định thư**

|  |
| --- |
| By now, you are familiar with IP and MAC addresses. You’ve learned that each device on a network has a public IP address, a private IP address, and a MAC address that identify it on the network. A device’s IP address may change over time, but its MAC address is permanent because it is unique to a device's network interface card. The MAC address is used to communicate with devices within the same network, but sometimes, the MAC address is unknown. This is why the Address Resolution Protocol (ARP) is needed. ARP is mainly a network access layer protocol in the TCP/IP model used to translate the IP addresses that are found in data packets into the MAC address of the hardware device. |

Đến bây giờ, bạn đã quen thuộc với địa chỉ IP và MAC. Bạn đã biết rằng mỗi thiết bị trên mạng đều có địa chỉ IP công cộng, địa chỉ IP riêng tư và địa chỉ MAC nhận dạng thiết bị đó trên mạng. Địa chỉ IP của thiết bị có thể thay đổi theo thời gian, nhưng địa chỉ MAC của nó là vĩnh viễn vì nó là duy nhất cho card giao diện mạng của thiết bị. Địa chỉ MAC được sử dụng để liên lạc với các thiết bị trong cùng một mạng, nhưng đôi khi, địa chỉ MAC không xác định. Đây là lý do tại sao Giao thức phân giải địa chỉ (ARP) là cần thiết. ARP chủ yếu là giao thức lớp truy cập mạng trong mô hình TCP/IP được sử dụng để dịch các địa chỉ IP được tìm thấy trong các gói dữ liệu thành địa chỉ MAC của thiết bị phần cứng.

|  |
| --- |
| Each device on the network performs ARP and keeps track of matching IP and MAC addresses in an ARP cache. ARP does not have a specific port number since it is a layer 2 protocol and port numbers are associated with the layer 7 application layer. |

Mỗi thiết bị trên mạng thực hiện ARP và theo dõi các địa chỉ IP và MAC phù hợp trong bộ đệm ARP. ARP không có số cổng cụ thể vì đây là giao thức lớp 2 và số cổng được liên kết với lớp ứng dụng lớp 7.

|  |
| --- |
| **Telnet** |

**Telnet**

|  |
| --- |
| Telnet is an application layer protocol that is used to connect with a remote system. Telnet sends all information in clear text. It uses command line prompts to control another device similar to secure shell (SSH), but Telnet is not as secure as SSH. Telnet can be used to connect to local or remote devices and uses TCP port 23. |

Telnet là một giao thức lớp ứng dụng được sử dụng để kết nối với hệ thống từ xa. Telnet gửi tất cả thông tin ở dạng văn bản rõ ràng. Nó sử dụng lời nhắc dòng lệnh để điều khiển một thiết bị khác tương tự như shell bảo mật (SSH), nhưng Telnet không an toàn như SSH. Telnet có thể được sử dụng để kết nối với các thiết bị cục bộ hoặc từ xa và sử dụng cổng TCP 23.

|  |
| --- |
| **Secure shell** |

**Vỏ an toàn**

|  |
| --- |
| Secure shell protocol (SSH) is used to create a secure connection with a remote system. This application layer protocol provides an alternative for secure authentication and encrypted communication. SSH operates over the TCP port 22 and is a replacement for less secure protocols, such as Telnet. |

Giao thức shell an toàn (SSH) được sử dụng để tạo kết nối an toàn với hệ thống từ xa. Giao thức lớp ứng dụng này cung cấp một giải pháp thay thế cho việc xác thực an toàn và liên lạc được mã hóa. SSH hoạt động trên cổng TCP 22 và là sự thay thế cho các giao thức kém an toàn hơn, chẳng hạn như Telnet.

|  |
| --- |
| **Post office protocol** |

**Giao thức bưu điện**

|  |
| --- |
| Post office protocol (POP) is an application layer (layer 4 of the TCP/IP model) protocol used to manage and retrieve email from a mail server. POP3 is the most commonly used version of POP. Many organizations have a dedicated mail server on the network that handles incoming and outgoing mail for users on the network. User devices will send requests to the remote mail server and download email messages locally. If you have ever refreshed your email application and had new emails populate in your inbox, you are experiencing POP and internet message access protocol (IMAP) in action. Unencrypted, plaintext authentication uses TCP/UDP port 110 and encrypted emails use Secure Sockets Layer/Transport Layer Security (SSL/TLS) over TCP/UDP port 995.  When using POP, mail has to finish downloading on a local device before it can be read. After downloading, the mail may or may not be deleted from the mail server, so it does not guarantee that a user can sync the same email across multiple devices. |

Giao thức bưu điện (POP) là giao thức lớp ứng dụng (lớp 4 của mô hình TCP/IP) được sử dụng để quản lý và truy xuất email từ máy chủ thư. POP3 là phiên bản POP được sử dụng phổ biến nhất. Nhiều tổ chức có một máy chủ thư chuyên dụng trên mạng để xử lý thư đến và đi cho người dùng trên mạng. Thiết bị người dùng sẽ gửi yêu cầu đến máy chủ thư từ xa và tải xuống các email cục bộ. Nếu bạn đã từng làm mới ứng dụng email của mình và có email mới được đưa vào hộp thư đến của mình thì bạn đang gặp phải giao thức truy cập thư POP và Internet (IMAP) đang hoạt động. Xác thực văn bản gốc, không được mã hóa sử dụng cổng TCP/UDP 110 và các email được mã hóa sử dụng Lớp cổng bảo mật/Bảo mật lớp truyền tải (SSL/TLS) qua cổng TCP/UDP 995. Khi sử dụng POP, thư phải hoàn tất tải xuống trên thiết bị cục bộ trước khi có thể đọc. Sau khi tải xuống, thư có thể bị xóa hoặc không khỏi máy chủ thư nên không đảm bảo rằng người dùng có thể đồng bộ cùng một email trên nhiều thiết bị.

|  |
| --- |
| **Internet Message Access Protocol (IMAP)** |

**Giao thức truy cập tin nhắn Internet (IMAP)**

|  |
| --- |
| IMAP is used for incoming email. It downloads the headers of emails and the message content. The content also remains on the email server, which allows users to access their email from multiple devices. IMAP uses TCP port 143 for unencrypted email and TCP port 993 over the TLS protocol. Using IMAP allows users to partially read email before it is finished downloading. Since the mail is kept on the mail server, it allows a user to sync emails across multiple devices. |

IMAP được sử dụng cho email đến. Nó tải xuống các tiêu đề của email và nội dung tin nhắn. Nội dung cũng vẫn còn trên máy chủ email, cho phép người dùng truy cập email của họ từ nhiều thiết bị. IMAP sử dụng cổng TCP 143 cho email không được mã hóa và cổng TCP 993 qua giao thức TLS. Sử dụng IMAP cho phép người dùng đọc một phần email trước khi tải xuống xong. Vì thư được lưu giữ trên máy chủ thư nên nó cho phép người dùng đồng bộ hóa email trên nhiều thiết bị.

|  |
| --- |
| **Simple Mail Transfer Protocol** |

**Giao thức chuyển thư đơn giản**

|  |
| --- |
| Simple Mail Transfer Protocol (SMTP) is used to transmit and route email from the sender to the recipient’s address. SMTP works with Message Transfer Agent (MTA) software, which searches DNS servers to resolve email addresses to IP addresses, to ensure emails reach their intended destination. SMTP uses TCP/UDP port 25 for unencrypted emails and TCP/UDP port 587 using TLS for encrypted emails. The TCP port 25 is often used by high-volume spam. SMTP helps to filter out spam by regulating how many emails a source can send at a time. |

Giao thức truyền thư đơn giản (SMTP) được sử dụng để truyền và định tuyến email từ người gửi đến địa chỉ người nhận. SMTP hoạt động với phần mềm Tác nhân truyền tin nhắn (MTA), phần mềm này tìm kiếm máy chủ DNS để phân giải địa chỉ email thành địa chỉ IP, nhằm đảm bảo email đến được đích dự kiến. SMTP sử dụng cổng TCP/UDP 25 cho các email không được mã hóa và cổng TCP/UDP 587 sử dụng TLS cho các email được mã hóa. Cổng TCP 25 thường được sử dụng bởi thư rác có số lượng lớn. SMTP giúp lọc thư rác bằng cách điều chỉnh số lượng email mà một nguồn có thể gửi cùng một lúc.

|  |
| --- |
| **Protocols and port numbers** |

**Giao thức và số cổng**

|  |
| --- |
| Remember that port numbers are used by network devices to determine what should be done with the information contained in each data packet once they reach their destination. Firewalls can filter out unwanted traffic based on port numbers. For example, an organization may configure a firewall to only allow access to TCP port 995 (POP3) by IP addresses belonging to the organization. |

Hãy nhớ rằng số cổng được các thiết bị mạng sử dụng để xác định những gì nên làm với thông tin có trong mỗi gói dữ liệu khi chúng đến đích. Tường lửa có thể lọc lưu lượng không mong muốn dựa trên số cổng. Ví dụ: một tổ chức có thể định cấu hình tường lửa để chỉ cho phép truy cập vào cổng TCP 995 (POP3) bằng các địa chỉ IP thuộc tổ chức đó.

|  |
| --- |
| As a security analyst, you will need to know about many of the protocols and port numbers mentioned in this course. They may be used to determine your technical knowledge in interviews, so it’s a good idea to memorize them. You will also learn about new protocols on the job in a security position. |

Là một nhà phân tích bảo mật, bạn sẽ cần biết về nhiều giao thức và số cổng được đề cập trong khóa học này. Chúng có thể được sử dụng để xác định kiến ​​thức kỹ thuật của bạn trong các cuộc phỏng vấn, vì vậy bạn nên ghi nhớ chúng. Bạn cũng sẽ tìm hiểu về các giao thức mới trong công việc ở vị trí bảo mật.

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

**Bài học chính**

|  |
| --- |
| As a cybersecurity analyst, you will encounter various common protocols in your everyday work. The protocols covered in this reading include NAT, DHCP, ARP, Telnet, SSH, POP3, IMAP, and SMTP. It is equally important to understand where each protocol is structured in the TCP/IP model and which ports they occupy. |

Là một nhà phân tích an ninh mạng, bạn sẽ gặp nhiều giao thức phổ biến khác nhau trong công việc hàng ngày của mình. Các giao thức được đề cập trong bài đọc này bao gồm NAT, DHCP, ARP, Telnet, SSH, POP3, IMAP và SMTP. Điều quan trọng không kém là phải hiểu mỗi giao thức được cấu trúc ở đâu trong mô hình TCP/IP và chúng chiếm giữ những cổng nào.

|  |  |
| --- | --- |
| **Protocol** | **Port** |
| DHCP | UDP port 67 (servers)  UDP port 68 (clients) |
| ARP | none |
| Telnet | TCP port 23 |
| SSH | TCP port 22 |
| POP3 | TCP/UDP port 110 (unencrypted)  TCP/UDP port 995 (encrypted, SSL/TLS) |
| IMAP | TCP port 143 (unencrypted)  TCP port 993 (encrypted, SSL/TLS) |
| SMTP | TCP/UDP Port 25 (unencrypted) |
| SMTPS | TCP/UDP port 587 (encrypted, TLS) |

|  |  |
| --- | --- |
| **Giao thức** | **Cổng** |
| DHCP | Cổng UDP 67 (máy chủ)  Cổng UDP 68 (máy khách) |
| ARP | không có |
| Telnet | cổng TCP 23 |
| SSH | cổng TCP 22 |
| POP3 | Cổng TCP/UDP 110 (không được mã hóa)  Cổng TCP/UDP 995 (được mã hóa, SSL/TLS) |
| IMAP | Cổng TCP 143 (không được mã hóa)  Cổng TCP 993 (được mã hóa, SSL/TLS) |
| SMTP | Cổng TCP/UDP 25 (không được mã hóa) |
| SMTPS | Cổng TCP/UDP 587 (được mã hóa, TLS) |

***1.5. Antara: Working in network security – Antara: Làm việc trong lĩnh vực an ninh mạng***

|  |
| --- |
| [MUSIC] My name is Antara, I work on the Enterprise Infrastructure Protection Team at Google. And our main job responsibility is to protect the infrastructure that all the amazing Google products run on. I didn't start with a background in computers, and I did my undergrad in electronics and communication, which is far away from computers. I took up the challenge to actually pivot into computers with my first job. That actually led me to explore the security world even more. And that's how it led to doing my masters in security, getting expertise in that area and then come to Google as a security engineer. A typical day in the life of an entry-level network security engineer would start with solving a problem. Maybe you're trying to debug, why is this particular endpoint flooded with so much traffic? Or why is this endpoint actually slowing down? And you would start with, okay, let me get to the endpoint. Let me capture some traffic on the endpoint and see what kind of traffic is coming in and going out through this endpoint. So I would typically go back, think about the problem during lunch. Sometimes things would click. When you're thinking you might not have thought about a problem from a different perspective, you might want to actually see how it looks like. So you would go about maybe doing a lab recreate. Let me connect these endpoints and let me try to reproduce the issue. You might see some things in the lab recreate that you might have not thought of. And you might need to actually consult with experts from different domains who might know better about this area. Get their view on what the problem is, analyze, show them everything that you have done. You might get your solution just by talking to people. It's a pretty busy day, but it's also a very fun day. It's like solving puzzles all the time, which is pretty exciting. Some of the best practices in network security that I've learned are, don't try to always reinvent the wheel. There are certain protocols, there are certain algorithms that have been tried, tested, analyzed, and they have been deemed secure for being used in network security. The time that you spend on reinventing the wheel is not going to give you the benefits that you need. So it's always good to think about the unsolved challenges instead of trying to solve the same problem in a different way. I feel cybersecurity is actually a great field to get into right now, because, as you see, we are in this information age where tech is exponentially growing. Just getting into this field is just going to be exciting because there are amazing new challenges coming up in this field. |

[ÂM NHẠC]Tên tôi là Antara,Tôi làm việc trong Nhóm bảo vệ cơ sở hạ tầng doanh nghiệp tại Google.Và trách nhiệm công việc chính của chúng tôi là bảo vệcơ sở hạ tầng chạy trên đó tất cả các sản phẩm tuyệt vời của Google.Tôi không bắt đầu với kiến ​​thức nền tảng về máy tính và tôi đã học xong chương trình đại học.trong lĩnh vực điện tử và truyền thông, vốn ở rất xa máy tính.Tôi đã thực hiện thử thách chuyển sang lĩnh vực máy tính với công việc đầu tiên của mình.Điều đó thực sự khiến tôi khám phá thế giới bảo mật nhiều hơn.Và đó là lý do khiến tôi học thạc sĩ về bảo mật, có được kiến ​​thức chuyên môn về lĩnh vực đó.và sau đó đến Google với tư cách là kỹ sư bảo mật.Một ngày điển hình trong cuộc đời của một kỹ sư an ninh mạng mới vào nghềsẽ bắt đầu bằng việc giải quyết một vấn đề.Có thể bạn đang cố gắng gỡ lỗi, tại sao điểm cuối cụ thể này lại tràn ngập như vậygiao thông đông đúc?Hoặc tại sao điểm cuối này thực sự chậm lại?Và bạn sẽ bắt đầu với, được rồi, hãy để tôi đi đến điểm cuối.Hãy để tôi nắm bắt một số lưu lượng truy cập ở điểm cuối vàxem loại lưu lượng truy cập nào đang đến và đi qua điểm cuối này.Vì vậy, tôi thường quay lại và suy nghĩ về vấn đề trong bữa trưa.Đôi khi mọi thứ sẽ nhấp chuột.Khi bạn đang suy nghĩ, có thể bạn đã không nghĩ đến một vấn đề từ một góc độ khác.phối cảnh, bạn có thể muốn thực sự thấy nó trông như thế nào.Vì vậy, bạn có thể tiến hành tạo lại phòng thí nghiệm.Hãy để tôi kết nối các điểm cuối này và thử tái hiện vấn đề.Bạn có thể thấy một số thứ trong phòng thí nghiệm được tạo lại mà bạn có thể chưa cónghĩ đến.Và bạn có thể thực sự cần tham khảo ý kiến ​​của các chuyên gia từ các lĩnh vực khác nhau, những ngườicó thể biết rõ hơn về khu vực này.Tìm hiểu quan điểm của họ về vấn đề là gì, phân tích,cho họ thấy mọi thứ bạn đã làm.Bạn có thể nhận được giải pháp chỉ bằng cách nói chuyện với mọi người.Một ngày khá bận rộn nhưng cũng là một ngày rất vui.Nó giống như việc giải các câu đố mọi lúc, điều này khá thú vị.Một số phương pháp hay nhất về bảo mật mạng mà tôi đã học được là,đừng cố gắng luôn phát minh lại bánh xe.Có một số giao thức nhất định,có một số thuật toán nhất định đã được thử nghiệm, kiểm tra,được phân tích và chúng được coi là an toàn khi sử dụng trong an ninh mạng.Thời gian bạn bỏ ra để phát minh lại cái bánh xe sẽ không mang lại cho bạnnhững lợi ích mà bạn cần.Vì vậy, việc nghĩ về những thách thức chưa được giải quyết luôn là điều tốt thay vìcố gắng giải quyết cùng một vấn đề theo một cách khác.Tôi cảm thấy an ninh mạng thực sự là một lĩnh vực tuyệt vời để tham gia ngay bây giờ, bởi vì,như bạn thấy, chúng ta đang ở thời đại thông tin nơi công nghệ đang phát triển theo cấp số nhân.Chỉ cần tham gia vào lĩnh vực này sẽ rất thú vị bởi vì cólà những thách thức mới đáng kinh ngạc sắp xảy ra trong lĩnh vực này.

***1.6. Wireless protocols – Giao thức không dây***

|  |
| --- |
| So far, you've learned about a variety of network protocols, including communication protocols like TCP/IP. Now we're going to go more in depth into a class of communication protocols called the IEEE802.11. |

Cho đến nay, bạn đã tìm hiểu vềmột loạt các giao thức mạng,bao gồm các giao thức truyền thông như TCP/IP.Bây giờ chúng ta sẽ đi sâu hơnvào một lớp các giao thức truyền thôngđược gọi là IEEE802.11.

|  |
| --- |
| IEEE802.11, commonly known as Wi-Fi, is a set of standards that define communications for wireless LANs. IEEE stands for the Institute of Electrical and Electronics Engineers, which is an organization that maintains Wi-Fi standards, and 802.11 is a suite of protocols used in wireless communications. |

IEEE802.11, thường được gọi là Wi-Fi,là một tập hợp các tiêu chuẩn xác địnhtruyền thông cho mạng LAN không dây.IEEE là viết tắt củaViện Kỹ sư Điện và Điện tử,là một tổ chức duy trì các tiêu chuẩn Wi-Fi,và 802.11 là một bộcác giao thức được sử dụng trong truyền thông không dây.

|  |
| --- |
| Wi-Fi protocols have adapted over the years to become more secure and reliable to provide the same level of security as a wired connection. In 2004, a security protocol called the Wi-Fi Protected Access, or WPA, was introduced. WPA is a wireless security protocol for devices to connect to the internet. Since then, WPA has evolved into newer versions, like WPA2 and WPA3, which include further security improvements, like more advanced encryption. As a security analyst, you might be responsible for making sure that the wireless connections in your organization are secure. Let's learn more about security measures. |

Giao thức Wi-Fi đã thích nghiqua nhiều năm để trở nên an toàn và đáng tin cậy hơnđể cung cấp cùng một mức độbảo mật như một kết nối có dây.Trong năm 2004,một giao thức bảo mật được gọi là Truy cập Wi-Fi được bảo vệ,hoặc WPA, đã được giới thiệu.WPA là một giao thức bảo mật không dâycho các thiết bị kết nối với internet.Kể từ đó, WPA đã phát triểnsang các phiên bản mới hơn, như WPA2 và WPA3,bao gồm các cải tiến bảo mật hơn nữa,thích mã hóa nâng cao hơn.Là một nhà phân tích chứng khoán,bạn có thể chịu trách nhiệm đảm bảo rằngcác kết nối không dây trong tổ chức của bạn được an toàn.Hãy cùng tìm hiểu thêm về các biện pháp an ninh.

***1.7. The evolution of wireless security protocols – Sự phát triển của các giao thức bảo mật không dây***

|  |
| --- |
| **The evolution of wireless security protocols** |

**Sự phát triển của các giao thức bảo mật không dây**

|  |
| --- |
| In the early days of the internet, all internet communication happened across physical cables. It wasn’t until the mid-1980s that authorities in the United States designated a spectrum of radio wave frequencies that could be used without a license, so there was more opportunity for the internet to expand. |

Trong những ngày đầu của Internet, tất cả hoạt động liên lạc trên Internet đều diễn ra thông qua các dây cáp vật lý. Phải đến giữa những năm 1980, chính quyền Hoa Kỳ mới chỉ định một dải tần số sóng vô tuyến có thể được sử dụng mà không cần giấy phép, nhờ đó Internet có nhiều cơ hội mở rộng hơn.

|  |
| --- |
| In the late 1990s and early 2000s, technologies were developed to send and receive data over radio. Today, users access wireless internet through laptops, smart phones, tablets, and desktops. Smart devices, like thermostats, door locks, and security cameras, also use wireless internet to communicate with each other and with services on the internet. |

Vào cuối những năm 1990 và đầu những năm 2000, công nghệ gửi và nhận dữ liệu qua sóng vô tuyến đã được phát triển. Ngày nay, người dùng truy cập internet không dây thông qua máy tính xách tay, điện thoại thông minh, máy tính bảng và máy tính để bàn. Các thiết bị thông minh, như máy điều nhiệt, khóa cửa và camera an ninh, cũng sử dụng Internet không dây để liên lạc với nhau và với các dịch vụ trên Internet.



|  |
| --- |
| **Introduction to wireless communication protocols** |

**Giới thiệu các giao thức truyền thông không dây**

|  |
| --- |
| Many people today refer to wireless internet as Wi-Fi. **Wi-Fi** refers to a set of standards that define communication for wireless LANs. Wi-Fi is a marketing term commissioned by the Wireless Ethernet Compatibility Alliance (WECA). WECA has since renamed their organization Wi-Fi Alliance. |

Nhiều người ngày nay gọi Internet không dây là Wi-Fi. **Wi-Fi** đề cập đến một bộ tiêu chuẩn xác định giao tiếp cho mạng LAN không dây. Wi-Fi là một thuật ngữ tiếp thị được ủy quyền bởi Liên minh tương thích Ethernet không dây (WECA). WECA kể từ đó đã đổi tên tổ chức của họ là Wi-Fi Alliance.

|  |
| --- |
| Wi-Fi standards and protocols are based on the 802.11 family of internet communication standards determined by the Institute of Electrical and Electronics Engineers (IEEE). So, as a security analyst, you might also see Wi-Fi referred to as IEEE 802.11. |

Các tiêu chuẩn và giao thức Wi-Fi dựa trên dòng tiêu chuẩn truyền thông internet 802.11 do Viện Kỹ sư Điện và Điện tử (IEEE) xác định. Vì vậy, với tư cách là một nhà phân tích bảo mật, bạn cũng có thể thấy Wi-Fi được gọi là IEEE 802.11.

|  |
| --- |
| Wi-Fi communications are secured by wireless networking protocols. Wireless security protocols have evolved over the years, helping to identify and resolve vulnerabilities with more advanced wireless technologies. |

Thông tin liên lạc Wi-Fi được bảo mật bằng các giao thức mạng không dây. Các giao thức bảo mật không dây đã phát triển qua nhiều năm, giúp xác định và giải quyết các lỗ hổng bằng các công nghệ không dây tiên tiến hơn.

|  |
| --- |
| In this reading, you will learn about the evolution of wireless security protocols from WEP to WPA, WPA2, and WPA3. You’ll also learn how the Wireless Application Protocol was used for mobile internet communications. |

Trong bài đọc này, bạn sẽ tìm hiểu về sự phát triển của các giao thức bảo mật không dây từ WEP sang WPA, WPA2 và WPA3. Bạn cũng sẽ tìm hiểu cách sử dụng Giao thức ứng dụng không dây cho truyền thông internet di động.

|  |
| --- |
| **Wired Equivalent Privacy** |

**Quyền riêng tư tương đương có dây**

|  |
| --- |
| Wired equivalent privacy (WEP) is a wireless security protocol designed to provide users with the same level of privacy on wireless network connections as they have on wired network connections. WEP was developed in 1999 and is the oldest of the wireless security standards. |

Quyền riêng tư tương đương có dây (WEP) là một giao thức bảo mật không dây được thiết kế để cung cấp cho người dùng mức độ riêng tư trên các kết nối mạng không dây giống như trên các kết nối mạng có dây. WEP được phát triển vào năm 1999 và là tiêu chuẩn bảo mật không dây lâu đời nhất.

|  |
| --- |
| WEP is largely out of use today, but security analysts should still understand WEP in case they encounter it. For example, a network router might have used WEP as the default security protocol and the network administrator never changed it. Or, devices on a network might be too old to support newer Wi-Fi security protocols. Nevertheless, a malicious actor could potentially break the WEP encryption, so it’s now considered a high-risk security protocol. |

Ngày nay WEP phần lớn không còn được sử dụng nữa, nhưng các nhà phân tích bảo mật vẫn nên hiểu WEP trong trường hợp họ gặp phải nó. Ví dụ: bộ định tuyến mạng có thể đã sử dụng WEP làm giao thức bảo mật mặc định và quản trị viên mạng chưa bao giờ thay đổi giao thức đó. Hoặc các thiết bị trên mạng có thể quá cũ để hỗ trợ các giao thức bảo mật Wi-Fi mới hơn. Tuy nhiên, một tác nhân độc hại có thể phá vỡ mã hóa WEP, vì vậy nó hiện được coi là giao thức bảo mật có rủi ro cao.

|  |
| --- |
| **Wi-Fi Protected Access** |

**Truy cập được bảo vệ bằng Wi-Fi**

|  |
| --- |
| Wi-Fi Protected Access (WPA) was developed in 2003 to improve upon WEP, address the security issues that it presented, and replace it. WPA was always intended to be a transitional measure so backwards compatibility could be established with older hardware. |

Truy cập được bảo vệ Wi-Fi (WPA) được phát triển vào năm 2003 để cải thiện WEP, giải quyết các vấn đề bảo mật mà nó đưa ra và thay thế nó. WPA luôn được coi là một biện pháp chuyển tiếp để có thể thiết lập khả năng tương thích ngược với phần cứng cũ hơn.

|  |
| --- |
| The flaws with WEP were in the protocol itself and how the encryption was used. WPA addressed this weakness by using a protocol called Temporal Key Integrity Protocol (TKIP). WPA encryption algorithm uses larger secret keys than WEPs, making it more difficult to guess the key by trial and error. |

Các sai sót của WEP nằm ở chính giao thức và cách sử dụng mã hóa. WPA đã giải quyết điểm yếu này bằng cách sử dụng giao thức có tên Giao thức toàn vẹn khóa tạm thời (TKIP). Thuật toán mã hóa WPA sử dụng các khóa bí mật lớn hơn WEP, khiến việc đoán khóa bằng cách thử và sai trở nên khó khăn hơn.

|  |
| --- |
| WPA also includes a message integrity check that includes a message authentication tag with each transmission. If a malicious actor attempts to alter the transmission in any way or resend at another time, WPA’s message integrity check will identify the attack and reject the transmission. |

WPA cũng bao gồm kiểm tra tính toàn vẹn của tin nhắn bao gồm thẻ xác thực tin nhắn với mỗi lần truyền. Nếu một tác nhân độc hại cố gắng thay đổi việc truyền tải theo bất kỳ cách nào hoặc gửi lại vào lúc khác, quá trình kiểm tra tính toàn vẹn tin nhắn của WPA sẽ xác định cuộc tấn công và từ chối việc truyền tải.

|  |
| --- |
| Despite the security improvements of WPA, it still has vulnerabilities. Malicious actors can use a key reinstallation attack (or KRACK attack) to decrypt transmissions using WPA. Attackers can insert themselves in the WPA authentication handshake process and insert a new encryption key instead of the dynamic one assigned by WPA. If they set the new key to all zeros, it is as if the transmission is not encrypted at all. |

Bất chấp những cải tiến về bảo mật của WPA, nó vẫn có những lỗ hổng. Tác nhân độc hại có thể sử dụng cuộc tấn công cài đặt lại khóa (hoặc tấn công KRACK) để giải mã đường truyền bằng WPA. Những kẻ tấn công có thể tự chèn mình vào quá trình bắt tay xác thực WPA và chèn khóa mã hóa mới thay vì khóa động do WPA chỉ định. Nếu họ đặt khóa mới thành toàn số 0, thì có vẻ như quá trình truyền tải hoàn toàn không được mã hóa.

|  |
| --- |
| Because of this significant vulnerability, WPA was replaced with an updated version of the protocol called WPA2. |

Do lỗ hổng nghiêm trọng này, WPA đã được thay thế bằng phiên bản cập nhật của giao thức có tên WPA2.

|  |
| --- |
| **WPA2 & WPA3** |

**WPA2 & WPA3**

|  |
| --- |
| **WPA2** |

**WPA2**

|  |
| --- |
| The second version of Wi-Fi Protected Access—known as WPA2—was released in 2004. WPA2 improves upon WPA by using the Advanced Encryption Standard (AES). WPA2 also improves upon WPA’s use of TKIP. WPA2 uses the Counter Mode Cipher Block Chain Message Authentication Code Protocol (CCMP), which provides encapsulation and ensures message authentication and integrity. Because of the strength of WPA2, it is considered the security standard for all Wi-Fi transmissions today. WPA2, like its predecessor, is vulnerable to KRACK attacks. This led to the development of WPA3 in 2018. |

Phiên bản thứ hai của Wi-Fi Protected Access—được gọi là WPA2—được phát hành vào năm 2004. WPA2 cải tiến dựa trên WPA bằng cách sử dụng Tiêu chuẩn mã hóa nâng cao (AES). WPA2 cũng cải thiện việc sử dụng TKIP của WPA. WPA2 sử dụng Giao thức mã xác thực tin nhắn chuỗi khối mã hóa chế độ đếm (CCMP), cung cấp khả năng đóng gói và đảm bảo tính xác thực và tính toàn vẹn của tin nhắn. Chính vì sức mạnh của WPA2 nên nó được coi là tiêu chuẩn bảo mật cho mọi đường truyền Wi-Fi hiện nay. WPA2, giống như người tiền nhiệm của nó, dễ bị tấn công KRACK. Điều này dẫn đến sự phát triển của WPA3 vào năm 2018.

|  |
| --- |
| **Personal** |

**Riêng tư**

|  |
| --- |
| WPA2 personal mode is best suited for home networks for a variety of reasons. It is easy to implement, initial setup takes less time for personal than enterprise version. The global passphrase for WPA2 personal version needs to be applied to each individual computer and access point in a network. This makes it ideal for home networks, but unmanageable for organizations. |

Chế độ cá nhân WPA2 phù hợp nhất cho mạng gia đình vì nhiều lý do. Dễ dàng thực hiện, thiết lập ban đầu mất ít thời gian hơn cho phiên bản cá nhân so với phiên bản doanh nghiệp. Cụm mật khẩu chung cho phiên bản cá nhân WPA2 cần được áp dụng cho từng máy tính và điểm truy cập trong mạng. Điều này khiến nó trở nên lý tưởng cho mạng gia đình nhưng khó quản lý đối với các tổ chức.

|  |
| --- |
| **Enterprise** |

**Doanh nghiệp**

|  |
| --- |
| WPA2 enterprise mode works best for business applications. It provides the necessary security for wireless networks in business settings. The initial setup is more complicated than WPA2 personal mode, but enterprise mode offers individualized and centralized control over the Wi-Fi access to a business network. This means that network administrators can grant or remove user access to a network at any time. Users never have access to encryption keys, this prevents potential attackers from recovering network keys on individual computers. |

Chế độ doanh nghiệp WPA2 hoạt động tốt nhất cho các ứng dụng kinh doanh. Nó cung cấp sự bảo mật cần thiết cho mạng không dây trong cài đặt doanh nghiệp. Thiết lập ban đầu phức tạp hơn chế độ cá nhân WPA2, nhưng chế độ doanh nghiệp cung cấp khả năng kiểm soát tập trung và cá nhân hóa đối với quyền truy cập Wi-Fi vào mạng doanh nghiệp. Điều này có nghĩa là quản trị viên mạng có thể cấp hoặc xóa quyền truy cập của người dùng vào mạng bất kỳ lúc nào. Người dùng không bao giờ có quyền truy cập vào khóa mã hóa, điều này ngăn cản những kẻ tấn công tiềm năng khôi phục khóa mạng trên từng máy tính.

|  |
| --- |
| **WPA3** |

**WPA3**

|  |
| --- |
| WPA3 is a secure Wi-Fi protocol and is growing in usage as more WPA3 compatible devices are released. These are the key differences between WPA2 and WPA3:   * WPA3 addresses the authentication handshake vulnerability to KRACK attacks, which is present in WPA2. * WPA3 uses Simultaneous Authentication of Equals (SAE), a password-authenticated, cipher-key-sharing agreement. This prevents attackers from downloading data from wireless network connections to their systems to attempt to decode it. * WPA3 has increased encryption to make passwords more secure  by using 128-bit encryption, with WPA3-Enterprise mode offering optional 192-bit encryption. |

WPA3 là giao thức Wi-Fi an toàn và ngày càng được sử dụng nhiều khi có nhiều thiết bị tương thích WPA3 được phát hành. Đây là những khác biệt chính giữa WPA2 và WPA3:

* WPA3 giải quyết lỗ hổng bắt tay xác thực đối với các cuộc tấn công KRACK, hiện có trong WPA2.
* WPA3 sử dụng Xác thực đồng thời bằng (SAE), một thỏa thuận chia sẻ khóa mật mã, xác thực bằng mật khẩu. Điều này ngăn cản kẻ tấn công tải dữ liệu từ kết nối mạng không dây về hệ thống của họ để cố gắng giải mã nó.
* WPA3 đã tăng cường mã hóa để làm cho mật khẩu an toàn hơn bằng cách sử dụng mã hóa 128-bit, với chế độ WPA3-Enterprise cung cấp mã hóa 192-bit tùy chọn.

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

**Bài học chính**

|  |
| --- |
| As a security analyst, knowing the history of how Wi-Fi security protocols developed helps you to better understand what to consider when protecting wireless networks. It’s important that you understand the vulnerabilities of each protocol and how important it is that devices on your network use the most up-to-date security technologies. |

Là một nhà phân tích bảo mật, việc biết lịch sử phát triển các giao thức bảo mật Wi-Fi sẽ giúp bạn hiểu rõ hơn những điều cần cân nhắc khi bảo vệ mạng không dây. Điều quan trọng là bạn phải hiểu các lỗ hổng của từng giao thức và tầm quan trọng của việc các thiết bị trên mạng của bạn sử dụng các công nghệ bảo mật cập nhật nhất.

***1.8. Test your knowledge: Recognize different network protocols – Kiểm tra kiến ​​thức của bạn: Nhận biết các giao thức mạng khác nhau***

**2. System identification – Nhận dạng hệ thống**

***2.1. Firewalls and network security measures – Tường lửa và các biện pháp an ninh mạng***

|  |
| --- |
| In this video, you'll learn about different types of firewalls. These include hardware, software, and cloud-based firewalls. You'll also learn the difference between a stateless and stateful firewall and cover some of the basic operations that a firewall performs. Finally, you will explore how proxy servers are used to add a layer of security to the network. |

Trong video này, bạn sẽtìm hiểu về các loại tường lửa khác nhau.Chúng bao gồm phần cứng,phần mềm và tường lửa dựa trên đám mây.Bạn cũng sẽ tìm hiểu sự khác biệt giữamột tường lửa không trạng thái và trạng thái vàbao gồm một số hoạt động cơ bảnmà tường lửa thực hiện.Cuối cùng, bạn sẽ khám phá cáchmáy chủ proxy được sử dụng đểthêm một lớp bảo mật cho mạng.

|  |
| --- |
| A firewall is a network security device that monitors traffic to and from your network. It either allows traffic or it blocks it based on a defined set of security rules. A firewall can use port filtering, which blocks or allows certain port numbers to limit unwanted communication. For example, it could have a rule that only allows communications on port 443 for HTTPS or port 25 for email and blocks everything else. These firewall settings will be determined by the organization's security policy. |

Tường lửa là một thiết bị an ninh mạng có chức nănggiám sát lưu lượng đến và đi từ mạng của bạn.Nó cho phép lưu lượng truy cập hoặc chặnnó dựa trên một bộ quy tắc bảo mật được xác định.Tường lửa có thể sử dụng tính năng lọc cổng,chặn hoặc cho phépsố cổng nhất định để hạn chế giao tiếp không mong muốn.Ví dụ, nó có thể có một quy tắcchỉ cho phép liên lạc trên cổng443 cho HTTPS hoặc cổng25 cho email và chặn mọi thứ khác.Các cài đặt tường lửa này sẽ được xác định bởichính sách bảo mật của tổ chức.

|  |
| --- |
| Let's talk about a few different kinds of firewalls. A hardware firewall is considered the most basic way to defend against threats to a network. A hardware firewall inspects each data packet before it's allowed to enter the network. A software firewall performs the same functions as a hardware firewall, but it's not a physical device. Instead, it's a software program installed on a computer or on a server. If the software firewall is installed on a computer, it will analyze all the traffic received by that computer. If the software firewall is installed on a server, it will protect all the devices connected to the server. A software firewall typically costs less than purchasing a separate physical device, and it doesn't take up any extra space. But because it is a software program, it will add some processing burden to the individual devices. |

Hãy nói về một vài loại tường lửa khác nhau.Tường lửa phần cứng được coi là tốt nhấtcách cơ bản để bảo vệ chống lại các mối đe dọa đối với mạng.Tường lửa phần cứng kiểm tramỗi gói dữ liệu trước nóđược phép vào mạng.Tường lửa phần mềm thực hiệncó chức năng tương tự như tường lửa phần cứng,nhưng nó không phải là một thiết bị vật lý.Thay vào đó, nó là một chương trình phần mềmđược cài đặt trên máy tính hoặc trên máy chủ.Nếu tường lửa phần mềm được cài đặt trên máy tính,nó sẽ phân tích tất cả lưu lượng truy cậpmáy tính đó nhận được.Nếu tường lửa phần mềm được cài đặt trên máy chủ,nó sẽ bảo vệ tất cả các thiết bị được kết nối với máy chủ.Tường lửa phần mềm thường có giáít hơn việc mua một thiết bị vật lý riêng biệt,và nó không chiếm thêm không gian.Nhưng vì nó là một chương trình phần mềm nênnó sẽ thêm một số gánh nặng xử lýtới các thiết bị riêng lẻ.

|  |
| --- |
| Organizations may choose to use a cloud-based firewall. Cloud service providers offer firewalls as a service, or FaaS, for organizations. Cloud-based firewalls are software firewalls hosted by a cloud service provider. Organizations can configure the firewall rules on the cloud service provider's interface, and the firewall will perform security operations on all incoming traffic before it reaches the organization’s onsite network. Cloud-based firewalls also protect any assets or processes that an organization might be using in the cloud. |

Các tổ chức có thể chọn sử dụng tường lửa dựa trên đám mây.Các nhà cung cấp dịch vụ đám mây cung cấp tường lửa nhưmột dịch vụ hoặc FaaS cho các tổ chức.Tường lửa dựa trên đám mây là tường lửa phần mềmđược lưu trữ bởi nhà cung cấp dịch vụ đám mây.Các tổ chức có thể cấu hình các quy tắc tường lửatrên giao diện của nhà cung cấp dịch vụ đám mây,và tường lửa sẽ thực hiện các hoạt động bảo mật trêntất cả lưu lượng truy cập đến trướcnó đến được mạng tại chỗ của tổ chức.Tường lửa dựa trên đám mây cũng bảo vệ mọi tài sản hoặccác quy trình mà một tổ chứccó thể đang sử dụng trên đám mây.

|  |
| --- |
| All the firewalls we have discussed can be either stateful or stateless. The terms "stateful" and "stateless" refer to how the firewall operates. Stateful refers to a class of firewall that keeps track of information passing through it and proactively filters out threats. A stateful firewall analyzes network traffic for characteristics and behavior that appear suspicious and stops them from entering the network. Stateless refers to a class of firewall that operates based on predefined rules and does not keep track of information from data packets. A stateless firewall only acts according to preconfigured rules set by the firewall administrator. The rules programmed by the firewall administrator tell the device what to accept and what to reject. A stateless firewall doesn't store analyzed information. It also doesn't discover suspicious trends like a stateful firewall does. For this reason, stateless firewalls are considered less secure than stateful firewalls. |

Tất cả các tường lửa mà chúng ta đã thảo luận có thểcó trạng thái hoặc không có trạng thái.Các thuật ngữ "có trạng thái" và "không có trạng thái"tham khảo cách hoạt động của tường lửa.Stateful đề cập đến một lớptường lửa theo dõithông tin đi qua nóvà chủ động lọc ra các mối đe dọa.Phân tích tường lửa trạng tháilưu lượng truy cập mạng cho các đặc điểm vàhành vi có vẻ đáng ngờvà ngăn chặn chúng xâm nhập vào mạng.Không trạng thái đề cập đến một lớptường lửa hoạt động dựa trênquy tắc được xác định trước và khôngtheo dõi thông tin từ các gói dữ liệu.Tường lửa không trạng thái chỉ hoạt động theocác quy tắc được cấu hình sẵn do quản trị viên tường lửa đặt ra.Các quy tắc được lập trình bởi quản trị viên tường lửa sẽ cho biếtthiết bị chấp nhận cái gì và từ chối cái gì.Tường lửa không trạng thái không lưu trữ thông tin được phân tích.Nó cũng không phát hiệnxu hướng đáng ngờ giống như tường lửa có trạng thái.Vì lý do này, tường lửa không trạng thái được coi làkém an toàn hơn so với tường lửa có trạng thái.

|  |
| --- |
| A next generation firewall, or NGFW, provides even more security than a stateful firewall. Not only does an NGFW provide stateful inspection of incoming and outgoing traffic, but it also performs more in-depth security functions like deep packet inspection and intrusion protection. Some NGFWs connect to cloud-based threat intelligence services so they can quickly update to protect against emerging cyber threats. |

Tường lửa thế hệ tiếp theo, hay NGFW,thậm chí còn cung cấp tính bảo mật cao hơn tường lửa có trạng thái.NGFW không chỉ cung cấpkiểm tra trạng thái lưu lượng đến và đi,nhưng nó cũng hoạt động nhiều hơnchức năng bảo mật chuyên sâu nhưkiểm tra gói sâu và bảo vệ chống xâm nhập.Một số NGFW kết nối vớidịch vụ tình báo mối đe dọa dựa trên đám mâyđể họ có thể nhanh chóng cập nhật lênbảo vệ chống lại các mối đe dọa mạng đang nổi lên.

|  |
| --- |
| Now you have a basic understanding of firewalls and how they work. We learned that firewalls can be hardware or software. We also discussed the difference between a stateless and stateful firewall and the security benefits of a stateful firewall. Finally, we discussed next generation firewalls and the security benefits they provide. Coming up, we'll learn more about virtual networks. |

Bây giờ bạn đã có sự hiểu biết cơ bảntường lửa và cách chúng hoạt động.Chúng tôi đã biết rằng tường lửa có thể là phần cứng hoặc phần mềm.Chúng tôi cũng đã thảo luận về sự khác biệt giữatường lửa không trạng thái và trạng tháivà lợi ích bảo mật của tường lửa có trạng thái.Cuối cùng, chúng ta đã thảo luận về tường lửa thế hệ tiếp theovà những lợi ích bảo mật mà chúng mang lại.Tiếp theo, chúng ta sẽ tìm hiểu thêm về mạng ảo.

***2.2. Virtual private networks (VPNs) – Mạng riêng ảo (VPN)***

|  |
| --- |
| In this video, we're going to discuss how virtual private networks, or VPNs, add security to your network. When you connect to the internet, your internet service provider receives your network's requests and forwards it to the correct destination server. But your internet requests include your private information. That means if the traffic gets intercepted, someone could potentially connect your internet activity with your physical location and your personal information. This includes some information that you want to keep private, like bank accounts and credit card numbers. A virtual private network, also known as a VPN, is a network security service that changes your public IP address and hides your virtual location so that you can keep your data private when you're using a public network like the internet. |

Trong video này, chúng ta sẽthảo luận về cách mạng riêng ảo,hoặc VPN, hãy tăng cường bảo mật cho mạng của bạn.Khi bạn kết nối với internet,nhà cung cấp dịch vụ internet của bạn nhận đượcyêu cầu của mạng của bạn vàchuyển tiếp nó đến đúng máy chủ đích.Nhưng yêu cầu internet của bạnbao gồm thông tin cá nhân của bạn.Điều đó có nghĩa là nếu giao thông bị chặn,ai đó có khả năng có thể kết nối hoạt động internet của bạnvới vị trí thực tế của bạnvà thông tin cá nhân của bạn.Điều này bao gồm một số thông tinmà bạn muốn giữ riêng tư,như tài khoản ngân hàng và số thẻ tín dụng.Một mạng riêng ảo,còn được gọi là VPN,là một dịch vụ an ninh mạng thay đổiđịa chỉ IP công cộng của bạn và ẩnvị trí ảo của bạn để bạn có thể lưu giữ dữ liệu của mìnhriêng tư khi bạn đang sử dụng công khaimạng giống như internet.

|  |
| --- |
| VPNs also encrypt your data as it travels across the internet to preserve confidentiality. A VPN service performs encapsulation on your data in transit. Encapsulation is a process performed by a VPN service that protects your data by wrapping sensitive data in other data packets. Previously, you learned how the MAC and IP address of the destination device is contained in the header and footer of a data packet. This is a security threat because it shows the IP and virtual location of your private network. You could secure a data packet by encrypting it to make sure your information can't be deciphered, but then network routers won't be able to read the IP and MAC address to know where to send it to. This means you won't be able to connect to the internet site or the service that you want. Encapsulation solves this problem while still maintaining your privacy. VPN services encrypt your data packets and encapsulate them in other data packets that the routers can read. This allows your network requests to reach their destination, but still encrypts your personal data so it's unreadable while in transit. A VPN also uses an encrypted tunnel between your device and the VPN server. The encryption is unhackable without a cryptographic key, so no one can access your data. |

VPN cũng mã hóa dữ liệu của bạn vì nódi chuyển trên internet để bảo vệ bí mật.Một dịch vụ VPN thực hiệnđóng gói dữ liệu của bạn trong quá trình chuyển tiếp.Đóng gói là một quá trình được thực hiệnbởi một dịch vụ VPN bảo vệdữ liệu của bạn bằng cách góidữ liệu nhạy cảm trong các gói dữ liệu khác.Trước đây, bạn đã tìm hiểu cách địa chỉ MAC và IP củathiết bị đích được chứatrong đầu trang và chân trang của gói dữ liệu.Đây là một mối đe dọa an ninh bởi vì nó cho thấyIP và vị trí ảo của mạng riêng của bạn.Bạn có thể bảo mật gói dữ liệu bằng cách mã hóanó để đảm bảo thông tin của bạn không thể bị giải mã,nhưng khi đó bộ định tuyến mạng sẽ không thể đọc đượcđịa chỉ IP và MAC để biết nơi gửi nó đến.Điều này có nghĩa là bạn sẽ không thể kết nối vớitrang web hoặc dịch vụ mà bạn muốn.Đóng gói giải quyết vấn đề nàytrong khi vẫn duy trì sự riêng tư của bạn.Dịch vụ VPN mã hóa các gói dữ liệu của bạn vàgói gọn chúng trong các gói dữ liệu khácmà các bộ định tuyến có thể đọc được.Điều này cho phép các yêu cầu mạng của bạnđể đến đích,nhưng vẫn mã hóa dữ liệu cá nhân của bạnvì vậy nó không thể đọc được trong khi vận chuyển.VPN cũng sử dụng đường hầm được mã hóagiữa thiết bị của bạn và máy chủ VPN.Mã hóa không thể bị hack nếu không có khóa mật mã,để không ai có thể truy cập dữ liệu của bạn.

|  |
| --- |
| VPN services are simple and offer significant protection while you're on the internet. With a VPN, you have the added assurance that your data is encrypted, and your IP address and virtual location are unreadable to malicious actors. |

Dịch vụ VPN rất đơn giản và cung cấpsự bảo vệ đáng kể khi bạn truy cập internet.Với VPN,bạn có thêm sự đảm bảo rằng dữ liệu của bạn được mã hóa vàđịa chỉ IP của bạn vàvị trí ảo không thể đọc được đối với các tác nhân độc hại.

***2.3. Security zones – Khu an ninh***

|  |
| --- |
| In this section, we'll discuss a type of network security feature called a security zone. Security zones are a segment of a network that protects the internal network from the internet. They are a part of a security technique called network segmentation that divides the network into segments. Each network segment has its own access permissions and security rules. Security zones control who can access different segments of a network. Security zones act as a barrier to internal networks, maintain privacy within corporate groups, and prevent issues from spreading to the whole network. One example of network segmentation is a hotel that offers free public Wi-Fi. The unsecured guest network is kept separate from another encrypted network used by the hotel staff. |

Trong phần này chúng ta sẽ thảo luận về một loạitính năng bảo mật mạng được gọi là vùng bảo mật.Vùng bảo mật là một phần của mạngbảo vệ mạng nội bộ khỏi internet.Chúng là một phần của kỹ thuật bảo mậtgọi là phân đoạn mạngđó chia mạng thành các phân đoạn.Mỗi phân đoạn mạng cóquyền truy cập và quy tắc bảo mật riêng của nó.Khu vực an ninh kiểm soát ai có thểtruy cập các phân đoạn khác nhau của mạng.Vùng an ninh hoạt động như một rào cản đối với mạng nội bộ,duy trì sự riêng tư trong các nhóm công ty,và ngăn chặn sự cố lan rộng ra toàn mạng.Một ví dụ về phân đoạn mạng làmột khách sạn cung cấp Wi-Fi công cộng miễn phí.Mạng khách không an toàn được tách biệt khỏimột mạng mã hóa khác được nhân viên khách sạn sử dụng.

|  |
| --- |
| Additionally, an organization's network can be divided into subnetworks, or subnets, to maintain privacy for each department in a organization. For instance, at a university, there may be a faculty subnet and a separate students subnet. If there is contamination on the student's subnet, network administrators can isolate it and keep the rest of the network free from contamination. |

Ngoài ra, một tổ chứcmạng có thể được chia thànhmạng con hoặc mạng con đểduy trì sự riêng tư cho từng bộ phận trong một tổ chức.Ví dụ, tại một trường đại học,có thể có một mạng con của khoavà một mạng con sinh viên riêng biệt.Nếu có sự ô nhiễm trên mạng con của học sinh,quản trị viên mạng có thể cô lập nó vàgiữ cho phần còn lại của mạng không bị ô nhiễm.

|  |
| --- |
| An organization's network is classified into two types of security zones. First, there's the uncontrolled zone, which is any network outside of the organization's control, like the internet. Then, there's the controlled zone, which is a subnet that protects the internal network from the uncontrolled zone. There are several types of networks within the controlled zone. On the outer layer is the demilitarized zone, or DMZ, which contains public-facing services that can access the internet. This includes web servers, proxy servers that host websites for the public, and DNS servers that provide IP addresses for internet users. It also includes email and file servers that handle external communications. The DMZ acts as a network perimeter to the internal network. The internal network contains private servers and data that the organization needs to protect. Inside the internal network is another zone called the restricted zone. The restricted zone protects highly confidential information that is only accessible to employees with certain privileges. |

Mạng của một tổ chức được phân loại thànhhai loại vùng an ninh. Đầu tiên,có vùng không được kiểm soát,đó là bất kỳ mạng nào bên ngoàisự kiểm soát của tổ chức, giống như internet.Sau đó là vùng kiểm soát,đó là một mạng con bảo vệmạng nội bộ từ vùng không được kiểm soát.Có một số loạimạng trong vùng được kiểm soát.Lớp ngoài cùng là khu phi quân sự,hoặc DMZ, chứacác dịch vụ công cộng có thể truy cập internet.Điều này bao gồm các máy chủ web,máy chủ proxy lưu trữ các trang web cho công chúng,và máy chủ DNS cung cấpĐịa chỉ IP cho người dùng internet.Nó cũng bao gồm email và tập tinmáy chủ xử lý thông tin liên lạc bên ngoài.DMZ hoạt động nhưmột chu vi mạng đến mạng nội bộ.Mạng nội bộ chứa các máy chủ riêng vàdữ liệu mà tổ chức cần bảo vệ.Bên trong mạng nội bộ làvùng khác gọi là vùng hạn chế.Vùng hạn chế bảo vệthông tin có tính bảo mật cao chỉnhân viên có thể truy cập với những đặc quyền nhất định.

|  |
| --- |
| Now, let's try to picture these security zones. Ideally, the DMZ is situated between two firewalls. One of them filters traffic outside the DMZ, and one of them filters traffic entering the internal network. This protects the internal network with several lines of defense. If there's a restricted zone, that too would be protected with another firewall. This way, attacks that penetrate into the DMZ network cannot spread to the internal network, and attacks that penetrate the internal network cannot access the restricted zone. As a security analyst, you may be responsible for regulating access control policies on these firewalls. Security teams can control traffic reaching the DMZ and the internal network by restricting IPs and ports. For example, an analyst may ensure that only HTTPS traffic is allowed to access web servers in the DMZ. |

Bây giờ chúng ta hãy thử hình dung những vùng an ninh này.Lý tưởng nhất là DMZ nằm giữahai bức tường lửa. Một trong số chúnglọc lưu lượng truy cập bên ngoài DMZ,và một trong số đó lọc lưu lượng truy cậpxâm nhập vào mạng nội bộ.Điều này bảo vệ mạng nội bộvới nhiều tuyến phòng thủ.Nếu có vùng cấmđiều đó cũng sẽ được bảo vệ vớitường lửa khác. Cách này,các cuộc tấn công xâm nhập vàomạng DMZ không thể lan sang mạng nội bộ,và các cuộc tấn công xuyên quamạng nội bộ không thể truy cập vào vùng hạn chế.Là một nhà phân tích chứng khoán,bạn có thể chịu trách nhiệm điều chỉnhchính sách kiểm soát truy cập trên các tường lửa này.Đội an ninh có thể kiểm soát lưu lượng truy cậpDMZ và mạng nội bộbằng cách hạn chế IP và cổng.Ví dụ, một nhà phân tích có thể đảm bảo rằngchỉ có lưu lượng truy cập HTTPS làđược phép truy cập các máy chủ web trong DMZ.

|  |
| --- |
| Security zones are an important part of securing networks, especially in large organizations. Understanding how they are used is essential for all security analysts. Coming up, we'll learn about securing internal networks. |

Các khu vực an ninh đượcmột phần quan trọng của việc bảo mật mạng,đặc biệt là trong các tổ chức lớn.Hiểu cách chúng được sử dụng làcần thiết cho tất cả các nhà phân tích chứng khoán.Tiếp theo, chúng ta sẽ tìm hiểu về việc bảo mật mạng nội bộ.

***2.4. Subnetting and CIDR – Mạng con và CIDR***

|  |
| --- |
| **Subnetting and CIDR** |

**Mạng con và CIDR**

|  |
| --- |
| Earlier in this course, you learned about network segmentation, a security technique that divides networks into sections. A private network can be segmented to protect portions of the network from the internet, which is an unsecured global network. |

Trước đó trong khóa học này, bạn đã tìm hiểu về phân đoạn mạng, một kỹ thuật bảo mật chia mạng thành các phần. Mạng riêng có thể được phân đoạn để bảo vệ các phần của mạng khỏi Internet, đây là mạng toàn cầu không bảo mật.

|  |
| --- |
| For example, you learned about the uncontrolled zone, the controlled zone, the demilitarized zone, and the restricted zone. Feel free to review the video about [security zones](https://www.coursera.org/learn/networks-and-network-security/lecture/GccYm/security-zones) for a refresher on how network segmentation can be used to add a layer of security to your organization’s network operations. Creating security zones is one example of a networking strategy called subnetting. |

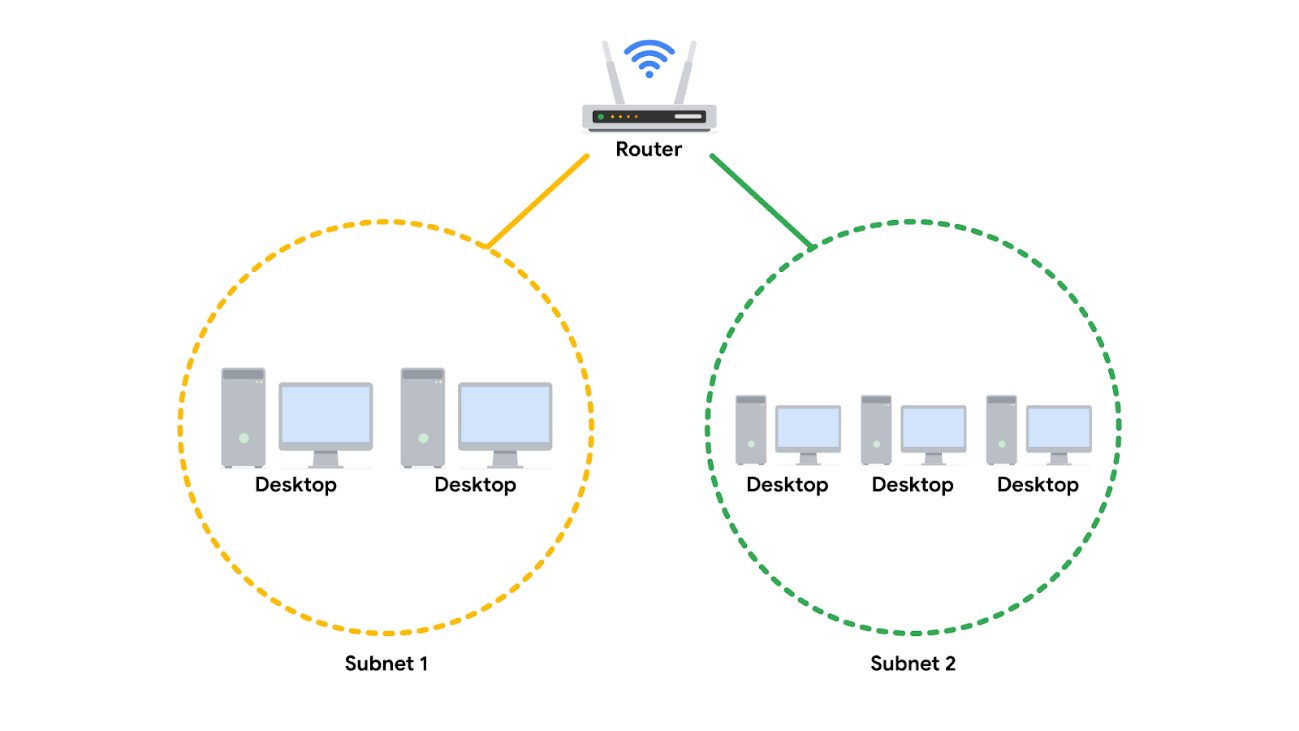
Ví dụ: bạn đã tìm hiểu về vùng không kiểm soát, vùng kiểm soát, vùng phi quân sự và vùng hạn chế. Hãy thoải mái xem lại video về[khu an ninh](https://www.coursera.org/learn/networks-and-network-security/lecture/GccYm/security-zones)để biết thêm về cách sử dụng phân đoạn mạng để thêm lớp bảo mật cho hoạt động mạng của tổ chức bạn. Tạo vùng bảo mật là một ví dụ về chiến lược mạng được gọi là mạng con.

|  |
| --- |
| **Overview of subnetting** |

**Tổng quan về mạng con**

|  |
| --- |
| **Subnetting** is the subdivision of a network into logical groups called subnets. It works like a network inside a network. Subnetting divides up a network address range into smaller subnets within the network. These smaller subnets form based on the IP addresses and network mask of the devices on the network. Subnetting creates a network of devices to function as their own network. This makes the network more efficient and can also be used to create security zones. If devices on the same subnet communicate with each other, the switch changes the transmissions to stay on the same subnet, improving speed and efficiency of the communications. |

**Mạng con** là sự chia nhỏ mạng thành các nhóm logic gọi là mạng con. Nó hoạt động giống như một mạng bên trong một mạng. Mạng con chia dải địa chỉ mạng thành các mạng con nhỏ hơn trong mạng. Các mạng con nhỏ hơn này hình thành dựa trên địa chỉ IP và mặt nạ mạng của các thiết bị trên mạng. Mạng con tạo ra một mạng lưới các thiết bị hoạt động như mạng riêng của chúng. Điều này làm cho mạng hiệu quả hơn và cũng có thể được sử dụng để tạo vùng bảo mật. Nếu các thiết bị trên cùng một mạng con giao tiếp với nhau, bộ chuyển mạch sẽ thay đổi đường truyền để duy trì trên cùng một mạng con, cải thiện tốc độ và hiệu quả của việc liên lạc.



|  |
| --- |
| **Classless Inter-Domain Routing notation for subnetting** |

**Ký hiệu định tuyến liên miền không phân lớp cho mạng con**

|  |
| --- |
| Classless Inter-Domain Routing (CIDR) is a method of assigning subnet masks to IP addresses to create a subnet. Classless addressing replaces classful addressing. Classful addressing was used in the 1980s as a system of grouping IP addresses into classes (Class A to Class E). Each class included a limited number of IP addresses, which were depleted as the number of devices connecting to the internet outgrew the classful range in the 1990s. Classless CIDR addressing expanded the number of available IPv4 addresses. |

Định tuyến giữa các miền không phân loại (CIDR) là phương pháp gán mặt nạ mạng con cho các địa chỉ IP để tạo mạng con. Địa chỉ không phân lớp thay thế địa chỉ có phân lớp. Địa chỉ phân loại được sử dụng vào những năm 1980 như một hệ thống nhóm các địa chỉ IP thành các lớp (Loại A đến Loại E). Mỗi lớp bao gồm một số lượng địa chỉ IP hạn chế, đã cạn kiệt khi số lượng thiết bị kết nối với Internet tăng vượt xa phạm vi phân loại vào những năm 1990. Địa chỉ CIDR không phân loại đã mở rộng số lượng địa chỉ IPv4 có sẵn.

|  |
| --- |
| CIDR allows cybersecurity professionals to segment classful networks into smaller chunks. CIDR IP addresses are formatted like IPv4 addresses, but they include a slash (“/’”) followed by a number at the end of the address, This extra number is called the IP network prefix.  For example, a regular IPv4 address uses the 198.51.100.0 format, whereas a CIDR IP address would include the IP network prefix at the end of the address, 198.51.100.0/24. This CIDR address encompasses all IP addresses between 198.51.100.0 and 198.51.100.255. The system of CIDR addressing reduces the number of entries in routing tables and provides more available IP addresses within networks. You can try converting CIDR to IPv4 addresses and vice versa through an online conversion tool, like [IPAddressGuide](https://www.ipaddressguide.com/cidr), for practice and to better understand this concept. |

CIDR cho phép các chuyên gia an ninh mạng phân chia các mạng phân loại thành các phần nhỏ hơn. Địa chỉ IP CIDR được định dạng giống địa chỉ IPv4, nhưng chúng bao gồm dấu gạch chéo (“/'”) theo sau là một số ở cuối địa chỉ. Số bổ sung này được gọi là tiền tố mạng IP. Ví dụ: địa chỉ IPv4 thông thường sử dụng định dạng 198.51.100.0, trong khi địa chỉ IP CIDR sẽ bao gồm tiền tố mạng IP ở cuối địa chỉ, 198.51.100.0/24. Địa chỉ CIDR này bao gồm tất cả các địa chỉ IP trong khoảng từ 198.51.100.0 đến 198.51.100.255. Hệ thống địa chỉ CIDR làm giảm số lượng mục trong bảng định tuyến và cung cấp nhiều địa chỉ IP khả dụng hơn trong mạng. Bạn có thể thử chuyển đổi CIDR sang địa chỉ IPv4 và ngược lại thông qua công cụ chuyển đổi trực tuyến, như[Hướng dẫn địa chỉ IP](https://www.ipaddressguide.com/cidr), để thực hành và hiểu rõ hơn về khái niệm này.

|  |
| --- |
| **Note:** You may learn more about CIDR during your career, but it won't be covered in any additional depth in this certificate program. For now, you only need a basic understanding of this concept. |

**Lưu ý:** Bạn có thể tìm hiểu thêm về CIDR trong quá trình làm việc của mình nhưng nó sẽ không được đề cập sâu hơn trong chương trình chứng chỉ này. Hiện tại, bạn chỉ cần hiểu biết cơ bản về khái niệm này.

|  |
| --- |
| **Security benefits of subnetting** |

**Lợi ích bảo mật của mạng con**

|  |
| --- |
| Subnetting allows network professionals and analysts to create a network within their own network without requesting another network IP address from their internet service provider. This process uses network bandwidth more efficiently and improves network performance. Subnetting is one component of creating isolated subnetworks through physical isolation, routing configuration, and firewalls. |

Mạng con cho phép các chuyên gia và nhà phân tích mạng tạo một mạng trong mạng riêng của họ mà không yêu cầu địa chỉ IP mạng khác từ nhà cung cấp dịch vụ internet của họ. Quá trình này sử dụng băng thông mạng hiệu quả hơn và cải thiện hiệu suất mạng. Mạng con là một thành phần của việc tạo các mạng con bị cô lập thông qua cách ly vật lý, cấu hình định tuyến và tường lửa.

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

**Bài học chính**

|  |
| --- |
| Subnetting is a common security strategy used by organizations. Subnetting allows organizations to create smaller networks within their private network. This improves the efficiency of the network and can be used to create security zones. |

Mạng con là một chiến lược bảo mật phổ biến được các tổ chức sử dụng. Mạng con cho phép các tổ chức tạo các mạng nhỏ hơn trong mạng riêng của họ. Điều này cải thiện hiệu quả của mạng và có thể được sử dụng để tạo vùng bảo mật.

***2.5. Proxy servers – Máy chủ proxy***

|  |
| --- |
| Previously, we discussed how firewalls, VPNs, and security zones help to secure networks. Next, we'll cover how to secure internal networks with proxy servers. |

Trước đây, chúng ta đã thảo luận về cách tường lửa, VPN vàvùng bảo mật giúp bảo mật mạng.Tiếp theo, chúng tôi sẽ đề cập đến cách bảo mật mạng nội bộ bằng máy chủ proxy.

|  |
| --- |
| Proxy servers are another system that helps secure networks. The definition of a proxy server is a server that fulfills the request of a client by forwarding them on to other servers. The proxy server is a dedicated server that sits between the internet and the rest of the network. When a request to connect to the network comes in from the internet, the proxy server will determine if the connection request is safe. The proxy server is a public IP address that is different from the rest of the private network. This hides the private network's IP address from malicious actors on the internet and adds a layer of security. |

Máy chủ proxy là một hệ thống khác giúp bảo mật mạng.Định nghĩa máy chủ proxy là máy chủ đáp ứng yêu cầu củamột khách hàng bằng cách chuyển tiếp chúng đến các máy chủ khác.Máy chủ proxy là một máy chủ chuyên dụng nằm giữa Internet vàphần còn lại của mạng.Khi có yêu cầu kết nối mạng đến từ internet,máy chủ proxy sẽ xác định xem yêu cầu kết nối có an toàn hay không.Máy chủ proxy là một địa chỉ IP công cộng khác với phần còn lạicủa mạng riêng.Điều này ẩn địa chỉ IP của mạng riêng khỏi các tác nhân độc hại trên internet vàthêm một lớp bảo mật.

|  |
| --- |
| Let's examine how this will work with an example. When a client receives an HTTPS response, they will notice a distorted IP address or no IP address rather than the real IP address of the organization's web server. A proxy server can also be used to block unsafe websites that users aren't allowed to access on an organization's network. A proxy server uses temporary memory to store data that's regularly requested by external servers. This way, it doesn't have to fetch data from an organization's internal servers every time. This enhances security by reducing contact with the internal server. |

Hãy xem xét điều này sẽ hoạt động như thế nào bằng một ví dụ.Khi khách hàng nhận được phản hồi HTTPS, họ sẽ nhận thấy địa chỉ IP bị sai lệch hoặckhông có địa chỉ IP nào thay vì địa chỉ IP thực của máy chủ web của tổ chức.Máy chủ proxy cũng có thể được sử dụng để chặn các trang web không an toàn mà người dùng không được phépđể truy cập vào mạng của một tổ chức.Máy chủ proxy sử dụng bộ nhớ tạm thời để lưu trữ dữ liệuthường xuyên được yêu cầu bởi các máy chủ bên ngoài.Bằng cách này, nó không phải lấy dữ liệu từ nội bộ của tổ chứcmáy chủ mọi lúc.Điều này tăng cường bảo mật bằng cách giảm liên lạc với máy chủ nội bộ.

|  |
| --- |
| There are different types of proxy servers that support network security. This is important for security analysts who monitor traffic from various proxy servers and may need to know what purpose they serve. Let's explore some different types of proxy servers. A forward proxy server regulates and restricts a person with access to the internet. The goal is to hide a user's IP address and approve all outgoing requests. In the context of an organization, a forward proxy server receives outgoing traffic from an employee, approves it, and then forwards it on to the destination on the internet. A reverse proxy server regulates and restricts the internet access to an internal server. The goal is to accept traffic from external parties, approve it, and forward it to the internal servers. This setup is useful for protecting internal web servers containing confidential data from exposing their IP address to external parties. An email proxy server is another valuable security tool. It filters spam email by verifying whether a sender's address was forged. This reduces the risk of phishing attacks that impersonate people known to the organization. |

Có nhiều loại máy chủ proxy khác nhau hỗ trợ bảo mật mạng.Điều này rất quan trọng đối với các nhà phân tích bảo mật, những người theo dõilưu lượng truy cập từ nhiều máy chủ proxy khác nhau và có thể cần biết chúng phục vụ mục đích gì.Hãy cùng khám phá một số loại máy chủ proxy khác nhau.Một máy chủ proxy chuyển tiếp điều chỉnh vàhạn chế một người có quyền truy cập vào internet.Mục đích là ẩn địa chỉ IP của người dùng và phê duyệt tất cả các yêu cầu gửi đi.Trong bối cảnh của một tổ chức,máy chủ proxy chuyển tiếp nhận lưu lượng truy cập đi từ nhân viên, phê duyệt nó vàsau đó chuyển tiếp nó đến đích trên internet.Một máy chủ proxy ngược điều chỉnh vàhạn chế truy cập internet vào một máy chủ nội bộ.Mục tiêu là chấp nhận lưu lượng truy cập từ các bên bên ngoài, phê duyệt nó vàchuyển tiếp nó đến các máy chủ nội bộ.Thiết lập này hữu ích để bảo vệ các máy chủ web nội bộ có chứadữ liệu bí mật khỏi việc tiết lộ địa chỉ IP của họ cho các bên bên ngoài.Máy chủ proxy email là một công cụ bảo mật có giá trị khác.Nó lọc email spam bằng cách xác minh xem địa chỉ của người gửi có bị giả mạo hay không.Điều này làm giảm nguy cơ xảy ra các cuộc tấn công lừa đảo mạo danh những người được biết đếntổ chức.

|  |
| --- |
| Let's talk about a real world example of an email proxy. Several years ago when I was working at a large U.S. broadband ISP, we used a proxy server to implement multiple layers of anti-spam filtering before a message was allowed in for delivery. It ended up tagging around 95% of messages as spam. The proxy servers would've allowed us to filter and then scale those filters without impacting the underlying email platform. |

Hãy nói về một ví dụ thực tế về proxy email.Cách đây vài năm, khi tôi đang làm việc tại một ISP băng thông rộng lớn của Mỹ,chúng tôi đã sử dụng máy chủ proxy để triển khai nhiều lớp lọc chống thư ráctrước khi tin nhắn được phép gửi đi.Cuối cùng, nó đã gắn thẻ khoảng 95% thư là thư rác.Các máy chủ proxy sẽ cho phép chúng tôi lọc vàsau đó mở rộng quy mô các bộ lọc đó mà không ảnh hưởng đến nền tảng email cơ bản.

|  |
| --- |
| Proxy servers play an important part in network security by filtering incoming and outgoing traffic and staying alert to network attacks. These devices add a layer of protection from the unsecured public network that we call the internet. |

Máy chủ proxy đóng vai trò quan trọng trong bảo mật mạng bằng cách lọc các thư đến vàlưu lượng đi và luôn cảnh giác với các cuộc tấn công mạng.Các thiết bị này thêm một lớp bảo vệ khỏi mạng công cộng không bảo mật mà chúng tôi gọi làInternet.

***2.6. Virtual networks and privacy – Mạng ảo và quyền riêng tư***

|  |
| --- |
| **Virtual networks and privacy** |

**Mạng ảo và quyền riêng tư**

|  |
| --- |
| This section of the course covered a lot of information about network operations. You reviewed the fundamentals of network architecture and communication and can now use this knowledge as you learn how to secure networks. Securing a private network requires maintaining the confidentiality of your data and restricting access to authorized users. |

Phần này của khóa học bao gồm rất nhiều thông tin về hoạt động mạng. Bạn đã xem lại các nguyên tắc cơ bản về kiến ​​trúc và giao tiếp mạng và bây giờ có thể sử dụng kiến ​​thức này khi tìm hiểu cách bảo mật mạng. Bảo mật mạng riêng yêu cầu duy trì tính bảo mật của dữ liệu của bạn và hạn chế quyền truy cập đối với người dùng được ủy quyền.

|  |
| --- |
| In this reading, you will review several network security topics previously covered in the course, including virtual private networks (VPNs), proxy servers, firewalls, and security zones. You'll continue to learn more about these concepts and how they relate to each other as you continue through the course. |

Trong bài đọc này, bạn sẽ xem lại một số chủ đề bảo mật mạng đã được đề cập trước đây trong khóa học, bao gồm mạng riêng ảo (VPN), máy chủ proxy, tường lửa và vùng bảo mật. Bạn sẽ tiếp tục tìm hiểu thêm về những khái niệm này và cách chúng liên quan với nhau khi bạn tiếp tục khóa học.

|  |
| --- |
| **Common network protocols** |

**Các giao thức mạng phổ biến**

|  |
| --- |
| Network protocols are used to direct traffic to the correct device and service depending on the kind of communication being performed by the devices on the network. Protocols are the rules used by all network devices that provide a mutually agreed upon foundation for how to transfer data across a network. |

Các giao thức mạng được sử dụng để hướng lưu lượng truy cập đến đúng thiết bị và dịch vụ tùy thuộc vào loại giao tiếp được thực hiện bởi các thiết bị trên mạng. Giao thức là các quy tắc được sử dụng bởi tất cả các thiết bị mạng nhằm cung cấp nền tảng được các bên thống nhất về cách truyền dữ liệu qua mạng.

|  |
| --- |
| There are three main categories of network protocols: communication protocols, management protocols, and security protocols.   1. Communication protocols are used to establish connections between servers. Examples include TCP, UDP, and Simple Mail Transfer Protocol (SMTP), which provides a framework for email communication. 2. Management protocols are used to troubleshoot network issues. One example is the Internet Control Message Protocol (ICMP). 3. Security protocols provide encryption for data in transit. Examples include IPSec and SSL/TLS. |

Có ba loại giao thức mạng chính: giao thức truyền thông, giao thức quản lý và giao thức bảo mật.

1. Giao thức truyền thông được sử dụng để thiết lập kết nối giữa các máy chủ. Các ví dụ bao gồm TCP, UDP và Giao thức truyền thư đơn giản (SMTP), cung cấp khuôn khổ cho giao tiếp qua email.
2. Các giao thức quản lý được sử dụng để khắc phục sự cố mạng. Một ví dụ là Giao thức tin nhắn điều khiển Internet (ICMP).
3. Các giao thức bảo mật cung cấp mã hóa cho dữ liệu được truyền đi. Ví dụ bao gồm IPSec và SSL/TLS.

|  |
| --- |
| Some other commonly used protocols are:   * HyperText Transfer Protocol (HTTP). HTTP is an application layer communication protocol. This allows the browser and the web server to communicate with one another. * Domain Name System (DNS). DNS is an application layer protocol that translates, or maps, host names to IP addresses. * Address Resolution Protocol (ARP). ARP is a network layer communication protocol that maps IP addresses to physical machines or a MAC address recognized on the local area network. |

Một số giao thức thường được sử dụng khác là:

* Giao thức truyền siêu văn bản (HTTP). HTTP là một giao thức truyền thông lớp ứng dụng. Điều này cho phép trình duyệt và máy chủ web giao tiếp với nhau.
* Hệ thống tên miền (DNS). DNS là một giao thức lớp ứng dụng có chức năng dịch hoặc ánh xạ tên máy chủ thành địa chỉ IP.
* Giao thức phân giải địa chỉ (ARP). ARP là giao thức truyền thông lớp mạng ánh xạ địa chỉ IP tới máy vật lý hoặc địa chỉ MAC được nhận dạng trên mạng cục bộ.

|  |
| --- |
| **Wi-Fi** |

**Wifi**

|  |
| --- |
| This section of the course also introduced various wireless security protocols, including WEP, WPA, WPA2, and WPA3. WPA3 encrypts traffic with the Advanced Encryption Standard (AES) cipher as it travels from your device to the wireless access point. WPA2 and WPA3 offer two modes: personal and enterprise. Personal mode is best suited for home networks while enterprise mode is generally utilized for business networks and applications. |

Phần này của khóa học cũng giới thiệu nhiều giao thức bảo mật không dây khác nhau, bao gồm WEP, WPA, WPA2 và WPA3. WPA3 mã hóa lưu lượng truy cập bằng mật mã Tiêu chuẩn mã hóa nâng cao (AES) khi nó truyền từ thiết bị của bạn đến điểm truy cập không dây. WPA2 và WPA3 cung cấp hai chế độ: cá nhân và doanh nghiệp. Chế độ cá nhân phù hợp nhất cho mạng gia đình trong khi chế độ doanh nghiệp thường được sử dụng cho các ứng dụng và mạng doanh nghiệp.

|  |
| --- |
| **Network security tools and practices** |

**Các công cụ và thực tiễn bảo mật mạng**

|  |
| --- |
| **Firewalls** |

**Tường lửa**

|  |
| --- |
| Previously, you learned that firewalls are network virtual appliances (NVAs) or hardware devices that inspect and can filter network traffic before it’s permitted to enter the private network. Traditional firewalls are configured with rules that tell it what types of data packets are allowed based on the port number and IP address of the data packet. |

Trước đây, bạn đã biết rằng tường lửa là các thiết bị ảo mạng (NVA) hoặc thiết bị phần cứng có chức năng kiểm tra và có thể lọc lưu lượng truy cập mạng trước khi được phép truy cập vào mạng riêng. Tường lửa truyền thống được cấu hình với các quy tắc cho biết loại gói dữ liệu nào được phép dựa trên số cổng và địa chỉ IP của gói dữ liệu.

|  |
| --- |
| There are two main categories of firewalls.   * **Stateless:** A class of firewall that operates based on predefined rules and does not keep track of information from data packets * **Stateful:** A class of firewall that keeps track of information passing through it and proactively filters out threats. Unlike stateless firewalls, which require rules to be configured in two directions, a stateful firewall only requires a rule in one direction. This is because it uses a "state table" to track connections, so it can match return traffic to an existing session |

Có hai loại tường lửa chính.

* **Không trạng thái:** Một lớp tường lửa hoạt động dựa trên các quy tắc được xác định trước và không theo dõi thông tin từ các gói dữ liệu
* **Stateful:** Một lớp tường lửa theo dõi thông tin đi qua nó và chủ động lọc ra các mối đe dọa. Không giống như tường lửa không trạng thái yêu cầu các quy tắc phải được cấu hình theo hai hướng, tường lửa có trạng thái chỉ yêu cầu quy tắc theo một hướng. Điều này là do nó sử dụng "bảng trạng thái" để theo dõi các kết nối, do đó, nó có thể khớp lưu lượng truy cập quay lại với phiên hiện có

|  |
| --- |
| Next generation firewalls (NGFWs) are the most technologically advanced firewall protection. They exceed the security offered by stateful firewalls because they include deep packet inspection (a kind of packet sniffing that examines data packets and takes actions if threats exist) and intrusion prevention features that detect security threats and notify firewall administrators. NGFWs can inspect traffic at the application layer of the TCP/IP model and are typically application aware. Unlike traditional firewalls that block traffic based on IP address and ports, NGFWs rules can be configured to block or allow traffic based on the application. Some NGFWs have additional features like Malware Sandboxing, Network Anti-Virus, and URL and DNS Filtering. |

Tường lửa thế hệ tiếp theo (NGFW) là giải pháp bảo vệ tường lửa có công nghệ tiên tiến nhất. Chúng vượt xa khả năng bảo mật do tường lửa trạng thái cung cấp vì chúng bao gồm kiểm tra gói sâu (một loại đánh hơi gói để kiểm tra gói dữ liệu và thực hiện hành động nếu có mối đe dọa) và các tính năng ngăn chặn xâm nhập giúp phát hiện các mối đe dọa bảo mật và thông báo cho quản trị viên tường lửa. NGFW có thể kiểm tra lưu lượng ở lớp ứng dụng của mô hình TCP/IP và thường nhận biết ứng dụng. Không giống như tường lửa truyền thống chặn lưu lượng truy cập dựa trên địa chỉ IP và cổng, quy tắc NGFW có thể được cấu hình để chặn hoặc cho phép lưu lượng truy cập dựa trên ứng dụng. Một số NGFW có các tính năng bổ sung như Hộp cát phần mềm độc hại, Chống vi-rút mạng cũng như Lọc URL và DNS.

|  |
| --- |
| **Proxy servers** |

**Máy chủ proxy**

|  |
| --- |
| A proxy server is another way to add security to your private network. Proxy servers utilize network address translation (NAT) to serve as a barrier between clients on the network and external threats. Forward proxies handle queries from internal clients when they access resources external to the network. Reverse proxies function opposite of forward proxies; they handle requests from external systems to services on the internal network. Some proxy servers can also be configured with rules, like a firewall.  For example, you can create filters to block websites identified as containing malware. |

Máy chủ proxy là một cách khác để tăng cường bảo mật cho mạng riêng của bạn. Máy chủ proxy sử dụng dịch địa chỉ mạng (NAT) để đóng vai trò là rào cản giữa các máy khách trên mạng và các mối đe dọa bên ngoài. Proxy chuyển tiếp xử lý các truy vấn từ máy khách nội bộ khi chúng truy cập các tài nguyên bên ngoài mạng. Proxy ngược có chức năng ngược lại với proxy chuyển tiếp; họ xử lý các yêu cầu từ hệ thống bên ngoài đến các dịch vụ trên mạng nội bộ. Một số máy chủ proxy cũng có thể được cấu hình bằng các quy tắc, như tường lửa. Ví dụ: bạn có thể tạo bộ lọc để chặn các trang web được xác định là có chứa phần mềm độc hại.

|  |
| --- |
| **Virtual Private Networks (VPN)** |

**Mạng riêng ảo (VPN)**

|  |
| --- |
| A VPN is a service that encrypts data in transit and disguises your IP address. VPNs use a process called encapsulation. Encapsulation wraps your unencrypted data in an encrypted data packet, which allows your data to be sent across the public network while remaining anonymous. Enterprises and other organizations use VPNs to help protect communications from users’ devices to corporate resources. Some of these resources include servers or virtual machines that host business applications. Individuals also use VPNs to increase personal privacy. VPNs protect user privacy by concealing personal information, including IP addresses, from external servers. A reputable VPN also minimizes its own access to user internet activity by using strong encryption and other security measures. Organizations are increasingly using a combination of VPN and SD-WAN capabilities to secure their networks. A software-defined wide area network (SD-WAN) is a virtual WAN service that allows organizations to securely connect users to applications across multiple locations and over large geographical distances. |

VPN là dịch vụ mã hóa dữ liệu khi truyền và ngụy trang địa chỉ IP của bạn. VPN sử dụng một quy trình gọi là đóng gói. Tính năng đóng gói bao bọc dữ liệu không được mã hóa của bạn trong gói dữ liệu được mã hóa, cho phép dữ liệu của bạn được gửi qua mạng công cộng trong khi vẫn ẩn danh. Các doanh nghiệp và các tổ chức khác sử dụng VPN để giúp bảo vệ thông tin liên lạc từ thiết bị của người dùng đến tài nguyên của công ty. Một số tài nguyên này bao gồm máy chủ hoặc máy ảo lưu trữ các ứng dụng kinh doanh. Các cá nhân cũng sử dụng VPN để tăng cường quyền riêng tư cá nhân. VPN bảo vệ quyền riêng tư của người dùng bằng cách che giấu thông tin cá nhân, bao gồm cả địa chỉ IP, khỏi các máy chủ bên ngoài. VPN uy tín cũng giảm thiểu quyền truy cập của chính nó vào hoạt động internet của người dùng bằng cách sử dụng mã hóa mạnh và các biện pháp bảo mật khác. Các tổ chức đang ngày càng sử dụng kết hợp khả năng VPN và SD-WAN để bảo mật mạng của họ. Mạng diện rộng được xác định bằng phần mềm (SD-WAN) là dịch vụ WAN ảo cho phép các tổ chức kết nối người dùng một cách an toàn với các ứng dụng trên nhiều địa điểm và trên khoảng cách địa lý lớn.

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

**Bài học chính**

|  |
| --- |
| There are three main categories of network protocols: communication, management, and security protocols. In this reading, you learned the fundamentals of firewalls, proxy servers, and VPNs. More organizations are implementing a cloud-based approach to network security by incorporating a combination of VPN and SD-WAN capabilities as a service. |

Có ba loại giao thức mạng chính: giao thức truyền thông, quản lý và bảo mật. Trong bài đọc này, bạn đã tìm hiểu các kiến ​​thức cơ bản về tường lửa, máy chủ proxy và VPN. Ngày càng có nhiều tổ chức triển khai phương pháp tiếp cận dựa trên đám mây để bảo mật mạng bằng cách kết hợp khả năng VPN và SD-WAN làm dịch vụ.

***2.7. VPN protocols: Wireguard and IPSec – Giao thức VPN: Wireguard và IPSec***

|  |
| --- |
| **VPN protocols: Wireguard and IPSec** |

**Giao thức VPN: Wireguard và IPSec**

|  |
| --- |
| A VPN, or virtual private network, is a network security service that changes your public IP address and hides your virtual location so that you can keep your data private when you’re using a public network like the internet. VPNs provide a server that acts as a gateway between a computer and the internet. This server creates a path similar to a virtual tunnel that hides the computer’s IP address and encrypts the data in transit to the internet. The main purpose of a VPN is to create a secure connection between a computer and a network. Additionally, a VPN allows trusted connections to be established on non-trusted networks. VPN protocols determine how the secure network tunnel is formed. Different VPN providers provide different VPN protocols. |

VPN hay mạng riêng ảo là một dịch vụ bảo mật mạng thay đổi địa chỉ IP công cộng và ẩn vị trí ảo của bạn để bạn có thể giữ dữ liệu của mình ở chế độ riêng tư khi sử dụng mạng công cộng như Internet. VPN cung cấp một máy chủ hoạt động như một cổng kết nối giữa máy tính và internet. Máy chủ này tạo một đường dẫn tương tự như một đường hầm ảo để ẩn địa chỉ IP của máy tính và mã hóa dữ liệu khi truyền tới internet. Mục đích chính của VPN là tạo kết nối an toàn giữa máy tính và mạng. Ngoài ra, VPN cho phép thiết lập các kết nối đáng tin cậy trên các mạng không đáng tin cậy. Các giao thức VPN xác định cách hình thành đường hầm mạng an toàn. Các nhà cung cấp VPN khác nhau cung cấp các giao thức VPN khác nhau.

|  |
| --- |
| This reading will cover the differences between remote access and site-to-site VPNs, and two VPN protocols: WireGuard VPN and IPSec VPN. A VPN protocol is similar to a network protocol: It’s a set of rules or instructions that will determine how data moves between endpoints. An endpoint is any device connected on a network. Some examples of endpoints include computers, mobile devices, and servers. |

Bài đọc này sẽ đề cập đến sự khác biệt giữa truy cập từ xa và VPN site-to-site cũng như hai giao thức VPN: WireGuard VPN và IPSec VPN. Giao thức VPN tương tự như giao thức mạng: Đó là một bộ quy tắc hoặc hướng dẫn sẽ xác định cách dữ liệu di chuyển giữa các điểm cuối. Điểm cuối là bất kỳ thiết bị nào được kết nối trên mạng. Một số ví dụ về điểm cuối bao gồm máy tính, thiết bị di động và máy chủ.

|  |
| --- |
| **Remote access and site-to-site VPNs** |

**Truy cập từ xa và VPN site-to-site**

|  |
| --- |
| Individual users use remote access VPNs to establish a connection between a personal device and a VPN server. Remote access VPNs encrypt data sent or received through a personal device. The connection between the user and the remote access VPN is established through the internet. |

Người dùng cá nhân sử dụng VPN truy cập từ xa để thiết lập kết nối giữa thiết bị cá nhân và máy chủ VPN. VPN truy cập từ xa mã hóa dữ liệu được gửi hoặc nhận thông qua thiết bị cá nhân. Kết nối giữa người dùng và VPN truy cập từ xa được thiết lập thông qua internet.

|  |
| --- |
| Enterprises use site-to-site VPNs largely to extend their network to other networks and locations. This is particularly useful for organizations that have many offices across the globe. IPSec is commonly used in site-to-site VPNs to create an encrypted tunnel between the primary network and the remote network. One disadvantage of site-to-site VPNs is how complex they can be to configure and manage compared to remote VPNs. |

Các doanh nghiệp chủ yếu sử dụng VPN site-to-site để mở rộng mạng của họ sang các mạng và địa điểm khác. Điều này đặc biệt hữu ích cho các tổ chức có nhiều văn phòng trên toàn cầu. IPSec thường được sử dụng trong VPN site-to-site để tạo đường hầm được mã hóa giữa mạng chính và mạng từ xa. Một nhược điểm của VPN site-to-site là mức độ phức tạp trong việc cấu hình và quản lý so với VPN từ xa.

|  |
| --- |
| **WireGuard VPN vs. IPSec VPN** |

**WireGuard VPN so với IPSec VPN**

|  |
| --- |
| WireGuard and IPSec are two different VPN protocols used to encrypt traffic over a secure network tunnel. The majority of VPN providers offer a variety of options for VPN protocols, such as WireGuard or IPSec. Ultimately, choosing between IPSec and WireGuard depends on many factors, including connection speeds, compatibility with existing network infrastructure, and business or individual needs. |

WireGuard và IPSec là hai giao thức VPN khác nhau được sử dụng để mã hóa lưu lượng truy cập qua đường hầm mạng an toàn. Phần lớn các nhà cung cấp VPN cung cấp nhiều tùy chọn khác nhau cho giao thức VPN, chẳng hạn như WireGuard hoặc IPSec. Cuối cùng, việc lựa chọn giữa IPSec và WireGuard phụ thuộc vào nhiều yếu tố, bao gồm tốc độ kết nối, khả năng tương thích với cơ sở hạ tầng mạng hiện có và nhu cầu của doanh nghiệp hoặc cá nhân.

|  |
| --- |
| **WireGuard VPN** |

**WireGuard VPN**

|  |
| --- |
| WireGuard is a high-speed VPN protocol, with advanced encryption, to protect users when they are accessing the internet. It’s designed to be simple to set up and maintain. WireGuard can be used for both site-to-site connection and client-server connections. WireGuard is relatively newer than IPSec, and is used by many people due to the fact that its download speed is enhanced by using fewer lines of code. WireGuard is also open source, which makes it easier for users to deploy and debug. This protocol is useful for processes that require faster download speeds, such as streaming video content or downloading large files. |

WireGuard là giao thức VPN tốc độ cao, với mã hóa nâng cao, để bảo vệ người dùng khi họ truy cập internet. Nó được thiết kế để đơn giản hóa việc thiết lập và bảo trì. WireGuard có thể được sử dụng cho cả kết nối site-to-site và kết nối client-server. WireGuard tương đối mới hơn IPSec và được nhiều người sử dụng do tốc độ tải xuống của nó được nâng cao bằng cách sử dụng ít dòng mã hơn. WireGuard cũng là nguồn mở, giúp người dùng triển khai và gỡ lỗi dễ dàng hơn. Giao thức này hữu ích cho các quy trình yêu cầu tốc độ tải xuống nhanh hơn, chẳng hạn như truyền phát nội dung video hoặc tải xuống các tệp lớn.

|  |
| --- |
| **IPSec VPN** |

**IPSec VPN**

|  |
| --- |
| IPSec is another VPN protocol that may be used to set up VPNs. Most VPN providers use IPSec to encrypt and authenticate data packets in order to establish secure, encrypted connections. Since IPSec is one of the earlier VPN protocols, many operating systems support IPSec from VPN providers. |

IPSec là một giao thức VPN khác có thể được sử dụng để thiết lập VPN. Hầu hết các nhà cung cấp VPN đều sử dụng IPSec để mã hóa và xác thực các gói dữ liệu nhằm thiết lập các kết nối được mã hóa an toàn. Vì IPSec là một trong những giao thức VPN ra đời sớm hơn nên nhiều hệ điều hành hỗ trợ IPSec từ các nhà cung cấp VPN.

|  |
| --- |
| Although IPSec and WireGuard are both VPN protocols, IPSec is older and more complex than WireGuard. Some clients may prefer IPSec due to its longer history of use, extensive security testing, and widespread adoption. However, others may prefer WireGuard because of its potential for better performance and simpler configuration. |

Mặc dù IPSec và WireGuard đều là giao thức VPN nhưng IPSec cũ hơn và phức tạp hơn WireGuard. Một số khách hàng có thể thích IPSec do lịch sử sử dụng lâu hơn, thử nghiệm bảo mật rộng rãi và áp dụng rộng rãi. Tuy nhiên, những người khác có thể thích WireGuard vì tiềm năng mang lại hiệu suất tốt hơn và cấu hình đơn giản hơn.

|  |
| --- |
| **Key Takeaways** |

**Bài học chính**

|  |
| --- |
| A VPN protocol is similar to a network protocol: It’s a set of rules or instructions that will determine how data moves between endpoints. There are two types of VPNs: remote access and site-to-site. Remote access VPNs establish a connection between a personal device and a VPN server and encrypt or decrypt data exchanged with a personal device. Enterprises use site-to-site VPNs largely to extend their network to different locations and networks. IPSec can be used to create site-to-site connections and WireGuard can be used for both site-to-site and remote access connections. |

Giao thức VPN tương tự như giao thức mạng: Đó là một bộ quy tắc hoặc hướng dẫn sẽ xác định cách dữ liệu di chuyển giữa các điểm cuối. Có hai loại VPN: truy cập từ xa và site-to-site. VPN truy cập từ xa thiết lập kết nối giữa thiết bị cá nhân và máy chủ VPN và mã hóa hoặc giải mã dữ liệu được trao đổi với thiết bị cá nhân. Các doanh nghiệp chủ yếu sử dụng VPN site-to-site để mở rộng mạng của họ đến các vị trí và mạng khác nhau. IPSec có thể được sử dụng để tạo kết nối site-to-site và WireGuard có thể được sử dụng cho cả kết nối site-to-site và truy cập từ xa.

***2.8. Test your knowledge: System identification – Kiểm tra kiến ​​thức của bạn: Nhận dạng hệ thống***

**3. Review: Network operations – Đánh giá: Vận hành mạng**

***3.1. Wrap-up – Gói lại***

|  |
| --- |
| You've learned a lot about some complex topics. I want to congratulate you for coming this far in the program. Let's recap what we've covered in this section. First, we discussed common network protocols like TCP, ARP, HTTPS, and DNS. And then we covered how virtual private networks, or VPNs, can be used to maintain privacy on a public network. Finally, we explored how firewalls, security zones, and proxy servers help to secure network infrastructure. |

Bạn đã học được rất nhiều về một số chủ đề phức tạp.Tôi muốn chúc mừng bạn vì đã tiến xa đến mức này trong chương trình.Hãy tóm tắt lại những gì chúng ta đã đề cập trong phần này.Đầu tiên, chúng ta thảo luận về các giao thức mạng phổ biến như TCP, ARP, HTTPS và DNS.Và sau đó chúng tôi đã đề cập đến cách các mạng riêng ảo hoặcVPN, có thể được sử dụng để duy trì quyền riêng tư trên mạng công cộng.Cuối cùng, chúng tôi đã khám phá cách tường lửa, vùng bảo mật vàmáy chủ proxy giúp bảo mật cơ sở hạ tầng mạng.

|  |
| --- |
| Overall, network operations is a vast topic involving various tools, protocols, and techniques that help networks run smoothly and securely. Feel free to come back and review these videos at any time. You'll use this information in any type of role as a security analyst. |

Nhìn chung, hoạt động mạng là một chủ đề rộng lớn liên quan đến nhiều công cụ khác nhau,các giao thức và kỹ thuật giúp mạng chạy trơn tru và an toàn.Vui lòng quay lại và xem lại những video này bất kỳ lúc nào.Bạn sẽ sử dụng thông tin này trong bất kỳ vai trò nào với tư cách là nhà phân tích bảo mật.

***3.2. 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 3, Module 2** |

**Các thuật ngữ và định nghĩa trong Khóa 3, Học phần 2**

|  |
| --- |
| **Address Resolution Protocol (ARP):** A network protocol used to determine the MAC address of the next router or device on the path |

**Giao thức phân giải địa chỉ (ARP):** Giao thức mạng được sử dụng để xác định địa chỉ MAC của bộ định tuyến hoặc thiết bị tiếp theo trên đường dẫn

|  |
| --- |
| **Cloud-based firewalls:** Software firewalls that are hosted by the cloud service provider |

**Tường lửa dựa trên đám mây:** Tường lửa phần mềm được nhà cung cấp dịch vụ đám mây lưu trữ

|  |
| --- |
| **Controlled zone:** A subnet that protects the internal network from the uncontrolled zone |

**Vùng được kiểm soát:** Mạng con bảo vệ mạng nội bộ khỏi vùng không được kiểm soát

|  |
| --- |
| **Domain Name System (DNS):** A networking protocol that translates internet domain names into IP addresses |

**Hệ thống tên miền (DNS):** Một giao thức mạng dịch tên miền internet thành địa chỉ IP

|  |
| --- |
| **Encapsulation:** A process performed by a VPN service that protects your data by wrapping sensitive data in other data packets |

**Đóng gói:** Một quy trình được thực hiện bởi dịch vụ VPN nhằm bảo vệ dữ liệu của bạn bằng cách gói dữ liệu nhạy cảm trong các gói dữ liệu khác

|  |
| --- |
| **Firewall:** A network security device that monitors traffic to or from your network |

**Tường lửa:** Thiết bị bảo mật mạng giám sát lưu lượng đến hoặc đi từ mạng của bạn

|  |
| --- |
| **Forward proxy server:** A server that regulates and restricts a person’s access to the internet |

**Máy chủ proxy chuyển tiếp:** Máy chủ điều chỉnh và hạn chế quyền truy cập internet của một người

|  |
| --- |
| **Hypertext Transfer Protocol (HTTP):** An application layer protocol that provides a method of communication between clients and website servers |

**Giao thức truyền siêu văn bản (HTTP):** Giao thức lớp ứng dụng cung cấp phương thức liên lạc giữa máy khách và máy chủ trang web

|  |
| --- |
| **Hypertext Transfer Protocol Secure (HTTPS):** A network protocol that provides a secure method of communication between clients and servers |

**Bảo mật Giao thức Truyền Siêu văn bản (HTTPS):** Giao thức mạng cung cấp phương thức liên lạc an toàn giữa máy khách và máy chủ

|  |
| --- |
| **IEEE 802.11 (Wi-Fi):** A set of standards that define communication for wireless LANs |

**IEEE 802.11 (Wi-Fi):** Bộ tiêu chuẩn xác định giao tiếp cho mạng LAN không dây

|  |
| --- |
| **Network protocols:** A set of rules used by two or more devices on a network to describe the order of delivery of data and the structure of data |

**Giao thức mạng:** Một bộ quy tắc được sử dụng bởi hai hoặc nhiều thiết bị trên mạng để mô tả thứ tự phân phối dữ liệu và cấu trúc dữ liệu

|  |
| --- |
| **Network segmentation:** A security technique that divides the network into segments |

**Phân đoạn mạng:** Một kỹ thuật bảo mật chia mạng thành các phân đoạn

|  |
| --- |
| **Port filtering:** Afirewall function that blocks or allows certain port numbers to limit unwanted communication |

**Lọc cổng:** Chức năng tường lửa chặn hoặc cho phép một số cổng nhất định hạn chế giao tiếp không mong muốn

|  |
| --- |
| **Proxy server:** A server that fulfills the requests of its clients by forwarding them to other servers |

**Máy chủ proxy:** Máy chủ đáp ứng các yêu cầu của khách hàng bằng cách chuyển tiếp chúng đến các máy chủ khác

|  |
| --- |
| **Reverse proxy server:** A server that regulates and restricts the internet's access to an internal server |

**Máy chủ proxy ngược:** Máy chủ điều chỉnh và hạn chế quyền truy cập của internet vào máy chủ nội bộ

|  |
| --- |
| **Secure File Transfer Protocol (SFTP):** A secure protocol used to transfer files from one device to another over a network |

**Giao thức truyền tệp an toàn (SFTP):** Giao thức an toàn được sử dụng để truyền tệp từ thiết bị này sang thiết bị khác qua mạng

|  |
| --- |
| **Secure shell (SSH):** A security protocol used to create a shell with a remote system |

**Secure shell (SSH):** Giao thức bảo mật được sử dụng để tạo shell với hệ thống từ xa

|  |
| --- |
| **Security zone:** A segment of a company’s network that protects the internal network from the internet |

**Vùng bảo mật:** Một phân đoạn mạng của công ty bảo vệ mạng nội bộ khỏi internet

|  |
| --- |
| **Simple Network Management Protocol (SNMP):** A network protocol used for monitoring and managing devices on a network |

**Giao thức quản lý mạng đơn giản (SNMP):** Giao thức mạng được sử dụng để giám sát và quản lý các thiết bị trên mạng

|  |
| --- |
| **Stateful:** A class of firewall that keeps track of information passing through it and proactively filters out threats |

**Stateful:** Một lớp tường lửa theo dõi thông tin đi qua nó và chủ động lọc ra các mối đe dọa

|  |
| --- |
| **Stateless:** A class of firewall that operates based on predefined rules and does not keep track of information from data packets |

**Không trạng thái:** Một lớp tường lửa hoạt động dựa trên các quy tắc được xác định trước và không theo dõi thông tin từ các gói dữ liệu

|  |
| --- |
| **Subnetting:** The subdivision of a network into logical groups called subnets |

**Mạng con:** Việc chia mạng thành các nhóm logic gọi là mạng con

|  |
| --- |
| **Transmission Control Protocol (TCP):** An internet communication protocol that allows two devices to form a connection and stream data |

**Giao thức điều khiển truyền dẫn (TCP):** Giao thức truyền thông internet cho phép hai thiết bị tạo thành kết nối và truyền dữ liệu

|  |
| --- |
| **Uncontrolled zone:** The portion of the network outside the organization |

**Vùng không được kiểm soát:** Phần mạng bên ngoài tổ chức

|  |
| --- |
| **Virtual private network (VPN):** A network security service that changes your public IP address and masks your virtual location so that you can keep your data private when you are using a public network like the internet |

**Mạng riêng ảo (VPN):** Dịch vụ bảo mật mạng thay đổi địa chỉ IP công cộng của bạn và che giấu vị trí ảo của bạn để bạn có thể giữ dữ liệu của mình ở chế độ riêng tư khi sử dụng mạng công cộng như internet

|  |
| --- |
| **Wi-Fi Protected Access (WPA):** A wireless security protocol for devices to connect to the internet |

**Truy cập được bảo vệ Wi-Fi (WPA):** Giao thức bảo mật không dây cho các thiết bị kết nối với internet

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

**Module 3: Secure against network intrusions – Bảo mật chống lại sự xâm nhập mạng**

|  |
| --- |
| You will understand types of network attacks and techniques used to secure compromised network systems and devices. You'll explore the many ways that malicious actors exploit vulnerabilities in network infrastructure and how cybersecurity professionals identify and close potential loopholes. |

Bạn sẽ hiểu các loại tấn công mạng và kỹ thuật được sử dụng để bảo mật các hệ thống và thiết bị mạng bị xâm phạm. Bạn sẽ khám phá nhiều cách mà các tác nhân độc hại khai thác lỗ hổng trong cơ sở hạ tầng mạng cũng như cách các chuyên gia an ninh mạng xác định và đóng các lỗ hổng tiềm ẩn.

|  |
| --- |
| **Learning Objectives**   * Describe network intrusion tactics * Explain how to secure a network against intrusion tactics * Investigate security breaches * Understand different types of network attacks * Troubleshoot basic network issues using appropriate tools and methods |

**Mục tiêu học tập**

* Mô tả các chiến thuật xâm nhập mạng
* Giải thích cách bảo mật mạng khỏi các chiến thuật xâm nhập
* Điều tra các vi phạm an ninh
* Hiểu các loại tấn công mạng khác nhau
* Khắc phục sự cố mạng cơ bản bằng các công cụ và phương pháp thích hợp

**1. Introduction to network intrusion tactics – Giới thiệu chiến thuật xâm nhập mạng**

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

|  |
| --- |
| Hey there! Welcome to this video about securing networks from attacks. You've come a long way already in your understanding of networks and network security. |

Này! Chào mừng bạn đến với video này về cách bảo vệ mạng khỏi các cuộc tấn công.Bạn đã tiến được một chặng đường dài trong sự hiểu biết về mạng vàan ninh mạng.

|  |
| --- |
| Now you'll learn how to secure networks, so that the valuable information they contain doesn't get into the wrong hands. We're going to discuss how network intrusion tactics can present a threat to networks and how a security analyst can protect against network attacks. Let's get started. |

Bây giờ bạn sẽ học cách bảo mật mạng,để những thông tin có giá trị trong đó không rơi vào tay kẻ xấu.Chúng ta sẽ thảo luận về cách các chiến thuật xâm nhập mạng có thể gây ra mối đe dọa chomạng và cách nhà phân tích bảo mật có thể bảo vệ khỏi các cuộc tấn công mạng.Bắt đầu nào.

***1.2. The case for securing networks – Trường hợp bảo mật mạng***

|  |
| --- |
| Let's start by answering the question, why do we need secure networks? As you've learned, networks are constantly at risk of attack from malicious hackers. Attackers can infiltrate networks via malware, spoofing, or packet sniffing. Network operations can also be disrupted by attacks such as packet flooding. As we go along, you're going to learn about these and other common network intrusion attacks in more detail. |

Hãy bắt đầu bằng việc trả lời câu hỏi, tại sao chúng ta cần mạng an toàn?Như bạn đã biết, mạng luôn có nguy cơ bị tấn công từ các tin tặc độc hại.Những kẻ tấn công có thể xâm nhập vào mạng thông qua phần mềm độc hại, giả mạo hoặc đánh hơi gói.Hoạt động mạng cũng có thể bị gián đoạn bởi các cuộc tấn công như làm tràn gói.Khi chúng ta tiếp tục, bạn sẽ tìm hiểu về những điều này vàcác cuộc tấn công xâm nhập mạng phổ biến khác một cách chi tiết hơn.

|  |
| --- |
| Protecting a network from these types of attacks is important. If even one of them happens, it could have a catastrophic impact on an organization. Attacks can harm an organization by leaking valuable or confidential information. They can also be damaging to an organization's reputation and impact customer retention. Mitigating attacks may also cost the organization money and time. |

Việc bảo vệ mạng khỏi các kiểu tấn công này là rất quan trọng.Nếu thậm chí một trong số chúng xảy ra, nó có thể gây ra tác động thảm khốc đối với một tổ chức.Các cuộc tấn công có thể gây hại cho tổ chức bằng cách làm rò rỉ thông tin có giá trị hoặcthông tin bí mật.Chúng cũng có thể gây tổn hại đến danh tiếng của tổ chức vàtác động đến việc giữ chân khách hàng.Việc giảm nhẹ các cuộc tấn công cũng có thể khiến tổ chức tốn kém tiền bạc và thời gian.

|  |
| --- |
| Over the last few years, there have been a number of examples of damage that cyber attacks can cause. One notorious example was an attack against the American home-improvement chain, Home Depot, in 2014. A group of hackers compromised and infected Home Depot servers with malware. By the time network administrators shut down the attack, the hackers had already taken the credit and debit card information for over 56 million customers. |

Trong vài năm qua,đã có một số ví dụ về thiệt hại mà các cuộc tấn công mạng có thể gây ra.Một ví dụ khét tiếng là cuộc tấn công chống lại công ty cải thiện nhà ở Mỹchuỗi, Home Depot, vào năm 2014.Một nhóm tin tặc đã xâm nhập và lây nhiễm phần mềm độc hại vào máy chủ Home Depot.Vào thời điểm quản trị viên mạng ngừng cuộc tấn công, tin tặc đãđã lấy thông tin thẻ tín dụng và thẻ ghi nợ của hơn 56 triệu khách hàng.

|  |
| --- |
| Now, you know why it's so important to secure a network. But to keep a network secure, you need to know what kinds of attacks to protect it from. Coming up, you'll learn about some common network attacks. |

Bây giờ, bạn đã biết tại sao việc bảo mật mạng lại quan trọng đến vậy.Nhưng để giữ an toàn cho mạng,bạn cần biết những loại tấn công nào để bảo vệ nó khỏi.Tiếp theo, bạn sẽ tìm hiểu về một số cuộc tấn công mạng phổ biến.

***1.3. How intrusions compromise your system – Sự xâm nhập làm tổn hại hệ thống của bạn như thế nào***

|  |
| --- |
| **How intrusions compromise your system** |

**Sự xâm nhập làm tổn hại hệ thống của bạn như thế nào**

|  |
| --- |
| In this section of the course, you learned that every network has inherent vulnerabilities and could become the target of a network attack. |

Trong phần này của khóa học, bạn đã biết rằng mọi mạng đều có lỗ hổng cố hữu và có thể trở thành mục tiêu của một cuộc tấn công mạng.

|  |
| --- |
| Attackers could have varying motivations for attacking your organization’s network. They may have financial, personal, or political motivations, or they may be a disgruntled employee or an activist who disagrees with the company's values and wants to harm an organization’s operations. Malicious actors can target any network. Security analysts must be constantly alert to potential vulnerabilities in their organization’s network and take quick action to mitigate them. |

Những kẻ tấn công có thể có nhiều động cơ khác nhau để tấn công mạng của tổ chức bạn. Họ có thể có động cơ tài chính, cá nhân hoặc chính trị, hoặc họ có thể là một nhân viên bất mãn hoặc một nhà hoạt động không đồng tình với các giá trị của công ty và muốn làm tổn hại đến hoạt động của tổ chức. Tác nhân độc hại có thể nhắm mục tiêu bất kỳ mạng nào. Các nhà phân tích bảo mật phải liên tục cảnh giác về các lỗ hổng tiềm ẩn trong mạng của tổ chức và thực hiện hành động nhanh chóng để giảm thiểu chúng.

|  |
| --- |
| In this reading, you’ll learn about network interception attacks and backdoor attacks, and the possible impacts these attacks could have on an organization. |

Trong bài đọc này, bạn sẽ tìm hiểu về các cuộc tấn công chặn mạng và tấn công cửa sau cũng như những tác động có thể xảy ra mà các cuộc tấn công này có thể gây ra đối với một tổ chức.

|  |
| --- |
| **Network interception attacks** |

**Tấn công chặn mạng**

|  |
| --- |
| Network interception attacks work by intercepting network traffic and stealing valuable information or interfering with the transmission in some way. |

Các cuộc tấn công chặn mạng hoạt động bằng cách chặn lưu lượng mạng và đánh cắp thông tin có giá trị hoặc can thiệp vào quá trình truyền tải theo một cách nào đó.

|  |
| --- |
| Malicious actors can use hardware or software tools to capture and inspect data in transit. This is referred to as **packet sniffing**. In addition to seeing information that they are not entitled to, malicious actors can also intercept network traffic and alter it. These attacks can cause damage to an organization’s network by inserting malicious code modifications or altering the message and interrupting network operations. For example, an attacker can intercept a bank transfer and change the account receiving the funds to one that the attacker controls. |

Tác nhân độc hại có thể sử dụng các công cụ phần cứng hoặc phần mềm để thu thập và kiểm tra dữ liệu trong quá trình truyền. Điều này được gọi là **đánh hơi gói tin** . Ngoài việc xem thông tin mà họ không có quyền, các tác nhân độc hại còn có thể chặn lưu lượng truy cập mạng và thay đổi nó. Những cuộc tấn công này có thể gây thiệt hại cho mạng của tổ chức bằng cách chèn các sửa đổi mã độc hoặc thay đổi tin nhắn và làm gián đoạn hoạt động của mạng. Ví dụ: kẻ tấn công có thể chặn chuyển khoản ngân hàng và thay đổi tài khoản nhận tiền thành tài khoản mà kẻ tấn công kiểm soát.

|  |
| --- |
| Later in this course you will learn more about malicious packet sniffing, and other types of network interception attacks: on-path attacks and replay attacks. |

Ở phần sau của khóa học này, bạn sẽ tìm hiểu thêm về việc đánh hơi gói độc hại và các loại tấn công chặn mạng khác: tấn công trên đường đi và tấn công phát lại.

|  |
| --- |
| **Backdoor attacks** |

**Tấn công cửa sau**

|  |
| --- |
| A **backdoor attack** is another type of attack you will need to be aware of as a security analyst. An organization may have a lot of security measures in place, including cameras, biometric scans and access codes to keep employees from entering and exiting without being seen. However, an employee might work around the security measures by finding a backdoor to the building that is not as heavily monitored, allowing them to sneak out for the afternoon without being seen. |

Tấn **công cửa sau** là một loại tấn công khác mà bạn cần phải biết với tư cách là nhà phân tích bảo mật. Một tổ chức có thể áp dụng nhiều biện pháp an ninh, bao gồm camera, quét sinh trắc học và mã truy cập để ngăn nhân viên ra vào mà không bị nhìn thấy. Tuy nhiên, một nhân viên có thể lách các biện pháp an ninh bằng cách tìm một cửa sau dẫn vào tòa nhà không bị giám sát chặt chẽ, cho phép họ lẻn ra ngoài vào buổi chiều mà không bị phát hiện.

|  |
| --- |
| In cybersecurity, backdoors are weaknesses intentionally left by programmers or system and network administrators that bypass normal access control mechanisms. Backdoors are intended to help programmers conduct troubleshooting or administrative tasks. However, backdoors can also be installed by attackers after they’ve compromised an organization to ensure they have persistent access. |

Trong an ninh mạng, cửa sau là những điểm yếu do các lập trình viên hoặc quản trị viên hệ thống và mạng cố tình để lại, qua đó bỏ qua các cơ chế kiểm soát truy cập thông thường. Backdoor nhằm mục đích giúp các lập trình viên tiến hành xử lý sự cố hoặc thực hiện các nhiệm vụ quản trị. Tuy nhiên, những kẻ tấn công cũng có thể cài đặt các cửa sau sau khi chúng xâm nhập được một tổ chức để đảm bảo chúng có quyền truy cập liên tục.

|  |
| --- |
| Once the hacker has entered an insecure network through a backdoor, they can cause extensive damage: installing malware, performing a denial of service (DoS) attack, stealing private information or changing other security settings that leaves the system vulnerable to other attacks. A **DoS attack** is an attack that targets a network or server and floods it with network traffic. |

Khi tin tặc đã xâm nhập vào mạng không an toàn thông qua cửa sau, chúng có thể gây ra thiệt hại lớn: cài đặt phần mềm độc hại, thực hiện tấn công từ chối dịch vụ (DoS), đánh cắp thông tin cá nhân hoặc thay đổi cài đặt bảo mật khác khiến hệ thống dễ bị tấn công khác. **Tấn công DoS** là một cuộc tấn công nhắm vào mạng hoặc máy chủ và làm tràn ngập lưu lượng mạng.

|  |
| --- |
| **Possible impacts on an organization** |

**Những tác động có thể xảy ra đối với một tổ chức**

|  |
| --- |
| As you’ve learned already, network attacks can have a significant negative impact on an organization. Let’s examine some potential consequences. |

Như bạn đã biết, các cuộc tấn công mạng có thể có tác động tiêu cực đáng kể đến một tổ chức. Hãy xem xét một số hậu quả có thể xảy ra.

|  |
| --- |
| * **Financial**: When a system is taken offline with a DoS attack or some other tactic, they prevent a company from performing tasks that generate revenue. Depending on the size of an organization, interrupted operations can cost millions of dollars. Reparation costs to rebuild software infrastructure and to pay large sums associated with potential ransomware can be financially difficult. In addition, if a malicious actor gets access to the personal information of the company’s clients or customers, the company may face heavy litigation and settlement costs if customers seek legal recourse. * **Reputation**: Attacks can also have a negative impact on the reputation of an organization. If it becomes public knowledge that a company has experienced a cyber attack, the public may become concerned about the security practices of the organization. They may stop trusting the company with their personal information and choose a competitor to fulfill their needs. * **Public safety**: If an attack occurs on a government network, this can potentially impact the safety and welfare of the citizens of a country. In recent years, defense agencies across the globe are investing heavily in combating cyber warfare tactics. If a malicious actor gained access to a power grid, a public water system, or even a military defense communication system, the public could face physical harm due to a network intrusion attack. |

* **Tài chính** : Khi một hệ thống bị ngoại tuyến bằng một cuộc tấn công DoS hoặc một số chiến thuật khác, chúng sẽ ngăn công ty thực hiện các nhiệm vụ tạo ra doanh thu. Tùy thuộc vào quy mô của một tổ chức, các hoạt động bị gián đoạn có thể tiêu tốn hàng triệu đô la. Chi phí sửa chữa để xây dựng lại cơ sở hạ tầng phần mềm và trả số tiền lớn liên quan đến phần mềm ransomware tiềm ẩn có thể khó khăn về mặt tài chính. Ngoài ra, nếu kẻ xấu có quyền truy cập vào thông tin cá nhân của khách hàng của công ty, công ty có thể phải đối mặt với chi phí kiện tụng và giải quyết nặng nề nếu khách hàng tìm kiếm sự trợ giúp pháp lý.
* **Danh tiếng** : Các cuộc tấn công cũng có thể có tác động tiêu cực đến danh tiếng của một tổ chức. Nếu công chúng biết rằng một công ty đã trải qua một cuộc tấn công mạng, công chúng có thể trở nên lo ngại về các hoạt động bảo mật của tổ chức đó. Họ có thể ngừng tin tưởng cung cấp thông tin cá nhân của mình cho công ty và chọn một đối thủ cạnh tranh để đáp ứng nhu cầu của họ.
* **An toàn công cộng** : Nếu một cuộc tấn công xảy ra trên mạng của chính phủ, điều này có khả năng ảnh hưởng đến sự an toàn và phúc lợi của công dân một quốc gia. Trong những năm gần đây, các cơ quan quốc phòng trên toàn cầu đang đầu tư mạnh vào việc chống lại các chiến thuật chiến tranh mạng. Nếu một tác nhân độc hại có quyền truy cập vào lưới điện, hệ thống nước công cộng hoặc thậm chí hệ thống thông tin liên lạc phòng thủ quân sự, công chúng có thể phải đối mặt với tổn hại vật chất do một cuộc tấn công xâm nhập mạng.

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

**Bài học chính**

|  |
| --- |
| Malicious actors are constantly looking for ways to exploit systems. They learn about new vulnerabilities as they arise and attempt to exploit every vulnerability in a system. Attackers leverage backdoor attack methods and network interception attacks to gain access to sensitive information they can use to exploit an organization or cause serious damage. These types of attacks can impact an organization financially, damage its reputation, and potentially put the public in danger.  It is important that security analysts stay educated in order to maintain network safety and reduce the likelihood and impact of these types of attacks. Securing networks has never been more important. |

Những kẻ độc hại không ngừng tìm cách khai thác hệ thống. Họ tìm hiểu về các lỗ hổng mới khi chúng phát sinh và cố gắng khai thác mọi lỗ hổng trong hệ thống. Những kẻ tấn công tận dụng các phương pháp tấn công cửa sau và tấn công chặn mạng để có quyền truy cập vào thông tin nhạy cảm mà chúng có thể sử dụng để khai thác một tổ chức hoặc gây ra thiệt hại nghiêm trọng. Những kiểu tấn công này có thể ảnh hưởng đến tài chính của một tổ chức, gây tổn hại đến danh tiếng của tổ chức đó và có khả năng khiến công chúng gặp nguy hiểm. Điều quan trọng là các nhà phân tích bảo mật phải được đào tạo để duy trì sự an toàn của mạng và giảm khả năng cũng như tác động của các kiểu tấn công này. Bảo mật mạng chưa bao giờ quan trọng hơn.

***1.4. Matt: A professional on dealing with attacks – Matt: Chuyên gia xử lý các cuộc tấn công***

|  |
| --- |
| My name's Matt, I'm a chaos specialist at Google. They let us choose our own job titles to best describe what it is we do. I spend a lot of my time planning for how to take care of anything that might possibly be going wrong, and when it does happen, putting a team in place to fix it as quickly as possible. I had no intention of being in technology at all. In high school, I was a lifeguard, first at public pools and then at a state beach. Lifeguarding got me into really enjoying rescue. So I got an EMT license, went through firefighter school. About halfway through my college process, and well into when I was being a firefighter on a daily basis. I was dealing with some burnout, some stress. I needed a change in my life. And a friend of mine who I'd been online gaming with since the early days of online gaming, when it was all text based, he said, I can tell you're burning out hard and you need a change. My friends and I are going to San Francisco to start a startup. Will you come with us? And I said, you realize I am not a computer guy, right? And he said, no, you're a computer guy, you just won't admit it. The same thing that has drawn me into incident response in tech is what originally drew me to medical response. I really love being there for people on their worst day. Being there when people really need you and they don't know where else to turn to has always just fed this part of me, and I'm lucky to find that same joy in DFIR, Digital Forensics and Incident Response. What type of attacks have we faced at Google? That's a hard question to answer, because we face all of the kinds of attacks that most other companies face. People after ransomware, people after industrial secrets, other countries looking for intelligence information. There was a really interesting attack that occurred a little while ago. They were interested in getting a lot of information from technical companies, specifically about vulnerabilities in software. And they put in place a long running campaign to build personalities on social media as though they were legitimate security researchers, and then reach out to other security researchers in our field, build relationships, and then just at the right moment, sneak in some malware. Being under attack by an adversary who's made some progress is incredibly stressful. The first things you're thinking and feeling are a little bit of a sense of panic. Oh no, this is going to be a bad day. How long am I going to be awake working on this? What have they done? What am I going to do? And for me, the mantra that I repeat to myself is, as an incident responder, I am here to help. The things that are most important to having a good outcome in an incident are what we call the 3Cs: Command, Control and Communications. Meaning someone needs to be in charge of it affirmatively leading. Someone needs to be exerting control over everyone involved so that everyone's aligned, focused on the mission, and the biggest and most important one of them all: proper communications. If you have something to offer to the incident, don't just go do it, Communicate to someone. I think I could do this to help us make progress. I think if we look over here, we'll find more data. The advice that I would give somebody who wants to get into cybersecurity is if you want it, you probably belong here. The more people we have in here, who are passionate, curious question askers, who want to know more, who want to build better, and who care about making every thing more secure for the people who have to use technology, those are people we want in the industry and I would want you here. |

Tên tôi là Matt, tôi là chuyên gia về hỗn loạn tại Google.Họ cho phép chúng tôi chọn chức danh công việc của riêng mình để mô tả chính xác nhất những gì chúng tôi làm.Tôi dành nhiều thời gian để lên kế hoạchcách xử lý mọi vấn đề có thể xảy ra vàkhi sự cố xảy ra, hãy cử một nhóm đến khắc phục sự cố đó càng nhanh càng tốt.Tôi không hề có ý định theo đuổi công nghệ.Ở trường trung học, tôi là nhân viên cứu hộ, đầu tiên là ở các bể bơi công cộng và sau đó là ở một bãi biển của bang.Nhân viên cứu hộ khiến tôi thực sự thích giải cứu.Vì vậy, tôi đã có được giấy phép EMT, đã tốt nghiệp trường lính cứu hỏa. Khoảng nửa chặng đườngquá trình học đại học của tôi và cả khi tôi làm lính cứu hỏa hàng ngày.Tôi đang phải đối mặt với tình trạng kiệt sức, căng thẳng.Tôi cần một sự thay đổi trong cuộc sống của tôi.Và một người bạn của tôi, người đã chơi game trực tuyến cùng tôi từ những ngày đầucủa trò chơi trực tuyến, khi tất cả đều dựa trên văn bản,anh ấy nói, tôi có thể nói rằng bạn đang kiệt sức và bạn cần một sự thay đổi.Bạn bè của tôi và tôi sẽ đến San Francisco để bắt đầu khởi nghiệp.Bạn sẽ đến với chúng tôi?Và tôi nói, bạn nhận ra tôi không phải là dân máy tính, phải không?Và anh ấy nói, không, bạn là dân máy tính, bạn sẽ không thừa nhận điều đó.Điều tương tự đã thu hút tôi vào việc ứng phó sự cố trong lĩnh vực công nghệ là điềuban đầu đã thu hút tôi đến phản ứng y tế.Tôi thực sự thích ở bên mọi người vào ngày tồi tệ nhất của họ.Có mặt khi mọi người thực sự cần bạn vàhọ không biết phải tìm nơi nào khác luôn luôn nuôi sống phần này của tôi, vàTôi may mắn tìm thấy niềm vui tương tự trong DFIR, Pháp y kỹ thuật số và Ứng phó sự cố.Chúng ta đã phải đối mặt với loại tấn công nào tại Google?Đó là một câu hỏi khó trả lời,bởi vì chúng tôi phải đối mặt với tất cả các kiểu tấn công mà hầu hết các công ty khác phải đối mặt.Mọi người theo đuổi ransomware, mọi người theo đuổi bí mật công nghiệp,các quốc gia khác đang tìm kiếm thông tin tình báo.Có một cuộc tấn công thực sự thú vị đã xảy ra cách đây ít lâu.Họ quan tâm đến việc thu thập nhiều thông tin từ các công ty kỹ thuật,đặc biệt là về các lỗ hổng trong phần mềm.Và họ thực hiện một chiến dịch lâu dài để xây dựng tính cách trênphương tiện truyền thông xã hội như thể họ là nhà nghiên cứu bảo mật hợp pháp vàsau đó liên hệ với các nhà nghiên cứu bảo mật khác trong lĩnh vực của chúng tôi,xây dựng các mối quan hệ và sau đó vào đúng thời điểm, lẻn vào một số phần mềm độc hại.Bị tấn công bởi một đối thủ đã đạt được một số tiến bộ là điều vô cùng khó tin.căng thẳng.Điều đầu tiên bạn nghĩ đến vàcảm giác có chút hoảng loạn.Ôi không, đây sẽ là một ngày tồi tệ.Tôi sẽ thức bao lâu để làm việc này?Họ đã làm gì?Tôi sẽ làm gì đây?Và đối với tôi, câu thần chú mà tôi lặp đi lặp lại với chính mình là, với tư cách là người ứng phó sự cố,Tôi ở đây là để giúp đỡ.Những điều quan trọng nhất để có kết quả tốttrong một sự cố chúng tôi gọi là 3C: Chỉ huy, Kiểm soát vàTruyền thông. Có nghĩa là cần phải có ai đó chịu trách nhiệm lãnh đạo nó.Ai đó cần phải kiểm soát mọi người có liên quan đểrằng mọi người đều liên kết, tập trung vào sứ mệnh và mục tiêu lớn nhất vàđiều quan trọng nhất trong số đó: giao tiếp phù hợp.Nếu bạn có điều gì muốn đề nghị về vụ việc này,đừng chỉ làm điều đó, hãy giao tiếp với ai đó.Tôi nghĩ tôi có thể làm điều này để giúp chúng tôi tiến bộ.Tôi nghĩ nếu chúng ta nhìn qua đây, chúng ta sẽ tìm thấy nhiều dữ liệu hơn.Lời khuyên mà tôi dành cho những người muốn tham gia vào lĩnh vực an ninh mạng là nếu bạnmuốn nó, có lẽ bạn thuộc về nơi này.Càng có nhiều người ở đây, những người đặt câu hỏi đầy đam mê và tò mò,những người muốn biết nhiều hơn, những người muốn xây dựng tốt hơn và những người quan tâm đếnkhiến mọi thứ trở nên an toàn hơn cho những người phải sử dụng công nghệ,đó là những người chúng tôi muốn trong ngành và tôi muốn bạn ở đây.

**2. Secure networks against Denial of Service (DoS) attacks – Mạng an toàn chống lại các cuộc tấn công từ chối dịch vụ (DoS)**

***2.1. Denial of Service (DoS) attacks – Tấn công từ chối dịch vụ (DoS)***

|  |
| --- |
| Welcome back. In this video, we're going to discuss denial of service attacks. A denial of service attack is an attack that targets a network or server and floods it with network traffic. The objective of a denial of service attack, or a DoS attack, is to disrupt normal business operations by overloading an organization's network. The goal of the attack is to send so much information to a network device that it crashes or is unable to respond to legitimate users. This means that the organization won't be able to conduct their normal business operations, which can cost them money and time. A network crash can also leave them vulnerable to other security threats and attacks. |

Chào mừng trở lại. Trong video này,chúng ta sẽ thảo luận về các cuộc tấn công từ chối dịch vụ.Một cuộc tấn công từ chối dịch vụ làmột cuộc tấn công nhắm vào mạng hoặc máy chủvà khiến nó tràn ngập lưu lượng mạng.Mục tiêu của tấn công từ chối dịch vụhoặc một cuộc tấn công DoS, là làm gián đoạnhoạt động kinh doanh bình thường củalàm quá tải mạng của tổ chức.Mục tiêu của cuộc tấn công là gửiquá nhiều thông tin cho một thiết bị mạngrằng nó gặp sự cố hoặckhông thể trả lời người dùng hợp pháp.Điều này có nghĩa là tổ chức sẽ khôngcó thể tiến hành các hoạt động kinh doanh bình thường của họ,điều này có thể khiến họ tốn tiền và thời gian.Sự cố mạng cũng có thể khiến họdễ bị tổn thương trước các mối đe dọa và tấn công bảo mật khác.

|  |
| --- |
| A distributed denial of service attack, or DDoS, is a kind of DoS attack that uses multiple devices or servers in different locations to flood the target network with unwanted traffic. Use of numerous devices makes it more likely that the total amount of traffic sent will overwhelm the target server. Remember, DoS stands for denial of service. So it doesn't matter what part of the network the attacker overloads; if they overload anything, they win. An unfortunate example I've seen is an attacker who crafted a very careful packet that caused a router to spend extra time processing the request. The overall traffic volume didn't overload the router; the specifics within the packet did. |

Một cuộc tấn công từ chối dịch vụ phân tán, hoặc DDoS,là một loại tấn công DoS sử dụngnhiều thiết bị hoặc máy chủ trongcác địa điểm khác nhau để lũ lụtmạng mục tiêu có lưu lượng truy cập không mong muốn.Việc sử dụng nhiều thiết bị có nhiều khả năng xảy ratổng lưu lượng truy cậpđược gửi sẽ áp đảo máy chủ mục tiêu.Hãy nhớ rằng, DoS là viết tắt của từ chối dịch vụ.Vì vậy, phần nào không quan trọngcủa mạng kẻ tấn công làm quá tải;nếu họ làm quá tải bất cứ thứ gì, họ sẽ thắng.Một ví dụ không may là tôi đãnhìn thấy là kẻ tấn công đã chế tạomột gói rất cẩn thận đã gây rabộ định tuyến để dành thêm thời gian xử lý yêu cầu.Lưu lượng tổng thể không làm quá tải bộ định tuyến;các chi tiết cụ thể trong gói đã làm.

|  |
| --- |
| Now we'll discuss network level DoS attacks that target network bandwidth to slow traffic. Let's learn about three common network level DoS attacks. The first is called a SYN flood attack. A SYN flood attack is a type of DoS attack that simulates the TCP connection and floods the server with SYN packets. Let's break this definition down a bit more by taking a closer look at the handshake process that is used to establish a TCP connection between a device and a server. The first step in the handshake is for the device to send a SYN, or synchronize, request to the server. Then, the server responds with a SYN/ACK packet to acknowledge the receipt of the device's request and leaves a port open for the final step of the handshake. Once the server receives the final ACK packet from the device, a TCP connection is established. Malicious actors can take advantage of the protocol by flooding a server with SYN packet requests for the first part of the handshake. But if the number of SYN requests is larger than the number of available ports on the server, then the server will be overwhelmed and become unable to function. |

Bây giờ chúng ta sẽ thảo luận về các cuộc tấn công DoS cấp mạngnhắm mục tiêu băng thông mạng để làm chậm lưu lượng truy cập.Hãy cùng tìm hiểu về ba cuộc tấn công DoS cấp mạng phổ biến.Đầu tiên được gọi là cuộc tấn công lũ lụt SYN.Tấn công lũ lụt SYN là một loạiTấn công DoS mô phỏng kết nối TCPvà làm tràn ngập máy chủ với các gói SYN.Hãy chia nhỏ định nghĩa này một chútnhiều hơn bằng cách xem xét kỹ hơnquá trình bắt tay được sử dụng để thiết lậpkết nối TCP giữa thiết bị và máy chủ.Bước đầu tiên trong quá trình bắt tay là để thiết bị gửiyêu cầu SYN hoặc đồng bộ hóa tới máy chủ.Sau đó, máy chủ phản hồi vớimột gói SYN/ACK tớixác nhận đã nhận được yêu cầu của thiết bịvà để lại một cổng mở chobước cuối cùng của cái bắt tay.Sau khi máy chủ nhận đượcgói ACK cuối cùng từ thiết bị,một kết nối TCP được thiết lập.Các tác nhân độc hại có thể lợi dụng giao thức bằng cáchlàm ngập một máy chủ vớiYêu cầu gói SYN cho phần đầu tiên của quá trình bắt tay.Nhưng nếu số lượng yêu cầu SYN làlớn hơn số lượng cổng có sẵn trên máy chủ,thì máy chủ sẽ bị choáng ngợpvà trở nên không thể hoạt động được.

|  |
| --- |
| Let's discuss two other common DoS attacks that use another protocol called ICMP. ICMP stands for Internet Control Message Protocol. ICMP is an internet protocol used by devices to tell each other about data transmission errors across the network. Think of ICMP like a request for a status update from a device. The device will return error messages if there is a network concern. You can think of this like the ICMP request checking in with the device to make sure that all is well. An ICMP flood attack is a type of DoS attack performed by an attacker repeatedly sending ICMP packets to a network server. This forces the server to send an ICMP packet. This eventually uses up all the bandwidth for incoming and outgoing traffic and causes the server to crash. Both of the attacks we've discussed so far, SYN flood and ICMP flood, take advantage of communication protocols by sending an overwhelming number of requests. There are also attacks that can overwhelm the server with one big request. One example that we'll discuss is called the ping of death. |

Hãy thảo luận về hai cuộc tấn công DoS phổ biến khácsử dụng một giao thức khác gọi là ICMP.ICMP là viết tắt của Giao thức tin nhắn điều khiển Internet.ICMP là giao thức internet được sử dụng bởi các thiết bịkể cho nhau nghe vềlỗi truyền dữ liệu qua mạng.Hãy coi ICMP như một lời yêu cầuđể cập nhật trạng thái từ thiết bị.Thiết bị sẽ trở lạithông báo lỗi nếu có vấn đề về mạng.Bạn có thể nghĩ về điều này nhưyêu cầu ICMP đang kiểm tra vớithiết bị để đảm bảo rằng tất cả đều ổn.Một cuộc tấn công lũ lụt ICMPlà một kiểu tấn công DoS được thực hiện bởi kẻ tấn côngliên tục gửi các gói ICMP đến máy chủ mạng.Điều này buộc máy chủ gửi gói ICMP.Điều này cuối cùng sử dụng hết băng thông chovà lưu lượng đi và khiến máy chủ gặp sự cố.Cả hai cuộc tấn công mà chúng ta đã thảo luận cho đến nay,Lũ SYN và lũ ICMP,tận dụng các giao thức truyền thôngbằng cách gửi một số lượng lớn các yêu cầu.Cũng có những cuộc tấn công có thể áp đảomáy chủ với một yêu cầu lớn.Một ví dụ mà chúng ta sẽ thảo luậnđược gọi là ping của cái chết.

|  |
| --- |
| A ping of death attack is a type of DoS attack that is caused when a hacker pings a system by sending it an oversized ICMP packet that is bigger than 64 kilobytes, the maximum size for a correctly formed ICMP packet. Pinging a vulnerable network server with an oversized ICMP packet will overload the system and cause it to crash. Think of this like dropping a rock on a small anthill. Each individual ant can carry a certain amount of weight while transporting food to and from the anthill. But if a large rock is dropped on the anthill, then many ants will be crushed, and the colony is unable to function until it rebuilds its operations elsewhere. |

Một ping tấn công chết chóc làmột kiểu tấn công DoS xảy ra khi một hackerping một hệ thống bằng cách gửi nómột gói ICMP quá khổlớn hơn 64 kilobyte,kích thước tối đa cho gói ICMP được định dạng chính xác.Ping một máy chủ mạng dễ bị tấn công bằngmột gói ICMP quá khổsẽ làm quá tải hệ thống và khiến nó bị hỏng.Hãy nghĩ về điều này giống như việc thả một hòn đá vào một tổ kiến ​​nhỏ.Mỗi con kiến ​​có thể mang theo một lượng nhất địnhtrọng lượng trong khi vận chuyển thức ăn đến và đi từ ổ kiến.Nhưng nếu một tảng đá lớn rơi xuống ổ kiến,khi đó nhiều con kiến ​​sẽ bị nghiền nát và đàn kiến ​​không thểhoạt động cho đến khi nó xây dựng lại hoạt động của mình ở nơi khác.

|  |
| --- |
| Now that's it for DoS and DDoS attacks. Coming up, we'll continue to discuss common network attacks. |

Bây giờ chỉ còn lại các cuộc tấn công DoS và DDoS.Sắp tới chúng ta sẽ tiếp tụcthảo luận về các cuộc tấn công mạng phổ biến

***2.2. Read tcpdump logs – Đọc nhật ký tcpdump***

|  |
| --- |
| **Read tcpdump logs** |

**Đọc nhật ký tcpdump**

|  |
| --- |
| A **network protocol analyzer**, sometimes called a packet sniffer or a packet analyzer, is a tool designed to capture and analyze data traffic within a network. They are commonly used as investigative tools to monitor networks and identify suspicious activity. There are a wide variety of network protocol analyzers available, but some of the most common analyzers  include:   * SolarWinds NetFlow Traffic Analyzer * ManageEngine OpManager * Azure Network Watcher * Wireshark * tcpdump |

Bộ **phân tích giao thức mạng** , đôi khi được gọi là bộ phân tích gói hoặc bộ phân tích gói, là một công cụ được thiết kế để thu thập và phân tích lưu lượng dữ liệu trong mạng. Chúng thường được sử dụng làm công cụ điều tra để giám sát mạng và xác định hoạt động đáng ngờ. Có rất nhiều loại máy phân tích giao thức mạng, nhưng một số máy phân tích phổ biến nhất bao gồm:

* Máy phân tích lưu lượng truy cập NetFlow của SolarWinds
* Quản lý công cụ quản lý
* Trình theo dõi mạng Azure
* Wireshark
* tcpdump

|  |
| --- |
| This reading will focus exclusively on tcpdump, though you can apply what you learn here to many of the other network protocol analyzers you'll use as a cybersecurity analyst to defend against any network intrusions. In an upcoming activity, you’ll review a tcpdump data traffic log and identify a DoS attack to practice these skills. |

Bài đọc này sẽ chỉ tập trung vào tcpdump, mặc dù bạn có thể áp dụng những gì bạn học được ở đây cho nhiều máy phân tích giao thức mạng khác mà bạn sẽ sử dụng với tư cách là nhà phân tích an ninh mạng để bảo vệ khỏi mọi hành vi xâm nhập mạng. Trong hoạt động sắp tới, bạn sẽ xem lại nhật ký lưu lượng dữ liệu tcpdump và xác định cuộc tấn công DoS để thực hành những kỹ năng này.

|  |
| --- |
| **tcpdump** |

**tcpdump**

|  |
| --- |
| **tcpdump** is a command-line network protocol analyzer. It is popular, lightweight–meaning it uses little memory and has a low CPU usage–and uses the open-source libpcap library. tcpdump is text based, meaning all commands in tcpdump are executed in the terminal. It can also be installed on other Unix-based operating systems, such as macOS®. It is preinstalled on many Linux distributions. |

**tcpdump** là một bộ phân tích giao thức mạng dòng lệnh. Nó phổ biến, nhẹ—có nghĩa là nó sử dụng ít bộ nhớ và mức sử dụng CPU thấp—và sử dụng thư viện libpcap nguồn mở. tcpdump dựa trên văn bản, nghĩa là tất cả các lệnh trong tcpdump đều được thực thi trong terminal. Nó cũng có thể được cài đặt trên các hệ điều hành dựa trên Unix khác, chẳng hạn như macOS®. Nó được cài đặt sẵn trên nhiều bản phân phối Linux.

|  |
| --- |
| tcpdump provides a brief packet analysis and converts key information about network traffic into formats easily read by humans. It prints information about each packet directly into your terminal. tcpdump also displays the source IP address, destination IP addresses, and the port numbers being used in the communications. |

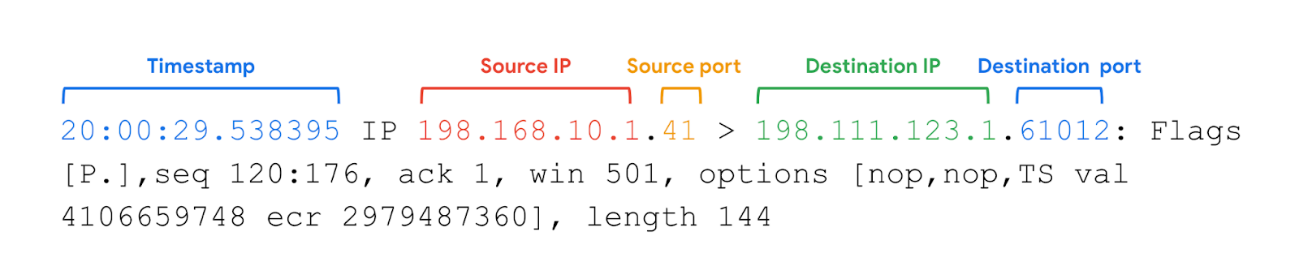
tcpdump cung cấp phân tích gói ngắn gọn và chuyển đổi thông tin chính về lưu lượng mạng thành các định dạng mà con người dễ đọc. Nó in thông tin về từng gói trực tiếp vào thiết bị đầu cuối của bạn. tcpdump cũng hiển thị địa chỉ IP nguồn, địa chỉ IP đích và số cổng đang được sử dụng trong liên lạc.

|  |
| --- |
| **Interpreting output** |

**Đầu ra phiên dịch**

|  |
| --- |
| tcpdump prints the output of the command as the sniffed packets in the command line, and optionally to a log file, after a command is executed. The output of a packet capture contains many pieces of important information about the network traffic. |

tcpdump in đầu ra của lệnh dưới dạng các gói được đánh hơi trong dòng lệnh và tùy chọn vào tệp nhật ký sau khi lệnh được thực thi. Đầu ra của gói chụp chứa nhiều thông tin quan trọng về lưu lượng mạng.



|  |
| --- |
| Some information you receive from a packet capture includes:   * **Timestamp**: The output begins with the timestamp, formatted as hours, minutes, seconds, and fractions of a second. * **Source IP**: The packet’s origin is provided by its source IP address. * **Source port**: This port number is where the packet originated. * **Destination IP**: The destination IP address is where the packet is being transmitted to. * **Destination port**: This port number is where the packet is being transmitted to. |

Một số thông tin bạn nhận được từ việc chụp gói bao gồm:

* **Dấu thời gian** : Đầu ra bắt đầu bằng dấu thời gian, được định dạng dưới dạng giờ, phút, giây và phân số của giây.
* **IP nguồn** : Nguồn gốc của gói được cung cấp bởi địa chỉ IP nguồn của nó.
* **Cổng nguồn** : Số cổng này là nơi gói tin bắt nguồn.
* **IP đích** : Địa chỉ IP đích là nơi gói được truyền tới.
* **Cổng đích** : Số cổng này là nơi gói được truyền tới.

|  |
| --- |
| **Note:** By default, tcpdump will attempt to resolve host addresses to hostnames. It'll also replace port numbers with commonly associated services that use these ports. |

**Lưu ý:** Theo mặc định, tcpdump sẽ cố gắng phân giải địa chỉ máy chủ thành tên máy chủ. Nó cũng sẽ thay thế số cổng bằng các dịch vụ thường được liên kết sử dụng các cổng này.

|  |
| --- |
| **Common uses** |

**Sử dụng phổ biến**

|  |
| --- |
| tcpdump and other network protocol analyzers are commonly used to capture and view network communications and to collect statistics about the network, such as troubleshooting network performance issues. They can also be used to:   * Establish a baseline for network traffic patterns and network utilization metrics. * Detect and identify malicious traffic * Create customized alerts to send the right notifications when network issues or security threats arise. * Locate unauthorized instant messaging (IM), traffic, or wireless access points. |

tcpdump và các máy phân tích giao thức mạng khác thường được sử dụng để nắm bắt và xem thông tin liên lạc mạng cũng như thu thập số liệu thống kê về mạng, chẳng hạn như khắc phục sự cố về hiệu suất mạng. Chúng cũng có thể được sử dụng để:

* Thiết lập đường cơ sở cho các mẫu lưu lượng truy cập mạng và số liệu sử dụng mạng.
* Phát hiện và xác định lưu lượng độc hại
* Tạo cảnh báo tùy chỉnh để gửi thông báo phù hợp khi phát sinh sự cố mạng hoặc mối đe dọa bảo mật.
* Xác định vị trí các điểm truy cập không dây, lưu lượng truy cập hoặc nhắn tin tức thời (IM) trái phép.

|  |
| --- |
| However, attackers can also use network protocol analyzers maliciously to gain information about a specific network. For example, attackers can capture data packets that contain sensitive information, such as account usernames and passwords. As a cybersecurity analyst, It’s important to understand the purpose and uses of network protocol analyzers. |

Tuy nhiên, kẻ tấn công cũng có thể sử dụng các bộ phân tích giao thức mạng một cách độc hại để lấy thông tin về một mạng cụ thể. Ví dụ: kẻ tấn công có thể nắm bắt các gói dữ liệu chứa thông tin nhạy cảm, chẳng hạn như tên người dùng và mật khẩu tài khoản. Là một nhà phân tích an ninh mạng, điều quan trọng là phải hiểu mục đích và cách sử dụng của máy phân tích giao thức mạng.

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

**Bài học chính**

|  |
| --- |
| Network protocol analyzers, like tcpdump, are common tools that can be used to monitor network traffic patterns and investigate suspicious activity. tcpdump is a command-line network protocol analyzer that is compatible with Linux/Unix and macOS®. When you run a tcpdump command, the tool will output packet routing information, like the timestamp, source IP address and port number, and the destination IP address and port number. Unfortunately, attackers can also use network protocol analyzers to capture data packets that contain sensitive information, such as account usernames and passwords. |

Các bộ phân tích giao thức mạng, như tcpdump, là những công cụ phổ biến có thể được sử dụng để giám sát các mẫu lưu lượng truy cập mạng và điều tra hoạt động đáng ngờ. tcpdump là trình phân tích giao thức mạng dòng lệnh tương thích với Linux/Unix và macOS®. Khi bạn chạy lệnh tcpdump, công cụ sẽ xuất thông tin định tuyến gói, như dấu thời gian, địa chỉ IP nguồn và số cổng cũng như địa chỉ IP đích và số cổng. Thật không may, những kẻ tấn công cũng có thể sử dụng máy phân tích giao thức mạng để thu thập các gói dữ liệu chứa thông tin nhạy cảm, chẳng hạn như tên người dùng và mật khẩu tài khoản.

***2.3. Real-life DDoS attack – Cuộc tấn công DDoS ngoài đời thực***

|  |
| --- |
| **Real-life DDoS attack** |

**Cuộc tấn công DDoS ngoài đời thực**

|  |
| --- |
| Previously, you were introduced to Denial of Service (DoS) attacks. You also learned that volumetric distributed DoS (DDoS) attacks overwhelm a network by sending unwanted data packets in such large quantities that the servers become unable to service normal users. This can be detrimental to an organization. When systems fail, organizations cannot meet their customers' needs. They often lose money, and in some cases, incur other losses. An organization’s reputation may also suffer if news of a successful DDoS attack reaches consumers, who then question the security of the organization. |

Trước đây, bạn đã được giới thiệu về các cuộc tấn công từ chối dịch vụ (DoS). Bạn cũng đã biết rằng các cuộc tấn công DoS (DDoS) phân tán theo quy mô lớn sẽ áp đảo mạng bằng cách gửi các gói dữ liệu không mong muốn với số lượng lớn đến mức máy chủ không thể phục vụ người dùng bình thường. Điều này có thể gây bất lợi cho một tổ chức. Khi hệ thống bị lỗi, tổ chức không thể đáp ứng được nhu cầu của khách hàng. Họ thường bị mất tiền và trong một số trường hợp còn phải gánh chịu những tổn thất khác. Danh tiếng của một tổ chức cũng có thể bị ảnh hưởng nếu tin tức về một cuộc tấn công DDoS thành công đến tay người tiêu dùng, những người sau đó đặt câu hỏi về tính bảo mật của tổ chức.

|  |
| --- |
| In this reading you’ll learn about a 2016 DDoS attack against DNS servers that caused major outages at multiple organizations that have millions of daily users. |

Trong bài đọc này, bạn sẽ tìm hiểu về cuộc tấn công DDoS năm 2016 nhằm vào các máy chủ DNS gây ra sự cố ngừng hoạt động lớn tại nhiều tổ chức có hàng triệu người dùng hàng ngày.

|  |
| --- |
| **A DDoS targeting a widely used DNS server** |

**DDoS nhắm mục tiêu máy chủ DNS được sử dụng rộng rãi**

|  |
| --- |
| In previous videos, you learned about the function of a DNS server. As a review, DNS servers translate website domain names into the IP address of the system that contains the information for the website. For instance, if a user were to type in a website URL, a DNS server would translate that into a numeric IP address that directs network traffic to the location of the website’s server. |

Trong các video trước, bạn đã tìm hiểu về chức năng của máy chủ DNS. Khi xem xét, máy chủ DNS sẽ dịch tên miền của trang web thành địa chỉ IP của hệ thống chứa thông tin cho trang web. Ví dụ: nếu người dùng nhập URL trang web, máy chủ DNS sẽ dịch URL đó thành địa chỉ IP dạng số để hướng lưu lượng truy cập mạng đến vị trí máy chủ của trang web.

|  |
| --- |
| On the day of the DDoS attack we are studying, many large companies were using a DNS service provider. The service provider was hosting the DNS system for these companies. This meant that when internet users typed in the URL of the website they wanted to access, their devices would be directed to the right place. On October 21, 2016, the service provider was the victim of a DDoS attack. |

Vào ngày xảy ra cuộc tấn công DDoS mà chúng tôi đang nghiên cứu, nhiều công ty lớn đang sử dụng nhà cung cấp dịch vụ DNS. Nhà cung cấp dịch vụ đã lưu trữ hệ thống DNS cho các công ty này. Điều này có nghĩa là khi người dùng internet nhập URL của trang web họ muốn truy cập, thiết bị của họ sẽ được chuyển đến đúng nơi. Vào ngày 21 tháng 10 năm 2016, nhà cung cấp dịch vụ là nạn nhân của một cuộc tấn công DDoS.

|  |
| --- |
| **Leading up to the attack** |

**Dẫn tới cuộc tấn công**

|  |
| --- |
| Before the attack on the service provider, a group of university students created a botnet with the intention to attack various gaming servers and networks. A **botnet** is a collection of computers infected by malware that are under the control of a single threat actor, known as the “bot-herder." Each computer in the botnet can be remotely controlled to send a data packet to a target system. In a botnet attack, cyber criminals instruct all the bots on the botnet to send data packets to the target system at the same time, resulting in a DDoS attack. |

Trước cuộc tấn công vào nhà cung cấp dịch vụ, một nhóm sinh viên đại học đã tạo ra một mạng botnet với mục đích tấn công nhiều máy chủ và mạng chơi game khác nhau. Botnet là một tập hợp các máy tính bị nhiễm phần mềm độc hại nằm dưới sự kiểm soát của một tác nhân đe dọa duy nhất, được gọi là “người chăn nuôi bot”. Mỗi máy tính trong mạng botnet có thể được điều khiển từ xa để gửi gói dữ liệu đến hệ thống mục tiêu. **Trong** Trong một cuộc tấn công botnet, tội phạm mạng sẽ hướng dẫn tất cả các bot trên botnet gửi các gói dữ liệu đến hệ thống mục tiêu cùng lúc, dẫn đến một cuộc tấn công DDoS.

|  |
| --- |
| The group of university students posted the code for the botnet online so that it would be accessible to thousands of internet users and authorities wouldn’t be able to trace the botnet back to the students. In doing so, they made it possible for other malicious actors to learn the code to the botnet and control it remotely. This included the cyber criminals who attacked the DNS service provider. |

Nhóm sinh viên đại học đã đăng mã của botnet lên mạng để hàng nghìn người dùng internet có thể truy cập được và chính quyền sẽ không thể truy tìm tung tích của sinh viên về botnet. Khi làm như vậy, họ đã tạo điều kiện cho các tác nhân độc hại khác tìm hiểu mã của mạng botnet và điều khiển nó từ xa. Điều này bao gồm cả tội phạm mạng đã tấn công nhà cung cấp dịch vụ DNS.

|  |
| --- |
| **The day of attack** |

**Ngày tấn công**

|  |
| --- |
| At 7:00 a.m. on the day of the attack, the botnet sent tens of millions of DNS requests to the service provider. This overwhelmed the system and the DNS service shut down. This meant that all of the websites that used the service provider could not be reached. When users tried to access various websites that used the service provider, they were not directed to the website they typed in their browser. Outages for each web service occurred all over North America and Europe. |

Vào lúc 7h sáng ngày xảy ra vụ tấn công, botnet đã gửi hàng chục triệu yêu cầu DNS tới nhà cung cấp dịch vụ. Điều này khiến hệ thống bị choáng ngợp và dịch vụ DNS bị tắt. Điều này có nghĩa là tất cả các trang web sử dụng nhà cung cấp dịch vụ đều không thể truy cập được. Khi người dùng cố gắng truy cập các trang web khác nhau sử dụng nhà cung cấp dịch vụ, họ không được chuyển hướng đến trang web mà họ đã nhập trong trình duyệt. Sự cố ngừng hoạt động đối với từng dịch vụ web xảy ra trên khắp Bắc Mỹ và Châu Âu.

|  |
| --- |
| The service provider’s systems were restored after only two hours of downtime. Although the cyber criminals sent subsequent waves of botnet attacks, the DNS company was prepared and able to mitigate the impact. |

Hệ thống của nhà cung cấp dịch vụ đã được khôi phục chỉ sau hai giờ ngừng hoạt động. Mặc dù tội phạm mạng đã gửi các đợt tấn công botnet tiếp theo nhưng công ty DNS đã chuẩn bị sẵn sàng và có thể giảm thiểu tác động.

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

**Bài học chính**

|  |
| --- |
| As demonstrated in the above example, DDoS attacks can be very damaging to an organization. As a security analyst, it’s important to acknowledge the seriousness of such an attack so that you’re aware of opportunities to protect the network from them. If your network has important operations distributed across hosts that can be dynamically scaled, then operations can continue if the baseline host infrastructure goes offline. DDoS attacks are damaging, but there are concrete actions that security analysts can take to help protect their organizations. Keep going through this course and you will learn about common mitigation strategies to protect against DDoS attacks. |

Như đã trình bày trong ví dụ trên, các cuộc tấn công DDoS có thể gây tổn hại rất lớn cho một tổ chức. Là một nhà phân tích bảo mật, điều quan trọng là phải thừa nhận mức độ nghiêm trọng của cuộc tấn công như vậy để bạn nhận thức được các cơ hội bảo vệ mạng khỏi chúng. Nếu mạng của bạn có các hoạt động quan trọng được phân phối trên các máy chủ có thể thay đổi quy mô linh hoạt thì các hoạt động có thể tiếp tục nếu cơ sở hạ tầng máy chủ cơ sở ngoại tuyến. Các cuộc tấn công DDoS gây thiệt hại nặng nề nhưng có những hành động cụ thể mà các nhà phân tích bảo mật có thể thực hiện để giúp bảo vệ tổ chức của họ. Hãy tiếp tục tham gia khóa học này và bạn sẽ tìm hiểu về các chiến lược giảm nhẹ phổ biến để bảo vệ khỏi các cuộc tấn công DDoS.

***2.4. Activity: Analyze network layer communication – Hoạt động: Phân tích giao tiếp lớp mạng***

|  |
| --- |
| **Activity Overview**  https://d3c33hcgiwev3.cloudfront.net/imageAssetProxy.v1/7575VRkfR42-7Xv1WSugQg_1e7fbf6b48534623bf908a7c50c56df1_image.png?expiry=1715385600000&hmac=AvLLCaWQfT5CG-7ydYngofKgOTsr0ScTAdu17ARr4Rc  In this activity, you will analyze DNS and ICMP traffic in transit using data from a network protocol analyzer tool. You will identify which network protocol was utilized in assessment of the cybersecurity incident.  In the internet layer of the TCP/IP model, the IP formats data packets into IP datagrams. The information provided in the datagram of an IP packet can provide security analysts with insight into suspicious data packets in transit.  Knowing how to identify potentially malicious traffic on a network can help cybersecurity analysts assess security risks on a network and reinforce network security.  Be sure to complete this activity before moving on. The next course item will provide you with a completed exemplar to compare to your own work. |
| **Scenario**  **https://d3c33hcgiwev3.cloudfront.net/imageAssetProxy.v1/oWLqT0BQR02lq2BsMbaiCA_ade0719eb03145d3a6627bf5a458cbf1_image.png?expiry=1715385600000&hmac=xcJSfZu09P1Ar-2solKWdlMOWGlX14XSqLLnPiU4bv0**  Review the scenario below. Then complete the step-by-step instructions.  You are a cybersecurity analyst working at a company that specializes in providing IT services for clients. Several customers of clients reported that they were not able to access the client company website www.yummyrecipesforme.com, and saw the error “destination port unreachable” after waiting for the page to load.  You are tasked with analyzing the situation and determining which network protocol was affected during this incident. To start, you attempt to visit the website and you also receive the error “destination port unreachable.” To troubleshoot the issue, you load your network analyzer tool, tcpdump, and attempt to load the webpage again. To load the webpage, your browser sends a query to a DNS server via the UDP protocol to retrieve the IP address for the website's domain name; this is part of the DNS protocol. Your browser then uses this IP address as the destination IP for sending an HTTPS request to the web server to display the webpage The analyzer shows that when you send UDP packets to the DNS server, you receive ICMP packets containing the error message: “udp port 53 unreachable.” |

|  |
| --- |
| **Tổng quan về hoạt động**  https://d3c33hcgiwev3.cloudfront.net/imageAssetProxy.v1/7575VRkfR42-7Xv1WSugQg_1e7fbf6b48534623bf908a7c50c56df1_image.png?expiry=1715385600000&hmac=AvLLCaWQfT5CG-7ydYngofKgOTsr0ScTAdu17ARr4Rc  Trong hoạt động này, bạn sẽ phân tích lưu lượng DNS và ICMP đang truyền bằng cách sử dụng dữ liệu từ công cụ phân tích giao thức mạng. Bạn sẽ xác định giao thức mạng nào đã được sử dụng để đánh giá sự cố an ninh mạng.  Trong lớp internet của mô hình TCP/IP, IP định dạng các gói dữ liệu thành các gói dữ liệu IP. Thông tin được cung cấp trong datagram của gói IP có thể cung cấp cho các nhà phân tích bảo mật cái nhìn sâu sắc về các gói dữ liệu đáng ngờ đang truyền đi.  Biết cách xác định lưu lượng truy cập độc hại tiềm ẩn trên mạng có thể giúp các nhà phân tích an ninh mạng đánh giá rủi ro bảo mật trên mạng và củng cố an ninh mạng.  Hãy chắc chắn hoàn thành hoạt động này 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. |
| **Kịch bản**  https://d3c33hcgiwev3.cloudfront.net/imageAssetProxy.v1/oWLqT0BQR02lq2BsMbaiCA_ade0719eb03145d3a6627bf5a458cbf1_image.png?expiry=1715385600000&hmac=xcJSfZu09P1Ar-2solKWdlMOWGlX14XSqLLnPiU4bv0  Xem lại kịch bản dưới đây. Sau đó hoàn thành các hướng dẫn từng bước.  Bạn là nhà phân tích an ninh mạng làm việc tại một công ty chuyên cung cấp dịch vụ CNTT cho khách hàng. Một số khách hàng của khách hàng đã báo cáo rằng họ không thể truy cập trang web của công ty khách hàng www.yummyrecipesforme.com và gặp lỗi “không thể truy cập cổng đích” sau khi đợi trang tải.  Bạn có nhiệm vụ phân tích tình huống và xác định giao thức mạng nào bị ảnh hưởng trong sự cố này. Để bắt đầu, bạn cố gắng truy cập trang web và bạn cũng nhận được lỗi “không thể truy cập cổng đích”. Để khắc phục sự cố, bạn tải công cụ phân tích mạng, tcpdump và thử tải lại trang web. Để tải trang web, trình duyệt của bạn sẽ gửi truy vấn đến máy chủ DNS thông qua giao thức UDP để lấy địa chỉ IP cho tên miền của trang web; đây là một phần của giao thức DNS. Sau đó, trình duyệt của bạn sử dụng địa chỉ IP này làm IP đích để gửi yêu cầu HTTPS đến máy chủ web để hiển thị trang web. Trình phân tích cho thấy rằng khi bạn gửi các gói UDP đến máy chủ DNS, bạn nhận được các gói ICMP chứa thông báo lỗi: “udp port 53 không thể truy cập được.” |



|  |
| --- |
| In the tcpdump log, you find the following information:   1. The first two lines of the log file show the initial outgoing request from your computer to the DNS server requesting the IP address of yummyrecipesforme.com. This request is sent in a UDP packet. 2. The third and fourth lines of the log show the response to your UDP packet. In this case, the ICMP 203.0.113.2 line is the start of the error message indicating that the UDP packet was undeliverable to port 53 of the DNS server. 3. In front of each request and response, you find timestamps that indicate when the incident happened. In the log, this is the first sequence of numbers displayed: 13:24:32.192571. This means the time is 1:24 p.m., 32.192571 seconds. 4. After the timestamps, you will find the source and destination IP addresses. In the first line, where the UDP packet travels from your browser to the DNS server, this information is displayed as: 192.51.100.15 > 203.0.113.2.domain. The IP address to the left of the greater than (>) symbol is the source address, which in this example is your computer’s IP address. The IP address to the right of the greater than (>) symbol is the destination IP address. In this case, it is the IP address for the DNS server: 203.0.113.2.domain. For the ICMP error response, the source address is 203.0.113.2 and the destination is your computers IP address 192.51.100.15. 5. After the source and destination IP addresses, there can be a number of additional details like the protocol, port number of the source, and flags. In the first line of the error log, the query identification number appears as: 35084. The plus sign after the query identification number indicates there are flags associated with the UDP message. The "A?" indicates a flag associated with the DNS request for an A record, where an A record maps a domain name to an IP address. The third line displays the protocol of the response message to the browser: "ICMP," which is followed by an ICMP error message. 6. The error message, "udp port 53 unreachable" is mentioned in the last line. Port 53 is a port for DNS service. The word "unreachable" in the message indicates the UDP message requesting an IP address for the domain "www.yummyrecipesforme.com" did not go through to the DNS server because no service was listening on the receiving DNS port. 7. The remaining lines in the log indicate that ICMP packets were sent two more times, but the same delivery error was received both times.   Now that you have captured data packets using a network analyzer tool, it is your job to identify which network protocol and service were impacted by this incident. Then, you will need to write a follow-up report.  As an analyst, you can inspect network traffic and network data to determine what is causing network-related issues during cybersecurity incidents. Later in this course, you will demonstrate how to manage and resolve incidents. For now, you only need to analyze the situation.  This event, in the meantime, is being handled by security engineers after you and other analysts have reported the issue to your direct supervisor. |

Trong nhật ký tcpdump, bạn tìm thấy thông tin sau:

1. Hai dòng đầu tiên của tệp nhật ký hiển thị yêu cầu gửi đi ban đầu từ máy tính của bạn đến máy chủ DNS yêu cầu địa chỉ IP của Yummyrecipesforme.com. Yêu cầu này được gửi trong gói UDP.
2. Dòng thứ ba và thứ tư của nhật ký hiển thị phản hồi cho gói UDP của bạn. Trong trường hợp này, dòng ICMP 203.0.113.2 là điểm bắt đầu của thông báo lỗi cho biết gói UDP không thể gửi tới cổng 53 của máy chủ DNS.
3. Trước mỗi yêu cầu và phản hồi, bạn sẽ thấy dấu thời gian cho biết thời điểm xảy ra sự cố. Trong nhật ký, đây là dãy số đầu tiên được hiển thị: 13:24:32.192571. Điều này có nghĩa là thời gian là 1:24 chiều, 32,192571 giây.
4. Sau dấu thời gian, bạn sẽ tìm thấy địa chỉ IP nguồn và đích. Ở dòng đầu tiên, nơi gói UDP di chuyển từ trình duyệt của bạn đến máy chủ DNS, thông tin này được hiển thị dưới dạng: 192.51.100.15 > 203.0.113.2.domain. Địa chỉ IP ở bên trái biểu tượng lớn hơn (>) là địa chỉ nguồn, trong ví dụ này là địa chỉ IP máy tính của bạn. Địa chỉ IP ở bên phải biểu tượng lớn hơn (>) là địa chỉ IP đích. Trong trường hợp này, đó là địa chỉ IP của máy chủ DNS: 203.0.113.2.domain. Đối với phản hồi lỗi ICMP, địa chỉ nguồn là 203.0.113.2 và đích đến là địa chỉ IP máy tính của bạn 192.51.100.15.
5. Sau địa chỉ IP nguồn và đích, có thể có một số chi tiết bổ sung như giao thức, số cổng của nguồn và cờ. Trong dòng đầu tiên của nhật ký lỗi, số nhận dạng truy vấn xuất hiện là: 35084. Dấu cộng sau số nhận dạng truy vấn cho biết có các cờ liên quan đến thông báo UDP. Chữ "A?" biểu thị cờ được liên kết với yêu cầu DNS cho bản ghi A, trong đó bản ghi A ánh xạ tên miền tới địa chỉ IP. Dòng thứ ba hiển thị giao thức của thông báo phản hồi tới trình duyệt: "ICMP", theo sau là thông báo lỗi ICMP.
6. Thông báo lỗi "không thể truy cập cổng udp 53" được đề cập ở dòng cuối cùng. Cổng 53 là cổng dành cho dịch vụ DNS. Từ "không thể truy cập" trong thông báo cho biết thông báo UDP yêu cầu địa chỉ IP cho tên miền "www.yummyrecipesforme.com" không đi qua máy chủ DNS vì không có dịch vụ nào lắng nghe trên cổng DNS nhận.
7. Các dòng còn lại trong nhật ký cho biết các gói ICMP đã được gửi thêm hai lần nữa nhưng cả hai lần đều nhận được cùng một lỗi gửi.

Bây giờ bạn đã thu thập các gói dữ liệu bằng công cụ phân tích mạng, công việc của bạn là xác định giao thức và dịch vụ mạng nào bị ảnh hưởng bởi sự cố này. Sau đó, bạn sẽ cần phải viết một báo cáo tiếp theo.

Với tư cách là nhà phân tích, bạn có thể kiểm tra lưu lượng mạng và dữ liệu mạng để xác định nguyên nhân gây ra sự cố liên quan đến mạng trong các sự cố an ninh mạng. Ở phần sau của khóa học này, bạn sẽ trình bày cách quản lý và giải quyết sự cố. Hiện tại, bạn chỉ cần phân tích tình hình.

Trong khi đó, sự kiện này đang được các kỹ sư bảo mật xử lý sau khi bạn và các nhà phân tích khác đã báo cáo vấn đề này với người giám sát trực tiếp của bạn.

***2.5. Activity Exemplar: Analyze network layer communication – Mẫu hoạt động: Phân tích giao tiếp lớp mạng***

***2.6. Test your knowledge: Secure networks against Denial of Service (DoS) attacks – Kiểm tra kiến ​​thức của bạn: Bảo mật mạng trước các cuộc tấn công từ chối dịch vụ (DoS)***

**3. Network attack tactics and defense – Chiến thuật tấn công mạng và phòng thủ**

***3.1. Malicious packet sniffing – Đánh hơi gói độc hại***

|  |
| --- |
| In this video, we'll discuss packet sniffing, with a focus on how threat actors may use this technique to gain unauthorized access to information. Previously, you learned about the information and data packets that travel across the network. Packets include a header which contains the sender's and receiver's IP addresses. Packets also contain a body, which may contain valuable information like names, date of birth, personal messages, financial information, and credit card numbers. |

Trong video này, chúng ta sẽ thảo luậnđánh hơi gói tin, tập trung vào cáchCác tác nhân đe dọa có thể sử dụng kỹ thuật này đểcó được quyền truy cập trái phép vào thông tin.Trước đây bạn đã tìm hiểu vềcác gói thông tin và dữ liệuđi qua mạng.Các gói bao gồm một tiêu đề chứađịa chỉ IP của người gửi và người nhận.Các gói cũng chứa phần thân, trong đócó thể chứa thông tin có giá trị như tên,ngày sinh, tin nhắn cá nhân,thông tin tài chính và số thẻ tín dụng.

|  |
| --- |
| Packet sniffing is the practice of using software tools to observe data as it moves across a network. As a security analyst, you may use packet sniffing to analyze and capture packets when investigating ongoing incidents or debugging network issues. Later in this certificate program, you'll gain hands-on practice with some packet sniffing software. However, malicious actors may also use packet sniffing to look at data that has not been sent to them. This is a little bit like opening somebody else's mail. It's important for you to learn about how threat actors use packet sniffing with harmful intent so you can be prepared to protect against these malicious acts. Malicious actors may insert themselves in the middle of an authorized connection between two devices. Then they can use packet sniffing to spy on every data packet as it comes across their device. The goal is to find valuable information in the data packets that they can then use to their advantage. Attackers can use software applications or a hardware device to look into data packets. Malicious actors can access a network packet with a packet sniffer and make changes to the data. They may change the information in the body of the packet, like altering a recipient's bank account number. |

Đánh hơi gói tin là việc sử dụngcông cụ phần mềm để quan sátdữ liệu khi nó di chuyển qua mạng.Là một nhà phân tích chứng khoán,bạn có thể sử dụng tính năng đánh hơi gói để phân tích và nắm bắtgói tin khi điều tra các sự cố đang diễn rahoặc gỡ lỗi các vấn đề về mạng.Sau này trong chương trình chứng chỉ này,bạn sẽ được thực hành thực hànhvới một số phần mềm đánh hơi gói tin.Tuy nhiên, những kẻ độc hại cũng có thể sử dụngđánh hơi gói để xem xétdữ liệu chưa được gửi cho họ.Điều này hơi giống việc mở thư của người khác.Điều quan trọng là bạn phải tìm hiểu về cáchTác nhân đe dọa sử dụng tính năng đánh hơi góivới mục đích có hại nên bạn có thểsẵn sàng bảo vệ chống lại những hành động độc hại này.Các tác nhân độc hại có thể tự chen vào giữamột kết nối được ủy quyền giữa hai thiết bị.Sau đó, họ có thể sử dụng tính năng đánh hơi gói tin để theo dõimọi gói dữ liệu khi nó đi qua thiết bị của họ.Mục đích là tìm kiếm thông tin có giá trị trongcác gói dữ liệu mà họ có thểsau đó sử dụng lợi thế của họ.Kẻ tấn công có thể sử dụng các ứng dụng phần mềmhoặc một thiết bị phần cứng để xem xét các gói dữ liệu.Tác nhân độc hại có thể truy cập gói mạng bằngmột trình thám thính gói và thực hiện các thay đổi đối với dữ liệu.Họ có thể thay đổi thông tintrong phần thân của gói tin,như thay đổi số tài khoản ngân hàng của người nhận.

|  |
| --- |
| Packet sniffing can be passive or active. Passive packet sniffing is a type of attack where data packets are read in transit. Since all the traffic on a network is visible to any host on the hub, malicious actors can view all the information going in and out of the device they are targeting. Thinking back to the example of a letter being delivered, we can compare a passive packet sniffing attack to a postal delivery person maliciously reading somebody's mail. The postal worker, or packet sniffer, has the right to deliver the mail, but not the right to read the information inside. Active packet sniffing is a type of attack where data packets are manipulated in transit. This may include injecting internet protocols to redirect the packets to an unintended port or changing the information the packet contains. Active packet sniffing attack would be like a neighbor telling the delivery person "I'll deliver that mail for you," and then reading the mail or changing the letter before putting it in your mailbox. Even though your neighbor knows you and even if they deliver it to the correct house, they are actively going out of their way to engage in malicious behavior. |

Đánh hơi gói có thể thụ động hoặc chủ động.Đánh hơi gói tin thụ động là một loạitấn công nơi các gói dữ liệu được đọc trong quá trình vận chuyển.Vì tất cả lưu lượng trên mạngđược hiển thị với bất kỳ máy chủ nào trên hub,những kẻ độc hại có thể xemtất cả thông tin đang diễn ravào và ra khỏi thiết bị mà họ đang nhắm mục tiêu.Nghĩ lại ví dụ về một lá thư được gửi đi,chúng ta có thể so sánh việc đánh hơi gói tin thụ độngtấn công người giao hàng bưu điệnđộc ác đọc thư của ai đó.Nhân viên bưu điện, hoặc góisniffer, có quyền chuyển thư,nhưng không có quyền đọc thông tin bên trong.Đánh hơi gói tích cực là một loạitấn công nơi các gói dữ liệu bị thao túng trong quá trình vận chuyển.Điều này có thể bao gồm việc tiêmgiao thức internet để chuyển hướng các gói đếnmột cổng ngoài ý muốn hoặcthay đổi thông tin chứa trong gói.Tấn công đánh hơi gói tích cực sẽgiống như người hàng xóm nói với người giao hàng"Tôi sẽ chuyển thư đó cho bạn," rồi đọc thưhoặc thay đổi chữ cái trước khi bỏ vào hộp thư.Mặc dù hàng xóm của bạn biết bạnvà thậm chí nếu họ giao nó đến đúng nhà,họ đang tích cực đi ra ngoàicách của họ để tham gia vào hành vi độc hại.

|  |
| --- |
| The good news is that malicious packet sniffing can be prevented. Let's look at a few ways the network security professional can prevent these attacks. One way to protect against malicious packet sniffing is to use a VPN to encrypt and protect data as it travels across the network. If you don't remember how VPNs work, you can revisit the video about this topic in the previous section of the program. When you use a VPN, hackers might interfere with your traffic, but they won't be able to decode it to read it and read your private information. Another way to add a layer of protection against packet sniffing is to make sure that websites you have use HTTPS at the beginning of the domain address. Previously, we discussed how HTTPS uses SSL/TLS to encrypt data and prevent eavesdropping when malicious actors spy on network transmissions. One final way to help protect yourself against malicious packet sniffing is to avoid using unprotected WiFi. You usually find unprotected WiFi in public places like coffee shops, restaurants, or airports. These networks don't use encryption. This means that anyone on the network can access all of the data traveling to and from your device. One precaution you can take is avoiding free public WiFi unless you have a VPN service already installed on your device. |

Tin tốt làviệc đánh hơi gói độc hại có thể được ngăn chặn.Hãy xem xét một số cáchchuyên gia an ninh mạngcó thể ngăn chặn những cuộc tấn công này.Một cách để bảo vệ chống lạiviệc đánh hơi gói độc hại là sử dụngVPN để mã hóa và bảo vệdữ liệu khi nó truyền qua mạng.Nếu bạn không nhớ cách VPN hoạt động,bạn có thể xem lại video vềchủ đề này trong phần trước của chương trình.Khi bạn sử dụng VPN,tin tặc có thể can thiệp vào lưu lượng truy cập của bạn,nhưng họ sẽ không thể giải mã nóđể đọc nó và đọc thông tin cá nhân của bạn.Một cách khác để thêm một lớpbảo vệ chống lại việc đánh hơi gói là để đảm bảonhững trang web bạn đã sử dụngHTTPS ở đầu địa chỉ tên miền.Trước đây, chúng ta đã thảo luận về cách HTTPS sử dụng SSL/TLS đểmã hóa dữ liệu và ngăn chặn nghe lénkhi các tác nhân độc hại theo dõi đường truyền mạng.Một cách cuối cùng để giúp bảo vệ bạn khỏiđánh hơi gói độc hại là đểtránh sử dụng WiFi không được bảo vệ.Bạn thường tìm thấy WiFi không được bảo vệ trongnhững nơi công cộng như quán cà phê,nhà hàng hoặc sân bay.Các mạng này không sử dụng mã hóa.Điều này có nghĩa là bất kỳ ai trên mạng đều có thể truy cậptất cả dữ liệu di chuyển đến và đi từ thiết bị của bạn.Một biện pháp phòng ngừa bạn có thể thực hiện là tránhWiFi công cộng miễn phí trừ khi bạn cómột dịch vụ VPN đã được cài đặt trên thiết bị của bạn.

|  |
| --- |
| Now you know how threat actors may use packet sniffing and how to protect a network from these attacks. Let's move on to discuss other network intrusions. |

Bây giờ bạn đã biết các tác nhân đe dọa có thể sử dụng như thế nàođánh hơi gói tin và cách thực hiệnbảo vệ mạng khỏi những cuộc tấn công này.Hãy chuyển sang thảo luận về các hành vi xâm nhập mạng khác.

***3.2. IP Spoofing – Giả mạo IP***

|  |
| --- |
| Next, let's learn about another kind of network attack called IP spoofing. IP spoofing is a network attack performed when an attacker changes the source IP of a data packet to impersonate an authorized system and gain access to a network. In this kind of attack, the hacker is pretending to be someone they are not so they can communicate over the network with the target computer and get past firewall rules that may prevent outside traffic. Some common IP spoofing attacks are on-path attacks, replay attacks, and smurf attacks. Let's discuss these one at a time. |

Tiếp theo chúng ta cùng tìm hiểu vềmột kiểu tấn công mạng khác gọi là giả mạo IP.Giả mạo IP là một cuộc tấn công mạngđược thực hiện khi kẻ tấn công thay đổi IP nguồn củamột gói dữ liệu để mạo danhmột hệ thống được ủy quyền và có quyền truy cập vào mạng.Trong kiểu tấn công này,hacker đang giả vờ là ai đókhông phải để họ có thể giao tiếp quamạng với máy tính mục tiêu và nhận đượccác quy tắc tường lửa trong quá khứ có thể ngăn chặn lưu lượng truy cập bên ngoài.Một số cuộc tấn công giả mạo IP phổ biến là các cuộc tấn công trên đường đi,các cuộc tấn công phát lại và các cuộc tấn công smurf.Chúng ta hãy thảo luận về những điều này cùng một lúc.

|  |
| --- |
| An on-path attack is an attack where the malicious actor places themselves in the middle of an authorized connection and intercepts or alters the data in transit. On-path attackers gain access to the network and put themselves between two devices, like a web browser and a web server. Then they sniff the packet information to learn the IP and MAC addresses to devices that are communicating with each other. After they have this information, they can pretend to be either of these devices. |

Một cuộc tấn công trên đường đi làmột cuộc tấn công trong đó tác nhân độc hại tự đặt mình vàogiữa một kết nối được ủy quyềnvà chặn hoặc thay đổi dữ liệu trong quá trình truyền.Những kẻ tấn công trên đường có quyền truy cập vàomạng và đặt chúng ở giữa hai thiết bị,giống như một trình duyệt web và một máy chủ web.Sau đó họ đánh hơi gói tinthông tin để tìm hiểu IP vàĐịa chỉ MAC cho thiết bịđang giao tiếp với nhau.Sau khi họ có thông tin này,họ có thể giả vờ là một trong những thiết bị này.

|  |
| --- |
| Another type of attack is a replay attack. A replay attack is a network attack performed when a malicious actor intercepts a data packet in transit and delays it or repeats it at another time. A delayed packet can cause connection issues between target computers, or a malicious actor may take a network transmission that was sent by an authorized user and repeat it at a later time to impersonate the authorized user. |

Một loại tấn công khác là tấn công lặp lại.Một cuộc tấn công lặp lại làmột cuộc tấn công mạng được thực hiện khimột diễn viên độc hại chặnmột gói dữ liệu đang được chuyển tiếp và có độ trễnó hoặc lặp lại nó vào lúc khác.Một gói tin bị trì hoãn có thể gây ravấn đề kết nối giữa các máy tính mục tiêu,hoặc một tác nhân độc hại có thể lấymột đường truyền mạng được gửi bởimột người dùng được ủy quyền và lặp lại nó tạimột thời gian sau để mạo danh người dùng được ủy quyền.

|  |
| --- |
| A smurf attack is a combination of a DDoS attack and an IP spoofing attack. The attacker sniffs an authorized user's IP address and floods it with packets. This overwhelms the target computer and can bring down a server or the entire network. |

Một cuộc tấn công smurf là ​​sự kết hợp củamột cuộc tấn công DDoS và một cuộc tấn công giả mạo IP.Kẻ tấn công đánh hơi địa chỉ IP của người dùng được ủy quyềnvà tràn ngập các gói tin.Điều này làm choáng ngợp máy tính mục tiêu và có thểđánh sập một máy chủ hoặc toàn bộ mạng.

|  |
| --- |
| Now that you've learned about different kinds of IP spoofing, let's talk about how you can protect the network from this kind of attack. As you previously learned, encryption should always be implemented so that the data in your network transfers can't be read by malicious actors. Firewalls can be configured to protect against IP spoofing. IP spoofing makes it seem like the malicious actor is an authorized user by changing the sender's address of the data packet to match the target network's address. So if a firewall receives a data packet from the internet where the sender's IP address is the same as the private network, then the firewall will deny the transmission since all the devices with that IP address should already be on the local network. You can make sure that your firewalls configure correctly by creating a rule to reject all incoming traffic that has the same IP address as the local network. |

Bây giờ bạn đã học vềcác loại giả mạo IP khác nhau,hãy nói về cách bạn có thể bảo vệmạng khỏi kiểu tấn công này.Như bạn đã học trước đó,mã hóa phải luôn được thực hiện để dữ liệutrong mạng của bạn thì không thể chuyểnđược đọc bởi những kẻ độc hại.Tường lửa có thể được cấu hìnhđể bảo vệ chống giả mạo IP.Việc giả mạo IP làm cho nó có vẻ nhưtác nhân độc hại là người dùng được ủy quyềnbằng cách thay đổi địa chỉ người gửi củagói dữ liệu phù hợp với địa chỉ của mạng mục tiêu.Vì vậy, nếu tường lửa nhận được gói dữ liệu từ internetđịa chỉ IP của người gửi ở đâugiống như mạng riêng,sau đó tường lửa sẽ từ chối việc truyền tảivì tất cả các thiết bị có địa chỉ IP đólẽ ra đã có trên mạng cục bộ.Bạn có thể đảm bảo rằng tường lửa của bạncấu hình chính xác bằng cách tạo quy tắc đểtừ chối tất cả lưu lượng truy cập đến cócùng địa chỉ IP với mạng cục bộ.

|  |
| --- |
| That's it for IP spoofing. You've learned how IP spoofing is used in some common attacks like on-path attacks, replay attacks, and smurf attacks. |

Đó là cách giả mạo IP.Bạn đã biết cách sử dụng giả mạo IP trongmột số cuộc tấn công phổ biến như tấn công trên đường đi,các cuộc tấn công phát lại và các cuộc tấn công smurf.

***3.3. Overview of interception tactics – Tổng quan về chiến thuật đánh chặn***

|  |
| --- |
| **Overview of interception tactics** |

**Tổng quan về chiến thuật đánh chặn**

|  |
| --- |
| In the previous course items, you learned how packet sniffing and IP spoofing are used in network attacks. Because these attacks intercept data packets as they travel across the network, they are called interception attacks. |

Trong các mục khóa học trước, bạn đã học cách sử dụng tính năng đánh hơi gói và giả mạo IP trong các cuộc tấn công mạng. Bởi vì các cuộc tấn công này chặn các gói dữ liệu khi chúng truyền qua mạng nên chúng được gọi là các cuộc tấn công chặn.

|  |
| --- |
| This reading will introduce you to some specific attacks that use packet sniffing and IP spoofing. You will learn how hackers use these tactics and how security analysts can counter the threat of interception attacks. |

Bài đọc này sẽ giới thiệu cho bạn một số cuộc tấn công cụ thể sử dụng việc đánh hơi gói và giả mạo IP. Bạn sẽ tìm hiểu cách tin tặc sử dụng các chiến thuật này và cách các nhà phân tích bảo mật có thể chống lại mối đe dọa từ các cuộc tấn công đánh chặn.

|  |
| --- |
| **A closer review of packet sniffing** |

**Đánh giá kỹ hơn về việc đánh hơi gói**

|  |
| --- |
| As you learned in a previous video, **packet sniffing** is the practice of capturing and inspecting data packets across a network. On a private network, data packets are directed to the matching destination device on the network. |

Như bạn đã tìm hiểu trong video trước, **dò tìm gói** là phương pháp thu thập và kiểm tra các gói dữ liệu trên mạng. Trên mạng riêng, các gói dữ liệu được chuyển hướng đến thiết bị đích phù hợp trên mạng.

|  |
| --- |
| The device’s Network Interface Card (NIC) is a piece of hardware that connects the device to a network. The NIC reads the data transmission, and if it contains the device’s MAC address, it accepts the packet and sends it to the device to process the information based on the protocol. This occurs in all standard network operations. However, a NIC can be set to promiscuous mode, which means that it accepts all traffic on the network, even the packets that aren’t addressed to the NIC’s device. You’ll learn more about NIC’s later in the program. Malicious actors might use software like Wireshark to capture the data on a private network and store it for later use. They can then use the personal information to their own advantage. Alternatively, they might use the IP and MAC addresses of authorized users of the private network to perform IP spoofing. |

Thẻ giao diện mạng (NIC) của thiết bị là một phần cứng kết nối thiết bị với mạng. NIC đọc đường truyền dữ liệu và nếu nó chứa địa chỉ MAC của thiết bị, nó sẽ chấp nhận gói và gửi đến thiết bị để xử lý thông tin dựa trên giao thức. Điều này xảy ra trong tất cả các hoạt động mạng tiêu chuẩn. Tuy nhiên, NIC có thể được đặt ở chế độ lăng nhăng, nghĩa là nó chấp nhận tất cả lưu lượng truy cập trên mạng, ngay cả các gói không được gửi đến thiết bị của NIC. Bạn sẽ tìm hiểu thêm về NIC sau trong chương trình. Những kẻ độc hại có thể sử dụng phần mềm như Wireshark để thu thập dữ liệu trên mạng riêng và lưu trữ để sử dụng sau. Sau đó, họ có thể sử dụng thông tin cá nhân để có lợi cho riêng mình. Ngoài ra, họ có thể sử dụng địa chỉ IP và MAC của người dùng được ủy quyền của mạng riêng để thực hiện giả mạo IP.

|  |
| --- |
| **A closer review of IP spoofing** |

**Đánh giá kỹ hơn về việc giả mạo IP**

|  |
| --- |
| After a malicious actor has sniffed packets on the network, they can impersonate the IP and MAC addresses of authorized devices to perform an IP spoofing attack. Firewalls can prevent IP spoofing attacks by configuring it to refuse unauthorized IP packets and suspicious traffic. Next, you’ll examine a few common IP spoofing attacks that are important to be familiar with as a security analyst. |

Sau khi kẻ độc hại đánh hơi được các gói tin trên mạng, chúng có thể mạo danh địa chỉ IP và MAC của các thiết bị được ủy quyền để thực hiện một cuộc tấn công giả mạo IP. Tường lửa có thể ngăn chặn các cuộc tấn công giả mạo IP bằng cách định cấu hình nó để từ chối các gói IP trái phép và lưu lượng truy cập đáng ngờ. Tiếp theo, bạn sẽ xem xét một số cuộc tấn công giả mạo IP phổ biến mà nhà phân tích bảo mật cần phải làm quen.

|  |
| --- |
| **On-path attack** |

**Tấn công trên đường đi**

|  |
| --- |
| An **on-path attack** happens when a hacker intercepts the communication between two devices or servers that have a trusted relationship. The transmission between these two trusted network devices could contain valuable information like usernames and passwords that the malicious actor can collect. An on-path attack is sometimes referred to as a **meddler-in-the middle attack** because the hacker is hiding in the middle of communications between two trusted parties. |

Một **cuộc tấn công trên đường** xảy ra khi tin tặc chặn liên lạc giữa hai thiết bị hoặc máy chủ có mối quan hệ đáng tin cậy. Quá trình truyền giữa hai thiết bị mạng đáng tin cậy này có thể chứa thông tin có giá trị như tên người dùng và mật khẩu mà tác nhân độc hại có thể thu thập. Một cuộc tấn công trên đường đi đôi khi được gọi là một **cuộc tấn công can thiệp vào giữa** vì tin tặc đang ẩn náu giữa quá trình liên lạc giữa hai bên đáng tin cậy.

|  |
| --- |
| Or, it could be that the intercepted transmission contains a DNS system look-up. You’ll recall from an earlier video that a DNS server translates website domain names into IP addresses. If a malicious actor intercepts a transmission containing a DNS lookup, they could spoof the DNS response from the server and redirect a domain name to a different IP address, perhaps one that contains malicious code or other threats. The most important way to protect against an on-path attack is to encrypt your data in transit, e.g. using TLS. |

Hoặc có thể đường truyền bị chặn có chứa bản tra cứu hệ thống DNS. Bạn sẽ nhớ lại video trước đó rằng máy chủ DNS dịch tên miền của trang web thành địa chỉ IP. Nếu một tác nhân độc hại chặn đường truyền có chứa tra cứu DNS, chúng có thể giả mạo phản hồi DNS từ máy chủ và chuyển hướng tên miền đến một địa chỉ IP khác, có thể là địa chỉ chứa mã độc hoặc các mối đe dọa khác. Cách quan trọng nhất để bảo vệ khỏi cuộc tấn công trên đường đi là mã hóa dữ liệu của bạn trong quá trình truyền, ví dụ như sử dụng TLS.

|  |
| --- |
| **Smurf attack** |

**tấn công xì trum**

|  |
| --- |
| A **smurf attack** is a network attack that is performed when an attacker sniffs an authorized user’s IP address and floods it with packets. Once the spoofed packet reaches the broadcast address, it is sent to all of the devices and servers on the network. |

Tấn **công smurf** là ​​một cuộc tấn công mạng được thực hiện khi kẻ tấn công đánh hơi địa chỉ IP của người dùng được ủy quyền và làm tràn ngập các gói tin. Khi gói giả mạo đến địa chỉ quảng bá, nó sẽ được gửi đến tất cả các thiết bị và máy chủ trên mạng.

|  |
| --- |
| In a smurf attack, IP spoofing is combined with another denial of service (DoS) technique to flood the network with unwanted traffic. For example, the spoofed packet could include an Internet Control Message Protocol (ICMP) ping. As you learned earlier, ICMP is used to troubleshoot a network. But if too many ICMP messages are transmitted, the ICMP echo responses overwhelm the servers on the network and they shut down. This creates a denial of service and can bring an organization’s operations to a halt. |

Trong một cuộc tấn công smurf, việc giả mạo IP được kết hợp với một kỹ thuật từ chối dịch vụ (DoS) khác để làm tràn ngập mạng với lưu lượng truy cập không mong muốn. Ví dụ: gói giả mạo có thể bao gồm ping Giao thức tin nhắn điều khiển Internet (ICMP). Như bạn đã tìm hiểu trước đó, ICMP được sử dụng để khắc phục sự cố mạng. Nhưng nếu có quá nhiều tin nhắn ICMP được truyền đi, phản hồi tiếng vang ICMP sẽ lấn át các máy chủ trên mạng và chúng sẽ tắt. Điều này tạo ra sự từ chối dịch vụ và có thể khiến hoạt động của tổ chức bị đình trệ.

|  |
| --- |
| An important way to protect against a smurf attack is to use an advanced firewall that can monitor any unusual traffic on the network. Most next generation firewalls (NGFW) include features that detect network anomalies to ensure that oversized broadcasts are detected before they have a chance to bring down the network. |

Một cách quan trọng để bảo vệ khỏi cuộc tấn công smurf là ​​sử dụng tường lửa tiên tiến có thể giám sát mọi lưu lượng truy cập bất thường trên mạng. Hầu hết các tường lửa thế hệ tiếp theo (NGFW) đều bao gồm các tính năng phát hiện sự bất thường của mạng để đảm bảo phát hiện các chương trình phát sóng quá khổ trước khi chúng có cơ hội làm hỏng mạng.

|  |
| --- |
| **DoS attack** |

**Tấn công vào hệ điều hành Dos**

|  |
| --- |
| As you’ve learned, once the malicious actor has sniffed the network traffic, they can impersonate an authorized user. A **Denial of Service attack** is a class of attacks where the attacker prevents the compromised system from performing legitimate activity or responding to legitimate traffic. Unlike IP spoofing, however, the attacker will not receive a response from the targeted host. Everything about the data packet is authorized including the IP address in the header of the packet. In IP spoofing attacks, the malicious actor uses IP packets containing fake IP addresses. The attackers keep sending IP packets containing fake IP addresses until the network server crashes. |

Như bạn đã biết, khi kẻ độc hại đã đánh hơi được lưu lượng truy cập mạng, chúng có thể mạo danh người dùng được ủy quyền. Tấn **công từ chối dịch vụ** là một loại tấn công trong đó kẻ tấn công ngăn chặn hệ thống bị xâm nhập thực hiện hoạt động hợp pháp hoặc phản hồi lưu lượng truy cập hợp pháp. Tuy nhiên, không giống như giả mạo IP, kẻ tấn công sẽ không nhận được phản hồi từ máy chủ được nhắm mục tiêu. Mọi thứ về gói dữ liệu đều được ủy quyền, bao gồm cả địa chỉ IP trong tiêu đề của gói. Trong các cuộc tấn công giả mạo IP, tác nhân độc hại sử dụng các gói IP chứa địa chỉ IP giả. Những kẻ tấn công tiếp tục gửi các gói IP chứa địa chỉ IP giả cho đến khi máy chủ mạng gặp sự cố.

|  |
| --- |
| **Pro Tip**: Remember the principle of defense-in-depth. There isn’t one perfect strategy for stopping each kind of attack. You can layer your defense by using multiple strategies. In this case, using industry standard encryption will strengthen your security and help you defend from DoS attacks on more than one level. |

**Mẹo chuyên nghiệp** : Hãy nhớ nguyên tắc phòng thủ theo chiều sâu. Không có một chiến lược hoàn hảo nào để ngăn chặn từng kiểu tấn công. Bạn có thể tạo lớp phòng thủ của mình bằng cách sử dụng nhiều chiến lược. Trong trường hợp này, việc sử dụng mã hóa tiêu chuẩn ngành sẽ tăng cường tính bảo mật của bạn và giúp bạn bảo vệ khỏi các cuộc tấn công DoS ở nhiều cấp độ.

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

**Bài học chính**

|  |
| --- |
| This reading covered several types of common IP spoofing attacks. You learned about how packet sniffing is performed and how gathering information from intercepting data transmissions can give malicious actors opportunities for IP spoofing. Whether it is an on-path attack, IP spoofing attack, or a smurf attack, analysts need to ensure that mitigation strategies are in place to limit the threat and prevent security breaches. |

Bài đọc này đề cập đến một số loại tấn công giả mạo IP phổ biến. Bạn đã tìm hiểu về cách thực hiện việc đánh hơi gói và cách thu thập thông tin từ việc chặn truyền dữ liệu có thể tạo cơ hội cho các tác nhân độc hại thực hiện giả mạo IP. Cho dù đó là cuộc tấn công trên đường đi, cuộc tấn công giả mạo IP hay cuộc tấn công smurf, các nhà phân tích cần đảm bảo rằng các chiến lược giảm thiểu được áp dụng để hạn chế mối đe dọa và ngăn chặn các vi phạm an ninh.

***3.4. Identify: Network attacks – Nhận diện: Tấn công mạng***

|  |  |
| --- | --- |
| Term | Definition |
| Denial of service attack (DoS) | A network attack that targets a network or server and floods it with network traffic |
| Distributed denial of service attack (DDoS) | A type of denial or service attack that uses multiple devices or servers in different locations to flood the target network with unwanted traffic |
| SYN flood attack | A type of DoS attack that simulates a TCP/IP connection and floods a server with SYN packets |
| Packet sniffing | The practice of capturing and inspecting data packets across a network |
| IP spoofing | A network attack performed when an attacker changes the source IP of a data packet to impersonate an authorized system and gain access to a network |
| On-path attack | An attack where a malicious actor places themselves in the middle of an authorized connection and intercepts or alters the data in transit |

|  |  |
| --- | --- |
| Thuật ngữ | Định nghĩa |
| Tấn công từ chối dịch vụ (DoS) | Một cuộc tấn công mạng nhắm vào mạng hoặc máy chủ và làm tràn ngập lưu lượng mạng |
| Tấn công từ chối dịch vụ phân tán (DDoS) | Một kiểu tấn công từ chối hoặc dịch vụ sử dụng nhiều thiết bị hoặc máy chủ ở các vị trí khác nhau để làm tràn ngập mạng mục tiêu với lưu lượng truy cập không mong muốn |
| Cuộc tấn công lũ lụt SYN | Một kiểu tấn công DoS mô phỏng kết nối TCP/IP và làm tràn ngập máy chủ bằng các gói SYN |
| Đánh hơi gói | Thực hành thu thập và kiểm tra các gói dữ liệu trên mạng |
| Giả mạo IP | Một cuộc tấn công mạng được thực hiện khi kẻ tấn công thay đổi IP nguồn của gói dữ liệu để mạo danh hệ thống được ủy quyền và giành quyền truy cập vào mạng |
| Tấn công trên đường đi | Một cuộc tấn công trong đó tác nhân độc hại đặt mình vào giữa kết nối được ủy quyền và chặn hoặc thay đổi dữ liệu trong quá trình truyền |

***3.5. Activity: Analyze network attacks – Hoạt động: Phân tích các cuộc tấn công mạng***

***3.6. Activity Exemplar: Analyze network attacks – Mẫu hoạt động: Phân tích các cuộc tấn công mạng***

***3.7. Test your knowledge: Network interception attack tactics – Kiểm tra kiến ​​thức của bạn: Chiến thuật tấn công đánh chặn mạng***

**4. Review: Secure against network intrusion – Đánh giá: Bảo mật chống xâm nhập** **mạng**

***4.1. Wrap-up – Gói lại***

|  |
| --- |
| Nice job finishing this section! Let's review what you've learned so far. We discussed how to secure networks. We also learned about network intrusion tactics like malicious packet sniffing and IP spoofing. Finally, we discussed how a security analyst can protect against these attacks. You've learned about DoS and DDoS attacks like ICMP flooding, SYN attacks, and the ping of death, which try to overwhelming a network by flooding it with unwanted data packets. |

Làm tốt lắm khi hoàn thành phần này!Hãy xem lại những gì bạn đã học được cho đến nay.Chúng tôi đã thảo luận về cách bảo mật mạng.Chúng tôi cũng đã tìm hiểu về chiến thuật xâm nhập mạngnhư đánh hơi gói độc hại và giả mạo IP.Cuối cùng, chúng tôi đã thảo luận về cáchmột nhà phân tích bảo mật có thể bảo vệ khỏi những cuộc tấn công này.Bạn đã tìm hiểu về DoS và DDoScác cuộc tấn công như lũ lụt ICMP, tấn công SYN,và tiếng ping của cái chết,cố gắng áp đảo mạng lưới bằng cáchlàm ngập nó với các gói dữ liệu không mong muốn.

|  |
| --- |
| Now, just think about everything you know already about network attacks. What you've learned in these videos will be essential in your work as a security analyst. Coming up, you'll learn about how security analysts can protect the network using various security hardening techniques. |

Bây giờ, hãy nghĩ về mọi thứ bạnđã biết về các cuộc tấn công mạng.Những gì bạn đã học được trong những video này sẽ làcần thiết trong công việc của bạn với tư cách là một nhà phân tích bảo mật.Sắp tới, bạn sẽ họcvề cách các nhà phân tích bảo mật có thể bảo vệmạng bằng cách sử dụng các kỹ thuật tăng cường bảo mật khác nhau.

***4.2. 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 3, Module 3** |

**Các thuật ngữ và định nghĩa trong Khóa 3, Học phần 3**

|  |
| --- |
| **Active packet sniffing:** A type of attack where data packets are manipulated in transit |

**Đánh hơi gói tích cực:** Một kiểu tấn công trong đó các gói dữ liệu bị thao túng trong quá trình vận chuyển

|  |
| --- |
| **Botnet:** A collection of computers infected by malware that are under the control of a single threat actor, known as the “bot-herder" |

**Botnet:** Một tập hợp các máy tính bị nhiễm phần mềm độc hại nằm dưới sự kiểm soát của một tác nhân đe dọa duy nhất, được gọi là “người chăn nuôi bot”

|  |
| --- |
| **Denial of service (DoS) attack:** An attack that targets a network or server and floods it with network traffic |

**Tấn công từ chối dịch vụ (DoS):** Một cuộc tấn công nhắm vào mạng hoặc máy chủ và làm tràn ngập lưu lượng mạng

|  |
| --- |
| **Distributed denial of service (DDoS) attack:** A type of denial of service attack that uses multiple devices or servers located in different locations to flood the target network with unwanted traffic |

**Tấn công từ chối dịch vụ phân tán (DDoS):** Một loại tấn công từ chối dịch vụ sử dụng nhiều thiết bị hoặc máy chủ đặt ở các vị trí khác nhau để làm tràn ngập mạng mục tiêu với lưu lượng truy cập không mong muốn

|  |
| --- |
| **Internet Control Message Protocol (ICMP):** An internet protocol used by devices to tell each other about data transmission errors across the network |

**Giao thức thông báo điều khiển Internet (ICMP):** Giao thức internet được các thiết bị sử dụng để thông báo cho nhau về lỗi truyền dữ liệu qua mạng

|  |
| --- |
| **Internet Control Message Protocol (ICMP) flood:** A type of DoS attack performed by an attacker repeatedly sending ICMP request packets to a network server |

**Lũ lụt Giao thức tin nhắn điều khiển Internet (ICMP):** Một loại tấn công DoS được thực hiện bởi kẻ tấn công liên tục gửi các gói yêu cầu ICMP đến máy chủ mạng

|  |
| --- |
| **IP spoofing:** A network attack performed when an attacker changes the source IP of a data packet to impersonate an authorized system and gain access to a network |

**Giả mạo IP:** Một cuộc tấn công mạng được thực hiện khi kẻ tấn công thay đổi IP nguồn của gói dữ liệu để mạo danh hệ thống được ủy quyền và giành quyền truy cập vào mạng

|  |
| --- |
| **On-path attack:** An attack where a malicious actor places themselves in the middle of an authorized connection and intercepts or alters the data in transit |

**Tấn công trên đường đi:** Một cuộc tấn công trong đó tác nhân độc hại đặt mình vào giữa kết nối được ủy quyền và chặn hoặc thay đổi dữ liệu trong quá trình truyền

|  |
| --- |
| **Packet sniffing:** The practice of capturing and inspecting data packets across a network |

**Đánh hơi gói:** Thực hành thu thập và kiểm tra các gói dữ liệu trên mạng

|  |
| --- |
| **Passive packet sniffing:** A type of attack where a malicious actor connects to a network hub and looks at all traffic on the network |

**Đánh hơi gói thụ động:** Một kiểu tấn công trong đó tác nhân độc hại kết nối với trung tâm mạng và xem xét tất cả lưu lượng truy cập trên mạng

|  |
| --- |
| **Ping of death:** A type of DoS attack caused when a hacker pings a system by sending it an oversized ICMP packet that is bigger than 64KB |

**Ping of death:** Một kiểu tấn công DoS xảy ra khi hacker ping hệ thống bằng cách gửi cho nó một gói ICMP quá khổ lớn hơn 64KB

|  |
| --- |
| **Replay attack:** A network attack performed when a malicious actor intercepts a data packet in transit and delays it or repeats it at another time |

**Tấn công phát lại:** Một cuộc tấn công mạng được thực hiện khi một tác nhân độc hại chặn gói dữ liệu đang truyền và trì hoãn hoặc lặp lại gói dữ liệu đó vào lúc khác

|  |
| --- |
| **Smurf attack:** A network attack performed when an attacker sniffs an authorized user’s IP address and floods it with ICMP packets |

**Tấn công Smurf:** Một cuộc tấn công mạng được thực hiện khi kẻ tấn công đánh hơi địa chỉ IP của người dùng được ủy quyền và làm tràn ngập các gói ICMP

|  |
| --- |
| **Synchronize (SYN) flood attack:** A type of DoS attack that simulates a TCP/IP connection and floods a server with SYN packets |

**Tấn công lũ đồng bộ hóa (SYN):** Một kiểu tấn công DoS mô phỏng kết nối TCP/IP và làm tràn ngập máy chủ bằng các gói SYN

***4.3. Module 3 challenge – Thử thách mô-đun 3***

**Module 4: Security hardening – Tăng cường an ninh**

|  |
| --- |
| You will become familiar with network hardening practices that strengthen network systems. You'll learn how security hardening helps defend against malicious actors and intrusion methods. You'll also learn how to use security hardening to address the unique security challenges posed by cloud infrastructures. |

Bạn sẽ làm quen với các phương pháp tăng cường mạng nhằm củng cố hệ thống mạng. Bạn sẽ tìm hiểu cách tăng cường bảo mật giúp bảo vệ chống lại các tác nhân độc hại và các phương pháp xâm nhập. Bạn cũng sẽ tìm hiểu cách sử dụng biện pháp tăng cường bảo mật để giải quyết các thách thức bảo mật đặc biệt do cơ sở hạ tầng đám mây đặt ra.

|  |
| --- |
| **Learning Objectives**   * Describe OS hardening techniques * Describe network and cloud hardening techniques that target network vulnerabilities * Describe network hardening techniques * Explain cloud security practices |

**Mục tiêu học tập**

* Mô tả các kỹ thuật tăng cường hệ điều hành
* Mô tả các kỹ thuật tăng cường mạng và đám mây nhằm vào các lỗ hổng mạng
* Mô tả các kỹ thuật làm cứng mạng
* Giải thích các biện pháp bảo mật đám mây

**1. Introduction to security hardening – Giới thiệu về tăng cường bảo mật**

***1.1. Welcome to module 4 – Chào mừng đến với mô-đun 4***

|  |
| --- |
| I want to take a moment to congratulate you on your progress so far. First, you learned about network operations. Then, you learned about the tools and protocols that help network systems function. Next, you learned how vulnerabilities in networks expose them to various security intrusions. |

Tôi muốn dành một chút thời gian để chúc mừng sự tiến bộ của bạn cho đến nay.Đầu tiên, bạn đã tìm hiểu về hoạt động của mạng.Sau đó, bạn đã tìm hiểu về các công cụ vàcác giao thức giúp hệ thống mạng hoạt động.Tiếp theo, bạn đã tìm hiểu về các lỗ hổng trongmạng khiến họ gặp phải nhiều sự xâm nhập bảo mật khác nhau.

|  |
| --- |
| Now, we'll discuss security hardening. Then, we'll learn about OS hardening, explore network hardening practices, and discuss cloud hardening practices. Security hardening can be implemented in devices, networks, applications, and cloud infrastructure. Security analysts may perform tasks, such as patch updates and backups, as part of security hardening. |

Bây giờ, chúng ta sẽ thảo luận về việc tăng cường bảo mật.Sau đó, chúng ta sẽ tìm hiểu về tăng cường hệ điều hành, khám phá các phương pháp tăng cường mạng vàthảo luận về các phương pháp tăng cường độ cứng của đám mây.Tăng cường bảo mật có thể được thực hiện trong các thiết bị, mạng,ứng dụng và cơ sở hạ tầng đám mây.Các nhà phân tích bảo mật có thể thực hiện các nhiệm vụ, chẳng hạn như cập nhật bản vá vàsao lưu, như một phần của việc tăng cường bảo mật.

|  |
| --- |
| We'll discuss these tasks as you progress through the course. As a security analyst, hardening will play a major role in your day-to-day tasks, which is why it's important for you to understand how it works. I'm excited to accompany you on this journey. Meet you in the next video. |

Chúng ta sẽ thảo luận về những nhiệm vụ này khi bạn tiến bộ trong suốt khóa học.Là một nhà phân tích bảo mật, việc tăng cường sẽ đóng một vai trò quan trọng trong công việc hàng ngày của bạn,đó là lý do tại sao điều quan trọng là bạn phải hiểu cách thức hoạt động của nó.Tôi rất vui được đồng hành cùng bạn trên hành trình này.Hẹn gặp lại các bạn ở video tiếp theo.

***1.2. Security hardening – Tăng cường an ninh***

|  |
| --- |
| Security analysts and the organizations they work with have to be proactive about protecting systems from attack. This is where security hardening comes in. Security hardening is the process of strengthening a system to reduce its vulnerability and attack surface. All the potential vulnerabilities that a threat actor could exploit are referred to as a system's attack surface. |

Các nhà phân tích bảo mật và các tổ chức mà họ làm việc cùng phảichủ động bảo vệ hệ thống khỏi bị tấn công.Đây là nơi tăng cường bảo mật.Tăng cường bảo mật là quá trình tăng cường hệ thống để giảm thiểuđiểm yếu và bề mặt tấn công.Tất cả các lỗ hổng tiềm ẩn mà kẻ đe dọa có thể khai thácđược gọi là bề mặt tấn công của hệ thống.

|  |
| --- |
| Let's use an example that compares a network to a house. The attack surface would be all the doors and windows that a robber could use to gain access to that house. Just like putting locks on all the doors and windows in the house, security hardening involves minimizing the attack surface or potential vulnerabilities and keeping a network as secure as possible. |

Hãy sử dụng một ví dụ so sánh mạng với một ngôi nhà.Bề mặt tấn công sẽ là tất cả các cửa vàcửa sổ mà tên cướp có thể sử dụng để đột nhập vào ngôi nhà đó.Cũng giống như việc khóa tất cả các cửa ra vào và cửa sổ trong nhà,tăng cường bảo mật liên quan đến việc giảm thiểu bề mặt tấn công hoặccác lỗ hổng tiềm ẩn và giữ cho mạng an toàn nhất có thể.

|  |
| --- |
| As part of security hardening, security analysts perform regular maintenance procedures to keep network devices and systems functioning securely and optimally. Security hardening can be conducted on any device or system that can be compromised, such as hardware, operating systems, applications, computer networks, and databases. Physical security is also a part of security hardening. This may include securing a physical space with security cameras and security guards. |

Là một phần của việc tăng cường bảo mật, các nhà phân tích bảo mật thực hiện bảo trì thường xuyêncác quy trình để giữ cho các thiết bị và hệ thống mạng hoạt động an toàn vàmột cách tối ưu.Việc tăng cường bảo mật có thể được tiến hành trên bất kỳ thiết bị hoặchệ thống có thể bị xâm phạm, chẳng hạn như phần cứng, hệ điều hành,ứng dụng, mạng máy tính và cơ sở dữ liệu.An ninh vật lý cũng là một phần của việc tăng cường an ninh.Điều này có thể bao gồm việc đảm bảo một không gian vật lý có camera an ninh và nhân viên bảo vệ.

|  |
| --- |
| Some common types of hardening procedures include software updates, also called patches, and device application configuration changes. These updates and changes are done to increase security and fix security vulnerabilities on a network. An example of a security configuration change would be requiring longer passwords or more frequent password changes. This makes it harder for a malicious actor to gain login credentials. An example of a configuration check is updating the encryption standards for data that is stored in a database. Keeping encryption up to date makes it harder for malicious actors to access the database. |

Một số loại quy trình tăng cường phổ biến bao gồm cập nhật phần mềm,còn được gọi là bản vá và thay đổi cấu hình ứng dụng thiết bị.Những cập nhật và thay đổi này được thực hiện để tăng cường tính bảo mật vàkhắc phục các lỗ hổng bảo mật trên mạng.Một ví dụ về thay đổi cấu hình bảo mật sẽ cần nhiều thời gian hơnmật khẩu hoặc thay đổi mật khẩu thường xuyên hơn.Điều này khiến tác nhân độc hại khó lấy được thông tin đăng nhập hơn.Một ví dụ về kiểm tra cấu hình là cập nhật các tiêu chuẩn mã hóa chodữ liệu được lưu trữ trong cơ sở dữ liệu.Việc luôn cập nhật mã hóa sẽ gây khó khăn hơn chotác nhân độc hại truy cập vào cơ sở dữ liệu.

|  |
| --- |
| Other examples of security hardening include removing or disabling unused applications and services, disabling unused ports, and reducing access permissions across devices and network. Minimizing the number of applications, devices, ports, and access permissions makes network and device monitoring more efficient and reduces the overall attack surface, which is one of the best ways to secure an organization. |

Các ví dụ khác về tăng cường bảo mật bao gồm việc loại bỏ hoặcvô hiệu hóa các ứng dụng và dịch vụ không sử dụng, vô hiệu hóa các cổng không sử dụng vàgiảm quyền truy cập trên các thiết bị và mạng.Giảm thiểu số lượng ứng dụng, thiết bị, cổng và quyền truy cậpgiúp việc giám sát mạng và thiết bị hiệu quả hơn và giảm thiểu các cuộc tấn công tổng thểbề mặt, đó là một trong những cách tốt nhất để bảo vệ một tổ chức.

|  |
| --- |
| Another important strategy for security hardening is to conduct regular penetration testing. A penetration test, also called a pen test, is a simulated attack that helps identify vulnerabilities in a system, network, website, application, and process. Penetration testers document their findings in a report. Depending on where the test fails, security teams can determine the type of security vulnerabilities that require fixing. Organizations can then review these vulnerabilities and come up with a plan to fix them. |

Một chiến lược quan trọng khác chotăng cường bảo mật là tiến hành kiểm tra thâm nhập thường xuyên.Kiểm tra thâm nhập, còn được gọi là kiểm tra bút, là một cuộc tấn công mô phỏng giúp xác địnhcác lỗ hổng trong hệ thống, mạng, trang web, ứng dụng và quy trình.Người kiểm tra thâm nhập ghi lại những phát hiện của họ trong một báo cáo.Tùy thuộc vào vị trí thử nghiệm thất bại, đội bảo mật có thể xác định loạilỗ hổng bảo mật cần khắc phục.Sau đó, các tổ chức có thể xem xét các lỗ hổng này vàđưa ra kế hoạch để khắc phục chúng.

|  |
| --- |
| Coming up, you'll learn more about how security hardening is an essential aspect of securing networks. It's a foundational part of network security that strengthens the network in order to reduce the number of successful attacks. |

Sắp tới, bạn sẽ tìm hiểu thêm về việc tăng cường bảo mật là một khía cạnh thiết yếu như thế nàovề việc bảo mật các mạng.Đó là một phần nền tảng của an ninh mạng nhằm tăng cườngmạng nhằm giảm số lần tấn công thành công.

**2. OS hardening – Tăng cường hệ điều hành**

***2.1. OS hardening practices – Thực hành tăng cường hệ điều hành***

|  |
| --- |
| Hi there. In this video, we'll discuss operating system, or OS, hardening and why it's essential to keep the entire network secure. The operating system is the interface between computer hardware and the user. The OS is the first program loaded when a computer turns on. The OS acts as an intermediary between software applications and the computer hardware. It's important to secure the OS in each system because one insecure OS can lead to a whole network being compromised. There are many types of operating systems, and they all share similar security hardening practices. Let's talk about some of those security hardening practices that are recommended to secure an OS. |

Chào bạn. Trong video này,chúng ta sẽ thảo luận về hệ điều hành, hoặcHệ điều hành, việc tăng cường độ cứng và lý do tại sao lại như vậycần thiết để giữ an toàn cho toàn bộ mạng.Hệ điều hành làgiao diện giữa phần cứng máy tính và người sử dụng.Hệ điều hành là chương trình đầu tiênđược tải khi máy tính bật.Hệ điều hành đóng vai trò trung giangiữa các ứng dụng phần mềm và phần cứng máy tính.Điều quan trọng là phải bảo mật hệ điều hành trong mỗi hệ thốngbởi vì một hệ điều hành không an toàn có thểdẫn đến toàn bộ mạng bị xâm phạm.Có nhiều loại hệ điều hành và chúngtất cả đều chia sẻ các biện pháp tăng cường bảo mật tương tự.Hãy nói về một sốnhững biện pháp tăng cường bảo mật đóđược khuyến nghị để bảo mật một hệ điều hành.

|  |
| --- |
| Some OS hardening tasks are performed at regular intervals, like updates, backups, and keeping an up-to-date list of devices and authorized users. Other tasks are performed only once as part of preliminary safety measures. One example would be configuring a device setting to fit a secure encryption standard. Let's begin with OS hardening tasks that are performed at a regular interval, such as patch installation, also known as patch updates. |

Một số nhiệm vụ tăng cường hệ điều hànhđược thực hiện đều đặn,như cập nhật, sao lưu và lưu giữdanh sách cập nhật các thiết bị và người dùng được ủy quyền.Các nhiệm vụ khác chỉ được thực hiệnmột lần như một phần của các biện pháp an toàn sơ bộ.Một ví dụ sẽ là cấu hìnhcài đặt thiết bị để phù hợp với tiêu chuẩn mã hóa an toàn.Hãy bắt đầu với nhiệm vụ tăng cường hệ điều hànhđược thực hiện đều đặn,chẳng hạn như cài đặt bản vá,còn được gọi là cập nhật bản vá.

|  |
| --- |
| A patch update is a software and operating system, or OS, update that addresses security vulnerabilities within a program or product. Now we'll discuss patch updates provided to the company by the OS software vendor. With patch updates, the OS should be upgraded to its latest software version. Sometimes patches are released to fix a security vulnerability in the software. As soon as OS vendors publish a patch and the vulnerability fix, malicious actors know exactly where the vulnerability is in systems running the out-of-date OS. This is why it's important for organizations to run patch updates as soon as they are released. For example, my team had to perform an emergency patch to address a recent vulnerability found in a commonly used programming library. The library is used almost everywhere, so we had to quickly patch most of our servers and applications to fix the vulnerability. The newly updated OS should be added to the baseline configuration, also called the baseline image. A baseline configuration is a documented set of specifications within a system that is used as a basis for future builds, releases, and updates. For example, a baseline may contain a firewall rule with a list of allowed and disallowed network ports. If a security team suspects unusual activity affecting the OS, they can compare the current configuration to the baseline and make sure that nothing has been changed. |

Bản cập nhật bản vá là một phần mềm và hệ điều hành, hoặcHệ điều hành, cập nhật địa chỉ đólỗ hổng bảo mật trong một chương trình hoặc sản phẩm.Bây giờ chúng ta sẽ thảo luận về các bản cập nhật bản vá được cung cấpcho công ty bởi nhà cung cấp phần mềm hệ điều hành.Với các bản cập nhật bản vá, hệ điều hành sẽđược nâng cấp lên phiên bản phần mềm mới nhất.Đôi khi các bản vá được phát hànhđể khắc phục lỗ hổng bảo mật trong phần mềm.Ngay sau khi các nhà cung cấp hệ điều hành xuất bảnmột bản vá và sửa chữa lỗ hổng,những kẻ độc hại biết chính xác ở đâulỗ hổng nằm trong hệ thốngchạy hệ điều hành lỗi thời.Đây là lý do tại sao điều quan trọng đối với các tổ chức là phải thực hiệncập nhật bản vá ngay khi chúng được phát hành.Ví dụ, nhóm của tôiđã phải thực hiện một bản vá khẩn cấp đểgiải quyết một lỗ hổng gần đâyđược tìm thấy trong thư viện lập trình thường được sử dụng.Thư viện được sử dụng ở hầu hết mọi nơi,vì vậy chúng tôi phải nhanh chóng vá hầu hết các máy chủ của mình vàcác ứng dụng để khắc phục lỗ hổng.Hệ điều hành mới được cập nhật sẽđược thêm vào cấu hình cơ bản,còn được gọi là ảnh cơ sở.Cấu hình cơ sở là một tập hợp tài liệu củathông số kỹ thuật trong một hệ thốngđược sử dụng làm cơ sở cho các bản dựng trong tương lai,phát hành và cập nhật.Ví dụ: đường cơ sở có thể chứamột quy tắc tường lửa với một danh sáchcổng mạng được phép và không được phép.Nếu đội an ninh nghi ngờhoạt động bất thường ảnh hưởng đến hệ điều hành,họ có thể so sánh cấu hình hiện tại vớiđường cơ sở và đảm bảo rằng không có gì thay đổi.

|  |
| --- |
| Another hardening task performed regularly is hardware and software disposal. This ensures that all old hardware is properly wiped and disposed of. It's also a good idea to delete any unused software applications since some popular programming languages have known vulnerabilities. Removing unused software makes sure that there aren't any unnecessary vulnerabilities connected with the programs that the software uses. |

Một nhiệm vụ tăng cường khác được thực hiện thường xuyên làthanh lý phần cứng và phần mềm.Điều này đảm bảo rằng tất cả phần cứng cũđược xóa sạch và xử lý đúng cách.Xóa đi cũng là một ý kiến ​​haymọi ứng dụng phần mềm không được sử dụng kể từ đómột số ngôn ngữ lập trình phổ biếncó những lỗ hổng đã biết.Loại bỏ phần mềm không sử dụng để đảm bảo rằng không cóbất kỳ lỗ hổng không cần thiết nào được kết nốivới các chương trình mà phần mềm sử dụng.

|  |
| --- |
| The final OS hardening technique that we'll discuss is implementing a strong password policy. Strong password policies require that passwords follow specific rules. For example, an organization may set a password policy that requires a minimum of eight characters, a capital letter, a number, and a symbol. To discourage malicious actors, a password policy usually states that a user will lose access to the network after entering the wrong password a certain number of times in a row. Some systems also require multi-factor authentication, or MFA. MFA is a security measure which requires a user to verify their identity in two or more ways to access a system or network. Ways of identifying yourself include something you know, like a password, something you have like an ID card, or something unique about you, like your fingerprint. |

Kỹ thuật tăng cường hệ điều hành cuối cùng mà chúng tôi sẽthảo luận đang thực hiện chính sách mật khẩu mạnh.Chính sách mật khẩu mạnh đòi hỏimật khẩu tuân theo các quy tắc cụ thể.Ví dụ: một tổ chức có thể thiết lậpchính sách mật khẩu yêu cầutối thiểu tám ký tự,một chữ in hoa, một số và một ký hiệu.Để ngăn chặn những kẻ độc hại,chính sách mật khẩu thườngtuyên bố rằng người dùng sẽ mất quyền truy cập vàomạng sau khi vàosai mật khẩu một số lần nhất định liên tiếp.Một số hệ thống cũng yêu cầuxác thực đa yếu tố, hoặc MFA.MFA là một biện pháp bảo mậtyêu cầu người dùng xác minh danh tính của họ tronghai hoặc nhiều cách để truy cập vào hệ thống hoặc mạng.Các cách nhận dạng bản thân bao gồmthứ gì đó bạn biết, như mật khẩu,thứ gì đó bạn có như thẻ căn cước,hoặc điều gì đó độc đáo về bạn, như dấu vân tay của bạn.

|  |
| --- |
| To review, OS hardening is a set of procedures that maintains OS security and improves it. Security measures like access privileges and password policies frequently undergo regular security checks as part of OS hardening. Coming up, we'll discuss network hardening practices. |

Để xem xét, việc tăng cường hệ điều hành là một tập hợp các quy trìnhduy trì tính bảo mật của hệ điều hành và cải thiện nó.Các biện pháp an ninh nhưđặc quyền truy cập và chính sách mật khẩuthường xuyên trải qua kiểm tra an ninh thường xuyênnhư một phần của việc tăng cường hệ điều hành.Sắp tới, chúng ta sẽ thảo luận về các phương pháp tăng cường mạng.

***2.2. Brute force attacks and OS hardening – Các cuộc tấn công bạo lực và làm cứng hệ điều hành***

|  |
| --- |
| **Brute force attacks and OS hardening** |

**Các cuộc tấn công bạo lực và làm cứng hệ điều hành**

|  |
| --- |
| In this reading, you’ll learn about brute force attacks. You’ll consider how vulnerabilities can be assessed using virtual machines and sandboxes, and learn ways to prevent brute force attacks using a combination of authentication measures. Implementing various OS hardening tasks can help prevent brute force attacks. An attacker can use a brute force attack to gain access and compromise a network. |

Trong bài đọc này, bạn sẽ tìm hiểu về các cuộc tấn công vũ phu. Bạn sẽ xem xét cách đánh giá các lỗ hổng bằng cách sử dụng máy ảo và hộp cát, đồng thời tìm hiểu cách ngăn chặn các cuộc tấn công vũ phu bằng cách sử dụng kết hợp các biện pháp xác thực. Việc thực hiện các nhiệm vụ tăng cường hệ điều hành khác nhau có thể giúp ngăn chặn các cuộc tấn công vũ phu. Kẻ tấn công có thể sử dụng một cuộc tấn công vũ phu để giành quyền truy cập và xâm phạm mạng.

|  |
| --- |
| Usernames and passwords are among the most common and important security controls in place today. They are used and enforced on everything that stores or accesses sensitive or private information, like personal phones, computers, and restricted applications within an organization. However, a major issue with relying on login credentials as a critical line of defense is that they’re vulnerable to being stolen and guessed by malicious actors. |

Tên người dùng và mật khẩu là một trong những biện pháp kiểm soát bảo mật phổ biến và quan trọng nhất hiện nay. Chúng được sử dụng và thực thi trên mọi thứ lưu trữ hoặc truy cập thông tin nhạy cảm hoặc riêng tư, như điện thoại cá nhân, máy tính và các ứng dụng bị hạn chế trong một tổ chức. Tuy nhiên, một vấn đề lớn khi dựa vào thông tin xác thực đăng nhập như một tuyến phòng thủ quan trọng là chúng dễ bị đánh cắp và đoán bởi các tác nhân độc hại.

|  |
| --- |
| **Brute force attacks** |

**Tấn công bạo lực**

|  |
| --- |
| A **brute force attack** is a trial-and-error process of discovering private information. There are different types of brute force attacks that malicious actors use to guess passwords, including:   * *Simple brute force attacks.* When attackers try to guess a user's login credentials, it’s considered a simple brute force attack. They might do this by entering any combination of usernames and passwords that they can think of until they find the one that works. * *Dictionary attacks* use a similar technique. In dictionary attacks, attackers use a list of commonly used passwords and stolen credentials from previous breaches to access a system. These are called “dictionary” attacks because attackers originally used a list of words from the dictionary to guess the passwords, before complex password rules became a common security practice. |

Tấn **công vũ phu** là một quá trình thử và sai để khám phá thông tin cá nhân. Có nhiều kiểu tấn công vũ phu khác nhau mà kẻ độc hại sử dụng để đoán mật khẩu, bao gồm:

* *Các cuộc tấn công vũ phu đơn giản.* Khi những kẻ tấn công cố gắng đoán thông tin đăng nhập của người dùng, đó được coi là một cuộc tấn công vũ phu đơn giản. Họ có thể làm điều này bằng cách nhập bất kỳ tổ hợp tên người dùng và mật khẩu nào mà họ có thể nghĩ ra cho đến khi tìm thấy tổ hợp phù hợp.
* *Các cuộc tấn công từ điển* sử dụng một kỹ thuật tương tự. Trong các cuộc tấn công từ điển, kẻ tấn công sử dụng danh sách mật khẩu thường được sử dụng và thông tin xác thực bị đánh cắp từ các lần vi phạm trước đó để truy cập vào hệ thống. Chúng được gọi là các cuộc tấn công “từ điển” vì những kẻ tấn công ban đầu sử dụng danh sách các từ trong từ điển để đoán mật khẩu, trước khi các quy tắc mật khẩu phức tạp trở thành phương pháp bảo mật phổ biến.

|  |
| --- |
| Using brute force to access a system can be a tedious and time consuming process, especially when it’s done manually. There are a range of tools attackers use to conduct their attacks. |

Sử dụng vũ lực để truy cập hệ thống có thể là một quá trình tẻ nhạt và tốn thời gian, đặc biệt là khi nó được thực hiện thủ công. Có một loạt các công cụ mà kẻ tấn công sử dụng để tiến hành các cuộc tấn công của chúng.

|  |
| --- |
| **Assessing vulnerabilities** |

**Đánh giá lỗ hổng**

|  |
| --- |
| Before a brute force attack or other cybersecurity incident occurs, companies can run a series of tests on their network or web applications to assess vulnerabilities. Analysts can use virtual machines and sandboxes to test suspicious files, check for vulnerabilities before an event occurs, or to simulate a cybersecurity incident. |

Trước khi một cuộc tấn công vũ phu hoặc sự cố an ninh mạng khác xảy ra, các công ty có thể chạy một loạt thử nghiệm trên mạng hoặc ứng dụng web của họ để đánh giá các lỗ hổng. Các nhà phân tích có thể sử dụng máy ảo và hộp cát để kiểm tra các tệp đáng ngờ, kiểm tra lỗ hổng trước khi sự kiện xảy ra hoặc để mô phỏng sự cố an ninh mạng.

|  |
| --- |
| **Virtual machines (VMs)** |

**Máy ảo (VM)**

|  |
| --- |
| Virtual machines (VMs) are software versions of physical computers. VMs provide an additional layer of security for an organization because they can be used to run code in an isolated environment, preventing malicious code from affecting the rest of the computer or system. VMs can also be deleted and replaced by a pristine image after testing malware. |

Máy ảo (VM) là phiên bản phần mềm của máy tính vật lý. Máy ảo cung cấp một lớp bảo mật bổ sung cho tổ chức vì chúng có thể được sử dụng để chạy mã trong môi trường biệt lập, ngăn chặn mã độc hại ảnh hưởng đến phần còn lại của máy tính hoặc hệ thống. Máy ảo cũng có thể bị xóa và thay thế bằng hình ảnh nguyên sơ sau khi kiểm tra phần mềm độc hại.

|  |
| --- |
| VMs are useful when investigating potentially infected machines or running malware in a constrained environment. Using a VM may prevent damage to your system in the event its tools are used improperly. VMs also give you the ability to revert to a previous state. However, there are still some risks involved with VMs. There’s still a small risk that a malicious program can escape virtualization and access the host machine. |

Máy ảo rất hữu ích khi điều tra các máy có khả năng bị nhiễm hoặc chạy phần mềm độc hại trong môi trường bị hạn chế. Sử dụng VM có thể ngăn ngừa hư hỏng hệ thống của bạn trong trường hợp các công cụ của nó được sử dụng không đúng cách. Máy ảo cũng cung cấp cho bạn khả năng hoàn nguyên về trạng thái trước đó. Tuy nhiên, vẫn có một số rủi ro liên quan đến VM. Vẫn có một rủi ro nhỏ là chương trình độc hại có thể thoát khỏi ảo hóa và truy cập vào máy chủ.

|  |
| --- |
| You can test and explore applications easily with VMs, and it’s easy to switch between different VMs from your computer. This can also help in streamlining many security tasks. |

Bạn có thể dễ dàng kiểm tra và khám phá các ứng dụng bằng máy ảo và thật dễ dàng chuyển đổi giữa các máy ảo khác nhau từ máy tính của mình. Điều này cũng có thể giúp hợp lý hóa nhiều nhiệm vụ bảo mật.

|  |
| --- |
| **Sandbox environments** |

**Môi trường hộp cát**

|  |
| --- |
| A sandbox is a type of testing environment that allows you to execute software or programs separate from your network. They are commonly used for testing patches, identifying and addressing bugs, or detecting cybersecurity vulnerabilities. Sandboxes can also be used to evaluate suspicious software, evaluate files containing malicious code, and simulate attack scenarios. |

Hộp cát là một loại môi trường thử nghiệm cho phép bạn thực thi phần mềm hoặc chương trình tách biệt khỏi mạng của mình. Chúng thường được sử dụng để kiểm tra các bản vá, xác định và giải quyết các lỗi hoặc phát hiện các lỗ hổng an ninh mạng. Hộp cát cũng có thể được sử dụng để đánh giá phần mềm đáng ngờ, đánh giá các tệp chứa mã độc và mô phỏng các tình huống tấn công.

|  |
| --- |
| Sandboxes can be stand-alone physical computers that are not connected to a network; however, it is often more time- and cost-effective to use software or cloud-based virtual machines as sandbox environments. Note that some malware authors know how to write code to detect if the malware is executed in a VM or sandbox environment. Attackers can program their malware to behave as harmless software when run inside these types of  testing environments. |

Hộp cát có thể là các máy tính vật lý độc lập không được kết nối với mạng; tuy nhiên, việc sử dụng phần mềm hoặc máy ảo dựa trên đám mây làm môi trường hộp cát thường tiết kiệm thời gian và chi phí hơn. Lưu ý rằng một số tác giả phần mềm độc hại biết cách viết mã để phát hiện xem phần mềm độc hại có được thực thi trong môi trường VM hoặc hộp cát hay không. Những kẻ tấn công có thể lập trình phần mềm độc hại của chúng hoạt động như phần mềm vô hại khi chạy trong các loại môi trường thử nghiệm này.

|  |
| --- |
| **Prevention measures** |

**Các biện pháp phòng ngừa**

|  |
| --- |
| Some common measures organizations use to prevent brute force attacks and similar attacks from occurring include:   * **Salting and hashing:** Hashing converts information into a unique value that can then be used to determine its integrity. It is a one-way function, meaning it is impossible to decrypt and obtain the original text. Salting adds random characters to hashed passwords. This increases the length and complexity of hash values, making them more secure. * **Multi-factor authentication (MFA) and two-factor authentication (2FA):** MFA is a security measure which requires a user to verify their identity in two or more ways to access a system or network. This verification happens using a combination of authentication factors: a username and password, fingerprints, facial recognition, or a one-time password (OTP) sent to a phone number or email. 2FA is similar to MFA, except it uses only two forms of verification. * **CAPTCHA and reCAPTCHA:** CAPTCHA stands for Completely Automated Public Turing test to tell Computers and Humans Apart. It asks users to complete a simple test that proves they are human. This helps prevent software from trying to brute force a password. reCAPTCHA is a free CAPTCHA service from Google that helps protect websites from bots and malicious software. * **Password policies:** Organizations use password policies to standardize good password practices throughout the business. Policies can include guidelines on how complex a password should be, how often users need to update passwords, whether passwords can be reused or not, and if there are limits to how many times a user can attempt to log in before their account is suspended. |

Một số biện pháp phổ biến mà các tổ chức sử dụng để ngăn chặn các cuộc tấn công vũ phu và các cuộc tấn công tương tự xảy ra bao gồm:

* **Muối và băm:** Băm chuyển đổi thông tin thành một giá trị duy nhất mà sau đó có thể được sử dụng để xác định tính toàn vẹn của nó. Đây là chức năng một chiều, nghĩa là không thể giải mã và lấy được văn bản gốc. Salting thêm các ký tự ngẫu nhiên vào mật khẩu băm. Điều này làm tăng độ dài và độ phức tạp của các giá trị băm, khiến chúng an toàn hơn.
* **Xác thực đa yếu tố (MFA) và xác thực hai yếu tố (2FA):** MFA là biện pháp bảo mật yêu cầu người dùng xác minh danh tính của họ theo hai cách trở lên để truy cập hệ thống hoặc mạng. Việc xác minh này diễn ra bằng cách sử dụng kết hợp các yếu tố xác thực: tên người dùng và mật khẩu, dấu vân tay, nhận dạng khuôn mặt hoặc mật khẩu một lần (OTP) được gửi tới số điện thoại hoặc email. 2FA tương tự như MFA, ngoại trừ việc nó chỉ sử dụng hai hình thức xác minh.
* **CAPTCHA và reCAPTCHA:** CAPTCHA là viết tắt của bài kiểm tra Turing công cộng hoàn toàn tự động để phân biệt Máy tính và Con người. Nó yêu cầu người dùng hoàn thành một bài kiểm tra đơn giản để chứng minh họ là con người. Điều này giúp ngăn phần mềm cố gắng ép buộc mật khẩu. reCAPTCHA là dịch vụ CAPTCHA miễn phí của Google giúp bảo vệ trang web khỏi bot và phần mềm độc hại.
* **Chính sách mật khẩu:** Các tổ chức sử dụng chính sách mật khẩu để tiêu chuẩn hóa các phương pháp thực hành mật khẩu hiệu quả trong toàn doanh nghiệp. Các chính sách có thể bao gồm các hướng dẫn về mức độ phức tạp của mật khẩu, tần suất người dùng cần cập nhật mật khẩu, liệu mật khẩu có thể được sử dụng lại hay không và liệu có giới hạn về số lần người dùng có thể cố gắng đăng nhập trước khi tài khoản của họ bị tạm ngưng hay không.

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

**Bài học chính**

|  |
| --- |
| Brute force attacks are a trial-and-error process of guessing passwords. Attacks can be launched manually or through software tools. Methods include simple brute force attacks and dictionary attacks. To protect against brute force attacks, cybersecurity analysts can use sandboxes to test suspicious files, check for vulnerabilities, or to simulate real attacks and virtual machines to conduct vulnerability tests. Some common measures to prevent brute force attacks include: hashing and salting, MFA and/or 2FA, CAPTCHA and reCAPTCHA, and password policies. |

Các cuộc tấn công Brute Force là một quá trình thử và sai để đoán mật khẩu. Các cuộc tấn công có thể được thực hiện thủ công hoặc thông qua các công cụ phần mềm. Các phương pháp bao gồm các cuộc tấn công vũ phu đơn giản và các cuộc tấn công từ điển. Để bảo vệ khỏi các cuộc tấn công vũ phu, các nhà phân tích an ninh mạng có thể sử dụng hộp cát để kiểm tra các tệp đáng ngờ, kiểm tra lỗ hổng hoặc mô phỏng các cuộc tấn công thực và máy ảo để tiến hành kiểm tra lỗ hổng. Một số biện pháp phổ biến để ngăn chặn các cuộc tấn công vũ phu bao gồm: băm và tạo muối, MFA và/hoặc 2FA, CAPTCHA và reCAPTCHA cũng như các chính sách mật khẩu.

***2.3. Activity: Apply OS hardening techniques – Hoạt động: Áp dụng kỹ thuật tăng cường hệ điều hành***

***2.4. Activity Exemplar: Apply OS hardening techniques – Ví dụ hoạt động: Áp dụng các kỹ thuật tăng cường hệ điều hành***

***2.5. Test your knowledge: OS hardening – Kiểm tra kiến ​​thức của bạn: Tăng cường hệ điều hành***

**3. Network hardening – Tăng cường mạng**

***3.1. Network hardening practices – Thực hành tăng cường mạng***

|  |
| --- |
| Earlier, you learned that OS hardening focuses on device safety and uses patch updates, secure configuration, and account access policies. Now we'll focus on network hardening. Network hardening focuses on network-related security hardening, like port filtering, network access privileges, and encryption over networks. Certain network hardening tasks are performed regularly, while others are performed once and then updated as needed. |

Trước đó, bạn đã biết rằng việc tăng cường hệ điều hành tập trung vàovề an toàn thiết bị và sử dụng các bản cập nhật bản vá,cấu hình an toàn và chính sách truy cập tài khoản.Bây giờ chúng ta sẽ tập trung vào việc củng cố mạng.Tập trung củng cố mạngvề việc tăng cường an ninh liên quan đến mạng,như lọc cổng, đặc quyền truy cập mạng,và mã hóa qua mạng.Một số nhiệm vụ tăng cường mạng được thực hiện thường xuyên,trong khi những người khác được thực hiệnmột lần và sau đó cập nhật khi cần thiết.

|  |
| --- |
| Some tasks that are regularly performed are firewall rules maintenance, network log analysis, patch updates, and server backups. Earlier, you learned that a log is a record of events that occurs within an organization's systems. Network log analysis is the process of examining network logs to identify events of interest. Security teams use a log analyzer tool or a security information and event management tool, also known as a SIEM, to conduct network log analysis. A SIEM tool is an application that collects and analyzes log data to monitor critical activities in an organization. It gathers security data from a network and presents that data on a single dashboard. The dashboard interface is sometimes called a single pane of glass. A SIEM helps analysts to inspect, analyze, and react to security events across the network based on their priority. Reports from the SIEM provide a list of new or ongoing network vulnerabilities and list them on a scale of priority from high to low, where high priority vulnerabilities have a much shorter deadline for mitigation. |

Một số nhiệm vụ thường xuyênđược thực hiện là bảo trì các quy tắc tường lửa,phân tích nhật ký mạng, cập nhật bản vá và sao lưu máy chủ.Trước đó, bạn đã biết rằng nhật ký là bản ghi củacác sự kiện xảy ra trong hệ thống của một tổ chức.Phân tích nhật ký mạng là quá trìnhkiểm tra nhật ký mạng để xác định các sự kiện quan tâm.Nhóm bảo mật sử dụng công cụ phân tích nhật kýhoặc một công cụ quản lý sự kiện và thông tin bảo mật,còn được gọi là SIEM,để tiến hành phân tích nhật ký mạng.Công cụ SIEM là một ứng dụng thu thập và phân tíchghi dữ liệu để theo dõinhững hoạt động quan trọng trong một tổ chức.Nó thu thập dữ liệu bảo mật từ mạng vàtrình bày dữ liệu đó trên một trang tổng quan duy nhất.Giao diện bảng điều khiển đôi khigọi là một tấm kính duy nhất.SIEM giúp các nhà phân tích kiểm tra, phân tích,và phản ứng với các sự kiện bảo mậttrên toàn mạng dựa trên mức độ ưu tiên của chúng.Các báo cáo từ SIEM cung cấp một danh sáchlỗ hổng mạng mới hoặc đang diễn ravà liệt kê chúng theo thang điểmmức độ ưu tiên từ cao đếnthấp, nơi có lỗ hổng có mức độ ưu tiên caocó thời hạn giảm thiểu ngắn hơn nhiều.

|  |
| --- |
| Now that we've covered tasks that are performed regularly, let's examine tasks that are performed once. These tasks include port filtering on firewalls, network access privileges, and encryption for communication, among many things. Let's start with port filtering. Port filtering can be formed over the network. Port filtering is a firewall function that blocks or allows certain port numbers to limit unwanted communication. A basic principle is that the only ports that are needed are the ones that are allowed. Any port that isn't being used by the normal network operations should be disallowed. This protects against port vulnerabilities. Networks should be set up with the most up-to-date wireless protocols available and older wireless protocols should be disabled. Security analysts also use network segmentation to create isolated subnets for different departments in an organization. For example, they might make one for the marketing department and one for the finance department. This is done so the issues in each subnet don't spread across the whole company and only specified users are given access to the part of the network that they require for their role. Network segmentation may also be used to separate different security zones. Any restricted zone on a network containing highly classified or confidential data should be separate from the rest of the network. Lastly, all network communication should be encrypted using the latest encryption standards. Encryption standards are rules or methods used to conceal outgoing data and uncover or decrypt incoming data. Data in restricted zones should have much higher encryption standards, which makes them more difficult to access. |

Bây giờ chúng ta đã đề cập đến các nhiệm vụđược thực hiện thường xuyên,hãy kiểm tra các nhiệm vụ được thực hiện một lần.Những tác vụ này bao gồm lọc cổng trên tường lửa,đặc quyền truy cập mạng vàmã hóa để liên lạc, trong số nhiều thứ.Hãy bắt đầu với việc lọc cổng.Lọc cổng có thể được hình thành qua mạng.Lọc cổng là một chức năng tường lửa chặn hoặccho phép số cổng nhất địnhđể hạn chế những giao tiếp không mong muốn.Một nguyên tắc cơ bản lànhững cổng duy nhất đượccần thiết là những thứ được phép.Bất kỳ cổng nào không được sử dụng bởicác hoạt động mạng bình thường sẽ không được phép.Điều này bảo vệ chống lại các lỗ hổng cổng.Mạng nên được thiết lập vớicác giao thức không dây cập nhật nhấtcó sẵn vàcác giao thức không dây cũ hơn nên bị vô hiệu hóa.Các nhà phân tích bảo mật cũng sử dụngphân đoạn mạng để tạomạng con bị cô lập chocác phòng ban khác nhau trong một tổ chức.Ví dụ: họ có thể làm một cái chobộ phận tiếp thị vàmột cho bộ phận tài chính.Điều này được thực hiện để các vấn đề trongmỗi mạng con không trải rộng trên toàn bộ công ty vàchỉ những người dùng được chỉ định mới được cấp quyền truy cập vàophần mạng mà họ yêu cầu cho vai trò của mình.Phân đoạn mạng cũng có thể được sử dụngđể phân chia các vùng bảo mật khác nhau.Bất kỳ vùng hạn chế nào trên mạng có chứadữ liệu được phân loại cao hoặc bí mậtnên tách biệt khỏi phần còn lại của mạng.Cuối cùng, tất cả các giao tiếp mạng phải đượcđược mã hóa bằng các tiêu chuẩn mã hóa mới nhất.Tiêu chuẩn mã hóa là các quy tắc hoặc phương pháp được sử dụng đểche giấu dữ liệu đi vàkhám phá hoặc giải mã dữ liệu đến.Dữ liệu trong vùng hạn chế nêncó tiêu chuẩn mã hóa cao hơn nhiều,điều này làm cho việc tiếp cận chúng trở nên khó khăn hơn.

|  |
| --- |
| You've learned about the most common hardening practices. This knowledge will be useful as you complete the certificate program and it's essential to your career as a security analyst. |

Bạn đã tìm hiểu về các phương pháp làm cứng phổ biến nhất.Kiến thức này sẽ hữu ích khi bạn hoàn thànhchương trình chứng chỉ và nócần thiết cho sự nghiệp của bạn với tư cách là nhà phân tích bảo mật.

***3.2. Network security applications – Ứng dụng an ninh mạng***

|  |
| --- |
| **Network security applications** |

**Ứng dụng an ninh mạng**

|  |
| --- |
| This section of the course covers the topic of network hardening and monitoring. Each device, tool, or security strategy put in place by security analysts further protects—or hardens—the network until the network owner is satisfied with the level of security. This approach of adding layers of security to a network is referred to as defense in depth. |

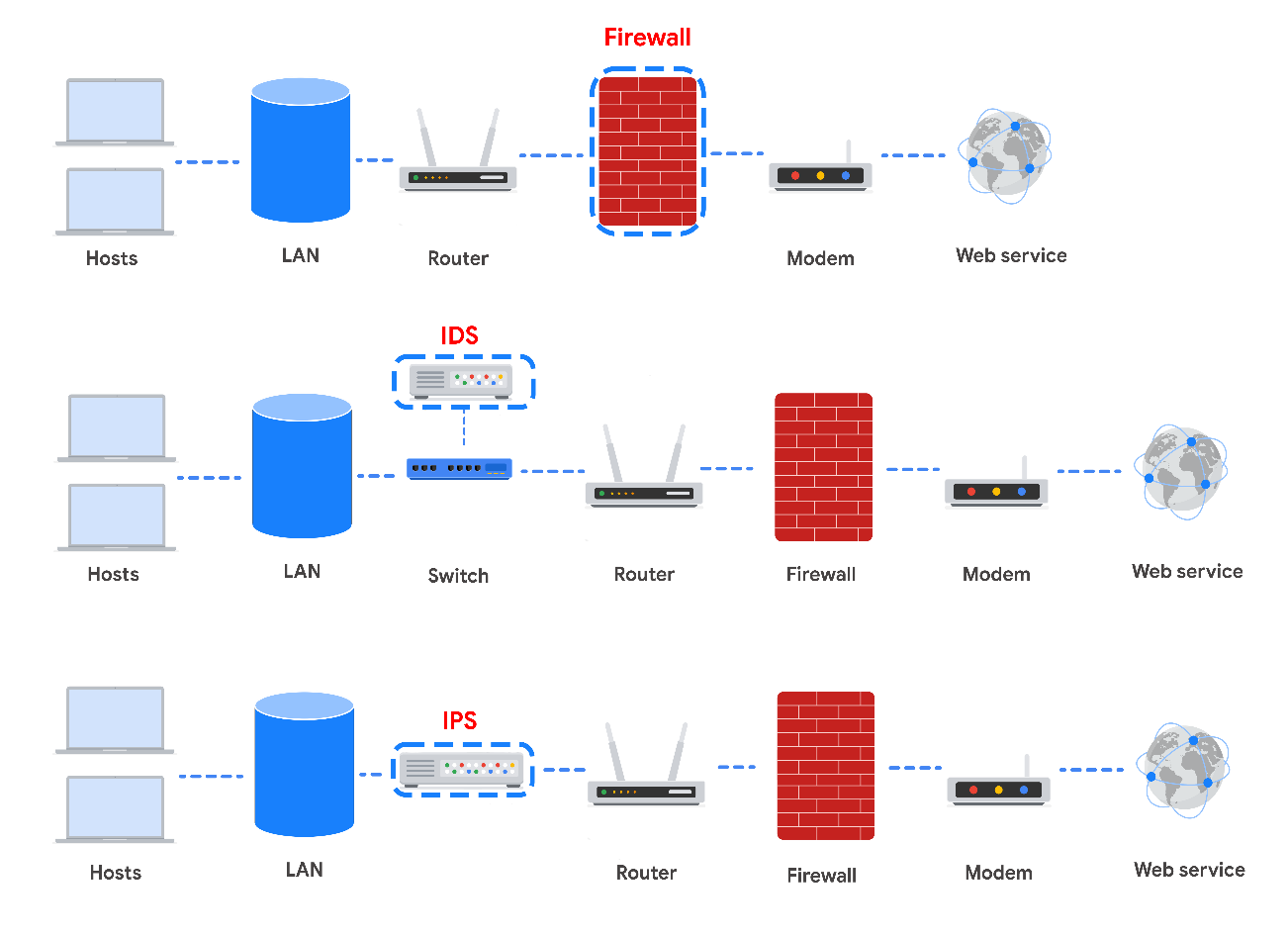
Phần này của khóa học đề cập đến chủ đề tăng cường và giám sát mạng. Mỗi thiết bị, công cụ hoặc chiến lược bảo mật được các nhà phân tích bảo mật đưa ra sẽ bảo vệ thêm—hoặc củng cố—mạng cho đến khi chủ sở hữu mạng hài lòng với mức độ bảo mật. Cách tiếp cận thêm các lớp bảo mật vào mạng này được gọi là phòng thủ theo chiều sâu.

|  |
| --- |
| In this reading, you are going to learn about the role of four devices used to secure a network—firewalls, intrusion detection systems, intrusion prevention systems, and security incident and event management tools. Network security professionals have the choice to use any or all of these devices and tools depending on the level of security that they hope to achieve. |

Trong bài đọc này, bạn sẽ tìm hiểu về vai trò của bốn thiết bị được sử dụng để bảo mật mạng—tường lửa, hệ thống phát hiện xâm nhập, hệ thống ngăn chặn xâm nhập và các công cụ quản lý sự kiện và sự cố bảo mật. Các chuyên gia an ninh mạng có quyền lựa chọn sử dụng bất kỳ hoặc tất cả các thiết bị và công cụ này tùy thuộc vào mức độ bảo mật mà họ hy vọng đạt được.

|  |
| --- |
| This reading will discuss the benefits of layered security. Each tool mentioned is an additional layer of defense that can incrementally harden a network, starting with the minimum level of security (provided by just a firewall), to the highest level of security (provided by combining a firewall, an intrusion detection and prevention device, and security event monitoring). |

Bài đọc này sẽ thảo luận về lợi ích của bảo mật lớp. Mỗi công cụ được đề cập là một lớp bảo vệ bổ sung có thể tăng cường độ cứng của mạng, bắt đầu từ mức bảo mật tối thiểu (chỉ được cung cấp bởi tường lửa), đến mức bảo mật cao nhất (được cung cấp bằng cách kết hợp tường lửa, thiết bị ngăn chặn và phát hiện xâm nhập). và giám sát sự kiện bảo mật).



|  |
| --- |
| Take note of where each tool is located on the network. Each tool has its own place in the network’s architecture. Security analysts are required to understand the network topologies shown in the diagrams throughout this reading. |

Hãy lưu ý vị trí của mỗi công cụ trên mạng. Mỗi công cụ đều có vị trí riêng trong kiến ​​trúc của mạng. Các nhà phân tích bảo mật được yêu cầu phải hiểu cấu trúc liên kết mạng được hiển thị trong sơ đồ trong suốt quá trình đọc này.

|  |
| --- |
| **Firewall** |

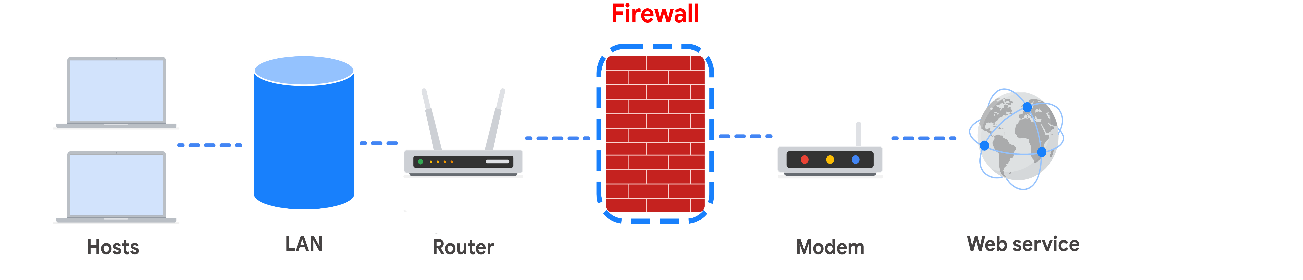
**Bức tường lửa**

|  |
| --- |
| So far in this course, you learned about stateless firewalls, stateful firewalls, and next-generation firewalls (NGFWs), and the security advantages of each of them. |

Cho đến nay trong khóa học này, bạn đã tìm hiểu về tường lửa không trạng thái, tường lửa trạng thái và tường lửa thế hệ tiếp theo (NGFW) cũng như lợi thế bảo mật của từng loại tường lửa đó.

|  |
| --- |
| Most firewalls are similar in their basic functions. Firewalls allow or block traffic based on a set of rules. As data packets enter a network, the packet header is inspected and allowed or denied based on its port number. NGFWs are also able to inspect packet payloads. Each system should have its own firewall, regardless of the network firewall. |

Hầu hết các tường lửa đều giống nhau về chức năng cơ bản. Tường lửa cho phép hoặc chặn lưu lượng truy cập dựa trên một bộ quy tắc. Khi các gói dữ liệu đi vào mạng, tiêu đề gói sẽ được kiểm tra và cho phép hoặc từ chối dựa trên số cổng của nó. NGFW cũng có thể kiểm tra tải trọng gói. Mỗi hệ thống nên có tường lửa riêng, bất kể tường lửa mạng là gì.



|  |
| --- |
| **Intrusion Detection System** |

**Hệ thống phát hiện xâm nhập**

|  |
| --- |
| An **intrusion detection system** (IDS) is an application that monitors system activity and alerts on possible intrusions. An IDS alerts administrators based on the signature of malicious traffic. |

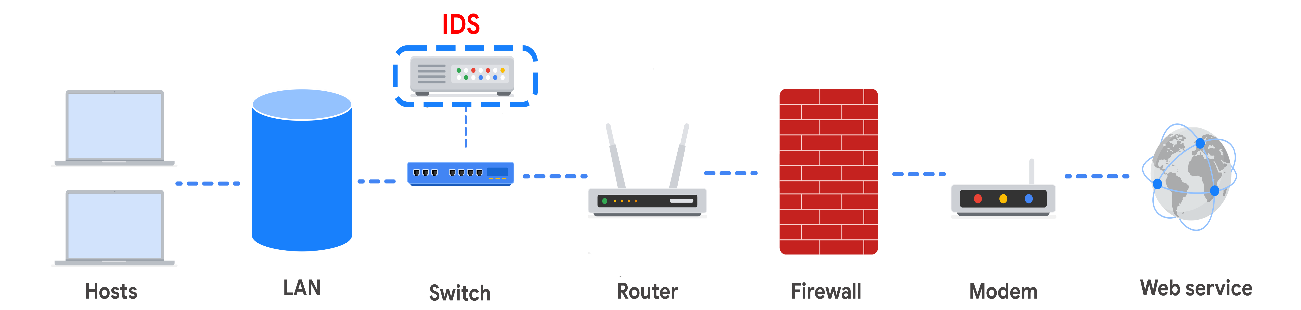
Hệ **thống phát hiện xâm nhập** (IDS) là một ứng dụng giám sát hoạt động của hệ thống và cảnh báo về những xâm nhập có thể xảy ra. IDS cảnh báo quản trị viên dựa trên dấu hiệu của lưu lượng độc hại.

|  |
| --- |
| The IDS is configured to detect known attacks. IDS systems often sniff data packets as they move across the network and analyze them for the characteristics of known attacks. Some IDS systems review not only for signatures of known attacks, but also for anomalies that could be the sign of malicious activity. When the IDS discovers an anomaly, it sends an alert to the network administrator who can then investigate further. |

IDS được cấu hình để phát hiện các cuộc tấn công đã biết. Hệ thống IDS thường đánh hơi các gói dữ liệu khi chúng di chuyển trên mạng và phân tích chúng để tìm ra đặc điểm của các cuộc tấn công đã biết. Một số hệ thống IDS xem xét không chỉ các dấu hiệu của các cuộc tấn công đã biết mà còn xem xét các điểm bất thường có thể là dấu hiệu của hoạt động độc hại. Khi IDS phát hiện ra điều bất thường, nó sẽ gửi cảnh báo đến quản trị viên mạng để họ có thể điều tra thêm.

|  |
| --- |
| The limitations to IDS systems are that they can only scan for known attacks or obvious anomalies. New and sophisticated attacks might not be caught. The other limitation is that the IDS doesn’t actually stop the incoming traffic if it detects something awry. It’s up to the network administrator to catch the malicious activity before it does anything damaging to the network. |

Hạn chế của hệ thống IDS là chúng chỉ có thể quét các cuộc tấn công đã biết hoặc các điểm bất thường rõ ràng. Các cuộc tấn công mới và tinh vi có thể không bị phát hiện. Hạn chế khác là IDS không thực sự dừng lưu lượng truy cập đến nếu phát hiện điều gì đó không ổn. Quản trị viên mạng có trách nhiệm phát hiện hoạt động độc hại trước khi nó thực hiện bất kỳ điều gì gây tổn hại cho mạng.



|  |
| --- |
| When combined with a firewall, an IDS adds another layer of defense. The IDS is placed behind the firewall and before entering the LAN, which allows the IDS to analyze data streams after network traffic that is disallowed by the firewall has been filtered out. This is done to reduce noise in IDS alerts, also referred to as false positives. |

Khi kết hợp với tường lửa, IDS sẽ bổ sung thêm một lớp phòng thủ khác. IDS được đặt phía sau tường lửa và trước khi vào mạng LAN, cho phép IDS phân tích luồng dữ liệu sau khi lưu lượng truy cập mạng không được tường lửa cho phép đã được lọc ra. Điều này được thực hiện để giảm nhiễu trong cảnh báo IDS, còn được gọi là báo động sai.

|  |
| --- |
| **Intrusion Prevention System** |

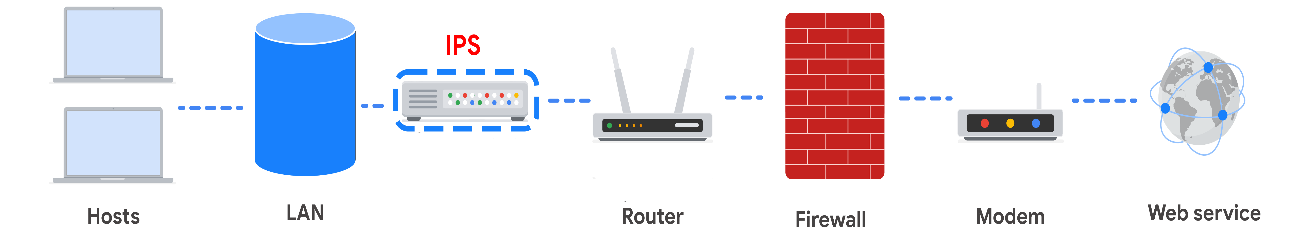
**Hệ thống ngăn chặn xâm nhập**

|  |
| --- |
| An **intrusion prevention system (IPS)** is an application that monitors system activity for intrusive activity and takes action to stop the activity. It offers even more protection than an IDS because it actively stops anomalies when they are detected, unlike the IDS that simply reports the anomaly to a network administrator. |

Hệ **thống ngăn chặn xâm nhập (IPS)** là một ứng dụng giám sát hoạt động của hệ thống để phát hiện hoạt động xâm nhập và thực hiện hành động để dừng hoạt động đó. Nó thậm chí còn cung cấp khả năng bảo vệ cao hơn IDS vì nó chủ động ngăn chặn các điểm bất thường khi chúng được phát hiện, không giống như IDS chỉ báo cáo sự bất thường cho quản trị viên mạng.

|  |
| --- |
| An IPS searches for signatures of known attacks and data anomalies. An IPS reports the anomaly to security analysts and blocks a specific sender or drops network packets that seem suspect. |

IPS tìm kiếm dấu hiệu của các cuộc tấn công đã biết và dữ liệu bất thường. IPS báo cáo sự bất thường cho các nhà phân tích bảo mật và chặn một người gửi cụ thể hoặc loại bỏ các gói mạng có vẻ đáng ngờ.



|  |
| --- |
| The IPS (like an IDS) sits behind the firewall in the network architecture. This offers a high level of security because risky data streams are disrupted before they even reach sensitive parts of the network. However, one potential limitation is that it is inline: If it breaks, the connection between the private network and the internet breaks. Another limitation of IPS is the possibility of false positives, which can result in legitimate traffic getting dropped. |

IPS (giống như IDS) nằm phía sau tường lửa trong kiến ​​trúc mạng. Điều này mang lại mức độ bảo mật cao vì các luồng dữ liệu rủi ro bị gián đoạn trước khi chúng đến được các phần nhạy cảm của mạng. Tuy nhiên, một hạn chế tiềm tàng là nó hoạt động nội tuyến: Nếu nó bị hỏng, kết nối giữa mạng riêng và internet sẽ bị ngắt. Một hạn chế khác của IPS là khả năng xảy ra kết quả dương tính giả, điều này có thể dẫn đến việc giảm lưu lượng truy cập hợp pháp.

|  |
| --- |
| **Full packet capture devices** |

**Thiết bị chụp gói đầy đủ**

|  |
| --- |
| Full packet capture devices can be incredibly useful for network administrators and security professionals. These devices allow you to record and analyze all of the data that is transmitted over your network. They also aid in investigating alerts created by an IDS. |

Các thiết bị chụp gói đầy đủ có thể cực kỳ hữu ích cho quản trị viên mạng và chuyên gia bảo mật. Các thiết bị này cho phép bạn ghi lại và phân tích tất cả dữ liệu được truyền qua mạng của bạn. Chúng cũng hỗ trợ điều tra các cảnh báo do IDS tạo ra.

|  |
| --- |
| **Security Information and Event Management** |

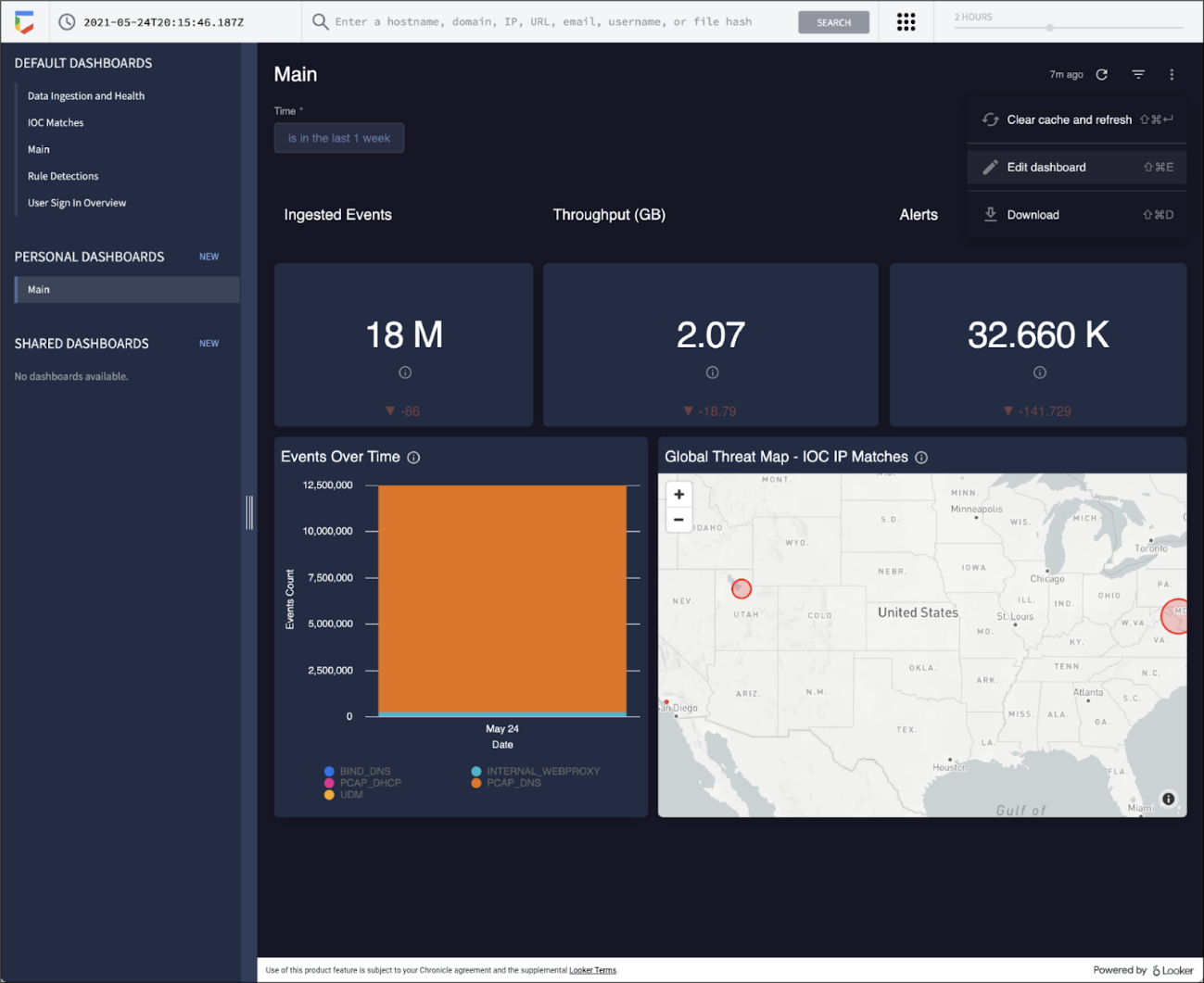
**Quản lý sự kiện và thông tin bảo mật**

|  |
| --- |
| A **security information and event management system (SIEM)** is an application that collects and analyzes log data to monitor critical activities in an organization. SIEM tools work in real time to report suspicious activity in a centralized dashboard. SIEM tools additionally analyze network log data sourced from IDSs, IPSs, firewalls, VPNs, proxies, and DNS logs. SIEM tools are a way to aggregate security event data so that it all appears in one place for security analysts to analyze. This is referred to as a single pane of glass. |

Hệ **thống quản lý sự kiện và thông tin bảo mật (SIEM)** là một ứng dụng thu thập và phân tích dữ liệu nhật ký để giám sát các hoạt động quan trọng trong một tổ chức. Các công cụ SIEM hoạt động theo thời gian thực để báo cáo hoạt động đáng ngờ trong bảng điều khiển tập trung. Các công cụ SIEM còn phân tích thêm dữ liệu nhật ký mạng có nguồn gốc từ IDS, IPS, tường lửa, VPN, proxy và nhật ký DNS. Các công cụ SIEM là một cách tổng hợp dữ liệu sự kiện bảo mật để tất cả dữ liệu đó xuất hiện ở một nơi để các nhà phân tích bảo mật phân tích. Điều này được gọi là một tấm kính duy nhất.

|  |
| --- |
| Below, you can review an example of a dashboard from Google Cloud’s SIEM tool, Chronicle. **Chronicle** is a cloud-native tool designed to retain, analyze, and search data. |

Dưới đây, bạn có thể xem lại ví dụ về trang tổng quan từ công cụ SIEM của Google Cloud, Chronicle. **Chronicle** là một công cụ dựa trên đám mây được thiết kế để lưu giữ, phân tích và tìm kiếm dữ liệu.



|  |
| --- |
| **Splunk** is another common SIEM tool. Splunk offers different SIEM tool options: Splunk Enterprise and Splunk Cloud. Both options include detailed dashboards which help security professionals to review and analyze an organization's data. There are also other similar SIEM tools available, and it's important for security professionals to research the different tools to determine which one is most beneficial to the organization. |

**Splunk** là một công cụ SIEM phổ biến khác. Splunk cung cấp các tùy chọn công cụ SIEM khác nhau: Splunk Enterprise và Splunk Cloud. Cả hai tùy chọn đều bao gồm bảng thông tin chi tiết giúp các chuyên gia bảo mật xem xét và phân tích dữ liệu của tổ chức. Ngoài ra còn có các công cụ SIEM tương tự khác và điều quan trọng là các chuyên gia bảo mật phải nghiên cứu các công cụ khác nhau để xác định công cụ nào có lợi nhất cho tổ chức.

|  |
| --- |
| A SIEM tool doesn’t replace the expertise of security analysts, or of the network- and system-hardening activities covered in this course, but they’re used in combination with other security methods. Security analysts often work in a Security Operations Center (SOC) where they can monitor the activity across the network. They can then use their expertise and experience to determine how to respond to the information on the dashboard and decide when the events meet the criteria to be escalated to oversight. |

Công cụ SIEM không thay thế chuyên môn của các nhà phân tích bảo mật hoặc các hoạt động tăng cường mạng và hệ thống được đề cập trong khóa học này nhưng chúng được sử dụng kết hợp với các phương pháp bảo mật khác. Các nhà phân tích bảo mật thường làm việc trong Trung tâm điều hành bảo mật (SOC) nơi họ có thể giám sát hoạt động trên mạng. Sau đó, họ có thể sử dụng chuyên môn và kinh nghiệm của mình để xác định cách phản hồi thông tin trên bảng thông tin và quyết định thời điểm các sự kiện đáp ứng tiêu chí sẽ được chuyển lên cấp giám sát.

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

**Bài học chính**

|  |  |  |
| --- | --- | --- |
| **Devices / Tools** | **Advantages** | **Disadvantages** |
| Firewall | A firewall allows or blocks traffic based on a set of rules. | A firewall is only able to filter packets based on information provided in the header of the packets. |
| Intrusion Detection System (IDS) | An IDS detects and alerts admins about possible intrusions, attacks, and other malicious traffic. | An IDS can only scan for known attacks or obvious anomalies; new and sophisticated attacks might not be caught. It doesn’t actually stop the incoming traffic. |
| Intrusion Prevention System (IPS) | An IPS monitors system activity for intrusions and anomalies and takes action to stop them. | An IPS is an inline appliance. If it fails, the connection between the private network and the internet breaks. It might detect false positives and block legitimate traffic. |
| Security Information and Event Management (SIEM) | A SIEM tool collects and analyzes log data from multiple network machines. It aggregates security events for monitoring in a central dashboard. | A SIEM tool only reports on possible security issues. It does not take any actions to stop or prevent suspicious events. |

|  |  |  |
| --- | --- | --- |
| **Thiết bị / Công cụ** | **Thuận lợi** | **Nhược điểm** |
| Bức tường lửa | Tường lửa cho phép hoặc chặn lưu lượng truy cập dựa trên một bộ quy tắc. | Tường lửa chỉ có thể lọc các gói dựa trên thông tin được cung cấp trong tiêu đề của gói. |
| Hệ thống phát hiện xâm nhập (IDS) | IDS phát hiện và cảnh báo quản trị viên về các hành vi xâm nhập, tấn công có thể xảy ra và lưu lượng độc hại khác. | IDS chỉ có thể quét các cuộc tấn công đã biết hoặc các điểm bất thường rõ ràng; các cuộc tấn công mới và tinh vi có thể không bị phát hiện. Nó không thực sự ngăn chặn lưu lượng truy cập đến. |
| Hệ thống ngăn chặn xâm nhập (IPS) | IPS giám sát hoạt động của hệ thống để phát hiện các hành vi xâm nhập và bất thường và thực hiện hành động để ngăn chặn chúng. | IPS là một thiết bị nội tuyến. Nếu thất bại, kết nối giữa mạng riêng và internet sẽ bị ngắt. Nó có thể phát hiện các kết quả dương tính giả và chặn lưu lượng truy cập hợp pháp. |
| Quản lý sự kiện và thông tin bảo mật (SIEM) | Công cụ SIEM thu thập và phân tích dữ liệu nhật ký từ nhiều máy mạng. Nó tổng hợp các sự kiện bảo mật để theo dõi trong bảng điều khiển trung tâm. | Công cụ SIEM chỉ báo cáo về các vấn đề bảo mật có thể xảy ra. Nó không thực hiện bất kỳ hành động nào để ngăn chặn hoặc ngăn chặn các sự kiện đáng ngờ. |

|  |
| --- |
| Each of these devices or tools cost money to purchase, install, and maintain. An organization might need to hire additional personnel to monitor the security tools, as in the case of a SIEM. Decision-makers are tasked with selecting the appropriate level of security based on cost and risk to the organization. You will learn more about choosing levels of security later in the course. |

Mỗi thiết bị hoặc công cụ này đều tốn tiền để mua, cài đặt và bảo trì. Một tổ chức có thể cần thuê thêm nhân sự để giám sát các công cụ bảo mật, như trong trường hợp SIEM. Những người ra quyết định có nhiệm vụ lựa chọn mức độ bảo mật phù hợp dựa trên chi phí và rủi ro cho tổ chức. Bạn sẽ tìm hiểu thêm về cách chọn mức độ bảo mật ở phần sau của khóa học.

***3.3. Activity: Analysis of network hardening – Hoạt động: Phân tích độ tăng cường của mạng***

***3.4. Activity Exemplar: Analysis of network hardening – Ví dụ hoạt động: Phân tích độ tăng cường của mạng***

***3.5. Test your knowledge: Network hardening – Kiểm tra kiến ​​thức của bạn: Tăng cường mạng***

**4. Cloud hardening – Tăng cường đám mây**

***4.1. Network security in the cloud – An ninh mạng trên đám mây***

|  |
| --- |
| In recent years, many organizations are using network services in the cloud. So in addition to securing on-premises networks, a security analyst will need to secure cloud networks. In a previous video, you learned that a cloud network is a collection of servers or computers that stores resources and data in a remote data center that can be accessed via the internet. They can host company data and applications using cloud computing to provide on-demand storage, processing power, and data analytics. Just like regular web servers, cloud servers also require proper maintenance done through various security hardening procedures. Although cloud servers are hosted by a cloud service provider, these providers cannot prevent intrusions in the cloud—especially intrusions from malicious actors, both internal and external to an organization. |

Trong những năm gần đây, nhiều tổ chức đang sử dụng dịch vụ mạng trên nền tảng đám mây.Vì vậy, ngoài việc bảo mật mạng tại chỗ,một nhà phân tích bảo mật sẽ cần bảo mật mạng đám mây.Trong video trước, bạn đã biết rằng mạng đám mây là một tập hợpmáy chủ hoặc máy tính lưu trữ tài nguyên vàdữ liệu trong một trung tâm dữ liệu từ xa có thể được truy cập qua internet.Họ có thể lưu trữ dữ liệu và ứng dụng của công ty bằng cách sử dụng điện toán đám mây đểcung cấp khả năng lưu trữ, sức mạnh xử lý và phân tích dữ liệu theo yêu cầu.Cũng giống như các máy chủ web thông thường, máy chủ đám mây cũng cần được bảo trì thích hợpđược thực hiện thông qua các thủ tục tăng cường bảo mật khác nhau.Mặc dù các máy chủ đám mây được lưu trữ bởi nhà cung cấp dịch vụ đám mây,những nhà cung cấp này không thể ngăn chặn sự xâm nhập vàođám mây—đặc biệt là sự xâm nhập từ các tác nhân độc hại, cả nội bộ vàbên ngoài một tổ chức.

|  |
| --- |
| One distinction between cloud network hardening and traditional network hardening is the use of a server baseline image for all server instances stored in the cloud. This allows you to compare data in the cloud servers to the baseline image to make sure there haven't been any unverified changes. An unverified change could come from an intrusion in the cloud network. Similar to OS hardening, data and applications on a cloud network are kept separate depending on their service category. For example, older applications should be kept separate from newer applications, and software that deals with internal functions should be kept separate from front-end applications seen by users. |

Một điểm khác biệt giữa việc tăng cường mạng lưới đám mây vàtăng cường mạng truyền thống là việc sử dụng hình ảnh cơ sở của máy chủ chotất cả các phiên bản máy chủ được lưu trữ trên đám mây.Điều này cho phép bạn so sánh dữ liệu trong máy chủ đám mây với hình ảnh cơ sở đểđảm bảo không có bất kỳ thay đổi nào chưa được xác minh.Một thay đổi chưa được xác minh có thể đến từ sự xâm nhập vào mạng đám mây.Tương tự như việc tăng cường hệ điều hành, dữ liệu và ứng dụng trên mạng đám mây được lưu giữriêng biệt tùy thuộc vào loại dịch vụ của họ.Ví dụ: các ứng dụng cũ hơn phải được tách biệt khỏi các ứng dụng mới hơn,và phần mềm liên quan đến các chức năng nội bộ phải được giữ riêng biệttừ các ứng dụng front-end mà người dùng nhìn thấy.

|  |
| --- |
| Even though the cloud service provider has a shared responsibility with the organization using their services, there are still security measures that need to be taken by the organization to make sure their cloud network is safe. Just like traditional networks, operations in the cloud need to be secured. You're doing great! Meet you in the next video. |

Mặc dù nhà cung cấp dịch vụ đám mây có trách nhiệm chung vớitổ chức sử dụng dịch vụ của họ vẫn có những biện pháp bảo mậttổ chức cần phải thực hiện để đảm bảo mạng đám mây của họ được an toàn.Cũng giống như các mạng truyền thống, hoạt động trên đám mây cần được bảo mật.Bạn đang làm rất tốt! Hẹn gặp lại các bạn ở video tiếp theo.

***4.2. Kelsey: Cloud security explained – Kelsey: Giải thích về bảo mật đám mây***

|  |
| --- |
| [MUSIC] I'm Kelsey, I'm a distinguished engineer at Google Cloud. I work on compute platforms and security related topics. When I was starting, the only jobs I had previous, the only jobs I was confident were accessible to me were fast food jobs. I wanted a career, I wanted more than just a job. So when I zoomed out and asked myself, what were my career options? I couldn't think of a better place in the year 1999 than going into the world of technologies. I mean, on the news people were lining up for the latest operating system. All the tech people were the new rock stars. And I remember flipping through the opening jobs or the job openings in the classified section, and it said anyone that has one of these certifications let us know because we're hiring. The delta between getting started and getting your first job into that career that I always wanted, it was $35 away in a certification book. So let's talk about Cloud. So before the time of Cloud, most companies had their own data center. Imagine it's just you alone in your house, you can put anything wherever you want. You may choose to never lock the doors on the inside, it's just you. And for a long time in our industry, that's the way people ran their data centers. Now, we just call that private Cloud, it's just you there. But Cloud is public. And so the analogy would be, imagine getting roommates, now you start to think differently about your stuff. You start to lock things up even while you're inside of the house, and your security discipline is going to be very different. As more and more companies move into Cloud. You may just be the person who can help one of those organizations finally make that leap because they have a professional on their team. All right, so you've gotten the certification, you've gotten the fundamental skills, how do you make sure that you can actually use them in the Cloud? I'm going to let you in a little secret. Go use the Cloud. Go take existing software, throw it in the Cloud, and find all the tools that poke and prod at the thing you just got running and it's going to tell you where you're weak. Learn those tools, because those are the tools that the professionals use. Learning is a superpower. It gives you the ability to not only get that job that you've been looking at, but it also gives you the ability to define the next one. [MUSIC] |

[ÂM NHẠC]Tôi là Kelsey, tôi là kỹ sư xuất sắc tại Google Cloud.Tôi làm việc trên nền tảng điện toán và các chủ đề liên quan đến bảo mật.Khi tôi mới bắt đầu, công việc duy nhất tôi có trước đây,công việc duy nhất mà tôi tin tưởng là mình có thể tiếp cận được là công việc bán đồ ăn nhanh.Tôi muốn có một sự nghiệp, tôi muốn nhiều hơn chỉ là một công việc.Vì vậy, khi tôi thu nhỏ và tự hỏi bản thân, lựa chọn nghề nghiệp của tôi là gì?Tôi không thể nghĩ ra nơi nào tốt hơn vào năm 1999 ngoài việc bước vào thế giớicủa các công nghệ.Ý tôi là, trên tin tức mọi người đang xếp hàng để mua hệ điều hành mới nhất.Tất cả dân công nghệ đều là những ngôi sao nhạc rock mới.Và tôi nhớ đã lướt qua các công việc mở đầu hoặccác cơ hội việc làm trong phần phân loại và nó cho biết bất kỳ ai có cơ hội việc làmtrong số những chứng chỉ này hãy cho chúng tôi biết vì chúng tôi đang tuyển dụng.Khoảng cách giữa việc bắt đầu vàcó được công việc đầu tiên trong sự nghiệp mà tôi luôn mong muốn,đó là 35 đô la trong sổ chứng nhận.Vậy hãy nói về Cloud.Vì vậy trước thời Cloud, hầu hết các công ty đều có trung tâm dữ liệu riêng.Hãy tưởng tượng chỉ có bạn trong nhà, bạn có thể đặt bất cứ thứ gì bạn muốn.Bạn có thể chọn không bao giờ khóa cửa bên trong, chỉ có bạn thôi.Và trong một thời gian dài trong ngành của chúng tôi,đó là cách mọi người vận hành trung tâm dữ liệu của họ.Bây giờ chúng ta chỉ gọi đó là Đám mây riêng tư, chỉ có bạn ở đó.Nhưng Cloud là công khai.Và sự tương tự sẽ là, hãy tưởng tượng việc có bạn cùng phòng,bây giờ bạn bắt đầu nghĩ khác về đồ đạc của mình.Bạn bắt đầu khóa mọi thứ ngay cả khi bạn đang ở trong nhà, vàkỷ luật an ninh của bạn sẽ rất khác.Khi ngày càng có nhiều công ty chuyển sang Đám mây.Bạn có thể chỉ là người có thể giúp một trong những tổ chức đó cuối cùng thực hiện đượcbước nhảy vọt đó bởi vì họ có một chuyên gia trong đội của họ.Được rồi, vậy là bạn đã nhận được giấy chứng nhận,bạn đã có được những kỹ năng cơ bản,làm cách nào để đảm bảo rằng bạn thực sự có thể sử dụng chúng trên Đám mây?Tôi sẽ cho bạn biết một bí mật nhỏ.Hãy sử dụng Đám mây.Hãy lấy phần mềm hiện có, đưa nó vào Đám mây vàtìm tất cả các công cụ chọc vào thứ bạn vừa chạy vànó sẽ cho bạn biết bạn yếu ở đâu.Hãy tìm hiểu những công cụ đó vì đó là những công cụ mà các chuyên gia sử dụng.Học tập là một siêu năng lực.Nó mang đến cho bạn khả năng không chỉ có được công việc mà bạn đang tìm kiếm,nhưng nó cũng cung cấp cho bạn khả năng xác định cái tiếp theo.[ÂM NHẠC]

***4.3. Secure the cloud – Bảo mật đám mây***

|  |
| --- |
| **Secure the cloud** |

**Bảo mật đám mây**

|  |
| --- |
| Earlier in this course, you were introduced to [cloud computing](https://www.coursera.org/learn/networks-and-network-security/lecture/BGlnq/cloud-networks). **Cloud computing** is a model for allowing convenient and on-demand network access to a shared pool of configurable computing resources. These resources can be configured and released with minimal management effort or interaction with the service provider. |

Trước đó trong khóa học này, bạn đã được giới thiệu về[điện toán đám mây](https://www.coursera.org/learn/networks-and-network-security/lecture/BGlnq/cloud-networks). **Điện toán đám mây** là mô hình cho phép truy cập mạng thuận tiện và theo yêu cầu vào nhóm tài nguyên máy tính có thể định cấu hình chung. Các tài nguyên này có thể được cấu hình và giải phóng với nỗ lực quản lý hoặc tương tác tối thiểu với nhà cung cấp dịch vụ.

|  |
| --- |
| Just like any other IT infrastructure, a cloud infrastructure needs to be secured. This reading will address some main security considerations that are unique to the cloud and introduce you to the shared responsibility model used for security in the cloud. Many organizations that use cloud resources and infrastructure express concerns about the privacy of their data and resources. This concern is addressed through cryptography and other additional security measures, which will be discussed later in this course. |

Cũng giống như bất kỳ cơ sở hạ tầng CNTT nào khác, cơ sở hạ tầng đám mây cần được bảo mật. Bài đọc này sẽ đề cập đến một số cân nhắc bảo mật chính dành riêng cho đám mây và giới thiệu cho bạn mô hình trách nhiệm chung được sử dụng để bảo mật trong đám mây. Nhiều tổ chức sử dụng tài nguyên và cơ sở hạ tầng đám mây bày tỏ lo ngại về quyền riêng tư của dữ liệu và tài nguyên của họ. Mối lo ngại này được giải quyết thông qua mật mã và các biện pháp bảo mật bổ sung khác, sẽ được thảo luận sau trong khóa học này.

|  |
| --- |
| **Cloud security considerations** |

**Cân nhắc về bảo mật đám mây**

|  |
| --- |
| Many organizations choose to use cloud services because of the ease of deployment, speed of deployment, cost savings, and scalability of these options. Cloud computing presents unique security challenges that cybersecurity analysts need to be aware of. |

Nhiều tổ chức chọn sử dụng dịch vụ đám mây vì tính dễ triển khai, tốc độ triển khai, tiết kiệm chi phí và khả năng mở rộng của các tùy chọn này. Điện toán đám mây đặt ra những thách thức bảo mật đặc biệt mà các nhà phân tích an ninh mạng cần lưu ý.

|  |
| --- |
| **Identity access management** |

**Quản lý truy cập danh tính**

|  |
| --- |
| **Identity access management (IAM)** is a collection of processes and technologies that helps organizations manage digital identities in their environment. This service also authorizes how users can use different cloud resources. A common problem that organizations face when using the cloud is the loose configuration of cloud user roles. An improperly configured user role increases risk by allowing unauthorized users to have access to critical cloud operations. |

**Quản lý truy cập danh tính (IAM)** là tập hợp các quy trình và công nghệ giúp các tổ chức quản lý danh tính kỹ thuật số trong môi trường của họ. Dịch vụ này cũng cho phép người dùng có thể sử dụng các tài nguyên đám mây khác nhau. Một vấn đề phổ biến mà các tổ chức gặp phải khi sử dụng đám mây là cấu hình lỏng lẻo về vai trò của người dùng trên đám mây. Vai trò người dùng được định cấu hình không đúng sẽ làm tăng rủi ro khi cho phép người dùng trái phép có quyền truy cập vào các hoạt động quan trọng trên đám mây.

|  |
| --- |
| **Configuration** |

**Cấu hình**

|  |
| --- |
| The number of available cloud services adds complexity to the network. Each service must be carefully configured to meet security and compliance requirements. This presents a particular challenge when organizations perform an initial migration into the cloud. When this change occurs on their network, they must ensure that every process moved into the cloud has been configured correctly. If network administrators and architects are not meticulous in correctly configuring the organization’s cloud services, they could leave the network open to compromise. Misconfigured cloud services are a common source of cloud security issues. |

Số lượng dịch vụ đám mây có sẵn làm tăng thêm độ phức tạp cho mạng. Mỗi dịch vụ phải được cấu hình cẩn thận để đáp ứng các yêu cầu về bảo mật và tuân thủ. Điều này đặt ra một thách thức cụ thể khi các tổ chức thực hiện quá trình di chuyển ban đầu vào đám mây. Khi thay đổi này xảy ra trên mạng của họ, họ phải đảm bảo rằng mọi quy trình được chuyển vào đám mây đều được định cấu hình chính xác. Nếu quản trị viên và kiến ​​trúc sư mạng không tỉ mỉ trong việc định cấu hình chính xác các dịch vụ đám mây của tổ chức, họ có thể khiến mạng bị xâm phạm. Các dịch vụ đám mây bị định cấu hình sai là nguyên nhân phổ biến gây ra các vấn đề về bảo mật đám mây.

|  |
| --- |
| **Attack surface** |

**Bề mặt tấn công**

|  |
| --- |
| Cloud service providers (CSPs) offer numerous applications and services for organizations at a low cost. |

Các nhà cung cấp dịch vụ đám mây (CSP) cung cấp nhiều ứng dụng và dịch vụ cho các tổ chức với chi phí thấp.

|  |
| --- |
| Every service or application on a network carries its own set of risks and vulnerabilities and increases an organization’s overall attack surface. An increased attack surface must be compensated for with increased security measures. |

Mỗi dịch vụ hoặc ứng dụng trên mạng đều có những rủi ro và lỗ hổng riêng, đồng thời làm tăng bề mặt tấn công tổng thể của tổ chức. Bề mặt tấn công gia tăng phải được bù đắp bằng các biện pháp bảo mật tăng cường.

|  |
| --- |
| Cloud networks that utilize many services introduce lots of entry points into an organization’s network. However, if the network is designed correctly, utilizing several services does not introduce more entry points into an organization’s network design. These entry points can be used to introduce malware onto the network and pose other security vulnerabilities. It is important to note that CSPs often defer to more secure options, and have undergone more scrutiny than a traditional on-premises network. |

Mạng đám mây sử dụng nhiều dịch vụ sẽ đưa ra nhiều điểm vào mạng của tổ chức. Tuy nhiên, nếu mạng được thiết kế chính xác, việc sử dụng nhiều dịch vụ sẽ không tạo ra nhiều điểm truy cập hơn vào thiết kế mạng của tổ chức. Những điểm truy cập này có thể được sử dụng để đưa phần mềm độc hại vào mạng và gây ra các lỗ hổng bảo mật khác. Điều quan trọng cần lưu ý là CSP thường sử dụng các tùy chọn an toàn hơn và đã trải qua quá trình xem xét kỹ lưỡng hơn so với mạng tại chỗ truyền thống.

|  |
| --- |
| **Zero-day attacks** |

**Các cuộc tấn công zero-day**

|  |
| --- |
| Zero-day attacks are an important security consideration for organizations using cloud or traditional on-premise network solutions. A **zero day** attack is an exploit that was previously unknown. CSPs are more likely to know about a zero day attack occurring before a traditional IT organization does. CSPs have ways of patching hypervisors and migrating workloads to other virtual machines. These methods ensure the customers are not impacted by the attack. There are also several tools available for patching at the operating system level that organizations can use. |

Các cuộc tấn công zero-day là một vấn đề bảo mật quan trọng cần cân nhắc đối với các tổ chức sử dụng giải pháp mạng tại chỗ truyền thống hoặc đám mây. Cuộc tấn công **zero day** là một cách khai thác chưa từng được biết đến trước đây. CSP có nhiều khả năng biết về cuộc tấn công zero day xảy ra trước khi tổ chức CNTT truyền thống biết. CSP có cách vá các bộ ảo hóa và di chuyển khối lượng công việc sang các máy ảo khác. Những phương pháp này đảm bảo khách hàng không bị ảnh hưởng bởi cuộc tấn công. Ngoài ra còn có một số công cụ có sẵn để vá lỗi ở cấp hệ điều hành mà các tổ chức có thể sử dụng.

|  |
| --- |
| **Visibility and tracking** |

**Khả năng hiển thị và theo dõi**

|  |
| --- |
| Network administrators have access to every data packet crossing the network with both on-premise and cloud networks. They can sniff and inspect data packets to learn about network performance or to check for possible threats and attacks. |

Quản trị viên mạng có quyền truy cập vào mọi gói dữ liệu qua mạng bằng cả mạng tại chỗ và mạng đám mây. Họ có thể đánh hơi và kiểm tra các gói dữ liệu để tìm hiểu về hiệu suất mạng hoặc kiểm tra các mối đe dọa và cuộc tấn công có thể xảy ra.

|  |
| --- |
| This kind of visibility is also offered in the cloud through flow logs and tools, such as packet mirroring. CSPs take responsibility for security in the cloud, but they do not allow the organizations that use their infrastructure to monitor traffic on the CSP’s servers. Many CSPs offer strong security measures to protect their infrastructure. Still, this situation might be a concern for organizations that are accustomed to having full access to their network and operations. CSPs pay for third-party audits to verify how secure a cloud network is and identify potential vulnerabilities. The audits can help organizations identify whether any vulnerabilities originate from on-premise infrastructure and if there are any compliance lapses from their CSP. |

Loại khả năng hiển thị này cũng được cung cấp trên đám mây thông qua các công cụ và nhật ký luồng, chẳng hạn như phản chiếu gói. CSP chịu trách nhiệm về bảo mật trên đám mây, nhưng họ không cho phép các tổ chức sử dụng cơ sở hạ tầng của họ giám sát lưu lượng truy cập trên máy chủ của CSP. Nhiều CSP cung cấp các biện pháp bảo mật mạnh mẽ để bảo vệ cơ sở hạ tầng của họ. Tuy nhiên, tình huống này có thể là mối lo ngại đối với các tổ chức đã quen với việc có toàn quyền truy cập vào mạng và hoạt động của họ. CSP trả tiền cho hoạt động kiểm tra của bên thứ ba để xác minh mức độ an toàn của mạng đám mây và xác định các lỗ hổng tiềm ẩn. Việc kiểm tra có thể giúp các tổ chức xác định xem có bất kỳ lỗ hổng nào bắt nguồn từ cơ sở hạ tầng tại chỗ hay không và liệu có bất kỳ sai sót tuân thủ nào từ CSP của họ hay không.

|  |
| --- |
| **Things change fast in the cloud** |

**Mọi thứ thay đổi nhanh chóng trên đám mây**

|  |
| --- |
| CSPs are large organizations that work hard to stay up-to-date with technology advancements. For organizations that are used to being in control of any adjustments made to their network, this can be a potential challenge to keep up with. Cloud service updates can affect security considerations for the organizations using them. For example, connection configurations might need to be changed based on the CSP’s updates. |

CSP là các tổ chức lớn làm việc chăm chỉ để cập nhật những tiến bộ công nghệ. Đối với các tổ chức đã quen với việc kiểm soát mọi điều chỉnh được thực hiện đối với mạng của họ, đây có thể là một thách thức tiềm ẩn cần theo kịp. Các bản cập nhật dịch vụ đám mây có thể ảnh hưởng đến những cân nhắc về bảo mật cho các tổ chức sử dụng chúng. Ví dụ: có thể cần thay đổi cấu hình kết nối dựa trên các bản cập nhật của CSP.

|  |
| --- |
| Organizations that use CSPs usually have to update their IT processes. It is possible for organizations to continue following established best practices for changes, configurations, and other security considerations. However, an organization might have to adopt a different approach in a way that aligns with changes made by the CSP. |

Các tổ chức sử dụng CSP thường phải cập nhật quy trình CNTT của họ. Các tổ chức có thể tiếp tục tuân theo các biện pháp thực hành tốt nhất đã được thiết lập đối với các thay đổi, cấu hình và các cân nhắc bảo mật khác. Tuy nhiên, tổ chức có thể phải áp dụng một cách tiếp cận khác sao cho phù hợp với những thay đổi do CSP thực hiện.

|  |
| --- |
| Cloud networking offers various options that might appear attractive to a small company—options that they could never afford to build on their own premises. However, it is important to consider that each service adds complexity to the security profile of the organization, and they will need security personnel to monitor all of the cloud services. |

Mạng đám mây cung cấp nhiều tùy chọn khác nhau có vẻ hấp dẫn đối với một công ty nhỏ—các tùy chọn mà họ không bao giờ có đủ khả năng để xây dựng trên cơ sở của mình. Tuy nhiên, điều quan trọng cần lưu ý là mỗi dịch vụ sẽ làm tăng thêm độ phức tạp cho hồ sơ bảo mật của tổ chức và họ sẽ cần nhân viên bảo mật giám sát tất cả các dịch vụ đám mây.

|  |
| --- |
| **Shared responsibility model** |

**Mô hình chia sẻ trách nhiệm**

|  |
| --- |
| A commonly accepted cloud security principle is the shared responsibility model. The **shared responsibility model** states that the CSP must take responsibility for security involving the cloud infrastructure, including physical data centers, hypervisors, and host operating systems. The company using the cloud service is responsible for the assets and processes that they store or operate in the cloud. |

Nguyên tắc bảo mật đám mây được chấp nhận rộng rãi là mô hình chia sẻ trách nhiệm. Mô **hình trách nhiệm chung** nêu rõ rằng CSP phải chịu trách nhiệm về bảo mật liên quan đến cơ sở hạ tầng đám mây, bao gồm các trung tâm dữ liệu vật lý, bộ ảo hóa và hệ điều hành máy chủ. Công ty sử dụng dịch vụ đám mây chịu trách nhiệm về tài sản và quy trình mà họ lưu trữ hoặc vận hành trên đám mây.

|  |
| --- |
| The shared responsibility model ensures that both the CSP and the users agree about where their responsibility for security begins and ends. A problem occurs when organizations assume that the CSP is taking care of security that they have not taken responsibility for. One example of this is cloud applications and configurations. The CSP takes responsibility for securing the cloud, but it is the organization’s responsibility to ensure that services are configured properly according to the security requirements of their organization. |

Mô hình trách nhiệm chung đảm bảo rằng cả CSP và người dùng đều đồng ý về nơi bắt đầu và kết thúc trách nhiệm bảo mật của họ. Sự cố xảy ra khi các tổ chức cho rằng CSP đang đảm nhiệm vấn đề bảo mật mà họ không chịu trách nhiệm. Một ví dụ về điều này là các ứng dụng và cấu hình đám mây. CSP chịu trách nhiệm bảo mật đám mây nhưng tổ chức có trách nhiệm đảm bảo rằng các dịch vụ được cấu hình đúng theo yêu cầu bảo mật của tổ chức của họ.

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

**Bài học chính**

|  |
| --- |
| It is essential to know the security considerations that are unique to the cloud and understanding the shared responsibility model for cloud security. Organizations are responsible for correctly configuring and maintaining best security practices for their cloud services. The shared responsibility model ensures that both the CSP and users agree about what the organization is responsible for and what the CSP is responsible for when securing the cloud infrastructure. |

Điều cần thiết là phải biết các cân nhắc về bảo mật dành riêng cho đám mây và hiểu mô hình trách nhiệm chung về bảo mật đám mây. Các tổ chức có trách nhiệm định cấu hình chính xác và duy trì các phương pháp bảo mật tốt nhất cho dịch vụ đám mây của mình. Mô hình trách nhiệm chung đảm bảo rằng cả CSP và người dùng đều đồng ý về những gì tổ chức chịu trách nhiệm và những gì CSP chịu trách nhiệm khi bảo mật cơ sở hạ tầng đám mây.

***4.4. Cryptography and cloud security – Mật mã và bảo mật đám mây***

|  |
| --- |
| **Cryptography and cloud security** |

**Mật mã và bảo mật đám mây**

|  |
| --- |
| Earlier in this course, you were introduced to the concepts of the shared responsibility model and identity and access management (IAM). Similar to on-premise networks, cloud networks also need to be secured through a mixture of security hardening practices and cryptography. |

Trước đó trong khóa học này, bạn đã được giới thiệu các khái niệm về mô hình trách nhiệm chung cũng như quản lý danh tính và quyền truy cập (IAM). Tương tự như mạng tại chỗ, mạng đám mây cũng cần được bảo mật thông qua sự kết hợp giữa các biện pháp tăng cường bảo mật và mật mã.

|  |
| --- |
| This reading will address common cloud security hardening practices, what to consider when implementing cloud security measures, and the fundamentals of cryptography. Since cloud infrastructure is becoming increasingly common, it’s important to understand how cloud networks operate and how to secure them. |

Bài đọc này sẽ đề cập đến các biện pháp tăng cường bảo mật đám mây phổ biến, những điều cần cân nhắc khi triển khai các biện pháp bảo mật đám mây và các nguyên tắc cơ bản của mật mã. Vì cơ sở hạ tầng đám mây ngày càng trở nên phổ biến nên điều quan trọng là phải hiểu cách mạng đám mây hoạt động và cách bảo mật chúng.

|  |
| --- |
| **Cloud security hardening** |

**Tăng cường bảo mật đám mây**

|  |
| --- |
| There are various techniques and tools that can be used to secure cloud network infrastructure and resources. Some common cloud security hardening techniques include incorporating IAM, hypervisors, baselining, cryptography, and cryptographic erasure. |

Có nhiều kỹ thuật và công cụ khác nhau có thể được sử dụng để bảo mật tài nguyên và cơ sở hạ tầng mạng đám mây. Một số kỹ thuật tăng cường bảo mật đám mây phổ biến bao gồm kết hợp IAM, bộ ảo hóa, tạo đường cơ sở, mật mã và xóa mật mã.

|  |
| --- |
| **Identity access management (IAM)** |

**Quản lý truy cập danh tính (IAM)**

|  |
| --- |
| **Identity access management (IAM)** is a collection of processes and technologies that helps organizations manage digital identities in their environment. This service also authorizes how users can leverage different cloud resources. |

**Quản lý truy cập danh tính (IAM)** là tập hợp các quy trình và công nghệ giúp các tổ chức quản lý danh tính kỹ thuật số trong môi trường của họ. Dịch vụ này cũng cho phép người dùng có thể tận dụng các tài nguyên đám mây khác nhau.

|  |
| --- |
| **Hypervisors** |

**Trình ảo hóa**

|  |
| --- |
| A **hypervisor** abstracts the host’s hardware from the operating software environment. There are two types of hypervisors. Type one hypervisors run on the hardware of the host computer. An example of a type one hypervisor is VMware®'s ESXi. Type two hypervisors operate on the software of the host computer. An example of a type two hypervisor is VirtualBox. Cloud service providers (CSPs) commonly use type one hypervisors. CSPs are responsible for managing the hypervisor and other virtualization components. The CSP ensures that cloud resources and cloud environments are available, and it provides regular patches and updates. Vulnerabilities in hypervisors or misconfigurations can lead to virtual machine escapes (VM escapes). A VM escape is an exploit where a malicious actor gains access to the primary hypervisor, potentially the host computer and other VMs. As a CSP customer, you will rarely deal with hypervisors directly. |

Trình **ảo hóa** sẽ trừu tượng hóa phần cứng của máy chủ khỏi môi trường phần mềm điều hành. Có hai loại hypervisor. Loại một trình ảo hóa chạy trên phần cứng của máy chủ. Một ví dụ về trình ảo hóa loại một là ESXi của VMware®. Loại hai hypervisors hoạt động trên phần mềm của máy chủ. Một ví dụ về trình ảo hóa loại hai là VirtualBox. Các nhà cung cấp dịch vụ đám mây (CSP) thường sử dụng các trình ảo hóa loại một. CSP chịu trách nhiệm quản lý bộ ảo hóa và các thành phần ảo hóa khác. CSP đảm bảo rằng tài nguyên đám mây và môi trường đám mây luôn sẵn có, đồng thời cung cấp các bản vá và cập nhật thường xuyên. Các lỗ hổng trong bộ ảo hóa hoặc cấu hình sai có thể dẫn đến việc thoát máy ảo (thoát VM). Lối thoát VM là một cách khai thác trong đó tác nhân độc hại có được quyền truy cập vào bộ ảo hóa chính, có thể là máy chủ và các máy ảo khác. Là khách hàng của CSP, bạn sẽ hiếm khi giao dịch trực tiếp với các nhà ảo hóa.

|  |
| --- |
| **Baselining** |

**Đường cơ sở**

|  |
| --- |
| Baselining for cloud networks and operations cover how the cloud environment is configured and set up. A baseline is a fixed reference point. This reference point can be used to compare changes made to a cloud environment. Proper configuration and setup can greatly improve the security and performance of a cloud environment. Examples of establishing a baseline in a cloud environment include: restricting access to the admin portal of the cloud environment, enabling password management, enabling file encryption, and enabling threat detection services for SQL databases. |

Cơ sở cho các hoạt động và mạng đám mây bao gồm cách cấu hình và thiết lập môi trường đám mây. Đường cơ sở là một điểm tham chiếu cố định. Điểm tham chiếu này có thể được sử dụng để so sánh các thay đổi được thực hiện đối với môi trường đám mây. Cấu hình và thiết lập phù hợp có thể cải thiện đáng kể tính bảo mật và hiệu suất của môi trường đám mây. Ví dụ về việc thiết lập đường cơ sở trong môi trường đám mây bao gồm: hạn chế quyền truy cập vào cổng quản trị của môi trường đám mây, cho phép quản lý mật khẩu, bật mã hóa tệp và bật các dịch vụ phát hiện mối đe dọa cho cơ sở dữ liệu SQL.

|  |
| --- |
| **Cryptography in the cloud** |

**Mật mã trên đám mây**

|  |
| --- |
| Cryptography can be applied to secure data that is processed and stored in a cloud environment. Cryptography uses encryption and secure key management systems to provide data integrity and confidentiality. Cryptographic encryption is one of the key ways to secure sensitive data and information in the cloud. |

Mật mã có thể được áp dụng để bảo mật dữ liệu được xử lý và lưu trữ trong môi trường đám mây. Mật mã sử dụng hệ thống mã hóa và quản lý khóa an toàn để cung cấp tính toàn vẹn và bảo mật dữ liệu. Mã hóa mật mã là một trong những cách quan trọng để bảo mật dữ liệu và thông tin nhạy cảm trên đám mây.

|  |
| --- |
| Encryption is the process of scrambling information into ciphertext, which is not readable to anyone without the encryption key. Encryption primarily originated from manually encoding messages and information using an algorithm to convert any given letter or number to a new value. Modern encryption relies on the secrecy of a key, rather than the secrecy of an algorithm. Cryptography is an important tool that helps secure cloud networks and data at rest to prevent unauthorized access. You’ll learn more about cryptography in-depth in an upcoming course. |

Mã hóa là quá trình xáo trộn thông tin thành văn bản mã hóa, không ai có thể đọc được nếu không có khóa mã hóa. Mã hóa chủ yếu bắt nguồn từ việc mã hóa thủ công các tin nhắn và thông tin bằng thuật toán để chuyển đổi bất kỳ chữ cái hoặc số nhất định nào thành một giá trị mới. Mã hóa hiện đại dựa vào tính bí mật của khóa chứ không phải tính bí mật của thuật toán. Mật mã là một công cụ quan trọng giúp bảo mật mạng đám mây và dữ liệu ở phần còn lại để ngăn chặn truy cập trái phép. Bạn sẽ tìm hiểu thêm về mật mã chuyên sâu trong khóa học sắp tới.

|  |
| --- |
| **Cryptographic erasure** |

**Xóa mật mã**

|  |
| --- |
| Cryptographic erasure is a method of erasing the encryption key for the encrypted data. When destroying data in the cloud, more traditional methods of data destruction are not as effective. Crypto-shredding is a newer technique where the cryptographic keys used for decrypting the data are destroyed. This makes the data undecipherable and prevents anyone from decrypting the data. When crypto-shredding, all copies of the key need to be destroyed so no one has any opportunity to access the data in the future. |

Xóa mật mã là phương pháp xóa khóa mã hóa cho dữ liệu được mã hóa. Khi hủy dữ liệu trên đám mây, các phương pháp hủy dữ liệu truyền thống hơn không hiệu quả bằng. Cắt nhỏ mật mã là một kỹ thuật mới hơn trong đó các khóa mật mã được sử dụng để giải mã dữ liệu sẽ bị hủy. Điều này làm cho dữ liệu không thể giải mã được và ngăn cản bất kỳ ai giải mã dữ liệu. Khi băm nhỏ mật mã, tất cả các bản sao của khóa cần phải bị hủy để không ai có cơ hội truy cập dữ liệu trong tương lai.

|  |
| --- |
| **Key Management** |

**Quản lý khóa**

|  |
| --- |
| Modern encryption relies on keeping the encryption keys secure. Below are the measures you can take to further protect your data when using cloud applications:   * Trusted platform module (TPM). TPM is a computer chip that can securely store passwords, certificates, and encryption keys. * Cloud hardware security module (CloudHSM). CloudHSM is a computing device that provides secure storage for cryptographic keys and processes cryptographic operations, such as encryption and decryption. |

Mã hóa hiện đại dựa vào việc giữ an toàn cho các khóa mã hóa. Dưới đây là các biện pháp bạn có thể thực hiện để bảo vệ dữ liệu của mình hơn nữa khi sử dụng các ứng dụng đám mây:

* Mô-đun nền tảng đáng tin cậy (TPM). TPM là chip máy tính có thể lưu trữ mật khẩu, chứng chỉ và khóa mã hóa một cách an toàn.
* Mô-đun bảo mật phần cứng đám mây (CloudHSM). CloudHSM là một thiết bị điện toán cung cấp khả năng lưu trữ an toàn cho các khóa mật mã và xử lý các hoạt động mã hóa, chẳng hạn như mã hóa và giải mã.

|  |
| --- |
| Organizations and customers do not have access to the cloud service provider (CSP) directly, but they can request audits and security reports by contacting the CSP. Customers typically do not have access to the specific encryption keys that CSPs use to encrypt the customers’ data. However, almost all CSPs allow customers to provide their own encryption keys, depending on the service the customer is accessing. In turn, the customer is responsible for their encryption keys and ensuring the keys remain confidential. The CSP is limited in how they can help the customer if the customer’s keys are compromised or destroyed. One key benefit of the shared responsibility model is that the customer is not entirely responsible for maintenance of the cryptographic infrastructure. Organizations can assess and monitor the risk involved with allowing the CSP to manage the infrastructure by reviewing a CSPs audit and security controls. For federal contractors, FEDRAMP provides a list of verified CSPs. |

Các tổ chức và khách hàng không có quyền truy cập trực tiếp vào nhà cung cấp dịch vụ đám mây (CSP), nhưng họ có thể yêu cầu kiểm tra và báo cáo bảo mật bằng cách liên hệ với CSP. Khách hàng thường không có quyền truy cập vào các khóa mã hóa cụ thể mà CSP sử dụng để mã hóa dữ liệu của khách hàng. Tuy nhiên, hầu hết tất cả các CSP đều cho phép khách hàng cung cấp khóa mã hóa riêng, tùy thuộc vào dịch vụ mà khách hàng đang truy cập. Đổi lại, khách hàng chịu trách nhiệm về các khóa mã hóa của mình và đảm bảo các khóa đó được giữ bí mật. CSP bị hạn chế về cách họ có thể giúp đỡ khách hàng nếu khóa của khách hàng bị xâm phạm hoặc bị phá hủy. Một lợi ích chính của mô hình chia sẻ trách nhiệm là khách hàng không hoàn toàn chịu trách nhiệm bảo trì cơ sở hạ tầng mật mã. Các tổ chức có thể đánh giá và giám sát rủi ro liên quan đến việc cho phép CSP quản lý cơ sở hạ tầng bằng cách xem xét kiểm tra CSP và kiểm soát bảo mật. Đối với các nhà thầu liên bang, FEDRAMP cung cấp danh sách các CSP đã được xác minh.

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

**Bài học chính**

|  |
| --- |
| Cloud security hardening is a critical component to consider when assessing the security of various public cloud environments and improving the security within your organization. Identity access management (IAM), correctly configuring a baseline for the cloud environment, securing hypervisors, cryptography, and cryptographic erasure are all methods to use to further secure cloud infrastructure. |

Tăng cường bảo mật đám mây là một thành phần quan trọng cần xem xét khi đánh giá tính bảo mật của các môi trường đám mây công cộng khác nhau và cải thiện tính bảo mật trong tổ chức của bạn. Quản lý quyền truy cập danh tính (IAM), định cấu hình đường cơ sở chính xác cho môi trường đám mây, bảo mật trình ảo hóa, mật mã và xóa mật mã đều là các phương pháp cần sử dụng để bảo mật hơn nữa cơ sở hạ tầng đám mây.

***4.5. Test your knowledge: Cloud hardening – Kiểm tra kiến ​​thức của bạn: Làm cứng đám mây***

**5. Review: Security hardening – Đánh giá: Tăng cường bảo mật**

***5.1. Wrap-up – Gói lại***

|  |
| --- |
| Great work on learning about security hardening! Let's take a few minutes to wrap up what you've learned. |

Thật tuyệt vời khi tìm hiểu về việc tăng cường bảo mật!Hãy dành vài phút để tóm tắt những gì bạn đã học được.

|  |
| --- |
| You learned about security hardening and its importance to an organization's infrastructure. First, we discussed how security hardening strengthens systems and networks to reduce the likelihood of an attack. Next, we covered the importance of OS hardening, including patch updates, baseline configurations, and hardware and software disposal. Then we explored network hardening practices, such as network log analysis and firewall rule maintenance. Finally, we examined cloud network hardening and the responsibilities of both organizations and cloud service providers in maintaining security. |

Bạn đã tìm hiểu về tăng cường bảo mật vàtầm quan trọng của nó đối với cơ sở hạ tầng của một tổ chức.Đầu tiên, chúng tôi thảo luận về cáchtăng cường an ninh tăng cường hệ thống vàmạng để giảm khả năng bị tấn công.Tiếp theo, chúng tôi đề cập đến tầm quan trọng của việc tăng cường hệ điều hành,bao gồm các bản cập nhật bản vá, cấu hình cơ bản,và xử lý phần cứng và phần mềm.Sau đó, chúng tôi khám phá các phương pháp tăng cường mạng, chẳng hạn nhưphân tích nhật ký mạng và bảo trì quy tắc tường lửa.Cuối cùng, chúng tôi đã kiểm tra đám mâycủng cố mạng lưới và trách nhiệm củacả tổ chức vànhà cung cấp dịch vụ đám mây trong việc duy trì bảo mật.

|  |
| --- |
| As a security analyst, you'll be working with operating systems, on-premise networks, and cloud networks. You'll be using all the knowledge that we learned in this section in your career as a security analyst. |

Là một nhà phân tích chứng khoán,bạn sẽ làm việc với hệ điều hành,mạng tại chỗ và mạng đám mây.Bạn sẽ sử dụng tất cả kiến ​​thức mà chúng ta đã học trongphần này trong sự nghiệp của bạn với tư cách là nhà phân tích bảo mật.

***5.2. 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 3, Module 4** |

**Các thuật ngữ và định nghĩa trong Khóa 3, Học phần 4**

|  |
| --- |
| **Baseline configuration (baseline image):** A documented set of specifications within a system that is used as a basis for future builds, releases, and updates |

**Cấu hình cơ sở (hình ảnh cơ sở):** Một bộ thông số kỹ thuật được ghi lại trong hệ thống được sử dụng làm cơ sở cho các bản dựng, bản phát hành và cập nhật trong tương lai

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

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

|  |
| --- |
| **Multi-factor authentication (MFA):** A security measure which requires a user to verify their identity in two or more ways to access a system or network |

**Xác thực đa yếu tố (MFA):** Một biện pháp bảo mật yêu cầu người dùng xác minh danh tính của họ theo hai hoặc nhiều cách để truy cập hệ thống hoặc mạng

|  |
| --- |
| **Network log analysis:** The process of examining network logs to identify events of interest |

**Phân tích nhật ký mạng:** Quá trình kiểm tra nhật ký mạng để xác định các sự kiện quan tâm

|  |
| --- |
| **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

|  |
| --- |
| **Patch update:** A software and operating system update that addresses security vulnerabilities within a program or product |

**Cập nhật bản vá:** Bản cập nhật phần mềm và hệ điều hành nhằm giải quyết các lỗ hổng bảo mật trong một chương trình hoặc sản phẩm

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

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

|  |
| --- |
| **Security hardening:** The process of strengthening a system to reduce its vulnerabilities and attack surface |

**Tăng cường bảo mật:** Quá trình tăng cường hệ thống để giảm các lỗ hổng và bề mặt tấn công của nó

|  |
| --- |
| **Security information and event management (SIEM):** An application that collects and analyzes log data to monitor critical activities for an organization |

**Quản lý sự kiện và thông tin bảo mật (SIEM):** Một ứng dụng thu thập và phân tích dữ liệu nhật ký để giám sát các hoạt động quan trọng của một tổ chức

|  |
| --- |
| **World-writable file:** A file that can be altered by anyone in the world |

**Tệp có thể ghi trên thế giới:** Một tệp có thể được sửa đổi bởi bất kỳ ai trên thế giới

***5.3. Module 4 challenge – Thử thách mô-đun 4***

***5.4. Portfolio Activity: Use the NIST Cybersecurity Framework to respond to a security incident – Hoạt động danh mục đầu tư: Sử dụng Khung bảo mật không gian mạng NIST để ứng phó với sự cố bảo mật***

|  |
| --- |
| **Activity Overview**  https://d3c33hcgiwev3.cloudfront.net/imageAssetProxy.v1/wBI365r0TCevN_1iKPj-9A_395ef074f51943288c6b8bdd1ce3eef1_image.png?expiry=1715731200000&hmac=W1FbQF1QckRKT5DwxsDnx8GcEwfGOrSWrPUQxN0GW2M  In this activity, you will create an incident report using the knowledge you’ve gained about networks throughout this course to analyze a network incident. You will analyze the situation using the National Institute of Standards and Technology's Cybersecurity Framework (NIST CSF). The CSF is a voluntary framework that consists of standards, guidelines, and best practices to manage cybersecurity risk. Creating a quality cybersecurity incident report and applying the CSF can demonstrate a proactive approach to security, improving communication and transparency with stakeholders, and improve security practices within your organization. You can also add the incident report you create to your cybersecurity portfolio when  you complete it.  The CSF is scalable and can be applied in a wide variety of contexts. As you continue to learn more and refine your understanding of key cybersecurity skills, you can use the templates provided in this activity in other situations. Knowing how to identify which security measures to apply in response to business needs will help you determine which are the best available options when it comes to network security.  Be sure to complete this activity before moving on. In the next course item, you will be able to self-assess your response. After that, there will be a completed exemplar to compare to your own work. It will also provide an opportunity for you to answer rubric questions that allow you to reflect on key elements of your professional statement. |

**Tổng quan về hoạt động**

https://d3c33hcgiwev3.cloudfront.net/imageAssetProxy.v1/wBI365r0TCevN_1iKPj-9A_395ef074f51943288c6b8bdd1ce3eef1_image.png?expiry=1715731200000&hmac=W1FbQF1QckRKT5DwxsDnx8GcEwfGOrSWrPUQxN0GW2M

Trong hoạt động này, bạn sẽ tạo báo cáo sự cố bằng cách sử dụng kiến ​​thức bạn đã có được về mạng trong suốt khóa học này để phân tích sự cố mạng. Bạn sẽ phân tích tình huống bằng cách sử dụng Khung an ninh mạng của Viện Tiêu chuẩn và Công nghệ Quốc gia (NIST CSF). CSF là một khuôn khổ tự nguyện bao gồm các tiêu chuẩn, hướng dẫn và biện pháp thực hành tốt nhất để quản lý rủi ro an ninh mạng. Việc tạo báo cáo sự cố an ninh mạng có chất lượng và áp dụng CSF có thể thể hiện cách tiếp cận chủ động về bảo mật, cải thiện khả năng giao tiếp và minh bạch với các bên liên quan, đồng thời cải thiện các biện pháp bảo mật trong tổ chức của bạn. Bạn cũng có thể thêm báo cáo sự cố mà bạn tạo vào danh mục an ninh mạng của mình khi hoàn thành báo cáo đó.

CSF có khả năng mở rộng và có thể được áp dụng trong nhiều bối cảnh khác nhau. Khi tiếp tục tìm hiểu thêm và hoàn thiện hiểu biết của mình về các kỹ năng an ninh mạng quan trọng, bạn có thể sử dụng các mẫu được cung cấp trong hoạt động này trong các tình huống khác. Biết cách xác định những biện pháp bảo mật nào cần áp dụng để đáp ứng nhu cầu kinh doanh sẽ giúp bạn xác định đâu là những lựa chọn khả dụng tốt nhất khi nói đến bảo mật mạng.

Hãy chắc chắn hoàn thành hoạt động này trước khi tiếp tục. Trong mục khóa học tiếp theo, bạn sẽ có thể tự đánh giá phản hồi của mình. Sau đó sẽ có một mẫu hoàn chỉnh để so sánh với tác phẩm của chính bạn. Nó cũng sẽ tạo cơ hội cho bạn trả lời các câu hỏi đánh giá cho phép bạn suy ngẫm về các yếu tố chính trong tuyên bố chuyên môn của mình.

|  |
| --- |
| **Scenario**  https://d3c33hcgiwev3.cloudfront.net/imageAssetProxy.v1/dDWqzsRPQqeCk0vSaDKmOA_42906106724e4c1d9d53026c020a46f1_image.png?expiry=1715731200000&hmac=d1WCLPU_PZUKPU_cNKCzQWW_74gN40RQ6WK1S8M93n0  Review the scenario below. Then complete the step-by-step instructions.  You are a cybersecurity analyst working for a multimedia company that offers web design services, graphic design, and social media marketing solutions to small businesses. Your organization recently experienced a DDoS attack, which compromised the internal network for two hours until it was resolved.  During the attack, your organization’s network services suddenly stopped responding due to an incoming flood of ICMP packets. Normal internal network traffic could not access any network resources. The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services.  The company’s cybersecurity team then investigated the security event. They found that a malicious actor had sent a flood of ICMP pings into the company’s network through an unconfigured firewall. This vulnerability allowed the malicious attacker to overwhelm the company’s network through a distributed denial of service (DDoS) attack.  To address this security event, the network security team implemented:   * A new firewall rule to limit the rate of incoming ICMP packets * Source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets * Network monitoring software to detect abnormal traffic patterns * An IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics   As a cybersecurity analyst, you are tasked with using this security event to create a plan to improve your company’s network security, following the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). You will use the CSF to help you navigate through the different steps of analyzing this cybersecurity event and integrate your analysis into a general security strategy. We have broken the analysis into different parts in the template below. You can explore them here:   * **Identify** security risks through regular audits of internal networks, systems, devices, and access privileges to identify potential gaps in security. * **Protect** internal assets through the implementation of policies, procedures, training and tools that help mitigate cybersecurity threats. * **Detect** potential security incidents and improve monitoring capabilities to increase the speed and efficiency of detections. * **Respond** to contain, neutralize, and analyze security incidents; implement improvements to the security process.   **Recover** affected systems to normal operation and restore systems data and/or assets that have been affected by an incident. |

**Kịch bản**

https://d3c33hcgiwev3.cloudfront.net/imageAssetProxy.v1/dDWqzsRPQqeCk0vSaDKmOA_42906106724e4c1d9d53026c020a46f1_image.png?expiry=1715731200000&hmac=d1WCLPU_PZUKPU_cNKCzQWW_74gN40RQ6WK1S8M93n0

Xem lại kịch bản dưới đây. Sau đó hoàn thành các hướng dẫn từng bước.

Bạn là nhà phân tích an ninh mạng làm việc cho một công ty đa phương tiện cung cấp dịch vụ thiết kế web, thiết kế đồ họa và giải pháp tiếp thị trên mạng xã hội cho các doanh nghiệp nhỏ. Tổ chức của bạn gần đây đã gặp phải một cuộc tấn công DDoS, khiến mạng nội bộ bị xâm phạm trong hai giờ cho đến khi được giải quyết.

Trong cuộc tấn công, các dịch vụ mạng của tổ chức của bạn đột nhiên ngừng phản hồi do có quá nhiều gói ICMP đến. Lưu lượng truy cập mạng nội bộ thông thường không thể truy cập bất kỳ tài nguyên mạng nào. Nhóm quản lý sự cố đã phản hồi bằng cách chặn các gói ICMP đến, dừng ngoại tuyến tất cả các dịch vụ mạng không quan trọng và khôi phục các dịch vụ mạng quan trọng.

Nhóm an ninh mạng của công ty sau đó đã điều tra sự kiện bảo mật. Họ phát hiện ra rằng một kẻ độc hại đã gửi hàng loạt ping ICMP vào mạng của công ty thông qua tường lửa chưa được định cấu hình. Lỗ hổng này cho phép kẻ tấn công độc hại áp đảo mạng của công ty thông qua cuộc tấn công từ chối dịch vụ phân tán (DDoS).

Để giải quyết sự kiện bảo mật này, nhóm an ninh mạng đã triển khai:

* Quy tắc tường lửa mới để hạn chế tốc độ gói ICMP đến
* Xác minh địa chỉ IP nguồn trên tường lửa để kiểm tra địa chỉ IP giả mạo trên các gói ICMP đến
* Phần mềm giám sát mạng để phát hiện các mẫu lưu lượng truy cập bất thường
* Hệ thống IDS/IPS để lọc một số lưu lượng ICMP dựa trên các đặc điểm đáng ngờ

Với tư cách là nhà phân tích an ninh mạng, bạn có nhiệm vụ sử dụng sự kiện bảo mật này để lập kế hoạch cải thiện an ninh mạng của công ty mình, tuân theo Khung bảo mật không gian mạng (CSF) của Viện Tiêu chuẩn và Công nghệ Quốc gia (NIST). Bạn sẽ sử dụng CSF để giúp bạn điều hướng qua các bước khác nhau trong quá trình phân tích sự kiện an ninh mạng này và tích hợp phân tích của bạn vào chiến lược bảo mật chung. Chúng tôi đã chia phân tích thành các phần khác nhau trong mẫu bên dưới. Bạn có thể khám phá chúng ở đây:

* **Xác định** rủi ro bảo mật thông qua kiểm tra thường xuyên mạng nội bộ, hệ thống, thiết bị và đặc quyền truy cập để xác định các lỗ hổng bảo mật tiềm ẩn.
* **Bảo vệ** tài sản nội bộ thông qua việc thực hiện các chính sách, quy trình, đào tạo và công cụ giúp giảm thiểu các mối đe dọa an ninh mạng.
* **Phát hiện** các sự cố bảo mật tiềm ẩn và cải thiện khả năng giám sát để tăng tốc độ và hiệu quả phát hiện.
* **Ứng phó** để ngăn chặn, vô hiệu hóa và phân tích các sự cố bảo mật; thực hiện các cải tiến đối với quy trình bảo mật.

**Khôi phục** các hệ thống bị ảnh hưởng về hoạt động bình thường và khôi phục dữ liệu và/hoặc tài sản của hệ thống đã bị ảnh hưởng bởi sự cố.

|  |
| --- |
| **Step-By-Step Instructions**  https://d3c33hcgiwev3.cloudfront.net/imageAssetProxy.v1/5hMqfCEPRVutrXU-S4uWWA_bb13bb0ab1d34ad49f708482f695a3f1_image.png?expiry=1715731200000&hmac=kPXuz4PdZja5t8hoeqFKV68aQrKkt5Oew648lfBJBqg  Follow the instructions and fill in the sections to complete the activity. Then, go to the next course item to compare your work to a completed exemplar. |

**Hướng dẫn từng bước một**

https://d3c33hcgiwev3.cloudfront.net/imageAssetProxy.v1/5hMqfCEPRVutrXU-S4uWWA_bb13bb0ab1d34ad49f708482f695a3f1_image.png?expiry=1715731200000&hmac=kPXuz4PdZja5t8hoeqFKV68aQrKkt5Oew648lfBJBqg

Làm theo hướng dẫn và điền vào các phần để hoàn thành hoạt động. Sau đó, chuyển sang mục khóa học tiếp theo để so sánh bài tập của bạn với một bài mẫu đã hoàn thành.

|  |
| --- |
| **Step 1: Access the incident report analysis template**  To access template for this course item, click the following link and select *Use Template*.  Link to template:   * [Incident report analysis](https://docs.google.com/document/d/1EnieOKYJyKGsVff5Gg-3-dVwrHrZ2m8Hig6tVpfKqyg/template/preview?usp=sharing&resourcekey=0-eb5t-d69zTPLEGthIpVlXw)   Link to supporting materials:   * [Applying the NIST CSF](https://docs.google.com/document/d/15yCDbDCOAcJw-LTz2DeCA7UeLRfvsf176T6MA6ku6ok/template/preview?usp=sharing) * [Example of an incident report analysis](https://docs.google.com/document/d/11eTIo1igTRFrY279DG9tHTO3tB3bugSGyknZxsvY5vI/template/preview?usp=sharing&resourcekey=0-97MA-eOwoGtqcfqky0vjmg) |

**Bước 1: Truy cập mẫu phân tích báo cáo sự cố**

Để truy cập mẫu cho mục khóa học này, hãy nhấp vào liên kết sau và chọn *Sử dụng Mẫu* .

Liên kết đến mẫu:

* [Phân tích báo cáo sự cố](https://docs.google.com/document/d/1EnieOKYJyKGsVff5Gg-3-dVwrHrZ2m8Hig6tVpfKqyg/template/preview?usp=sharing&resourcekey=0-eb5t-d69zTPLEGthIpVlXw)

Link các tài liệu hỗ trợ:

* [Áp dụng NIST CSF](https://docs.google.com/document/d/15yCDbDCOAcJw-LTz2DeCA7UeLRfvsf176T6MA6ku6ok/template/preview?usp=sharing)
* [Ví dụ về phân tích báo cáo sự cố](https://docs.google.com/document/d/11eTIo1igTRFrY279DG9tHTO3tB3bugSGyknZxsvY5vI/template/preview?usp=sharing&resourcekey=0-97MA-eOwoGtqcfqky0vjmg)

|  |
| --- |
| **Step 2: Summarize the security event**  Using the template provided, provide a summary of the security event that occurred. Include information about the security event, its cause, the impact, and the response. You can also include information about targeted systems, the attack source, and the estimated impact. |

Sử dụng mẫu được cung cấp, cung cấp bản tóm tắt về sự kiện bảo mật đã xảy ra. Bao gồm thông tin về sự kiện bảo mật, nguyên nhân, tác động và phản hồi của nó. Bạn cũng có thể bao gồm thông tin về các hệ thống được nhắm mục tiêu, nguồn tấn công và tác động ước tính.

|  |
| --- |
| **Step 3: Identify the type of attack and the systems affected**  Think about all of the concepts covered in the course so far and reflect on the scenario and define what type of attack occurred and which systems were affected. List this information in the incident report analysis worksheet in the section titled “Identify.” |

Hãy suy nghĩ về tất cả các khái niệm được đề cập trong khóa học cho đến nay và suy ngẫm về kịch bản cũng như xác định loại tấn công nào đã xảy ra và hệ thống nào bị ảnh hưởng. Liệt kê thông tin này trong bảng phân tích báo cáo sự cố trong phần có tiêu đề “Xác định”.

|  |
| --- |
| **Step 4: Protect the assets in your organization from being compromised**  Next, you will assess where the organization can improve to further protect its assets. In this step, you will focus on creating an immediate action plan to respond to the cybersecurity incident. When creating this plan, reflect on the following question:   * What systems or procedures need to be updated or changed to further secure the organization’s assets?   Write your response in the incident report analysis template in the “Protect” section. |

Tiếp theo, bạn sẽ đánh giá nơi tổ chức có thể cải thiện để bảo vệ tài sản của mình hơn nữa. Ở bước này, bạn sẽ tập trung vào việc lập kế hoạch hành động tức thời để ứng phó với sự cố an ninh mạng. Khi tạo kế hoạch này, hãy suy nghĩ về câu hỏi sau:

* Những hệ thống hoặc thủ tục nào cần được cập nhật hoặc thay đổi để bảo mật hơn nữa tài sản của tổ chức?

Viết phản hồi của bạn vào mẫu phân tích báo cáo sự cố ở phần “Bảo vệ”.

|  |
| --- |
| **Step 5: Detect similar incidents in the future**  It is important to continuously monitor network traffic on network devices to check for suspicious activity, such as incoming external ICMP packets from non-trusted IP addresses attempting to pass through the organization’s network firewall.  For this step, consider ways you and your team can monitor and analyze network traffic, software applications, track authorized versus unauthorized users, and detect any unusual activity on user accounts. Write your response in the incident response analysis worksheet in the “Detect” section. |

Điều quan trọng là phải liên tục giám sát lưu lượng mạng trên các thiết bị mạng để kiểm tra hoạt động đáng ngờ, chẳng hạn như các gói ICMP bên ngoài đến từ các địa chỉ IP không đáng tin cậy đang cố gắng vượt qua tường lửa mạng của tổ chức.

Đối với bước này, hãy xem xét các cách bạn và nhóm của bạn có thể giám sát và phân tích lưu lượng truy cập mạng, ứng dụng phần mềm, theo dõi người dùng được ủy quyền và người dùng trái phép cũng như phát hiện bất kỳ hoạt động bất thường nào trên tài khoản người dùng. Viết phản hồi của bạn vào bảng phân tích ứng phó sự cố ở phần “Phát hiện”.

|  |
| --- |
| **Step 6: Respond to future cybersecurity incidents**  After identifying the tools and methods you and your organization have in place for detecting potential vulnerabilities and threats, create a response plan in the event of a future incident. This typically happens after the incident occurred and has been resolved by you and your team. In this case, you will create a response plan for future cybersecurity incidents. Some items to consider when creating a response plan to any cybersecurity incident:   * How can you and your team contain cybersecurity incidents and affected devices? * What procedures are in place to help you and your team neutralize cybersecurity incidents? * What data or information can be used to analyze this incident? * How can your organization’s recovery process be improved to better handle future cybersecurity incidents?   Write your response in the incident report analysis template under the “respond” section. |

Sau khi xác định các công cụ và phương pháp mà bạn và tổ chức của bạn sẵn có để phát hiện các lỗ hổng và mối đe dọa tiềm ẩn, hãy tạo kế hoạch ứng phó trong trường hợp xảy ra sự cố trong tương lai. Điều này thường xảy ra sau khi sự cố xảy ra và đã được bạn và nhóm của bạn giải quyết. Trong trường hợp này, bạn sẽ tạo kế hoạch ứng phó cho các sự cố an ninh mạng trong tương lai. Một số mục cần cân nhắc khi tạo kế hoạch ứng phó với bất kỳ sự cố an ninh mạng nào:

* Làm thế nào bạn và nhóm của bạn có thể ngăn chặn sự cố an ninh mạng và các thiết bị bị ảnh hưởng?
* Những quy trình nào được áp dụng để giúp bạn và nhóm của bạn vô hiệu hóa các sự cố an ninh mạng?
* Dữ liệu hoặc thông tin nào có thể được sử dụng để phân tích sự cố này?
* Làm cách nào để cải thiện quy trình khôi phục của tổ chức bạn để xử lý tốt hơn các sự cố an ninh mạng trong tương lai?

Viết phản hồi của bạn vào mẫu phân tích báo cáo sự cố trong phần “phản hồi”.

|  |
| --- |
| **Step 7: Recover from the incident**  Consider what steps need to be taken to help the organization recover from the cybersecurity incident. Reflect on all the information you gathered about the incident in the previous steps to consider which devices, systems, and processes need to be restored and recovered.  Consider the following questions:   * What information do you need to be able to recover immediately? * What processes are in place to help the organization recover from the incident?   Write your response in the “recover” portion of the worksheet. |

Xem xét những bước cần thực hiện để giúp tổ chức phục hồi sau sự cố an ninh mạng. Suy ngẫm về tất cả thông tin bạn đã thu thập về sự cố ở các bước trước để xem xét thiết bị, hệ thống và quy trình nào cần được khôi phục và khôi phục.

Hãy xem xét các câu hỏi sau:

* Bạn cần những thông tin gì để có thể phục hồi ngay lập tức?
* Những quy trình nào được áp dụng để giúp tổ chức phục hồi sau sự cố?

Viết câu trả lời của bạn vào phần “khôi phục” của bài tập.

|  |
| --- |
| **Pro Tip: Save the incident report analysis template** |

**Mẹo chuyên nghiệp: Lưu mẫu phân tích báo cáo sự cố**

|  |
| --- |
| Finally, be sure to save a copy of your incident report analysis worksheet somewhere accessible so that you can access it as you progress through the course and into the security field. |

Cuối cùng, hãy nhớ lưu một bản sao của bảng tính phân tích báo cáo sự cố của bạn ở nơi nào đó có thể truy cập được để bạn có thể truy cập nó khi hoàn thành khóa học và vào lĩnh vực bảo mật.

|  |
| --- |
| **What to Include in Your Response**  Later, you will have the opportunity to assess your performance using the criteria listed. Be sure to address the following in your completed activity.  Course 3 incident report analysis   * Summarize the security event * Identifies the type of attack and the systems impacted by the incident * Offers a protection plan against future cybersecurity incidents * Describes detection methods that can be used to identify potential cybersecurity incidents * Includes a response plan for the cybersecurity incident and outline for future cybersecurity incidents * Outlines recovery plans you and the organization can implement in future cybersecurity incidents. |

**Những gì cần bao gồm trong phản hồi của bạn**

Sau đó, bạn sẽ có cơ hội đánh giá hiệu suất của mình bằng cách sử dụng các tiêu chí được liệt kê. Hãy chắc chắn giải quyết những điều sau đây trong hoạt động đã hoàn thành của bạn.

Phân tích báo cáo sự cố khóa 3

* Tóm tắt sự kiện bảo mật
* Xác định loại tấn công và hệ thống bị ảnh hưởng bởi sự cố
* Cung cấp kế hoạch bảo vệ chống lại các sự cố an ninh mạng trong tương lai
* Mô tả các phương pháp phát hiện có thể được sử dụng để xác định các sự cố an ninh mạng tiềm ẩn
* Bao gồm kế hoạch ứng phó với sự cố an ninh mạng và phác thảo về các sự cố an ninh mạng trong tương lai
* Phác thảo các kế hoạch khôi phục mà bạn và tổ chức có thể thực hiện trong các sự cố an ninh mạng trong tương lai.

|  |
| --- |
| **Step 8: Assess your activity**  You will complete a self-assessment for your incident report portfolio activity. Please use the questions that are presented 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 incident report.  To complete the self-assessment, first open the Portfolio Activity Exemplar in the next course item. Compare your completed incident report document. Respond yes or no to each statement provided at the end of the Portfolio Activity.   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%. 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 5 points before continuing on to the next course item. |

**Bước 8: Đánh giá hoạt động của bạn**

Bạn sẽ hoàn thành bản tự đánh giá cho hoạt động danh mục báo cáo sự cố của mình. Vui lòng sử dụng các câu hỏi được trình bày 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* báo cáo sự cố của mình.

Để hoàn thành quá trình tự đánh giá, trước tiên hãy mở Mẫu hoạt động danh mục đầu tư trong mục khóa học tiếp theo. So sánh tài liệu báo cáo sự cố đã hoàn thành của bạn. Trả lời có hoặc không cho từng câu được cung cấp ở cuối Hoạt động danh mục đầu tư.

 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 là ít nhất 80%. 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 5 điểm trước khi tiếp tục học mục tiếp theo của khóa học.

***5.5. Portfolio Activity Exemplar: Use the NIST Cybersecurity Framework to respond to a security incident – Ví dụ về hoạt động danh mục đầu tư: Sử dụng Khung bảo mật mạng NIST để ứng phó với sự cố bảo mật***

|  |
| --- |
| **Portfolio Activity Exemplar: Use the NIST Cybersecurity Framework to respond to a security incident** |

**Ví dụ về hoạt động danh mục đầu tư: Sử dụng Khung bảo mật mạng NIST để ứng phó với sự cố bảo mật**

|  |
| --- |
| Here is a completed exemplar along with an explanation of how the exemplar fulfills the expectations for the activity. |

Đây là một ví dụ hoàn chỉnh cùng với lời giải thích về cách ví dụ đó đáp ứng những kỳ vọng cho hoạt động.

|  |
| --- |
| **Completed Exemplar**  To review the exemplar for this course item, click the following link:  https://d3c33hcgiwev3.cloudfront.net/imageAssetProxy.v1/zPEu5OfwR0ONnXi5KJESQw_ccefc38c0020488b9cf92cf191369df1_image.png?expiry=1715731200000&hmac=yl37fHM4vU5NM1021YCXSPTVzp58p_hMIExVEks098M  Link to exemplar:   * [Incident report analysis](https://docs.google.com/document/d/1iPlKsGAVw1usT8JiR_CgGbL6rut783h_RCH-J8PavuA/template/preview?usp=sharing) |

**Mẫu đã hoàn thành**

Để xem lại ví dụ mẫu cho mục khóa học này, hãy nhấp vào liên kết sau:

https://d3c33hcgiwev3.cloudfront.net/imageAssetProxy.v1/zPEu5OfwR0ONnXi5KJESQw_ccefc38c0020488b9cf92cf191369df1_image.png?expiry=1715731200000&hmac=yl37fHM4vU5NM1021YCXSPTVzp58p_hMIExVEks098M

Liên kết đến ví dụ:

* [Phân tích báo cáo sự cố](https://docs.google.com/document/d/1iPlKsGAVw1usT8JiR_CgGbL6rut783h_RCH-J8PavuA/template/preview?usp=sharing)

|  |
| --- |
| **Assessment of Exemplar**  https://d3c33hcgiwev3.cloudfront.net/imageAssetProxy.v1/dqhcF4nnSryfLlQKdoHohw_9ffa72f392aa4cdc8e1c351edfa054f1_image.png?expiry=1715731200000&hmac=Pns7o9iDnS9KoPRuT_sZBiMWSVsjd0V0KyAyHpQG00s  Compare the exemplar to your completed incident report analysis and incident report. 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 guide you as you continue to progress through the program.  ***Note:*** *The exemplar represents one example of how to complete the activity. Yours may differ in certain ways. What’s important is that you have an idea of what your incident analysis should resemble.*  https://d3c33hcgiwev3.cloudfront.net/imageAssetProxy.v1/CTuXcARGTpicF6GtU7FLrA_f39fbb9d8d854217b7c49cefbaa6cef1_image.png?expiry=1715731200000&hmac=OxT3qQE2dgwMq1iRRjlPh-CucIs9Hrl7gscfAQLItJk  The exemplar is accompanied by the activity, and presents a complete incident report analysis to establish:   * What type of attack occurred, the scope of the incident, and its impact to the organization * Potential network vulnerabilities and protection measures * Detection tools to monitor and secure the network * How to respond to cybersecurity incidents in the future * Recovery plans to restore normal operations |

|  |
| --- |
|  |

|  |
| --- |
|  |

**6. Congratulations on completing Course 3! – Chúc mừng bạn đã hoàn thành Khóa 3!**

***6.1. Course wrap-up – Tóm tắt khóa học***

|  |
| --- |
| Wow, we have covered a lot in this course! Let's review everything we've discussed. You learned about networks, network architecture, and the best practices used by security professionals to secure a network against security breaches. As we bring this course to a close, let's review what you've learned about security networks so far. |

Ồ, chúng ta đã học được rất nhiều điều trong khóa học này!Hãy xem lại mọi thứ chúng ta đã thảo luận.Bạn đã tìm hiểu về mạng, kiến ​​trúc mạng và các phương pháp hay nhất được sử dụngbởi các chuyên gia bảo mật để bảo vệ mạng khỏi các vi phạm an ninh.Khi chúng ta kết thúc khóa học này,Hãy xem lại những gì bạn đã học được về mạng bảo mật cho đến nay.

|  |
| --- |
| First, we explored the structure of a network. A security analyst must understand how a network is designed to be able to identify parts of a network that present vulnerabilities and need to be secured. |

Đầu tiên, chúng tôi khám phá cấu trúc của một mạng.Một nhà phân tích bảo mật phải hiểu mạng được thiết kế như thế nào để có thểxác định các phần của mạng có lỗ hổng và cần được bảo mật.

|  |
| --- |
| Next, we learned about network operations and how they affect the communication of data. Network protocols determine how the data is transmitted over the network. As communication takes place over the network, malicious actors may use tactics such as denial of service attacks, packet sniffing, and IP spoofing. Security analysts employ tools and measures such as firewall rules to protect against these attacks. |

Tiếp theo, chúng ta đã tìm hiểu về hoạt động mạng vàchúng ảnh hưởng như thế nào đến việc truyền dữ liệu.Các giao thức mạng xác định cách dữ liệu được truyền qua mạng.Khi giao tiếp diễn ra qua mạng, các tác nhân độc hại có thể sử dụng các chiến thuậtchẳng hạn như tấn công từ chối dịch vụ, đánh hơi gói và giả mạo IP.Các nhà phân tích bảo mật sử dụng các công cụ vàcác biện pháp như quy tắc tường lửa để bảo vệ chống lại các cuộc tấn công này.

|  |
| --- |
| We also discussed security hardening. Security hardening is used to reduce the attack area of a network. This means the attack does not disable an entire network. Security hardening can be done at the hardware level, the software level, or the network level. Securing networks is an essential part of a security analyst's duties. Knowledge of a network and its operations and security practices will ensure that you are successful in your career as a security analyst. |

Chúng tôi cũng thảo luận về việc tăng cường an ninh.Tăng cường bảo mật được sử dụng để giảm vùng tấn công của mạng.Điều này có nghĩa là cuộc tấn công không vô hiệu hóa toàn bộ mạng.Tăng cường bảo mật có thể được thực hiện ở cấp độ phần cứng, cấp độ phần mềm hoặccấp độ mạng.Bảo mật mạng là một phần thiết yếu trong nhiệm vụ của nhà phân tích bảo mật.Kiến thức về mạng, hoạt động và thực tiễn bảo mật của mạng sẽ đảm bảo rằngbạn thành công trong sự nghiệp của mình với tư cách là nhà phân tích chứng khoán.

|  |
| --- |
| And that brings us to the topic of our next course, which will cover computing basics for security analysts. In that course, you'll learn how to use the Linux command line to authenticate and authorize users on the network, and to use S-Q-L, otherwise known as SQL, to communicate with databases. Great work getting here! All of the concepts you've learned in this section will be essential for success in your role as security analyst. Now you can move on to the next course. Enjoy! |

Và điều đó đưa chúng ta đến chủ đề của khóa học tiếp theo,sẽ bao gồm những vấn đề cơ bản về điện toán dành cho các nhà phân tích bảo mật.Trong khóa học đó, bạn sẽ học cách sử dụng dòng lệnh Linux để xác thực vàủy quyền cho người dùng trên mạng và sử dụng SQL,còn được gọi là SQL, để giao tiếp với cơ sở dữ liệu.Làm tốt lắm khi đến được đây!Tất cả các khái niệm bạn đã học trong phần này sẽ rất cần thiết chothành công trong vai trò là nhà phân tích bảo mật.Bây giờ bạn có thể chuyển sang khóa học tiếp theo. Thưởng thức!

***6.2. Course 3 glossary – Thuật ngữ khóa 3***

***6.3. Your Course 3 learning journey – Hành trình học tập Khóa 3 của bạn***

***6.4. Get started on the next course – Bắt đầu khóa học tiếp theo***

|  |
| --- |
| **Get started on the next course** |

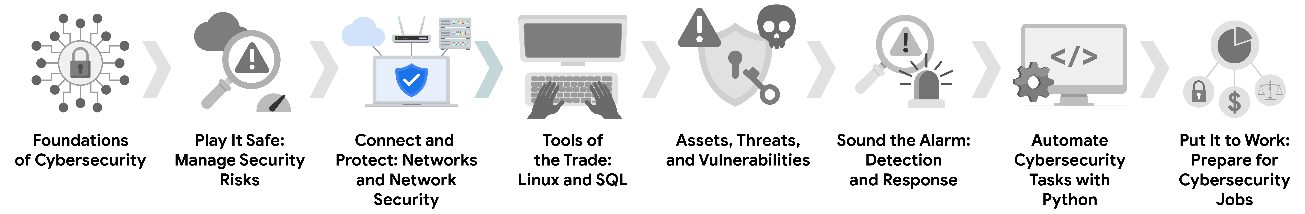
**Bắt đầu khóa học tiếp theo**

|  |
| --- |
| Congratulations on completing Course 3 of the Google Cybersecurity Certificate: **Connect and Protect: Networks and Network Security**! In this part of the program, you learned about the structure of networks and how to identify network vulnerabilities. You also explored network operations and how they affect the communication of data. Next, you discovered some common types of network attacks, their consequences on an organization, and ways to protect networks against attacks. Lastly, you learned how to reduce the attack surface of a network by applying various protective measures on a network. |

Chúc mừng bạn đã hoàn thành Khóa 3 của Chứng chỉ An ninh mạng của Google: **Kết nối và Bảo vệ: Mạng và An ninh Mạng** ! Trong phần này của chương trình, bạn đã tìm hiểu về cấu trúc của mạng và cách xác định các lỗ hổng mạng. Bạn cũng đã khám phá các hoạt động mạng và cách chúng ảnh hưởng đến việc truyền dữ liệu. Tiếp theo, bạn đã khám phá một số loại tấn công mạng phổ biến, hậu quả của chúng đối với một tổ chức và các cách bảo vệ mạng khỏi các cuộc tấn công. Cuối cùng, bạn đã học cách giảm bề mặt tấn công của mạng bằng cách áp dụng các biện pháp bảo vệ khác nhau trên mạng.

|  |
| --- |
| 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. *(This is the course you just completed. Well done!)* 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. 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 rõ về các lỗ hổng cấp độ mạng và cách bảo mật mạng. *(Đây là khóa học bạn vừa hoàn thành. Làm tốt lắm!)*
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.
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, leo thang 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.

|  |
| --- |
| Now that you have completed this course, you’re ready to move on to the next course: [**Tools of the Trade: Linux and SQL**](https://www.coursera.org/learn/linux-and-sql/home/week/1). |

Bây giờ bạn đã hoàn thành khóa học này, bạn đã sẵn sàng chuyển sang khóa học tiếp theo:[**Công cụ giao dịch: Linux và SQL**](https://www.coursera.org/learn/linux-and-sql/home/week/1).