## LESSON: Network Security Models and Cryptography

## Primer For this lesson and upcoming lessons, instructors are required to ensure the following activities are completed for each lesson

* Checking with the student to see if they have any questions or need further clarification from any subject from the last class “Network Security Foundations and Secure Management” and self study module.
* Review the “Lesson Opener” and “Real World Scenario” with the learners prior to starting the module.
* Throughout the module, you will find “Consider the Real World Scenario” slides. Review the questions found on these slides, tie the concepts back to the scenario discussed at the start of the lesson as well as content you are presenting, and encourage the learners to share their thoughts.
* For each lesson, you will find a “Pulse Check” slide which is the opportunity for instructors to open a poll to gather feedback from the learners. Leave the poll open for about 1 minute and after you close the poll, share the results with the learners. Encourage the learners to share their thoughts. This information will help the instructors as well as the learners better understand where they are with regards to the lesson.
* Labs are to be demonstrated live for each module. The demonstration of labs is the top priority for the lead instructor. While demonstrating each lab, encourage students to participate and explore.
* At the end of each lesson, it is important to take a few minutes to review the key concepts for the lesson, provide guidance on what the learners can do to prepare for the next lesson, and wrap up with Q&A.
* Instructors should manage breaks based on need, considering both timing and duration. You may take a break if you feel the students need it or if a particularly challenging topic has just been covered.

## Summary

In this lesson, learners will discover the fundamental concepts of cybersecurity, encryption, and secure communication. They will begin by exploring the zero trust approach, which challenges traditional security paradigms by emphasizing continuous verification and understanding of key principles like verification, least privilege, micro-segmentation, and data encryption. Next, they will be introduced to defense in depth, involving layered security measures akin to the layers of an onion, enhancing resilience, preventing attacks, and improving incident identification and response capabilities. The lesson will also cover cryptography, elucidating its role in securing data by converting it between readable and unreadable forms, along with encryption, decryption, various cryptographic methods, encoding techniques, and hashing algorithms. Furthermore, learners will gain insights into digital certificates, their role in web security, the SSL handshake flow for secure online connections, the Diffie-Hellman Algorithm, and public key infrastructure (PKI) management of digital keys and certificates for secure communication. By the end of this lesson, learners will possess a solid foundation of these essential cybersecurity and encryption concepts, equipping them with the skills to implement security measures in various technological contexts.

### Objectives

* Describe zero trust and its principles.
* Explain DiD and its principles.
* Compare and contrast zero-trust vs. DiD.
* Describe cryptography.
* Explain the main purpose and methods of encoding.
* Explain the Base64 encoding process and table.
* Explain hash algorithms.
* Compare and contrast salt and pepper and provide an example.
* Explain the rainbow table and its use.
* Explain the encryption process.
* Explain symmetric and asymmetric encryption.
* Describe cryptanalysis.
* Explain letter frequency.
* Explain web certificates.
* Explain the Diffie-Hellman Algorithm and its role.
* Describe the public key infrastructure (PKI) framework and the PKI certificate process.
* Illustrate the SSL Handshake Flow.

### 

### Lesson Activities and Teaching Strategies

|  |  |  |
| --- | --- | --- |
| Estimated Time | Lesson Portion | Directions |
| 5 min | **Lesson Opener:**  Network Security Models and Cryptography | * Introduce learners to the importance of network security models and cryptography in cybersecurity. |
| 5 min | **Real World Scenario:**  Network Security Models and Cryptography | * Review the real world scenario challenge and inform learners that you will be constantly coming back to this scenario throughout the lesson to discover how to solve and apply concepts to this real situation. |
| 20 min | **Cyber Uncovered:**  Network Security Models | * Begin by explaining the concept of zero trust as a cybersecurity approach built on "never trust, always verify." * Emphasize that it challenges traditional security perimeters and recognizes both external and internal threats. * Discuss the core principles of zero trust, including continuous verification, access control, and data encryption. * Dive deeper into the key principles of zero trust: Verification and least privilege, micro-segmentation, continuous monitoring, IAM, and data encryption. * Transition to the defense in depth (DiD) approach by explaining its layered security concept, akin to the layers of an onion. * Discuss the goals of DiD, such as enhancing resilience, proactive threat prevention, and incident response improvement. * Explore the concept of layered security within defense in depth. * Use visual aids to illustrate how multiple security layers cover various protection aspects. * Discuss the importance of redundancy and isolation in DiD. * Share examples of how organizations implement redundancy and isolate sensitive systems to limit the impact of breaches. * Explain how continuous monitoring is a crucial component of defense in depth. * Describe the process of watching for suspicious activity and responding rapidly to security incidents. * Conclude the lesson by emphasizing the significance of regularly assessing security through penetration tests and evaluations. * Encourage learners to consider how testing and evaluation fit into their organization's security practices. * Highlight the key differences between zero trust and defense in depth, focusing on primary goals, the trust approach, access control, monitoring, segmentation, response to breaches, and complexity. * Foster a discussion about when each approach might be more suitable based on specific security requirements. * Be prepared to discuss the implication of the real world scenario presented at the beginning of class on network types and devices. There are specific prompts that you should ask learners to reflect on to apply this concept to the real world scenario. |
| 20 min | **Cyber Uncovered:**  Cryptography Overview | * Start by explaining that cryptography is the science of securing information, allowing only authorized users to access and comprehend it. * Briefly introduce the core concepts of encryption, decryption, and data security assurance. * Dive deeper into encryption and decryption:   + Define encryption as the transformation of readable data into unreadable ciphertext.   + Explain decryption as the process of reverting encrypted data to its original form.   + Emphasize the role of encryption in ensuring data security. * Introduce various cryptographic methods. * Explore the four primary cryptographic techniques used in modern cryptography. * Explain how these techniques are often combined in various ways for enhanced security. * Focus on encoding and decoding processes:   + Define encoding as the conversion of data from one format to another.   + Explain decoding as the process of converting encoded data back to its original format.   + Provide a simple example of character encoding using ASCII. * Introduce common encoding methods. * Show examples of how each method transforms text and discuss their applications. * Explain Base64's use of 6-bit groups to represent characters. * Emphasize that Base64 is not a form of encryption and can be easily decoded. * Show a Base64 character set table for reference. * Conclude the lesson by introducing learners to Base64 encoding and decoding in Python. * Explain that Python's Base64 library simplifies these tasks. * Use an image to illustrate the use of Python for automatic encoding and decoding. * Be prepared to discuss the implication of the real world scenario presented at the beginning of class on network types and devices. There are specific prompts that you should ask learners to reflect on to apply this concept to the real world scenario. |
| 10-15 min | **Break** | * Share a timer on the screen so there is clarity as to when class will resume. Ensure cameras and microphones are disabled during the break. |
| 20 min | **Cyber Uncovered:**  Hash Algorithms | * Begin by explaining what a hash algorithm is: A mathematical process that converts input data into a fixed-length string. * Highlight the key aspects of hash algorithms, including data integrity, alteration detection, and their one-way nature. * Introduce learners to common hash algorithms:   + MD5   + SHA1   + SHA256   + SHA384   + SHA512   + NT Hash * Explain the key characteristics of each algorithm, such as key length and security considerations. * Explore how hashing is integral to various industries and technologies:   + LSASS in Windows for securing system access.   + Hash tables (hash maps) for relating characters to hash results.   + Digital forensics for validating evidence and maintaining custody chain integrity. * Introduce the concepts of "salt" and "pepper" as security techniques used in hashing to enhance password security. * Explain how salt is a random string added to passwords before hashing and is stored alongside the password. * Describe pepper as a static secret added to all passwords before hashing but stored in a secure external configuration file. * Walk learners through a practical example of using salt and pepper for password hashing:   + Show how the password, salt, and pepper are combined to create a hash.   + Emphasize how this approach enhances security against various attacks. * Define what a rainbow table is: A precomputed list of hashed values used to reverse hashed data, often for brute-force attacks. * Explain how salt and pepper can protect against both brute-force and rainbow table-based threats. * Be prepared to discuss the implication of the real world scenario presented at the beginning of class on network types and devices. There are specific prompts that you should ask learners to reflect on to apply this concept to the real world scenario. |
| 15-20 min | **Lab:**  Hash Algorithms | * Remind learners to use this lab to practice and apply the concepts they have learned throughout the day. * Learners will receive direct feedback on their lab to properly assess their knowledge and determine where they might need additional assistance. |
| 5 min | **Pulse Check** | * After the poll is concluded, spend a few minutes asking why students have selected their zones. Encourage them to share with each other. |
| 10-15 min | **Break** | * Share a timer on the screen so there is clarity as to when class will resume. Ensure cameras and microphones are disabled during the break. |
| 15-20 min | **Cyber Uncovered:**  Encryption | * Start by defining encryption as the process of concealing data through mathematical transformation. * Explain that decryption is the reverse process, requiring a specific key to access the original data. * Present the two common encryption approaches:   + Symmetric encryption: Uses a single key for both encryption and decryption, emphasizing its speed and the need for secure key sharing.   + Asymmetric encryption: Highlights the use of a key pair (public and private) for enhanced security, despite being slower. * Introduce learners to commonly known symmetric cipher keys. * Provide a brief explanation of how each cipher works and its typical use cases. * Walk learners through a practical example of XOR chip encryption:   + Use the word "HELLO" encrypted with the secret key "KEY" using ASCII values.   + Explain the XOR operation and how it yields different results for varying values.   + Show the encrypted message and how to decrypt it using the same key. * Define cryptanalysis as the exploration of cryptographic systems to identify weaknesses and hidden patterns. * Explain that cryptanalysis aims to reveal plaintext, discover keys, and improve security. * Briefly mention the techniques involved, such as mathematical analysis, statistics, and computational approaches. * Introduce the concept of letter frequency analysis, also known as frequency analysis. * Show the table displaying the frequency of English language letters in words. * Explain how cryptanalysts use this table and pattern recognition to effectively decode ciphers. * Be prepared to discuss the implication of the real world scenario presented at the beginning of class on network types and devices. There are specific prompts that you should ask learners to reflect on to apply this concept to the real world scenario. |
| 20 min | **Cyber Uncovered:**  Digital Signatures and Certificates | * Begin by explaining what web certificates (SSL/TLS) are and their importance in verifying website authenticity and ensuring secure data transmission. * Emphasize that these certificates are issued by trusted certificate authorities (CAs) and contain cryptographic keys and site owner details. * Discuss how web certificates enable HTTPS for encrypted user-server communication. * Highlight their role in ensuring data privacy and integrity, crucial for online security. * Mention that users can identify valid web certificates by looking for the padlock symbol and HTTPS in the website's address bar. * Introduce the Diffie-Hellman Algorithm as an early method for securely exchanging keys over the internet. * Explain its significance in addressing the challenge of key distribution and eliminating the need for physical key exchange. * Describe how it enables two computers to share a key even when communicating over an insecure channel. * Provide an overview of PKI and its role in managing digital keys and certificates for secure communication over untrusted networks. * Explain the combination of asymmetric and symmetric keys for data protection. * Discuss the role of certificate authorities (CAs) in validating digital certificates and fostering trust in transactions. * Mention the establishment of trust through a trust chain and the importance of the certificate revocation list (CRL) in identifying untrustworthy CAs to preserve PKI integrity. * Present the PKI infrastructure flow as encompassing the entire lifecycle of digital keys and certificates. * Describe key processes, such as generation (creating certificates with public keys), signing (certifying authenticity via CA's digital signature), distribution (securely sharing certificates), verification (validating identity and data integrity), trust chain (establishing trust from entity to root CA), and revocation (revoking compromised certificates for security). * Use visual aids or illustrations to help learners understand the flow and integrity verification in PKI. * Explain SSL as a protocol that encrypts traffic between a client and server. * Detail the SSL handshake flow as the process by which a client and server initiate secure communications. * Break down the steps, including ClientHello, ServerHello, server certificate validation, key exchange, session key derivation, finished messages, and encryption and data transfer. * Use visual aids to illustrate each step and emphasize the importance of certificate validation and encryption. * Discuss how SSL uses PKI, Diffie-Hellman, and symmetric encryption to ensure a more powerful encryption method. * Explain how these components work together to establish secure connections between clients and servers. * Be prepared to discuss the implication of the real world scenario presented at the beginning of class on network types and devices. There are specific prompts that you should ask learners to reflect on to apply this concept to the real world scenario. |
| 10-15 min | **Break** | * Share a timer on the screen so there is clarity as to when class will resume. Ensure cameras and microphones are disabled during the break. |
| 15 min | **Lesson Closure** | * For this first lesson, spend just a few minutes reminding the learners what the key ”take-aways'' were from the lesson and what they should do to prepare for the next module. The take-aways discussion should include key concepts such as the Network Security Models, Cryptography Overview, Hash Algorithms, Encryption and Digital Signatures and Certificates. * Students should review this information prior to moving to the next module. * Recommend that the students read-ahead and come prepared for the next lesson. * Q&A |
| N/A | **Additional Time Filler (if needed)** | * Kahoot * Discuss interview prep and questioning * Use breakout rooms for additional lab practice * Continue Real World Scenario Conversation |