Mục lục

[**Mục tiêu học tập** 1](#_Toc162043797)

[**Lịch sử an ninh mạng** 1](#_Toc162043798)

[**Chào mừng đến với mô-đun 2** 1](#_Toc162043799)

[**Các cuộc tấn công an ninh mạng trong quá khứ** 2](#_Toc162043800)

[**Tấn công trong thời đại kỹ thuật số** 4](#_Toc162043801)

[**Các cuộc tấn công phổ biến và hiệu quả của chúng** 7](#_Toc162043802)

[**Xác định: Phương thức tấn công** 13](#_Toc162043803)

[**Sean: Hãy bình tĩnh khi có sự cố vi phạm dữ liệu** 18](#_Toc162043804)

[**Tám miền bảo mật CISSP** 19](#_Toc162043805)

[**Giới thiệu về tám miền bảo mật CISSP, Phần 1** 19](#_Toc162043806)

[**Giới thiệu về tám miền bảo mật CISSP, Phần 2** 22](#_Toc162043807)

[**Xác định kiểu tấn công** 24](#_Toc162043808)

[**Hiểu kẻ tấn công** 24](#_Toc162043809)

[**Đánh giá: Sự phát triển của an ninh mạng** 24](#_Toc162043810)

[**Gói lại** 24](#_Toc162043811)

[**Thuật ngữ trong học phần 2** 25](#_Toc162043812)

[**Thử thách mô-đun 2** 27](#_Toc162043813)

Bạn sẽ khám phá các mối đe dọa an ninh mạng đã xuất hiện và phát triển như thế nào cùng với việc sử dụng máy tính. Bạn cũng sẽ hiểu các cuộc tấn công mạng trong quá khứ và hiện tại đã ảnh hưởng như thế nào đến sự phát triển của lĩnh vực bảo mật. Ngoài ra, bạn sẽ có được cái nhìn tổng quan về tám lĩnh vực bảo mật.

# **Mục tiêu học tập**

* Xác định các loại tấn công phổ biến nhất, trong quá khứ và hiện tại
* Xác định các cuộc tấn công bảo mật ảnh hưởng đến hoạt động kinh doanh như thế nào
* Nhận biết các cuộc tấn công trong quá khứ và hiện tại vào hoạt động kinh doanh đã dẫn đến sự phát triển của lĩnh vực bảo mật như thế nào
* Xác định tám miền bảo mật CISSP

# **Lịch sử an ninh mạng**

## **Chào mừng đến với mô-đun 2**

|  |
| --- |
| Welcome back! When it comes to security, there is so much to learn, and I'm thrilled to be part of your career journey. |

Chào mừng trở lại! Khi nói đến vấn đề bảo mật,có rất nhiều điều để học, và tôivui mừng được trở thành một phần trong hành trình sự nghiệp của bạn.

|  |
| --- |
| This is such an exciting time to be learning about security! When I learned about international hacks that impacted both private companies and government organizations, I was inspired to want to work in security because I realized how dynamic and important this field is. |

Đây quả là khoảng thời gian thú vịđang tìm hiểu về bảo mật!Khi tôi biết về các vụ hack quốc tếảnh hưởng đến cả các công ty tư nhânvà các tổ chức chính phủ,Tôi được truyền cảm hứng muốn làm việc trong lĩnh vực an ninh bởi vì tôinhận ra lĩnh vực này năng động và quan trọng như thế nào.

|  |
| --- |
| One reason there are so many jobs in the security field today, is because of attacks that happened in the 1980s and 1990s. Decades later, security professionals are still actively working to protect organizations and people from variations of these early computer attacks. |

Một lý do cóngày nay có rất nhiều việc làm trong lĩnh vực an ninh,là do các cuộc tấn công xảy ra vàonhững năm 1980 và 1990.Nhiều thập kỷ sau, các chuyên gia an ninhvẫn đang tích cực làm việc đểbảo vệ tổ chức và người dântừ các biến thể của những cuộc tấn công máy tính đầu tiên này.

|  |
| --- |
| In this section of the course, we'll discuss viruses and malware, and introduce the concept of social engineering. Then, we'll discuss how the digital age ushered in a new era of threat actors. Knowing the evolution of each attack is key to protecting against future attacks. Lastly, we'll provide an overview of eight security domains. |

Trong phần này của khóa học,chúng ta sẽ thảo luận về virus vàphần mềm độc hại và giới thiệu khái niệm về kỹ thuật xã hội.Sau đó, chúng ta sẽ thảo luận về cáchthời đại kỹ thuật số đã mở ra một kỷ nguyên mới của các tác nhân đe dọa.Biết diễn biến của mỗi đòn tấn công làchìa khóa để bảo vệ chống lại các cuộc tấn công trong tương lai.Cuối cùng, chúng tôi sẽ cung cấptổng quan về tám lĩnh vực bảo mật.

|  |
| --- |
| Next up, we'll travel back in time, to explore some of the viruses, data breaches, and malware attacks that have helped shape the industry as we know it today. |

Tiếp theo, chúng ta sẽ du hành ngược thời gian,để khám phá một số loại virus,vi phạm dữ liệu và tấn công phần mềm độc hạiđã giúp định hình ngành công nghiệp như chúng ta biết ngày nay.

## **Các cuộc tấn công an ninh mạng trong quá khứ**

|  |
| --- |
| **Past cybersecurity attacks**  The security industry is constantly evolving, but many present-day attacks are not entirely new. Attackers often alter or enhance previous methods. Understanding past attacks can provide direction for how to handle or investigate incidents in your job as a security analyst. First, let's go over a couple of key terms that will support your understanding of the attacks we'll discuss. A computer virus is malicious code written to interfere with computer operations and cause damage to data and software. The virus attaches itself to programs or documents on a computer, then spreads and infects one or more computers in a network. Today, viruses are more commonly referred to as malware, which is software designed to harm devices or networks. Two examples of early malware attacks that we'll cover are the Brain virus and the Morris worm. |

Ngành an ninh không ngừng phát triểnnhưng nhiều cuộc tấn công ngày nay không hoàn toàn mới.Những kẻ tấn công thường thay đổi hoặc nâng cao các phương pháp trước đó.Hiểu các cuộc tấn công trong quá khứ có thểđưa ra hướng xử lýhoặc điều tra các sự cố trongcông việc của bạn là một nhà phân tích bảo mật.Đầu tiên, chúng ta hãy điểm qua một số thuật ngữ chínhđiều đó sẽ hỗ trợ sự hiểu biết của bạnvề các cuộc tấn công mà chúng ta sẽ thảo luận.Virus máy tính làmã độc được viết để can thiệp vàohoạt động của máy tính và nguyên nhânhư hỏng dữ liệu và phần mềm.Virus tự bám vàochương trình hoặc tài liệu trên máy tính,sau đó lây lan và lây nhiễmmột hoặc nhiều máy tính trong mạng.Ngày nay, virus thường được gọi là phần mềm độc hại,là phần mềm được thiết kế để gây hại cho thiết bị hoặc mạng.Hai ví dụ về các cuộc tấn công phần mềm độc hại ban đầu mà chúng tôi sẽbao gồm virus Brain và sâu Morris.

|  |
| --- |
| They were created by malware developers to accomplish specific tasks. However, the developers underestimated the impact their malware would have and the amount of infected computers there would be. Let's take a closer look at these attacks and discuss how they helped shape security as we know it today. In 1986, the Alvi brothers created the Brain virus, although the intention of the virus was to track illegal copies of medical software and prevent pirated licenses, what the virus actually did was unexpected. Once a person used a pirated copy of the software, the virus-infected that computer. Then, any disk that was inserted into the computer was also infected. The virus spread to a new computer every time someone used one of the infected disks. Undetected, the virus spread globally within a couple of months. Although the intention was not to destroy data or hardware, the virus slowed down productivity and significantly impacted business operations. |

Chúng được tạo ra bởicác nhà phát triển phần mềm độc hại để hoàn thành các nhiệm vụ cụ thể.Tuy nhiên, các nhà phát triển đã đánh giá thấp tác độngphần mềm độc hại của họ sẽ có và số lượngsố máy tính bị nhiễm sẽ có.Chúng ta hãy xem xét kỹ hơn các cuộc tấn công này vàthảo luận về cách họ đã giúp hình thànhan ninh như chúng ta biết ngày nay.Năm 1986, anh em nhà Alvi đã tạo ra virus Brain,mặc dù mục đích của virus là theo dõisao chép bất hợp pháp phần mềm y tếvà ngăn chặn giấy phép vi phạm bản quyền,những gì virus thực sự đã làm thật bất ngờ.Khi một người sử dụng bản sao lậu của phần mềm,bị nhiễm virusmáy tính đó.Sau đó, bất kỳ đĩa nào đượcđưa vào máy tính cũng bị nhiễm virus.Virus lây lan sang máy tính mớimỗi khi ai đó sử dụng một trong các đĩa bị nhiễm.Virus không bị phát hiệnlan rộng trên toàn cầu trong vòng một vài tháng.Mặc dù mục đích không phải làphá hủy dữ liệu hoặc phần cứng,virus làm chậm năng suất vàđã ảnh hưởng đáng kể đến hoạt động kinh doanh.

|  |
| --- |
| The Brain virus fundamentally altered the computing industry, emphasizing the need for a plan to maintain security and productivity. As a security analyst, you will follow and maintain strategies put in place to ensure your organization has a plan to keep their data and people safe. Another influential computer attack was the Morris worm. |

Về cơ bản virus nãođã thay đổi ngành công nghiệp máy tính,nhấn mạnh sự cần thiết của một kế hoạchduy trì an ninh và năng suất.Là một nhà phân tích chứng khoán,bạn sẽ theo dõi và duy trìchiến lược được đưa ra để đảm bảotổ chức của bạn có một kế hoạchđể giữ an toàn cho dữ liệu của họ và mọi người.Một cuộc tấn công máy tính có ảnh hưởng khác là sâu Morris.

|  |
| --- |
| In 1988, Robert Morris developed a program to assess the size of the internet. The program crawled the web and installed itself onto other computers to tally the number of computers that were connected to the internet. Sounds simple, right? The program, however, failed to keep track of the computers it had already compromised and continued to re-install itself until the computers ran out of memory and crashed. About 6,000 computers were affected, representing 10% of the internet at the time. This attack cost millions of dollars in damages due to business disruptions and the efforts required to remove the worm. After the Morris worm, Computer Emergency Response Teams, known as CERTs®, were established to respond to computer security incidents. CERTs still exist today, but their place in the security industry has expanded to include more responsibilities. Later in this program, you'll learn more about the core functions of these security teams and gain hands-on practice with detection and response tools. Early attacks played a key role in shaping the current security industry. And coming up, we'll discuss how attacks evolved in the digital age. |

Năm 1988, Robert Morris đã phát triểnmột chương trình để đánh giá kích thước của internet.Chương trình đã thu thập thông tin trên web và tự cài đặt vàocác máy tính khác để kiểm đếm số lượngcủa các máy tính đã được kết nối với Internet.Nghe có vẻ đơn giản phải không?Tuy nhiên, chương trình đã thất bạitheo dõi các máy tính nó cóđã bị xâm phạm và tiếp tục cài đặt lạicho đến khi máy tính hết bộ nhớ và bị hỏng.Khoảng 6.000 máy tính bị ảnh hưởngchiếm 10% Internet vào thời điểm đó.Cuộc tấn công này gây thiệt hại hàng triệu đô la dosự gián đoạn kinh doanh và những nỗ lựccần thiết để loại bỏ sâu.Sau sâu Morris,Đội ứng phó khẩn cấp máy tính,được gọi là CERTs®, đượcđược thành lập để ứng phó với các sự cố an ninh máy tính.CERT vẫn tồn tại cho đến ngày nay,nhưng vị trí của họ trong ngành an ninh cóđược mở rộng để bao gồm nhiều trách nhiệm hơn.Sau đó trong chương trình này,bạn sẽ tìm hiểu thêm vềchức năng cốt lõi của các đội bảo mật nàyvà được thực hành thực tếvới các công cụ phát hiện và phản hồi.Các cuộc tấn công sớm đóng một vai trò quan trọngtrong việc định hình ngành công nghiệp an ninh hiện nay.Và sắp tới, chúng ta sẽ thảo luận về cáchcác cuộc tấn công phát triển trong thời đại kỹ thuật số.

## **Tấn công trong thời đại kỹ thuật số**

|  |
| --- |
| **Attacks in the digital age**  With the expansion of reliable high-speed internet, the number of computers connected to the internet increased dramatically. Because malware could spread through the internet, threat actors no longer needed to use physical disks to spread viruses. |

Với việc mở rộng mạng Internet tốc độ cao đáng tin cậy,số lượng máy tính kết nối internet tăng lên đáng kể.Vì phần mềm độc hại có thể lây lan qua internet,Các tác nhân đe dọa không còn cần thiết phải sử dụng đĩa vật lý để phát tán vi-rút.

|  |
| --- |
| To better understand attacks in the digital age, we'll discuss two notable attacks that relied on the internet: the LoveLetter attack and the Equifax breach. |

Để hiểu rõ hơn về các cuộc tấn công trong thời đại kỹ thuật số,chúng ta sẽ thảo luận về hai cuộc tấn công đáng chú ý dựa trên internet:cuộc tấn công LoveLetter và vi phạm Equachus.

|  |
| --- |
| In the year 2000, Onel De Guzman created the LoveLetter malware to steal internet login credentials. This attack spread rapidly and took advantage of people who had not developed a healthy suspicion for unsolicited emails. Users received an email with the subject line, "I Love You." Each email contained an attachment labeled, "Love Letter For You." When the attachment was opened, the malware scanned a user's address book. Then, it automatically sent itself to each person on the list and installed a program to collect user information and passwords. Recipients would think they were receiving an email from a friend, but it was actually malware. The LoveLetter ended up infecting 45 million computers globally and is believed to have caused over $10 billion dollars in damages. The LoveLetter attack is the first example of social engineering. |

Vào năm 2000, Onel De Guzman đã tạo ra Thư tìnhphần mềm độc hại để đánh cắp thông tin đăng nhập internet.Cuộc tấn công này lan truyền nhanh chóng và lợi dụng những người chưađã phát triển một sự nghi ngờ lành mạnh đối với các email không được yêu cầu.Người dùng đã nhận được một email có dòng tiêu đề "I Love You".Mỗi email đều chứa một tệp đính kèm có nhãn "Thư tình dành cho em".Khi tệp đính kèm được mở, phần mềm độc hại sẽ quét sổ địa chỉ của người dùng.Sau đó, nó tự động gửi đến từng người trong danh sách vàđã cài đặt một chương trình để thu thập thông tin người dùng và mật khẩu.Người nhận sẽ nghĩ rằng họ đang nhận được email từ một người bạn, nhưngnó thực sự là phần mềm độc hại.Bức thư tình cuối cùng đã lây nhiễm sang 45 triệu máy tính trên toàn cầuvà được cho là đã gây ra thiệt hại hơn 10 tỷ USD.Cuộc tấn công LoveLetter là ví dụ đầu tiên của kỹ thuật xã hội.

|  |
| --- |
| Social engineering is a manipulation technique that exploits human error to gain private information, access, or valuables. |

Kỹ thuật xã hội là một kỹ thuật thao túng khai tháclỗi của con người để có được thông tin cá nhân, quyền truy cập hoặc vật có giá trị.

|  |
| --- |
| After the LoveLetter, attackers understood the power of social engineering. The number of social engineering attacks is increasing with every new social media application that allows public access to people's data. Many people are now prioritizing convenience over privacy. The trade-off of this evolving shift is that these tools may lead to increased vulnerability, if people do not use them appropriately. |

Sau bức thư tình,Những kẻ tấn công hiểu được sức mạnh của kỹ thuật xã hội.Số lượng các cuộc tấn công kỹ thuật xã hội đang gia tăng với mỗiứng dụng truyền thông xã hội cho phép công chúng truy cập vào dữ liệu của mọi người.Nhiều người hiện đang ưu tiên sự thuận tiện hơn quyền riêng tư.Sự đánh đổi của sự thay đổi đang phát triển này là những công cụ này có thể dẫn đếntính dễ bị tổn thương tăng lên nếu người dân không sử dụng chúng một cách hợp lý.

|  |
| --- |
| As a security professional, your role is to identify and manage inappropriate use of technology that may place your organization and all the people associated with it at risk. One way to safeguard your organization is to conduct regular internal trainings, which you as a future security analyst may be asked to lead or participate in. |

Là một chuyên gia bảo mật, vai trò của bạn là xác định vàquản lý việc sử dụng công nghệ không phù hợp có thể khiến tổ chức của bạn vàtất cả những người liên quan đến nó đều gặp rủi ro.Một cách để bảo vệ tổ chức của bạn là tiến hành đào tạo nội bộ thường xuyên,mà bạn với tư cách là nhà phân tích bảo mật trong tương lai có thể được yêu cầu lãnh đạo hoặc tham gia.

|  |
| --- |
| Today, it's common for employees to receive training on how to identify social engineering attacks. Specifically, phishing through the emails they receive. Phishing is the use of digital communications to trick people into revealing sensitive data or deploying malicious software. |

Ngày nay, điều đó là phổ biến đối vớinhân viên được đào tạo về cách xác định các cuộc tấn công lừa đảo qua mạng xã hội.Cụ thể là lừa đảo qua email họ nhận được.Lừa đảo trực tuyến là việc sử dụng thông tin liên lạc kỹ thuật số để lừa mọi ngườitiết lộ dữ liệu nhạy cảm hoặc triển khai phần mềm độc hại.

|  |
| --- |
| Now, let's discuss the Equifax breach. In 2017, attackers successfully infiltrated the credit reporting agency, Equifax. This resulted in one of the largest known data breaches of sensitive information. Over 143 million customer records were stolen, and the breach affected approximately 40% of all Americans. |

Bây giờ, hãy thảo luận về vụ vi phạm Equachus.Năm 2017,Những kẻ tấn công đã xâm nhập thành công vào cơ quan báo cáo tín dụng Equifax.Điều này dẫn đến một trong những vụ vi phạm dữ liệu nhạy cảm lớn nhất được biết đến.Hơn 143 triệu hồ sơ khách hàng đã bị đánh cắpvi phạm đã ảnh hưởng đến khoảng 40% tổng số người Mỹ.

|  |
| --- |
| The records included personally identifiable information including social security numbers, birth dates, driver's license numbers, home addresses, and credit card numbers. From a security standpoint, the breach occurred due to multiple failures on Equifax's part. It wasn't just one vulnerability that the attackers took advantage of, there were several. The company failed to take the actions needed to fix multiple known vulnerabilities in the months leading up to the data breach. |

Các hồ sơ bao gồm thông tin nhận dạng cá nhân bao gồm số an sinh xã hội, ngày sinh, số giấy phép lái xe,địa chỉ nhà và số thẻ tín dụng.Từ quan điểm bảo mật,vi phạm xảy ra do nhiều lỗi từ phía Equachus.Những kẻ tấn công không chỉ lợi dụng một lỗ hổng,Có một vài.Công ty đã không thực hiện các hành động cần thiết để khắc phục nhiều lỗi đã biếtlỗ hổng trong những tháng dẫn đến vi phạm dữ liệu.

|  |
| --- |
| In the end, Equifax settled with the U.S. government and paid over $575 million dollars to resolve customer complaints and cover required fines. |

Cuối cùng, Equachus đã giải quyết với chính phủ Hoa Kỳ vàđã trả hơn 575 triệu đô la để giải quyết khiếu nại của khách hàng và trang trải các khoản tiền phạt bắt buộc.

|  |
| --- |
| While there have been other data breaches before and after the Equifax breach, the large settlement with the U.S. government alerted companies to the financial impact of a breach and the need to implement preventative measures. |

Mặc dù đã có những vụ vi phạm dữ liệu khác trước và sau vụ vi phạm Equachus,thỏa thuận lớn với chính phủ Hoa Kỳ đã cảnh báo các công tytác động tài chính của hành vi vi phạm và sự cần thiết phải thực hiện các biện pháp phòng ngừa.

|  |
| --- |
| These are just a couple of well-known incidents that have shaped the security industry. Knowing about them will help you in your security career. Understanding different types of malware and social engineering attacks will allow you to communicate about security risks during future job interviews. |

Đây chỉ là một vài sự cố nổi tiếng đã định hìnhngành an ninh.Biết về họ sẽ giúp ích cho sự nghiệp bảo mật của bạn.Việc hiểu rõ các loại phần mềm độc hại và tấn công kỹ thuật xã hội khác nhau sẽcho phép bạn trao đổi về các rủi ro bảo mật trong các cuộc phỏng vấn việc làm trong tương lai.

|  |
| --- |
| As a future security professional  constantly adapting and educating yourself on threat actors' tactics and techniques will be a part of your job. By noticing similar trends  patterns  and methodologies  you may be able to identify a potential breach and limit future damage. |

Là một chuyên gia bảo mật tương lai, không ngừng thích nghi và đào tạobản thân về chiến thuật và kỹ thuật của các tác nhân đe dọa sẽ là một phần công việc của bạn.Bằng cách nhận thấy các xu hướng, mô hình và phương pháp tương tự,bạn có thể xác định được hành vi vi phạm tiềm ẩn và hạn chế thiệt hại trong tương lai.

|  |
| --- |
| Finally  understanding how security affects people's lives is a good reminder of why the work you will do is so important! |

Cuối cùng, hiểu được an ninh ảnh hưởng như thế nào đến cuộc sống của con người làmột lời nhắc nhở hữu ích về lý do tại sao công việc bạn sẽ làm lại quan trọng đến vậy!

## **Các cuộc tấn công phổ biến và hiệu quả của chúng**

|  |
| --- |
| **Common attacks and their effectiveness**  Previously, you learned about past and present attacks that helped shape the cybersecurity industry. These included the LoveLetter attack, also called the ILOVEYOU virus, and the Morris worm. One outcome was the establishment of response teams, which are now commonly referred to as computer security incident response teams (CSIRTs). In this reading, you will learn more about common methods of attack. Becoming familiar with different attack methods, and the evolving tactics and techniques threat actors use, will help you better protect organizations and people. |

**Các cuộc tấn công phổ biến và hiệu quả của chúng**

Trước đây, bạn đã tìm hiểu về các cuộc tấn công trong quá khứ và hiện tại đã giúp định hình ngành an ninh mạng. Chúng bao gồm cuộc tấn công LoveLetter, còn được gọi là virus ILOVEYOU và sâu Morris. Một kết quả là việc thành lập các nhóm ứng phó, hiện nay thường được gọi là các nhóm ứng phó sự cố bảo mật máy tính (CSIRT). Trong bài đọc này, bạn sẽ tìm hiểu thêm về các phương pháp tấn công phổ biến. Làm quen với các phương thức tấn công khác nhau cũng như các chiến thuật và kỹ thuật ngày càng phát triển mà các tác nhân đe dọa sử dụng sẽ giúp bạn bảo vệ tổ chức và con người tốt hơn.

|  |
| --- |
| **Phishing**  **Phishing** is the use of digital communications to trick people into revealing sensitive data or deploying malicious software.  Some of the most common types of phishing attacks today include:   * **Business Email Compromise (BEC):** A threat actor sends an email message that seems to be from a known source to make a seemingly legitimate request for information, in order to obtain a financial advantage. * **Spear phishing:** A malicious email attack that targets a specific user or group of users. The email seems to originate from a trusted source. * **Whaling:** A form of spear phishing. Threat actors target company executives to gain access to sensitive data. * **Vishing:** The exploitation of electronic voice communication to obtain sensitive information or to impersonate a known source. * **Smishing:** The use of text messages to trick users, in order to obtain sensitive information or to impersonate a known source. |

**Lừa đảo**

**Lừa đảo** trực tuyến là việc sử dụng thông tin liên lạc kỹ thuật số để lừa mọi người tiết lộ dữ liệu nhạy cảm hoặc triển khai phần mềm độc hại.

Một số loại tấn công lừa đảo phổ biến nhất hiện nay bao gồm:

* **Thỏa hiệp email doanh nghiệp (BEC):** Kẻ đe dọa gửi một email có vẻ như đến từ một nguồn đã biết để đưa ra yêu cầu thông tin có vẻ hợp pháp nhằm đạt được lợi thế tài chính.
* **Lừa đảo trực tuyến:** Một cuộc tấn công bằng email độc hại nhắm vào một người dùng hoặc nhóm người dùng cụ thể. Email dường như có nguồn gốc từ một nguồn đáng tin cậy.
* **Whaling:** Một hình thức lừa đảo giáo. Các tác nhân đe dọa nhắm vào các giám đốc điều hành của công ty để có quyền truy cập vào dữ liệu nhạy cảm.
* **Vishing:** Việc khai thác giao tiếp bằng giọng nói điện tử để lấy thông tin nhạy cảm hoặc mạo danh một nguồn đã biết.
* **Smishing:** Việc sử dụng tin nhắn văn bản để lừa người dùng nhằm lấy được thông tin nhạy cảm hoặc mạo danh một nguồn đã biết.

|  |
| --- |
| **Malware**  **Malware** is software designed to harm devices or networks. There are many types of malware. The primary purpose of malware is to obtain money, or in some cases, an intelligence advantage that can be used against a person, an organization, or a territory.  Some of the most common types of malware attacks today include:   * **Viruses:** Malicious code written to interfere with computer operations and cause damage to data and software. A virus needs to be initiated by a user (i.e., a threat actor), who transmits the virus via a malicious attachment or file download. When someone opens the malicious attachment or download, the virus hides itself in other files in the now infected system. When the infected files are opened, it allows the virus to insert its own code to damage and/or destroy data in the system. * **Worms:** Malware that can duplicate and spread itself across systems on its own. In contrast to a virus, a worm does not need to be downloaded by a user. Instead, it self-replicates and spreads from an already infected computer to other devices on the same network. * **Ransomware:** A malicious attack where threat actors encrypt an organization's data and demand payment to restore access. * **Spyware:** Malware that’s used to gather and sell information without consent. Spyware can be used to access devices. This allows threat actors to collect personal data, such as private emails, texts, voice and image recordings, and locations. |

**Phần mềm độc hại** là phần mềm được thiết kế nhằm gây hại cho thiết bị hoặc mạng. Có nhiều loại phần mềm độc hại. Mục đích chính của phần mềm độc hại là lấy tiền hoặc trong một số trường hợp là lợi thế thông minh có thể được sử dụng để chống lại một cá nhân, tổ chức hoặc lãnh thổ.

Một số loại tấn công phần mềm độc hại phổ biến nhất hiện nay bao gồm:

* **Virus:** Mã độc được viết nhằm can thiệp vào hoạt động của máy tính và gây hư hỏng dữ liệu, phần mềm. Vi-rút cần được tạo ra bởi người dùng (tức là tác nhân đe dọa), người này truyền vi-rút thông qua tệp đính kèm hoặc tệp tải xuống độc hại. Khi ai đó mở tệp đính kèm hoặc tệp tải xuống độc hại, vi-rút sẽ ẩn mình trong các tệp khác trong hệ thống hiện đã bị nhiễm. Khi các tệp bị nhiễm được mở, nó cho phép vi-rút chèn mã riêng của nó để làm hỏng và/hoặc phá hủy dữ liệu trong hệ thống.
* **Worms:** Phần mềm độc hại có thể tự nhân bản và lây lan trên các hệ thống. Ngược lại với virus, người dùng không cần phải tải sâu xuống. Thay vào đó, nó tự sao chép và lây lan từ máy tính đã bị nhiễm sang các thiết bị khác trên cùng mạng.
* **Phần mềm tống tiền:** Một cuộc tấn công độc hại trong đó các tác nhân đe dọa mã hóa dữ liệu của tổ chức và yêu cầu thanh toán để khôi phục quyền truy cập.
* **Phần mềm gián điệp:** Phần mềm độc hại được sử dụng để thu thập và bán thông tin mà không có sự đồng ý. Phần mềm gián điệp có thể được sử dụng để truy cập các thiết bị. Điều này cho phép các tác nhân đe dọa thu thập dữ liệu cá nhân, chẳng hạn như email riêng tư, văn bản, bản ghi âm giọng nói và hình ảnh cũng như vị trí.

|  |
| --- |
| **Social Engineering**  **Social engineering** is a manipulation technique that exploits human error to gain private information, access, or valuables. Human error is usually a result of trusting someone without question. It’s the mission of a threat actor, acting as a social engineer, to create an environment of false trust and lies to exploit as many people as possible.  Some of the most common types of social engineering attacks today include:   * **Social media phishing:** A threat actor collects detailed information about their target from social media sites. Then, they initiate an attack. * **Watering hole attack:** A threat actor attacks a website frequently visited by a specific group of users. * **USB baiting:** A threat actor strategically leaves a malware USB stick for an employee to find and install, to unknowingly infect a network. * **Physical social engineering:** A threat actor impersonates an employee, customer, or vendor to obtain unauthorized access to a physical location.   **Social engineering principles**  Social engineering is incredibly effective. This is because people are generally trusting and conditioned to respect authority. The number of social engineering attacks is increasing with every new social media application that allows public access to people's data. Although sharing personal data—such as your location or photos—can be convenient, it’s also a risk.  Reasons why social engineering attacks are effective include:   * **Authority:** Threat actors impersonate individuals with power. This is because people, in general, have been conditioned to respect and follow authority figures. * **Intimidation:** Threat actors use bullying tactics. This includes persuading and intimidating victims into doing what they’re told. * **Consensus/Social proof:** Because people sometimes do things that they believe many others are doing, threat actors use others’ trust to pretend they are legitimate. For example, a threat actor might try to gain access to private data by telling an employee that other people at the company have given them access to that data in the past. * **Scarcity:** A tactic used to imply that goods or services are in limited supply. * **Familiarity:** Threat actors establish a fake emotional connection with users that can be exploited. * **Trust:** Threat actors establish an emotional relationship with users that can be exploited *over time*. They use this relationship to develop trust and gain personal information. * **Urgency:** A threat actor persuades others to respond quickly and without questioning. |

**Kỹ thuật xã hội** là một kỹ thuật thao túng khai thác lỗi của con người để lấy thông tin cá nhân, quyền truy cập hoặc vật có giá trị. Lỗi của con người thường là kết quả của việc tin tưởng ai đó mà không thắc mắc. Nhiệm vụ của kẻ đe dọa, hoạt động như một kẻ lừa đảo xã hội, là tạo ra một môi trường tin tưởng sai lầm và dối trá để lợi dụng càng nhiều người càng tốt.

Một số loại tấn công kỹ thuật xã hội phổ biến nhất hiện nay bao gồm:

* **Lừa đảo trên mạng xã hội:** Kẻ đe dọa thu thập thông tin chi tiết về mục tiêu của chúng từ các trang mạng xã hội. Sau đó, họ bắt đầu một cuộc tấn công.
* **Tấn công Watering Hole:** Kẻ đe dọa tấn công một trang web thường xuyên được một nhóm người dùng cụ thể truy cập.
* **Bẫy USB:** Kẻ đe dọa có chiến lược để lại thẻ USB chứa phần mềm độc hại để nhân viên tìm và cài đặt, nhằm vô tình lây nhiễm vào mạng.
* **Kỹ thuật xã hội vật lý:** Kẻ đe dọa mạo danh nhân viên, khách hàng hoặc nhà cung cấp để có quyền truy cập trái phép vào một vị trí thực tế.

**Nguyên tắc kỹ thuật xã hội**

Kỹ thuật xã hội cực kỳ hiệu quả. Điều này là do mọi người thường tin tưởng và có điều kiện để tôn trọng quyền lực. Số lượng các cuộc tấn công kỹ thuật xã hội đang gia tăng với mỗi ứng dụng truyền thông xã hội mới cho phép truy cập công khai vào dữ liệu của mọi người. Mặc dù việc chia sẻ dữ liệu cá nhân—chẳng hạn như vị trí hoặc ảnh của bạn—có thể thuận tiện nhưng cũng có rủi ro.

Lý do tại sao các cuộc tấn công kỹ thuật xã hội có hiệu quả bao gồm:

* **Quyền hạn:** Các tác nhân đe dọa mạo danh những cá nhân có quyền lực. Điều này là do mọi người nói chung đã có thói quen tôn trọng và tuân theo những người có thẩm quyền.
* **Đe dọa:** Những kẻ đe dọa sử dụng chiến thuật bắt nạt. Điều này bao gồm việc thuyết phục và đe dọa nạn nhân làm theo những gì họ được yêu cầu.
* **Sự đồng thuận/Bằng chứng xã hội:** Bởi vì mọi người đôi khi làm những việc mà họ tin rằng nhiều người khác đang làm, nên những kẻ đe dọa lợi dụng lòng tin của người khác để giả vờ rằng họ hợp pháp. Ví dụ: kẻ đe dọa có thể cố gắng giành quyền truy cập vào dữ liệu riêng tư bằng cách nói với nhân viên rằng những người khác trong công ty đã cấp cho họ quyền truy cập vào dữ liệu đó trước đây.
* **Sự khan hiếm:** Một chiến thuật được sử dụng để ám chỉ rằng hàng hóa hoặc dịch vụ có nguồn cung hạn chế.
* **Tính quen thuộc:** Các tác nhân đe dọa thiết lập kết nối cảm xúc giả tạo với người dùng và có thể bị lợi dụng.
* **Sự tin cậy:** Các tác nhân đe dọa thiết lập mối quan hệ tình cảm với người dùng và mối quan hệ này có thể bị lợi dụng *theo thời gian* . Họ sử dụng mối quan hệ này để phát triển lòng tin và thu thập thông tin cá nhân.
* **Khẩn cấp:** Kẻ đe dọa thuyết phục người khác phản ứng nhanh chóng và không đặt câu hỏi.

|  |
| --- |
| **Key takeaways**  In this reading, you learned about some common attacks and their impacts. You also learned about social engineering and why it’s so successful. While this is only a brief introduction to attack types, you will have many opportunities throughout the program to further develop your understanding of how to identify and defend against cybersecurity attacks. |

**Bài học chính**

Trong bài đọc này, bạn đã tìm hiểu về một số cuộc tấn công phổ biến và tác động của chúng. Bạn cũng đã tìm hiểu về kỹ thuật xã hội và lý do tại sao nó lại thành công như vậy. Mặc dù đây chỉ là phần giới thiệu ngắn gọn về các loại tấn công nhưng bạn sẽ có nhiều cơ hội trong suốt chương trình để phát triển hơn nữa sự hiểu biết của mình về cách xác định và phòng vệ trước các cuộc tấn công an ninh mạng.

## **Xác định: Phương thức tấn công**

|  |  |  |
| --- | --- | --- |
| **Malware** | **Virus** | **Worm** |
| **Ransomware** | **Spyware** | **Phishing** |
| **Spear phishing** | **Whaling** | **BEC** |
| **Vishing** | **Social engineering** | **Social media phishing** |
| **Watering hole attack** | **Physical social engineering** | **USB baiting** |

|  |  |
| --- | --- |
| **Malware – Phần mềm độc hại** | A software designed to harm devices or networks – Một phần mềm được thiết kế để gây hại cho thiết bị hoặc mạng  depiction |
| **Term: Virus – Thuật ngữ: Virus** | A malware program that modifies other computer programs by inserting its own code to damage and/or destroy data – Một chương trình phần mềm độc hại sửa đổi các chương trình máy tính khác bằng cách chèn mã của chính nó để làm hỏng và/hoặc phá hủy dữ liệu Example of: Malware  depiction |
| **Term: Worm – Thuật ngữ: Sâu** | Malware that self-replicates, spreading across the network and infecting computers – Phần mềm độc hại tự nhân bản, lây lan trên mạng và lây nhiễm vào máy tính Example of: Malware  depiction |
| **Term: Ransomware – Thuật ngữ: Phần mềm tống tiền** | A malicious attack during which threat actors encrypt an organization's data and demand payment to restore access – Một cuộc tấn công độc hại trong đó các tác nhân đe dọa mã hóa dữ liệu của tổ chức và yêu cầu thanh toán để khôi phục quyền truy cập Example of: Malware  depiction |
| **Term: Spyware – Thuật ngữ: Phần mềm gián điệp** | Malicious software installed on a user's computer without their permission, which is used to spy on and steal user data – Phần mềm độc hại được cài đặt trên máy tính của người dùng mà không có sự cho phép của họ, được sử dụng để theo dõi và đánh cắp dữ liệu của người dùng  Example of: Malware  depiction |
| **Term: Phishing – Thuật ngữ: Lừa đảo** | The use of digital communications to trick people into revealing sensitive data or deploying malicious software – Việc sử dụng thông tin liên lạc kỹ thuật số để lừa mọi người tiết lộ dữ liệu nhạy cảm hoặc triển khai phần mềm độc hại  depiction |
| **Term: Spear phishing – Thuật ngữ: Lừa đảo trực tuyến** | A malicious email attack targeting a specific user or group of users that appears to originate from a trusted source – Một cuộc tấn công bằng email độc hại nhắm vào một người dùng hoặc nhóm người dùng cụ thể có vẻ như đến từ một nguồn đáng tin cậy  Example of: Phishing  depiction |
| **Term: Whaling – Thuật ngữ: Whaling** | A form of spear phishing during which threat actors target executives in order to gain access to sensitive data – Một hình thức lừa đảo trực tuyến trong đó các tác nhân đe dọa nhắm mục tiêu vào các giám đốc điều hành để có quyền truy cập vào dữ liệu nhạy cảm  Example of: Phishing  depiction |
| **Term: Business email compromise (BEC) – Thuật ngữ: Thỏa hiệp email doanh nghiệp (BEC)** | An attack in which a threat actor impersonates a known source to obtain a financial advantage – Một cuộc tấn công trong đó kẻ đe dọa mạo danh một nguồn đã biết để đạt được lợi thế tài chính  Example of: Phishing  depiction |
| **Term: Vishing – Thuật ngữ: Vishing** | The exploitation of electronic voice communication to obtain sensitive information or to impersonate a known source – Việc khai thác liên lạc bằng giọng nói điện tử để lấy thông tin nhạy cảm hoặc mạo danh một nguồn đã biết  Example of: Phishing  depiction |
| **Term: Social engineering – Thuật ngữ: Kỹ thuật xã hội** | A manipulation technique that exploits human error to gain unauthorized access to sensitive, private, and/or valuable data – Một kỹ thuật thao túng khai thác lỗi của con người để có được quyền truy cập trái phép vào dữ liệu nhạy cảm, riêng tư và/hoặc có giá trị  depiction |
| **Term: Social media phishing – Thuật ngữ: Lừa đảo trên mạng xã hội** | An attack in which a threat actor collects detailed information about their target on social media sites before initiating an attack – Một cuộc tấn công trong đó kẻ đe dọa thu thập thông tin chi tiết về mục tiêu của chúng trên các trang truyền thông xã hội trước khi bắt đầu một cuộc tấn công  Example of: Social engineering  depiction |
| **Term**: **Watering hole attack – Thuật ngữ: Watering hole attack** | An attack in which a threat actor compromises a website frequently visited by a specific group of users – Một cuộc tấn công trong đó kẻ đe dọa xâm phạm một trang web thường xuyên được một nhóm người dùng cụ thể truy cập  Example of: Social engineering  depiction |
| **Term**: **Physical social engineering – Thuật ngữ: Kỹ thuật xã hội vật lý** | An attack in which a threat actor impersonates an employee, customer, or vendor to obtain unauthorized access to a physical location – Một cuộc tấn công trong đó kẻ đe dọa mạo danh nhân viên, khách hàng hoặc nhà cung cấp để có quyền truy cập trái phép vào một vị trí thực tế  Example of: Social engineering  depiction |
| **Term**: **USB baiting – Thuật ngữ: mồi USB** | An attack in which a threat actor strategically leaves a malware USB stick for an employee to find and unknowingly infect a network – Một cuộc tấn công trong đó kẻ đe dọa có chiến lược để lại một thanh USB chứa phần mềm độc hại để nhân viên tìm thấy và vô tình lây nhiễm vào mạng  Example of: Social engineering  depiction |

## **Sean: Hãy bình tĩnh khi có sự cố vi phạm dữ liệu**

|  |
| --- |
| **Sean: Keep your cool during a data breach**  Hi, my name is Sean. I'm a Technical Program Manager in Google workspace. I am a 30 year security veteran within the security space across six different industries. During your first data breach, the most important thing that you can do is keep your cool. Everyone around is going to be freaking out. If you are on the security team and you are managing the incident, you have to legitimately be the cool guy in the room. Be that person that has the pause in the conversation. Somebody might be like, do you know what's going on? I absolutely do. I think the biggest breach I've ever had was a phone call. An engineer for another financial, bought a server off eBay. That server fired it up hadn't been wiped. Twenty million credit card records were on it. That triggered a whole review of we had not been controlling for how do third parties because we were now outsourcing data centers. How do third parties wipe the servers that we no longer use? The first thing you're going to do is to contain the breach. If you are still hemorrhaging data, you go through your progressions to stop hemorrhaging data. So if that means shutting down a server, shutting down a data center, shutting down comms, whatever, stopping the data loss is that is your number one priority. Your job as an incident manager or as somebody working a breach is to stop the breach and then investigate the breach. So executing your incident management by plan is the most important thing that an entry level person can keep in mind. |

Xin chào, tên tôi là Sean.Tôi là Người quản lý chương trình kỹ thuật trong không gian làm việc của Google.Tôi là một cựu chiến binh an ninh 30 nămtrong không gian an ninhtrên sáu ngành công nghiệp khác nhau.Trong lần vi phạm dữ liệu đầu tiên của bạn,điều quan trọng nhất mà bạn có thểlàm là giữ bình tĩnh của bạn.Mọi người xung quanh sẽ phát hoảng.Nếu bạn đang ở trênđội an ninh và bạn đang quản lý vụ việc,bạn phải là một chàng trai tuyệt vời trong phòng một cách hợp pháp.Hãy là người tạm dừng cuộc trò chuyện.Ai đó có thể sẽ như thế này, bạn có biết chuyện gì đang xảy ra không?Tôi hoàn toàn làm được.Tôi nghĩ vi phạm lớn nhất tôi từng cóđã có một cuộc điện thoại.Một kỹ sư tài chính khác,đã mua một máy chủ từ eBay.Máy chủ đó kích hoạt nó vẫn chưa bị xóa.Hai mươi triệu hồ sơ thẻ tín dụng có trong đó.Điều đó đã kích hoạt một cuộc đánh giá toàn bộtrong số chúng tôi đã không kiểm soátđối với bên thứ ba thì sao vìchúng tôi hiện đang thuê ngoài các trung tâm dữ liệu.Làm thế nào để bên thứ ba xóa sạchcác máy chủ mà chúng tôi không còn sử dụng nữa?Điều đầu tiên bạn sẽ làmlà để ngăn chặn sự vi phạm.Nếu bạn vẫn đang xuất huyết dữ liệu,bạn trải qua quá trình tiến triển của mìnhđể ngừng xuất huyết dữ liệu.Vậy nếu điều đó có nghĩa là tắt máy chủ,đóng cửa trung tâm dữ liệu, tắt liên lạc,sao cũng được, ngăn chặn việc mất dữ liệu làđó là ưu tiên số một của bạn.Công việc của bạn với tư cách là người quản lý sự cố hoặc là người đang làm việcvi phạm là phải dừng lạivi phạm và sau đó điều tra vi phạm.Vì vậy, việc thực hiện quản lý sự cố theo kế hoạch làđiều quan trọng nhất đómột người ở trình độ đầu vào có thể ghi nhớ.

## **Kiểm tra kiến thức của bạn: Lịch sử an ninh mạng**

# **Tám miền bảo mật CISSP**

## **Giới thiệu về tám miền bảo mật CISSP, Phần 1**

|  |
| --- |
| **Introduction to the eight CISSP security domains, Part 1**  As the tactics of threat actors evolve, so do the roles of security professionals. Having a solid understanding of core security concepts will support your growth in this field. One way to better understand these core concepts is by organizing them into categories, called security domains. |

**Giới thiệu về tám miền bảo mật CISSP, Phần 1**

Khi chiến thuật của các tác nhân đe dọa phát triển thì vai trò của các chuyên gia bảo mật cũng thay đổi.Có sự hiểu biết vững chắc về các khái niệm bảo mật cốt lõi sẽ hỗ trợ sự phát triển của bạntrong lĩnh vực này.Một cách để hiểu rõ hơn những khái niệm cốt lõi này làtổ chức chúng thành các danh mục, được gọi là miền bảo mật.

|  |
| --- |
| As of 2022, CISSP has defined eight domains to organize the work of security professionals. It's important to understand that these domains are related and that gaps in one domain can result in negative consequences to an entire organization. |

Tính đến năm 2022, CISSP đã xác định tám miềntổ chức công việc của các chuyên gia an ninh.Điều quan trọng là phải hiểu rằng các lĩnh vực này có liên quan với nhau và những khoảng trống trong mộttên miền có thể dẫn đến hậu quả tiêu cực cho toàn bộ tổ chức.

|  |
| --- |
| It's also important to understand the domains because it may help you better understand your career goals and your role within an organization. As you learn more about the elements of each domain, the work involved in one may appeal to you more than the others. This domain may become a career path for you to explore further. |

Điều quan trọng là phải hiểu tên miền vì nó có thể giúp íchbạn hiểu rõ hơn về mục tiêu nghề nghiệp và vai trò của mình trong tổ chức.Khi bạn tìm hiểu thêm về các thành phần của từng miền,công việc liên quan đến một công việc có thể hấp dẫn bạn hơn những công việc khác.Tên miền này có thể trở thành con đường sự nghiệp để bạn khám phá thêm.

|  |
| --- |
| CISSP defines eight domains in total, and we'll discuss all eight between this video and the next. In this video, we're going to cover the first four: security and risk management, asset security, security architecture and engineering, and communication and network security. |

CISSP xác định tổng cộng tám miền vàchúng ta sẽ thảo luận về tất cả tám điều trong video này và video tiếp theo.Trong video này, chúng ta sẽ đề cập đến bốn điều đầu tiên:an ninh và quản lý rủi ro, bảo mật tài sản,kiến trúc và kỹ thuật an ninh, an ninh mạng và truyền thông.

|  |
| --- |
| Let's start with the first domain, security and risk management. Security and risk management focuses on defining security goals and objectives, risk mitigation, compliance, business continuity, and the law. For example, security analysts may need to update company policies related to private health information if a change is made to a federal compliance regulation such as the Health Insurance Portability and Accountability Act, also known as HIPAA. |

Hãy bắt đầu với lĩnh vực đầu tiên, bảo mật và quản lý rủi ro.Quản lý rủi ro và bảo mật tập trung vào việc xác định các mục tiêu và mục đích bảo mật,giảm thiểu rủi ro, tuân thủ, kinh doanh liên tục và pháp luật.Ví dụ: nhà phân tích bảo mật có thể cần cập nhật chính sách của công ty liên quan đến thông tin sức khỏe cá nhân nếu một thay đổi được thực hiện đối với quy định tuân thủ của liên bang như Đạo luật về trách nhiệm giải trình và cung cấp bảo hiểm y tế, còn được gọi là HIPAA.

|  |
| --- |
| The second domain is asset security. This domain focuses on securing digital and physical assets. It's also related to the storage, maintenance, retention, and destruction of data. When working with this domain, security analysts may be tasked with making sure that old equipment is properly disposed of and destroyed, including any type of confidential information. |

Lĩnh vực thứ hai là bảo mật tài sản.Miền này tập trung vào việc bảo mật tài sản vật lý và kỹ thuật số.Nó cũng liên quan đến việc lưu trữ, bảo trì, duy trì vàsự phá hủy dữ liệu.Khi làm việc với miền này, các nhà phân tích bảo mật có thể được giao nhiệm vụđảm bảo rằng thiết bị cũ được xử lý đúng cách vàbị phá hủy, bao gồm bất kỳ loại thông tin bí mật nào.

|  |
| --- |
| The third domain is security architecture and engineering. This domain focuses on optimizing data security by ensuring effective tools, systems, and processes are in place. As a security analyst, you may be tasked with configuring a firewall. A firewall is a device used to monitor and filter incoming and outgoing computer network traffic. Setting up a firewall correctly helps prevent attacks that could affect productivity. |

Lĩnh vực thứ ba là kiến ​​trúc và kỹ thuật bảo mật.Miền này tập trung vào việc tối ưu hóa bảo mật dữ liệu bằng cách đảm bảo các công cụ hiệu quả,các hệ thống và quy trình đang được thực hiện.Là một nhà phân tích bảo mật, bạn có thể được giao nhiệm vụ cấu hình tường lửa.Tường lửa là một thiết bị được sử dụng để giám sát và lọc các thông tin đến vàlưu lượng mạng máy tính đi.Thiết lập tường lửa đúng cách giúp ngăn chặn các cuộc tấn công có thể ảnh hưởng đếnnăng suất.

|  |
| --- |
| The fourth security domain is communication and network security. This domain focuses on managing and securing physical networks and wireless communications. As a security analyst, you may be asked to analyze user behavior within your organization. |

Lĩnh vực bảo mật thứ tư là an ninh mạng và truyền thông.Miền này tập trung vào việc quản lý và bảo mật mạng vật lý và giao tiếp không dây.Là một nhà phân tích chứng khoán,bạn có thể được yêu cầu phân tích hành vi của người dùng trong tổ chức của mình.

|  |
| --- |
| Imagine discovering that users are connecting to unsecured wireless hotspots. This could leave the organization and its employees vulnerable to attacks. To ensure communications are secure, you would create a network policy to prevent and mitigate exposure. |

Hãy tưởng tượng phát hiện ra rằng người dùng đang kết nối với các điểm truy cập không dây không an toàn.Điều này có thể khiến tổ chức và nhân viên của tổ chức dễ bị tấn công.Để đảm bảo thông tin liên lạc được an toàn, bạn sẽ tạo một chính sách mạng đểngăn ngừa và giảm thiểu phơi nhiễm.

|  |
| --- |
| Maintaining an organization's security is a team effort, and there are many moving parts. As an entry-level analyst, you will continue to develop your skills by learning how to mitigate risks to keep people and data safe. |

Duy trì an ninh của một tổ chức là nỗ lực của nhóm vàcó nhiều bộ phận chuyển động.Là một nhà phân tích cấp đầu vào, bạn sẽ tiếp tục phát triển kỹ năng của mìnhbằng cách học cách giảm thiểu rủi ro để giữ an toàn cho con người và dữ liệu.

|  |
| --- |
| You don't need to be an expert in all domains. But, having a basic understanding of them will aid you in your journey as a security professional. |

Bạn không cần phải là chuyên gia trong mọi lĩnh vực. Tuy nhiên, có sự hiểu biết cơ bảntrong số họ sẽ hỗ trợ bạn trong hành trình trở thành một chuyên gia bảo mật.

|  |
| --- |
| You're doing great! We have just introduced the first four security domains, and in the next video, we'll discuss four more! See you soon! |

Bạn đang làm rất tốt! Chúng tôi vừa giới thiệu bốn biện pháp bảo mật đầu tiêntên miền và trong video tiếp theo, chúng ta sẽ thảo luận thêm về bốn tên miền nữa!Hẹn sớm gặp lại!

## **Giới thiệu về tám miền bảo mật CISSP, Phần 2**

|  |
| --- |
| **Introduction to the eight CISSP security domains, Part 2**  Welcome back. In the last video, we introduced you to the first four security domains. In this video, we'll introduce you to the next four security domains: identity and access management, security assessment and testing, security operations, and software development security. |

**Giới thiệu về tám miền bảo mật CISSP, Phần 2**

Chào mừng trở lại. Trong video cuối cùng,chúng tôi đã giới thiệu cho bạn bốn miền bảo mật đầu tiên.Trong video này chúng tôi sẽ giới thiệubạn đến bốn miền bảo mật tiếp theo:quản lý danh tính và quyền truy cập,đánh giá và kiểm tra an ninh,hoạt động bảo mật và bảo mật phát triển phần mềm.

|  |
| --- |
| Familiarizing yourself with these domains will allow you to navigate the complex world of security. The domains outline and organize how a team of security professionals work together. Depending on the organization, analyst roles may sit at the intersection of multiple domains or focus on one specific domain. Knowing where a particular role fits within the security landscape will help you prepare for job interviews and work as part of a full security team. |

Làm quen với những miền này sẽcho phép bạn điều hướng thế giới bảo mật phức tạp.Các miền phác thảo và tổ chứccách một nhóm chuyên gia bảo mật làm việc cùng nhau.Tùy theo tổ chức,vai trò của nhà phân tích có thể nằm ở giao điểm củanhiều tên miền hoặc tập trung vào một tên miền cụ thể.Biết vai trò cụ thể ở đâuphù hợp với bối cảnh an ninhsẽ giúp bạn chuẩn bị cho cuộc phỏng vấn xin việcvà làm việc như một phần của đội bảo mật đầy đủ.

|  |
| --- |
| Let's move into the fifth domain: identity and access management. Identity and access management focuses on keeping data secure, by ensuring users follow established policies to control and manage physical assets, like office spaces, and logical assets, such as networks and applications. Validating the identities of employees and documenting access roles are essential to maintaining the organization's physical and digital security. For example, as a security analyst, you may be tasked with setting up employees' keycard access to buildings. |

Hãy chuyển sang miền thứ năm:quản lý danh tính và quyền truy cập.Quản lý danh tính và quyền truy cậptập trung vào việc giữ an toàn cho dữ liệu, bằng cáchđảm bảo người dùng tuân theo các chính sách đã thiết lậpđể kiểm soát và quản lý tài sản vật chất,như không gian văn phòng, vàcác tài sản logic, chẳng hạn như mạng và ứng dụng.Xác thực danh tính củanhân viên và ghi lại vai trò truy cậplà cần thiết để duy trìan ninh vật lý và kỹ thuật số của tổ chức.Ví dụ, với tư cách là một nhà phân tích chứng khoán,bạn có thể được giao nhiệm vụ thiết lậpthẻ khóa của nhân viên vào các tòa nhà.

|  |
| --- |
| The sixth domain is security assessment and testing. This domain focuses on conducting security control testing, collecting and analyzing data, and conducting security audits to monitor for risks, threats, and vulnerabilities. Security analysts may conduct regular audits of user permissions, to make sure that users have the correct level of access. For example, access to payroll information is often limited to certain employees, so analysts may be asked to regularly audit permissions to ensure that no unauthorized person can view employee salaries. |

Lĩnh vực thứ sáu là đánh giá và kiểm tra bảo mật.Miền này tập trung vàotiến hành kiểm tra kiểm soát an ninh,thu thập, phân tích dữ liệu và tiến hànhkiểm tra an ninh để giám sátrủi ro, mối đe dọa và điểm yếu.Các nhà phân tích chứng khoán có thể tiến hành kiểm tra thường xuyên cácquyền của người dùng, để đảm bảo rằngngười dùng có cấp độ truy cập chính xác.Ví dụ, truy cập vàoThông tin về bảng lương thường xuyêngiới hạn ở một số nhân viên nhất định, vì vậycác nhà phân tích có thể được yêu cầu thường xuyên kiểm tra quyềnđảm bảo rằng không có người trái phépcó thể xem lương nhân viên.

|  |
| --- |
| The seventh domain is security operations. This domain focuses on conducting investigations and implementing preventative measures. Imagine that you, as a security analyst, receive an alert that an unknown device has been connected to your internal network. You would need to follow the organization's policies and procedures to quickly stop the potential threat. |

Lĩnh vực thứ bảy là hoạt động an ninh.Miền này tập trung vào việc tiến hànhđiều tra và thực hiện các biện pháp ngăn chặn.Hãy tưởng tượng rằng bạn, với tư cách là một nhà phân tích chứng khoán,nhận được cảnh báo rằngmột thiết bị không xác định đã đượcđược kết nối với mạng nội bộ của bạn.Bạn sẽ cần phải tuân theo các chính sách của tổ chứcvà các thủ tục để nhanh chóng ngăn chặn mối đe dọa tiềm tàng.

|  |
| --- |
| The final, eighth domain is software development security. This domain focuses on using secure coding practices, which are a set of recommended guidelines that are used to create secure applications and services. A security analyst may work with software development teams to ensure security practices are incorporated into the software development life-cycle. If, for example, one of your partner teams is creating a new mobile app, then you may be asked to advise on the password policies or ensure that any user data is properly secured and managed. |

Lĩnh vực cuối cùng thứ tám là bảo mật phát triển phần mềm.Miền này tập trung vào việc sử dụng các phương pháp mã hóa an toàn,đó là một bộ hướng dẫn được đề xuất được sử dụngđể tạo ra các ứng dụng và dịch vụ an toàn.Một nhà phân tích bảo mật có thể làm việc vớinhóm phát triển phần mềm để đảm bảothực hành bảo mật được kết hợpvào vòng đời phát triển phần mềm.Nếu, ví dụ,một trong các nhóm đối tác của bạn đang tạo một ứng dụng di động mới,sau đó bạn có thể được yêu cầutư vấn về chính sách mật khẩu hoặcđảm bảo rằng mọi dữ liệu người dùng đều đượcđược bảo mật và quản lý đúng cách.

|  |
| --- |
| That ends our introduction to CISSP's eight security domains. Challenge yourself to better understand each of these domains and how they affect the overall security of an organization. While they may still be a bit unclear to you this early in the program, these domains will be discussed in greater detail in the next course. See you there! |

Điều đó kết thúc phần giới thiệu của chúng tôi vềTám miền bảo mật của CISSP.Thử thách bản thân để hiểu rõ hơn về từng điềunhững tên miền này và cách chúng ảnh hưởngan ninh tổng thể của một tổ chức.Mặc dù chúng có thể vẫn còn một chútbạn chưa rõ điều này ngay từ đầu chương trình,những lĩnh vực này sẽ được thảo luận trongchi tiết hơn trong khóa học tiếp theo. Hẹn gặp bạn ở đó!

## **Xác định kiểu tấn công**

## **Hiểu kẻ tấn công**

## **Kiểm tra kiến thức của bạn: Tám miền bảo mật CISSP**

# **Đánh giá: Sự phát triển của an ninh mạng**

## **Gói lại**

|  |
| --- |
| **Wrap-up**  **This concludes our brief introduction to some of the most influential security attacks throughout history and CISSP's eight security domains. Let's review what we've discussed.** |

**Gói lại**

Điều này kết thúc phần giới thiệu ngắn gọn của chúng tôi về một số người có ảnh hưởng nhấtcác cuộc tấn công bảo mật trong suốt lịch sử và tám lĩnh vực bảo mật của CISSP.Hãy xem lại những gì chúng ta đã thảo luận.

|  |
| --- |
| First, we covered viruses, including the Brain virus and the Morris worm, and discussed how these early forms of malware shaped the security industry. We also discussed how many attacks today are variants of these early examples. Understanding previous attacks is critical for security professionals who are working to protect organizations and people from possible future variants. |

Đầu tiên, chúng tôi đề cập đến các loại vi-rút, bao gồm vi-rút Brain và sâu Morris,và thảo luận về cách những dạng phần mềm độc hại ban đầu này đã định hình ngành bảo mật như thế nào.Chúng tôi cũng thảo luận về số lượng cuộc tấn công ngày nay là biến thể của những ví dụ ban đầu này.Hiểu các cuộc tấn công trước đó là rất quan trọng đối với các chuyên gia bảo mật, những ngườiđang làm việc để bảo vệ các tổ chức và con người khỏi các biến thể có thể xảy ra trong tương lai.

|  |
| --- |
| We also discussed social engineering and threat actor motives by learning about the LoveLetter attack and the Equifax data breach. These incidents showed the widespread impacts and associated costs of more recent security breaches in the digital age. |

Chúng tôi cũng thảo luận về kỹ thuật xã hội và động cơ của tác nhân đe dọa bằng cách tìm hiểu về cuộc tấn công LoveLetter và vụ vi phạm dữ liệu Equifax.Những sự cố này cho thấy tác động lan rộng và chi phí liên quan đến các vi phạm an ninh gần đây hơn trong thời đại kỹ thuật số.

|  |
| --- |
| Finally, we introduced CISSP's eight security domains and how they can be used to categorize different areas of focus within the security profession. |

Cuối cùng, chúng tôi đã giới thiệu tám miền bảo mật của CISSP và cách chúng có thể đượcđược sử dụng để phân loại các lĩnh vực trọng tâm khác nhau trong ngành bảo mật.

|  |
| --- |
| I hope you're feeling confident about your foundational security knowledge! Learning the history of security can allow you to better understand the current industry. CISSP's eight security domains provide a way to organize the work of security professionals. |

Tôi hy vọng bạn cảm thấy tự tin về kiến ​​thức bảo mật cơ bản của mình!Tìm hiểu lịch sử bảo mật có thể cho phép bạn hiểu rõ hơn về hiện tạingành công nghiệp.Tám miền bảo mật của CISSP cung cấp một cách để tổ chứccông việc của các chuyên gia an ninh.

|  |
| --- |
| Remember, every security professional is essential. Your unique point of view, professional background, and knowledge are valuable. So, the diversity you bring to the field will further improve the security industry as you work to keep organizations and people safe. |

Hãy nhớ rằng, mọi chuyên gia bảo mật đều cần thiết.Quan điểm độc đáo, nền tảng chuyên môn và kiến ​​thức của bạn rất có giá trị.Vì vậy, sự đa dạng mà bạn mang đến cho lĩnh vực này sẽ tiếp tụccải thiện ngành bảo mật khi bạn nỗ lực giữ an toàn cho các tổ chức và mọi người.

## **Thuật ngữ trong học phần 2**

|  |
| --- |
| **Glossary terms from module 2**  **Terms and definitions from Course 1, Module 2** |

**Thuật ngữ trong học phần 2**

**Các thuật ngữ và định nghĩa trong Khóa 1, Học phần 2**

|  |
| --- |
| **Adversarial artificial intelligence (AI):** A technique that manipulates artificial intelligence (AI) and machine learning (ML) technology to conduct attacks more efficiently |

**Trí tuệ nhân tạo đối nghịch (AI):** Một kỹ thuật vận dụng trí tuệ nhân tạo (AI) và công nghệ máy học (ML) để tiến hành các cuộc tấn công hiệu quả hơn

|  |
| --- |
| **Business Email Compromise (BEC):** A type of phishing attack where a threat actor impersonates a known source to obtain financial advantage |

**Thỏa hiệp email doanh nghiệp (BEC):** Một loại tấn công lừa đảo trong đó tác nhân đe dọa mạo danh một nguồn đã biết để đạt được lợi ích tài chính

|  |
| --- |
| **CISSP:** Certified Information Systems Security Professional is a globally recognized and highly sought-after information security certification, awarded by the International Information Systems Security Certification Consortium |

**CISSP:** Chuyên gia bảo mật hệ thống thông tin được chứng nhận là chứng chỉ bảo mật thông tin được công nhận trên toàn cầu và được săn đón nhiều, do Hiệp hội chứng nhận bảo mật hệ thống thông tin quốc tế trao tặng

|  |
| --- |
| **Computer virus:** Malicious code written to interfere with computer operations and cause damage to data and software |

**Virus máy tính:** Mã độc được viết nhằm can thiệp vào hoạt động của máy tính và gây hư hỏng dữ liệu, phần mềm

|  |
| --- |
| **Cryptographic attack:** An attack that affects secure forms of communication between a sender and intended recipient |

**Tấn công mật mã:** Một cuộc tấn công ảnh hưởng đến các hình thức liên lạc an toàn giữa người gửi và người nhận dự định

|  |
| --- |
| **Hacker:** Any person who uses computers to gain access to computer systems, networks, or data |

**Hacker:** Bất kỳ người nào sử dụng máy tính để truy cập vào hệ thống máy tính, mạng hoặc dữ liệu

|  |
| --- |
| **Malware:** Software designed to harm devices or networks |

**Phần mềm độc hại:** Phần mềm được thiết kế để gây hại cho thiết bị hoặc mạng

|  |
| --- |
| **Password attack:** An attempt to access password secured devices, systems, networks, or data |

**Tấn công mật khẩu:** Nỗ lực truy cập các thiết bị, hệ thống, mạng hoặc dữ liệu được bảo mật bằng mật khẩu

|  |
| --- |
| **Phishing:** The use of digital communications to trick people into revealing sensitive data or deploying malicious software |

**Lừa đảo:** Việc sử dụng thông tin liên lạc kỹ thuật số để lừa mọi người tiết lộ dữ liệu nhạy cảm hoặc triển khai phần mềm độc hại

|  |
| --- |
| **Physical attack:** A security incident that affects not only digital but also physical environments where the incident is deployed |

**Tấn công vật lý:** Một sự cố bảo mật không chỉ ảnh hưởng đến môi trường kỹ thuật số mà còn cả môi trường vật lý nơi sự cố được triển khai

|  |
| --- |
| **Physical social engineering:** An attack in which a threat actor impersonates an employee, customer, or vendor to obtain unauthorized access to a physical location |

**Kỹ thuật xã hội vật lý:** Một cuộc tấn công trong đó tác nhân đe dọa mạo danh nhân viên, khách hàng hoặc nhà cung cấp để có quyền truy cập trái phép vào một vị trí thực tế

|  |
| --- |
| **Social engineering:** A manipulation technique that exploits human error to gain private information, access, or valuables |

**Kỹ thuật xã hội:** Một kỹ thuật thao túng khai thác lỗi của con người để lấy thông tin cá nhân, quyền truy cập hoặc tài sản có giá trị

|  |
| --- |
| **Social media phishing:** A type of attack where a threat actor collects detailed information about their target on social media sites before initiating the attack |

**Lừa đảo trên mạng xã hội:** Một kiểu tấn công trong đó kẻ đe dọa thu thập thông tin chi tiết về mục tiêu của họ trên các trang mạng xã hội trước khi bắt đầu cuộc tấn công

|  |
| --- |
| **Spear phishing:** A malicious email attack targeting a specific user or group of users, appearing to originate from a trusted source |

**Phishing lừa đảo:** Một cuộc tấn công bằng email độc hại nhắm vào một người dùng hoặc nhóm người dùng cụ thể, dường như bắt nguồn từ một nguồn đáng tin cậy

|  |
| --- |
| **Supply-chain attack:** An attack that targets systems, applications, hardware, and/or software to locate a vulnerability where malware can be deployed |

**Tấn công chuỗi cung ứng:** Một cuộc tấn công nhắm vào các hệ thống, ứng dụng, phần cứng và/hoặc phần mềm để xác định lỗ hổng nơi phần mềm độc hại có thể được triển khai

|  |
| --- |
| **USB baiting:** An attack in which a threat actor strategically leaves a malware USB stick for an employee to find and install to unknowingly infect a network |

**USB baiting:** Một cuộc tấn công trong đó kẻ đe dọa có chiến lược để lại một thẻ USB chứa phần mềm độc hại để nhân viên tìm và cài đặt nhằm vô tình lây nhiễm vào mạng

|  |
| --- |
| **Virus:** refer to “computer virus” |

**Virus:** tham khảo “virus máy tính”

|  |
| --- |
| **Vishing:** The exploitation of electronic voice communication to obtain sensitive information or to impersonate a known source |

**Vishing:** Việc khai thác giao tiếp bằng giọng nói điện tử để lấy thông tin nhạy cảm hoặc mạo danh một nguồn đã biết

|  |
| --- |
| **Watering hole attack**: A type of attack when a threat actor compromises a website frequently visited by a specific group of users |

**Tấn công Watering Hole** : Một kiểu tấn công khi tác nhân đe dọa xâm phạm một trang web thường được một nhóm người dùng cụ thể truy cập

## **Thử thách mô-đun 2**