## LESSON: Network Traffic Analysis

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

* Checking with the students to see if they have any questions or need further clarification from any subject from the last class “Network Monitoring” 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 regard 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 network packet analysis and its crucial role in network monitoring and security, discovering how it optimizes network performance, reveals traffic patterns, and resolves issues. They'll explore .pcap files, essential tools like Wireshark, and a case study on the Target data breach and how it utilized packet analysis. The lesson covers Wireshark's features, such as capture filters, comments, and file extraction, along with NetworkMiner's role in simplifying file extraction. Learners will be introduced to Microsoft’s Network Monitor, highlighting its compatibility with Wireshark and features like live traffic capture and process identification. Overall, this lesson equips learners with the knowledge and skills needed for effective network packet analysis and monitoring.

### Objectives

* Describe network packet analysis and its tools.
* Explain the .pcap file and its primary role.
* Explain the main idea of Target’s data breach (2013).
* Illustrate Wireshark’s main features.
* Explain Wireshark Statistics: Conversations and HTTP Statistics.
* Explain protocol hierarchy, file extraction, and signature options.
* Define Wireshark’s protocol extraction and manual extraction.
* Define NetworkMiner.
* Explain NetworkMiner’s key features.
* Illustrate the process of capturing traffic.
* Explain Wireshark integration with NetworkMiner.
* Explain the challenges tcpdump and Zeek aim to address.
* Identify the use of tcpdump.
* Identify the use of Zeek.

### Lesson Activities and Teaching Strategies

|  |  |  |
| --- | --- | --- |
| Estimated Time | Lesson Portion | Directions |
| 5 min | **Career Outcomes Content Reminder** | * Remind learners about the Career Outcomes module to ensure that they know that the materials are available and to complete the assigned modules. * The first module will help the learners do the following:   + Continue to build their technical resume by adding projects, technical skills, and a professional summary to the Career Outcomes resume template.   + Submit their resume to receive actionable feedback from the Career Readiness team   + This module can be found in Week 2 of Securing your Network. * Additional information for the second module regarding the resume submission assignment:   + Students must use the Career Outcomes resume templates to receive credit for this assignment.   + This is step two of a two part resume writing process. Step one helped students format their resume, while this assignment allows students to write high-impact content. This review will provide feedback to help students develop strong content that will resonate with employers.   + This module can be found in the “Resume and LinkedIn Submissions” course in Canvas. * Students can reach out to their SSM for questions and help if they need it. |
| 5 min | **Lesson Opener:**  Network Traffic Analysis | * Introduce learners to the importance of network traffic analysis in cybersecurity. |
| 5 min | **Real World Scenario:**  Network Traffic Analysis | * 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:**  Introduction to Network Packet Analysis | * Begin by explaining the importance of network packet analysis in network monitoring and security. * Highlight how it involves examining data packets to gain insights into various aspects of network behavior. * Break down the significance of packet analysis into three key areas: Security, performance optimization, and troubleshooting. * Discuss how it helps identify intrusion attempts, optimize network performance, and resolve network issues quickly. * Describe what .pcap files are, their binary format, and the kind of data they contain, including data packets, metadata, and protocol information. * Explain that .pcap files are generated by network monitoring tools and how they are used by network administrators and security analysts. * Introduce the essential network packet analysis tools, focusing on Wireshark, tcpdump, and Snort. * Explain their roles in capturing, dissecting, and presenting network data. Mention Wireshark's user-friendly interface and the command-line capabilities of tcpdump. * Present the real world case of the 2013 Target data breach as an example of how network packet analysis tools played a crucial role in addressing a security incident. * Explain the security issue, data theft, late discovery, and the analysis conducted using Wireshark, tcpdump, and Snort. * Discuss how network packet analysis helped in spotting the problem by identifying unusual traffic patterns and signs of malicious software. * Explain the actions taken to isolate affected systems and enhance security based on the analysis results. * Engage the learners in a discussion about the importance of network packet analysis in today's digital landscape. * Encourage them to share any personal experiences or insights related to network monitoring and security. * 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. |
| 20-25 min | **Cyber Uncovered:**  Wireshark and Network Packet Analysis | * Begin by introducing Wireshark as a fundamental networking tool used by network defenders and forensic analysts. * Emphasize its role in collecting and analyzing network traffic for valuable insights. * Discuss the key features offered by Wireshark, including packet capturing, protocol analysis, and filtering and search capabilities. * Explain how these features contribute to network monitoring and analysis. * Explain the concept of capture filters and their importance. * Describe how capture filters help reduce the technical burden by selectively capturing relevant data and minimizing raw packet size for efficient storage. * Describe how learners can add custom comments to packets during packet capture analysis. * Highlight the utility of comments for making notes on important packets and how they are saved for future reference. * Discuss how Wireshark provides customization options for network monitoring through custom columns. * Explain how learners can create or modify columns to tailor their interface, displaying specific packet information. * Teach learners how to control display filters efficiently by adding queries, such as ‘Apply as Filter’ and ‘Prepare as Filter.’ * Explain the practical applications of these filtering options. * Introduce custom filters and logical operators in Wireshark, such as AND (&&) and OR (||). * Provide an example of how learners can use these operators to create filter expressions. * Explain how learners can conduct targeted string searches within captures using Wireshark. * Describe the steps involved in performing a string search and its usefulness in locating specific file header strings. * Discuss the comprehensive insights offered by Wireshark Statistics, covering capture file properties, protocol hierarchy, conversations, endpoints, and I/O graphs. * Explain how these statistics contribute to comprehensive network traffic analysis. * Focus on the importance of 'Conversations' within Wireshark's Statistics menu, including how it displays connections and data exchanged between IP addresses. * Explain how HTTP statistics provides insights into conversation volume between connections. * Discuss how protocol hierarchy breaks down protocols according to the OSI model. * Explain its role in offering detailed protocol metadata, statistics, and the application of filters within the hierarchy. * Cover the process of file extraction in Wireshark, including manual searches and the recognition of files using file signatures. * Provide a list of common file signatures and their associated file types. * Explain how Wireshark allows file extraction from network traffic captures, both manually and automatically. * Describe the steps for automatic extraction and its benefits. * Discuss Wireshark's ability to extract files from captures using various protocols, such as DICOM, HTTP, IMF, SMB, and TFTP. * Explain that for protocols beyond Wireshark's automatic processing, like FTP, manual extraction is required. * Describe the process of accessing the complete file stream using TCP stream and saving it as raw data. * **Provide learners with a 5 min break.** * 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. |
| 15-20 min | **Cyber Uncovered:**  NetworkMiner | * Start by introducing NetworkMiner as an open-source network forensic analysis tool (NFAT) designed for Windows, simplifying file extraction from captured network traffic. * Discuss the key features, including file and credential retrieval, system and network discovery, and automated file saving, emphasizing how they assist investigators in network traffic analysis. * Explain how to initiate traffic capture using NetworkMiner, detailing the steps, such as selecting an interface, clicking "Start," and exploring connection details and .pcap file opening options. * Highlight that NetworkMiner can be used alongside Wireshark, a renowned packet analysis tool. * Explain that while Wireshark specializes in in-depth packet analysis, NetworkMiner excels in automating data and artifact extraction from captured traffic. * Discuss the benefits of combining these tools for comprehensive network traffic analysis. * Provide examples of practical scenarios in which NetworkMiner can prove valuable, such as extracting images, files, and credentials from network traffic, detecting operating systems and network details, and automatically saving extracted files. * Encourage learners to perform a hands-on exercise using NetworkMiner. Guide them through capturing network traffic, extracting files, and conducting system and network discovery. * Demonstrate the integration between NetworkMiner and Wireshark, showcasing how investigators can use both tools together to gain deeper insights into network traffic. * 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:**  NetworkMiner | * 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. |
| 20 min | **Cyber Uncovered:**  tcpdump and Zeek | * 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:**  tcpdump and Zeek | * 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. |
| 2 min | **Midpoint Course Survey** | * Allocate 2 minutes to facilitate the completion of the Midpoint Survey. * Encourage learners to provide honest and constructive feedback about their learning experience. |
| 3 min | **Discussion Board** | * Allocate 3 minutes Review Discussion Board Slides and how it impacts students’ final grades. |
| 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 introduction to Network Monitoring, SNMP, and NetFlow. * 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 |

### 