## LESSON: Network Monitoring

## 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 Models and Cryptography” 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 network monitoring, focusing on its purpose in overseeing various network aspects, ensuring efficiency, and preventing disruptions. They'll delve into the role of the network operations center (NOC) and learn about Simple Network Management Protocol (SNMP) for device communication and security. SNMP's architecture, security features, and key concepts will be covered. The lesson also touches on network security through SNMP sniffing. Learners will understand NetFlow for data collection and analysis, Nagios for network monitoring, and deep packet inspection (DPI) for network data analysis and security. Various packet inspection levels are explained, along with protocol analyzers. Anomaly detection and the role of AI and ML in network optimization and security will also be explored.

### Objectives

* Explain network monitoring and its main process.
* Explain the reasons for monitoring a network.
* Identify the network operations center (NOC).
* Describe network monitoring functions.
* Identify the use of SNMP and its users.
* Compare and contrast the differences between SNMP versions.
* Illustrate the architecture and implementation of SNMP.
* Explain SNMP’s key concepts.
* Describe the role of SNMP sniffers.
* Identify NetFlow and its records.
* Explain the NetFlow header and what it includes.
* Explain the process of NetFlow analysis.
* Identify the Nagios tool.
* Explain Nagios communication methods.
* Identify deep packet inspection.
* Define the Packet Inspection Levels.
* Explain DPI in various domains.
* Explain the protocol analyzer and its features.
* Identify anomaly detection and what it involves.
* Define the three anomaly types.
* Explain the main role of behavioral analysis.
* Explain AI-powered network monitoring.
* Identify machine learning (ML) and its applications.
* Explain how AI and ML can perform real-time data analysis.

### Lesson Activities and Teaching Strategies

|  |  |  |
| --- | --- | --- |
| Estimated Time | Lesson Portion | Directions |
| 5 min | **Lesson Opener:**  Network Monitoring | * Introduce learners to the importance of network monitoring in cybersecurity. |
| 5 min | **Real World Scenario:**  Network Monitoring | * 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 Monitoring | * Start the lesson by explaining the concept of network monitoring, emphasizing its importance in ensuring the proper functioning of computer networks. * Provide a brief recap of common network devices, such as routers, switches, firewalls, and servers. * Highlight the critical role of networks as the lifelines of IT infrastructure, handling data, changes, and threats. * Emphasize the benefits of proactive monitoring, such as safeguarding organizational health and minimizing network issues. * Explain what a network operations center (NOC) is and its central role in network monitoring and control. * Highlight that NOC staff are experts responsible for overseeing network performance, troubleshooting issues, and implementing changes. * Clarify the key differences between the NOC and a traditional help desk, underscoring that the NOC handles high-level IT communications and collaborates with IT departments or managed service providers (MSPs). * Break down the core functions of network monitoring, including discovery, mapping, monitoring, and alerting/reporting. * Emphasize the significance of constant observation of network activity and timely outage notifications. * Engage learners with an interactive activity in which they create a basic network map, visualizing device information and connectivity. * Encourage learners to identify different devices and their connections within a sample network. * Provide real world examples of how effective network monitoring has saved organizations from potential disasters or downtime. * 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:**  Simple Network Management Protocol | * Begin by introducing SNMP as a critical protocol for network device communication and management. * Explain how SNMP facilitates communication between network devices through agents and how these agents share data with a network management system (NMS). * Highlight SNMP as an application-layer protocol that supports cross-platform and multi-protocol implementations. * Emphasize SNMP's role in enabling central management computers to monitor devices, fetch status information, and modify device behavior. * Discuss the extensive use of SNMP by various entities, including routers, servers, switches, IoT devices, cameras, and printers for communication and data sharing. * Explain the importance of SNMP in the context of remote telemetry units (RTUs) strategically positioned in critical sites like power stations and cell towers, ensuring operational continuity. * Describe the key differences among SNMP versions, focusing on SNMPv1 with limited security, SNMPv2c with improved performance, and SNMPv3, which emphasizes security and introduces the EngineID for unique identification. * Dive into SNMP architecture and implementation, emphasizing the communication between agents and managers. Use visual aids or diagrams if available to illustrate the concept. * Conclude by covering essential key concepts in SNMP, including object identifier (OID), management information base (MIB), and Windows Management Instrumentation (WMI). Mention the significance of these concepts in SNMP's role in device communication and status reporting. * Optionally, discuss SNMP sniffing as a security risk, explaining how intercepting and analyzing SNMP traffic can pose vulnerabilities, especially in SNMPv1 and v2. * 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 | **Lab:**  Simple Network Management Protocol | * 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. |
| 20 min | **Cyber Uncovered:**  NetFlow | * Begin the lesson by introducing NetFlow as a network monitoring protocol designed to collect IP traffic data from enabled switches and routers. * Emphasize the primary purpose of NetFlow, which is monitoring network performance and optimizing resource allocation. Mention that NetFlow data can be analyzed using Cisco programs or third-party software like Nagios. * Explain that despite various analysis tools available, there is no official program exclusively dedicated to NetFlow analysis, which highlights the importance of understanding its principles. * Move on to the topic of NetFlow records and discuss NetFlow versions v5 and v9. Describe the components of these records, including IP addresses, SNMP index, packet counts, port numbers, and protocol details. Highlight the enhanced support for IPv6 in NetFlow v9. * Discuss the structure of NetFlow records and underline the popularity of v9 due to its template-based approach, enabling flexible processing and analysis of NetFlow data by third-party applications. * Dive into how NetFlow analysis works by covering key steps: Data collection, flow identification, data export to collectors or analyzers, data storage for historical analysis, analysis and visualization tools for generating reports and graphs, traffic profiling for identifying top talkers and anomalies, resource optimization for efficient network resource allocation, security monitoring for threat detection, and reporting and alert generation for network events. * 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:**  Key Network Monitoring Tools | * Begin the lesson by introducing Nagios as a powerful open-source network monitoring tool compatible with Linux, Windows, and Unix OSs. * Emphasize Nagios's role as a comprehensive network monitoring and management system that can be extended with plugins and add-ons to support various protocols and data sources, including SNMP and NetFlow. * Discuss the reasons for using Nagios, highlighting its versatility in monitoring networks, servers, web services, and applications through a user-friendly GUI. * Explain the simplified setup process offered by Nagios, including the availability of an easy-to-use configuration wizard for software setup and data collection from diverse sources. * Discuss the importance of continuous monitoring provided by Nagios, ensuring system health and increased availability while reducing downtime. * Introduce Nagios's communication methods, emphasizing agent-based communication using software agents on target servers for retrieving system performance stats and sending alerts, as well as native protocol communication using SNMP (for Linux and network devices) or WMI (for Windows) for agentless monitoring. * Transition to the topic of deep packet inspection (DPI), explaining it as a technology used in network security and monitoring tools to inspect and analyze data packets, gaining insights into traffic types, applications, and potential security threats. * Describe how DPI works, covering packet capture, packet parsing, pattern recognition, decision making, logging, and real-time processing. * Explain the three levels of packet inspection: Shallow packet inspection (SPI), medium packet inspection (MPI), and deep packet inspection (DPI), highlighting their respective purposes. * Conclude by discussing the various domains where DPI is applied, including security, quality of service, content filtering, and network optimization. * Mention the role of protocol analyzers, which capture and display network traffic on a user interface, and their key functions in distinguishing communication protocols, aiding in development, debugging, troubleshooting, and network monitoring. * Highlight the features of protocol analyzers, including data capture, testing and debugging support, and enhanced insights into network environments for system administrators. * 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:**  Modern Network Monitoring Tools and Techniques | * Begin the lesson by discussing the importance of network monitoring in today's hyper-connected world, emphasizing the consequences of not detecting network issues and security threats. * Explain the role of modern monitoring tools in ensuring network reliability and security. * Describe the concept of anomaly detection in modern network monitoring and outline the three main steps involved: Evaluating network traffic, identifying irregularities, and conducting analysis. * Introduce the different types of anomalies: Point anomalies, contextual anomalies, and collective anomalies, providing examples for each type. * Discuss what network behavioral analysis (NBA) is and how it contributes to network security and performance by identifying deviations from established norms. * Explore practical applications of network behavioral analysis, such as insider threat detection and malware detection, using real-world examples. * Introduce the concept of AI automation in network management, emphasizing the efficiency and security benefits of using AI in network monitoring. * Explain how machine learning (ML), a subset of AI, plays a role in network monitoring by rapidly processing network data, automating pattern and anomaly identification, and adapting to evolving threats without constant rule updates. * Describe the applications of ML in network monitoring, including predictive maintenance, anomaly detection, traffic optimization, and predicting future network issues. * Discuss how AI and ML perform real-time data analysis in network monitoring and how data analysis and machine learning are integrated to make informed, autonomous decisions in network 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. |
| 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 | **Lab:**  Modern Network Monitoring Tools and Techniques | * 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 Structure and Configuration of Firewall Rules, Firewall Services and Features, NGFW and DPI * 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 |

### 