## LESSON: Network Security Foundations and Secure Management Primer

This is the first module of this course. Therefore, instructors should do the following:

* Introduce Themselves: Instructors should introduce themselves to students, highlighting their credentials and expertise to establish confidence and trust. Additionally, instructors can break the ice by asking students why they registered for the program and inviting them to share their hobbies and a fun fact about themselves.
* Review the Canvas System and syllabus: Spend some time reviewing the Canvas system, explaining the grading process, and going over the syllabus.
* Communication Protocols: Explain the methods available for students to reach out to instructors with questions or to share any information.

*All the above points should be covered within 30 minutes.*

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

* 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 2 minutes 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 explore various aspects of network devices and security. They will discover how network devices like NICs, switches, routers, firewalls, access points, and end devices collaborate to enable network communication. Understanding the role of Layer 3 devices, particularly routers, in determining optimal traffic routes will be emphasized, along with the concept of subnetting for enhanced network efficiency and security, as well as the use of VLANs for network segmentation. Additionally, learners will delve into access control through access-control lists (ACLs) and the management of network resources by servers, which host services such as web, database, mail, communication, and applications. The lesson will cover the importance of redundancy in network design, both physically and logically, along with the use of virtual IP addresses for failover scenarios. Learners will also explore failover clusters, load balancing, and network security design, including the concept of demilitarized zones (DMZ). They'll gain insights into network security systems, proxies (forward and reverse), mail relay servers, firewalls, and intrusion prevention/detection systems (IPS/IDS). The role of web application firewalls (WAFs) in filtering unwanted traffic will be addressed. The lesson will conclude by introducing the AAA protocol and its components (Authentication, Authorization, and Accounting/Auditing). Learners will understand the authentication process, the difference between local and remote authentication, and the use of protocols like RADIUS, TACACS+, and Diameter in AAA. Finally, they'll learn about the 802.1X security protocol, its components, and the Extensible Authentication Protocol (EAP) framework used for flexible authentication methods in network security.

### Objectives

* Identify network devices and their descriptions.
* Explain the routing process and subnetting.
* Define different concepts: VLAs, ACLs, ACEs, and their functions.
* Describe the purpose of servers.
* Explain the role of redundancy.
* Define the use of virtual IP addresses.
* Define a failover cluster and its process.
* Explain the load balancer and its main goal.
* Define network security design.
* Define DMZ and its purpose.
* Explain network security systems.
* Compare and contrast forward proxy vs. reverse proxy and identify their respective architectures.
* Explain the main purpose of the mail relay server.
* Define the network ACL.
* Describe what a firewall is and explain its architecture.
* Compare and contrast IPS vs. IDS and their main role.
* Explain the main role of a web application firewall (WAF) and its architecture.
* Define AAA concepts and their functional components.
* Explain system access.
* Compare and contrast local vs. remote authentication.
* Explain the role of AAA protocols.
* Define RADIUS and its features.
* Describe Diameter as an alternative to RADIUS.
* Define TACACS+ and its features.
* Illustrate the authentication process.
* Compare and contrast RADIUS vs. TACACS+.
* Explain what 802.1X is, its features, and its components.
* Explain what a supplicant is.
* Explain the authenticator's main role.
* Describe the authentication server and explain its process.
* Explain the EAP and its connection to 802.1X.
* Illustrate the 802.1X process.

### Lesson Activities and Teaching Strategies

|  |  |  |
| --- | --- | --- |
| Estimated Time | Lesson Portion | Directions |
| 20 min | **Introduction** | * The lead and associate instructor should introduce themselves to the learners * Encourage the learners to post something about themselves in the chat window |
| 10 | **Canvas and Syllabus Overview** | * Review the key areas of the Canvas platform so that learners could have a better understanding of where to find the resources they will need for this course. * Spend a few minutes reviewing the syllabus covering at a high level the expectations of the course |
| 5 min | **Lesson Opener:**  Network Security Foundations and Secure Management | * Introduce learners to the importance of network security foundations and secure management in cybersecurity. |
| 5 min | **Real World Scenario:**  Network Security Foundations and Secure Management | * 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:**  Networking Recap | * Start by introducing the concept of network devices and their crucial role in network communication. * Present the table listing common network devices along with their descriptions. * Explain the term "intermediary devices" and their significance in connecting end devices and managing data flow within a network. * Highlight devices like switches, routers, firewalls, and access points as examples of intermediary devices. * Describe the routing process and its role in determining the path traffic takes in a network. * Emphasize the function of Layer 3 devices in finding optimal routes for packets using routing tables. * Introduce the concept of subnetting and its benefits in enhancing IP-addressing efficiency. * Mention that subnetting is used for efficiency and security policy distribution. * Walk through the provided example of subnetting a class C network address into three subnets. * Explain the process step by step, ensuring students understand the practical application of subnetting. * Define VLANs (Virtual LANs) and their role in network management and security. * Explain how VLANs divide large networks into organized segments to enhance network structure and security. * Clarify that VLANs isolate traffic within their own segments and discuss the need for routing for inter-VLAN communication. * Highlight the role of routers in enabling data exchange across distinct VLANs. * Introduce access-control lists (ACLs) and their purpose in filtering inbound and outbound traffic. * Explain that ACLs are manually configured and are used to control traffic by permitting or denying it. * Describe access control entries (ACEs) and their role in ACLs. * Explain that ACEs are examined upon packet arrival and specified actions are applied if a match occurs. * Discuss the role of servers in managing network resources and responding to client requests. * Emphasize that servers are typically dedicated to specific functions and services. * Present examples of commonly used server types, including web servers, database servers, mail servers, communication servers, and application servers. * Briefly describe the purpose of each server type in a network. * 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 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. |
| 15-18 min | **Cyber Uncovered:**  Redundancy Methods | * Begin by explaining the concept of redundancy in a network and its importance in ensuring reliability. * Clarify that redundancy involves creating backup pathways or components to prevent downtime in case of primary element failure. * Differentiate between physical redundancy (duplicate hardware) and logical redundancy (backup routes) in network setups. * Discuss scenarios in which each type of redundancy might be more suitable. * Introduce the concept of virtual IP (VIP) addresses as the default gateway for end devices. * Explain the consequences of VIP failure, which leads to connectivity loss beyond the local subnet. * Describe how redundancy protocols allow multiple routers in a subnet to share a virtual IP as the gateway for end devices. * Provide examples of both open-source (CARP, VRRP) and proprietary (HSRP, GLBP) redundancy protocols. * Explain what a failover cluster is and its purpose in ensuring seamless service delivery. * Emphasize the automatic failover feature, where one server takes over when another encounters an issue. * Use the provided diagram to illustrate how failover clusters work. * Highlight the interconnected servers, shared storage, and the role of the load balancer in redirecting requests in case of server failure. * Introduce load balancers and their role in evenly distributing network traffic among clustered servers. * Emphasize how load balancers prevent server overload and ensure continuity in case of server failure. * Discuss the classification of load balancers into hardware, software, and virtual load balancers. * Explain the differences and applications of each type. * Use the provided diagram to visually depict the flow of network traffic through a load balancer. * Explain how load balancers maintain continuous service availability by rerouting traffic when a server becomes unavailable. * 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:**  Network Secure Design and Systems | * Begin the lesson by explaining the significance of network security design in protecting computer networks from unauthorized access and cyberthreats. * Emphasize the need for a layered defense system to effectively prevent, detect, and mitigate security risks. * Introduce the concept of a DMZ in network security design. * Explain how a DMZ isolates external-facing services from the internal network, enhancing security. * Describe the typical placement of services like web servers and databases within the DMZ. * Use the provided illustration to show the architecture of a DMZ. * Clarify that the DMZ serves as the initial point of contact for external users accessing a network. * Highlight the importance of avoiding sensitive services in the DMZ due to internet exposure. * Discuss the role of network security systems, which encompass both hardware and software, in safeguarding computer networks. * Emphasize their function in preventing unauthorized access, breaches, and cyberthreats. * Explain the concept of proxy servers and their intermediary role between clients and servers. * Differentiate between forward proxies (client-side) and reverse proxies (server-side). * Discuss typical use cases for each type, such as DDoS protection and load balancing. * Use the provided diagram to visually compare forward and reverse proxies. * Describe how forward proxies in the DMZ filter traffic between internal and external firewalls, while reverse proxies outside the DMZ filter traffic pre-firewall. * Explain the function of mail relay servers in utilizing SMTP to store and forward email messages. * Emphasize their role in verifying sender identity and ensuring message encryption. * Introduce ACLs as a security layer controlling traffic on one or more subnets. * Discuss the criteria used by ACLs to oversee and control incoming and outgoing traffic, including IPs, ports, protocols, and wildcard rules. * Define firewalls as network security systems that monitor and control incoming and outgoing network traffic. * Explain that firewalls typically operate at the Network Layer (Layer 3) and secure connections between internal and external networks. * Utilize the provided illustration to illustrate the placement of firewalls in the DMZ area. * Highlight how firewalls filter traffic at LAN edges and WAN entry points to ensure network security. * Explain the differences between IPS and IDS in terms of their functions, responses, and proactivity. * Discuss how IPS actively prevents attacks from reaching targets, while IDS generates alerts for human response. * Use the provided diagram to visually depict the architecture of IPS/IDS setups. * Clarify that IPS actively drops packets for threat prevention, while IDS solely monitors threats without enforcement. * Define WAF as a security measure that filters and blocks unwanted HTTP/HTTPS traffic based on predefined rules. * Provide examples of unwanted traffic, such as XSS and SQLi, that WAF can block. * Explain the deployment options for the WAF as a stand-alone device or server plug-in. * Use the provided diagram to show the placement of the WAF directly behind the firewall and in front of the web server. * Highlight the distinction between legitimate and malicious traffic in the diagram. * 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 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. |
| 15-18 min | **Cyber Uncovered:**  Authentication, Authorization, and Accounting | * Begin by introducing authentication, authorization, and accounting (AAA) as a fundamental framework in network security. * Emphasize its role in managing and safeguarding network access. * Explain the three core components of AAA security: Authentication, authorization, and accounting. * Provide concise definitions for each component:   + Authentication: Verifying a user's identity.   + Authorization: Determining user access to resources.   + Accounting/Auditing: Tracking user activity. * Mention that AAA services are typically provided by dedicated servers and standard protocols like RADIUS and TACACS+. * Describe the importance of verifying users' identities before granting access to network resources. * List various methods of authentication, including usernames, passwords, token cards, security questions, and biometrics. * Explain that this process is known as authentication. * Highlight that access can be granted either locally or remotely, covering login pages, SSH, and Remote Desktop Protocol. * Dive deeper into the concept of local authentication. * Explain that local authentication involves storing user credentials on the devices they are trying to access. * Describe the process where user input is compared to locally stored data and access is granted if they match. * Provide examples of devices where local authentication is commonly used, such as PCs, switches, routers, and firewalls. * Mention the role of the Security Account Manager (SAM) database in verifying credentials during computer login. * Transition to discussing remote authentication. * Define remote authentication as the process of storing user credentials on a remote server for authentication. * Explain how devices request the server to authenticate users based on the user database stored remotely. * Highlight the benefit of centralizing stored usernames and passwords. * Provide a practical example of remote authentication, such as checking a PC password against Active Directory in a domain environment. * Present a comparison between local and remote authentication methods. * List key points differentiating the two approaches, including management, security, and user configuration. * 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 min | **Pulse Check** | * Instructors are to spend a few minutes explaining the purpose of this poll as well as the zone. * After the poll is concluded, spend a few minutes asking why students have selected their zones. Encourage them to share with each other. * Future pulse checks should only take 3-5 min to administer. |
| 20 min | **Cyber Uncovered:**  RADIUS and TACACS+ | * Start by introducing the concept of AAA (Authentication, Authorization, and Accounting) and its critical role in user authentication and authorization across networks. * Explain that two prominent protocols in the AAA framework are RADIUS and TACACS+. * Emphasize that these protocols ensure secure access management by facilitating communication between clients and servers. * Dive into RADIUS (Remote Authentication Dial-In User Service) as a network protocol for centralized AAA services. * Describe its common use cases, such as dial-up and VPN connections, as well as its applicability in various network environments. * Mention that RADIUS operates using UDP for its operations. * Enumerate common features of RADIUS, including its versatility across platforms, integration with Active Directory, suitability for both wired and wireless networks, and its ability to allow Cisco routers to authenticate via Microsoft servers. * Explain that it was originally developed for Layer 2 authentication and highlight its encryption capabilities. * Mention the UDP port numbers associated with RADIUS. * Note its relevance to the 802.1X security protocol, which will be discussed later in the chapter. * Introduce Diameter as an alternative to RADIUS. * Explain that Diameter has gained popularity due to its enhanced capabilities and scalability in modern network environments. * Highlight the improvements it offers over RADIUS, making it a consideration for organizations seeking advanced AAA solutions. * Shift the focus to TACACS+ (Terminal Access Controller Access-Control System Plus) as an additional network protocol providing centralized AAA services. * Describe its versatility in a wide range of applications, including network access, device management, and application access. * Note that TACACS+ operates using TCP for its operations. * List common features of TACACS+, including support from Cisco and other vendors, separate implementation of AAA functions, encryption of the entire packet, and its use of TCP port 49. * Highlight its role in allowing a Cisco switch to authenticate and authorize administrative access via a TACACS+ server. * Provide an overview of the authentication process by showing a diagram illustrating the interaction between a client and an AAA server. * Use ALT text for the diagram and mention that visuals can be referred to for a better understanding. * Present a detailed comparison between RADIUS and TACACS+, highlighting key differences in terms of protocol usage, AAA functions, encryption, command authorization, accounting, vendor support, and logging. * Encourage students to understand the strengths and weaknesses of each protocol. * Conclude the lesson by briefly mentioning that server-based AAA configuration for TACACS+ and RADIUS is similar to a Cisco IOS device. * Offer an example of configuring RADIUS, outlining the essential steps:   + Enabling AAA with "aaa new-model."   + Configuring the RADIUS server with "radius-server" settings.   + Setting up device authentication using "aaa authentication." * 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. |
| 25min | **Lab:**  Authentication, Authorization, and Accounting | * 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. * **Note**: Although the lab is named the same as the previous subtopic, this is the correct location. |
| 10 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. |
| 15-18 min | **Cyber Uncovered:**  802.1X Authentication | * Start the lesson by introducing 802.1X as a security protocol defined by IEEE, emphasizing its role in authenticating users and devices seeking network access. * Explain that 802.1X can operate in various network environments, including wired or wireless LANs, campuses, and enterprise networks. This protocol ensures security in diverse settings. * Highlight key features of 802.1X:   + Access Control: Secure, identity-based access control at network endpoints.   + Network Security: Ensuring secure networks with minimal disruption to end users and infrastructure.   + Intelligence and Flexibility: Describe how 802.1X provides intelligent and flexible security operations. * Discuss the three essential components of 802.1X:   + Supplicant: The device requesting network access.   + Authenticator: The device responsible for controlling network access.   + Authentication Server: The device that verifies the supplicant's identity. * Describe the supplicant as the client workstation that collects user credentials and sends them to the authenticator. * Clarify that workstations can be any PC operating system or software component. * Explain that the authenticator receives credentials from the supplicant and can either relay them to the authentication server or perform local authentication itself. * Emphasize the term "local authentication" and its significance in certain scenarios. * Discuss the authentication server as the entity responsible for verifying the supplicant's identity. * Mention that it can be a physical device like a RADIUS server or software running on a server. * Provide an overview of EAP as an authentication framework for transporting request and response parameters. * Mention that EAP is extensible, allowing the addition of new methods. * Give examples of common EAP methods like EAP-MD5, EAP-TLS, and EAP-PEAP. * Explain how 802.1X encapsulates data and parameters within EAP packets. * Highlight that EAP serves purposes beyond authentication, including authorization, accounting, and more. * Display an illustration or diagram that visually explains the server-client authentication process in 802.1X, emphasizing the challenge and response authentication mechanism. * Walk through the general configuration steps for setting up 802.1X (dot1x) on a Cisco IOS switch device. Use this as an opportunity to provide practical insights. **Note**: ​​A PAE (Port Access Entity) can adopt one of two roles within an access control interaction:   • Authenticator - Port that enforces authentication before allowing access to services available via that Port.  •Supplicant - Port that attempts to access services offered by the Authenticator.  Additionally, there exists a third role:  • Authentication server - Server that performs the authentication function necessary to check the supplicant's credentials on behalf of the Authenticator.   * 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. |
| 25 min | **Lab:**  802.1X Authentication | * 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. |
| 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 Redundancy Methods, Network Secure Design and Systems, Authentication, Authorization, and Accounting,RADIUS and TACACS+, and 802.1X Authentication * 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 |