LESSON: Mail Security

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 “Patch 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 explore various aspects of DNS, email protocols, email security, and mail relay servers. They will understand the storage of DNS information by domain registrars and registries, the temporary nature of domain reservations, and the mechanics of DNS queries. Key DNS records like MX, NS, A, CNAME, and TXT will be introduced. The lesson will cover essential email protocols, including SMTP, POP3, and IMAP, as well as how to connect to mail servers using a command-line interface (CLI). Learners will become familiar with crucial POP3 and SMTP commands and grasp the concepts of email spoofing, DNS spoofing, and email authentication mechanisms such as SPF, DKIM, and DMARC. The significance of email headers in cybersecurity will be highlighted, along with practical steps for accessing them in Gmail and Outlook. The lesson will also delve into mail relay servers, their placement options, and the roles of mail transfer agents (MTAs) and mail delivery agents (MDAs). Lastly, learners will gain insights into email security measures, including mail relay sandboxes, antivirus software, and Content Disarm and Reconstruction (CDR), providing a well-rounded understanding of email communication and security.

Objectives

- Recognize the importance of DNS in mail security.
- Explain the role and significance of DNS records.
- Differentiate between the functions of domain name registrars and domain name registries.
- Describe the role of DNS queries.
- Identify common types of DNS records.
- Identify key email protocols and their respective roles in email communication.
- Explain how to establish a connection to a mail server.
- Summarize SMTP commands and describe their roles in initiating, authenticating, and completing an email transfer session.
- Define the concept of spoofing.
- Identify email spoofing tactics and the risks they pose.
- Explain the DNS spoofing attack mechanism.
- Recognize SPF, DKIM, and DMARC as tools to enhance mail security and prevent spoofing.
- Recognize the importance of email headers in cybersecurity.
- Identify email headers.
- Explain how to access and analyze email headers for effective security investigations.
- Explain the role of mail relay servers in email communication.
- Describe the benefits of using mail relay servers.
- Analyze the considerations for choosing the placement of mail relay servers.
- Define the roles of MTAs and MDAs in the email delivery process.

Lesson Activities and Teaching Strategies

Estimated Time	Lesson Portion	Directions

10 min	Questions/Clarifications from last class	● Last Class Highlights ● Address any lingering questions or concerns
5 min	**Lesson Opener:** Mail Security	● Introduce learners to the importance of mail security in cybersecurity.
5 min	**Real World Scenario:** Mail Security	● 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:** DNS Introduction	● Start by introducing the concept of DNS (Domain Name System) as a foundational and integral part of the internet's infrastructure that translates user-friendly domain names into IP addresses. Emphasize its role in making websites accessible and user-friendly. ● Explore the importance of DNS in mail security. Discuss how DNS is involved in email routing to ensure correct email delivery, how DNS extensions authenticate email origins, and how DNS awareness helps prevent phishing by spotting deceptive domain names. ● Proceed to explain DNS records. Describe DNS records as the automatic linking of website names to IP addresses, making it easier for users to access websites using simple domain names. Highlight the contrast with manual linking before DNS records. ● Discuss where DNS information is stored, emphasizing domain name registrars and domain name registries. Explain that domain registrars handle domain name registration and management, while domain registries are responsible for specific domain extensions, ensuring uniqueness within categories and periodic renewals. ● Dive into DNS queries, defining them as requests to the Domain Name System to translate domain names into IP addresses, enabling devices to locate websites using human-readable names. ● Cover common types of DNS records, which can be split into 2-3 slides. Explore address (A) records, canonical name (CNAME) records, mail exchanger (MX) records, text (TXT) records, and name server (NS) records. Explain their specific purposes and significance in DNS management. ● 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	**Lab:** nslookup	● 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.

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:** Mail Protocols	● Begin the lesson by introducing the concept of email communication protocols, emphasizing that communication between mail clients and servers relies on specific protocols. ● Introduce Simple Mail Transfer Protocol (SMTP) as the protocol responsible for outgoing mail. Explain its operation on port 25 and how it ensures reliable email delivery from senders to recipients' servers. ● Move on to Post Office Protocol version 3 (POP3) as a "Push Mail" protocol. Explain its function, that it works on port 110, and highlight its suitability for local storage, though not ideal for multi-device access. ● Discuss the Internet Message Access Protocol (IMAP), operating on port 143 (or securely on port 993). Explain how IMAP synchronizes emails across devices, making it ideal for users who need access everywhere. ● Transition to the topic of connecting to mail servers via the command-line interface (CLI) using the "telnet" or "nc" commands. Describe the requirements for connecting, including the server name or IP address and port "25" for SMTP. ● Explain how to interact with the server for testing, sending emails, and checking responses using the provided commands. ● Cover the specifics of the "telnet" and "nc" commands, highlighting their roles in connecting to network services and that they send data as plaintext. ● Introduce useful commands for POP3, including USER, PASS, LIST #, RETR, and TOP. Explain their purposes and how they contribute to email retrieval and management. ● Move on to useful commands for SMTP, such as HELO, AUTH, MAIL FROM, DATA, and RCPT TO. Describe their roles in initiating, authenticating, and completing the email transfer process. ● 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 min	**Lab:** Practice POP3 Commands	● 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.
25 min	**Cyber Uncovered:** DNS Mail Protection	● Start by introducing the concept of spoofing, emphasizing that it involves creating fake communications that appear legitimate but are not. Mention the various forms of spoofing, including fake emails, SMS, phone calls, websites, and network components like IP addresses and ARPs.

		● Discuss email spoofing, explaining that it is a deceptive practice in which malicious actors manipulate email headers to appear legitimate and trick recipients into taking harmful actions, such as clicking on links. Highlight its common use in phishing attacks. ● Describe DNS spoofing, which redirects network traffic to malicious destinations by altering DNS records. Explain how it is used to distribute malware or intercept data and introduce the role of security measures like DNS Security Extensions (DNSSEC) to mitigate risk. ● Transition to how to prevent spoofing in cybersecurity, highlighting that humans are often the weakest link in the security chain. Emphasize that phishing poses a significant threat to organizations. ● Review security mechanisms aimed at reducing or eliminating email spoofing, starting with the Sender Policy Framework (SPF). Explain that SPF authenticates emails by confirming their origin from authorized mail servers linked to a domain. Discuss challenges it faces with email forwarding, such as altered sending servers and lack of visibility. ● Introduce DomainKeys Identified Mail (DKIM) as an email authentication protocol that adds digital signatures to emails at the server level to verify email integrity and origin. ● Present Domain-based Message Authentication, Reporting, and Conformance (DMARC) as a solution that enhances mail security by validating the sender's domain. ● Explain how it allows senders to specify handling policies for emails that fail checks and includes reporting functions to monitor mail security. ● Summarize the importance of SPF, DKIM, and DMARC in combating spoofing and phishing, emphasizing that together, they bolster email authenticity and provide domain owners with control over email handling. ● Provide an overview of SPF, DKIM, and DMARC as key email security protocols. ● Emphasize their role in combating email spoofing and phishing. ● Explain how SPF checks the sending server's IP against the domain's records. ● Highlight SPF's role in mitigating spam and email spoofing. ● Describe DKIM's use of cryptographic signatures to authenticate emails. ● Explain how DKIM complements SPF in enhancing email security. ● Introduce DMARC as a protocol that builds on SPF and DKIM. ● Emphasize that DMARC requires SPF or DKIM to pass for email authentication. ● Discuss how SPF, DKIM, and DMARC work together to bolster email authenticity. ● Explain the control they provide to domain owners over email handling.

		● Describe SPF records as DNS records specifying authorized mail servers for a domain. ● Emphasize the importance of SPF records in email authentication. ● Introduce tools such as nslookup and MxToolbox for checking SPF records. ● Guide learners through a step-by-step procedure for verifying SPF records for domains like seriouseats.com and clutchburger.com. ● Demonstrate how to use services like anonymailer.net to send test emails with spoofed sender addresses. ● Instruct students to craft and dispatch emails to observe how SPF-protected domains handle unauthorized senders. ● Discuss the importance of email header analysis in identifying spoofing. ● Guide students on inspecting email headers, looking for discrepancies indicating a mismatch between the sender's domain and SPF records. ● Instruct students on using the sender's IP address from the email header for a reverse IP lookup on MxToolbox. ● Emphasize how this process helps uncover the true source of the email. ● 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.
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.
20 min	**Cyber Uncovered:** Mail Headers	● Begin the lesson by introducing the concept of email headers, emphasizing their importance as one of the main components of an email, along with the envelope and the body. ● Discuss the role of email headers in providing essential metadata, such as sender, recipient, content type, route, and authentication details, which are crucial for system communication, organization, and troubleshooting. ● Transition to the relevance of email headers in cybersecurity. ● Explain that cybersecurity professionals can use email headers to identify suspicious activity, including emails sent from spoofed addresses or that contain malicious attachments. ● Emphasize that email headers can help track the path of an email and identify the source of an attack, making them a valuable tool in cybersecurity. ● Introduce the method used to find email headers in popular email clients like Gmail and Outlook, ensuring learners are familiar with the practical aspects of accessing email headers.

		● Highlight the importance of various header fields, including temporal information, recipient and sender details, email content information, and authentication and integrity components. Explain their role in identifying email-borne 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.
5 min Break		
20 min	**Cyber Uncovered:** Mail Relay	● Start by introducing the concept of mail relay and its crucial role in directing emails between clients and recipients' servers, ensuring proper routing and enhancing email security through SPF and DKIM. ● Explain the benefits of mail relay servers, emphasizing their role in protecting IP reputation, scanning attachments for malware, and combating spam and phishing through effective filtering. ● Discuss topology placement, highlighting that mail relay servers can be located in the cloud or on a local network. ● Discuss the significance of this choice. ● Explore the advantages of cloud-based mail relay servers, including scalability, availability, and security. ● Provide real world examples to illustrate these advantages. ● Discuss on-premises mail relay servers and their benefits, focusing on the control, performance, and cost advantages they offer. ● Introduce hybrid mail relay topologies and explain how they combine the benefits of both cloud-based and on-premises solutions. Provide practical use cases for clarity. ● Shift the discussion to mail relay concepts, covering the roles of mail transfer agents (MTA) and mail delivery agents (MDA) in ensuring email delivery and security. ● Discuss the importance of a mail relay sandbox and a file extension block list in enhancing email security. Explain how they work, their limitations, and potential workarounds by attackers. ● Conclude the lesson by discussing antivirus and Content Disarm and Reconstruction (CDR) software, highlighting their respective roles in scanning emails for malware and sanitizing email attachments. Encourage learners to implement robust security measures for email protection. ● 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 min	**Lesson Closure**	● For this 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 importance of DNS in mail security and mail relay servers in email

		communication. 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