LESSON: Findings Analysis and Reporting

Primer

This module includes two short labs: the first lab focuses on Analyzing Linux Logs, while the second lab focuses on Windows Event Viewer Investigation. We highly recommend that instructors plan ahead to allocate sufficient time for these labs to ensure students have ample opportunity to practice.

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 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.

Summary

In this lesson, learners will explore network forensics, acquiring skills in analyzing network traffic and logs to identify and respond to cybersecurity incidents. The significance of network forensics lies in its ability to uncover crucial evidence dispersed across various network components. Distinguishing itself from network monitoring, the focus here is on detailed post-incident analysis rather than proactive threat detection. The challenge of resource-intensive continuous recording is explored, typically initiated after incident identification. Key log data sources, including firewall, server, DNS, and web application logs, are highlighted, alongside tools such as Tcpdump, Wireshark, and Zeek for effective traffic analysis. The lesson also covers Windows Event Viewer, its binary log format, and the

interpretation of event IDs for forensic investigations. Additionally, learners will gain insights into log analysis, its categorization, and the tools used, emphasizing the importance of chronological event organization and timeline creation in digital forensics. Lastly, the lesson covers anti-forensics, overcoming tampering, and the essential tools for a comprehensive investigative approach, providing learners with a robust foundation in network and digital forensics.

Objectives

- Define the concept of network forensics and its relevance within the cybersecurity industry.
- Differentiate between network forensics and network monitoring.
- Explain the importance of traffic capture in network investigations and identify several data sources.
- List relevant data to focus on during a network traffic investigation.
- Explain and illustrate how to use different network forensics tools.
- Define the concept of log analysis and its role in digital forensics.
- Describe the classification and structure of logs.
- Explain the log collection and log correlation processes.
- Identify relevant log examples.
- List commands used to search through logs.
- Define the role of the Windows Event Viewer in log monitoring, analysis, and troubleshooting.
- Explain and illustrate how to use the Windows Event Viewer.
- Identify relevant event IDs.
- Describe alternative utilities that can be used to view Windows events.
- Describe the role and importance of chronological event organization in forensic investigations.
- Compare and contrast between a Filesystem Timeline and a Super Timeline.
- Identify tools used in timeline creation and explain how to create a timeline using Autopsy.
- Discuss strategies for overcoming tampering in digital forensics.

Lesson Activities and Teaching Strategies

Estimated Time	Lesson Portion	Directions
2 min	**Lesson Opener:** Findings Analysis and Reporting	● Introduce learners to the importance of findings analysis and reporting in cybersecurity.
5 min	**Real World Scenario:** Findings Analysis and Reporting	● 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.
2 min	**Lesson Companion:** Findings Analysis and Reporting	● Review the lesson companion, 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 Forensics	● Discuss the significance of network forensics within digital forensics. ● Explain the focus on analyzing network traffic for cybersecurity incidents. ● Explore the role of network forensics in discovering evidence related to cybersecurity incidents. ● Emphasize the value of analyzing data dispersed across various network components. ● Compare and contrast network forensics and network monitoring in terms of tools, approaches, and mindset. ● Highlight the difference in goals: Real-time threat prevention vs. post-incident analysis. ● Introduce packet capture as the primary source for network investigations. ● Discuss challenges faced by small and medium businesses in continuous traffic recording. ● Explore the challenges of tampering with network traffic compared to static endpoint data. ● Discuss the complexity introduced by multiple independent devices logging traffic. ● Identify essential log data sources, such as firewall logs, server logs, DNS logs, and web application logs. ● Explain their significance in uncovering unauthorized access attempts and domain-related activities. ● Introduce additional data sources like intrusion detection systems (IDS), deep packet inspection, and proxy servers. ● Discuss how these sources enhance network forensic analysis. ● Explain the role of proxy servers in maintaining web traffic logs and aiding investigations. ● Highlight the benefits of proxy servers in identifying malicious requests and reconstructing user actions. ● Discuss key areas of focus in analyzing network traffic, including protocol irregularities and anomalous patterns. ● Emphasize the importance of analyzing timestamps and correlating data from various sources. ● Introduce essential network forensic tools such as Tcpdump, Wireshark, and Zeek. ● Explain their purposes and contributions to network traffic analysis. ● Explore Wireshark's statistical capabilities, including protocol usage analysis and traffic volume filtering. ● Discuss how Wireshark aids investigators in focusing on specific devices. ● Provide examples of Zeek filters for scenarios like finding transferred files and inspecting SSL/TLS traffic. ● Explain the purpose of each Zeek filter in enhancing network forensic analysis.

		● Discuss indicators of missed alerts, such as malware signatures, unusual DNS requests, and known payloads. ● Emphasize the importance of identifying these indicators for effective network security. ● Introduce TCPReplay and its role in editing and replaying captured network traffic. ● Provide the basic command for replaying traffic and its significance in forensic analysis. ● Be prepared to discuss the implication of the real world scenario presented at the beginning of class on Network Forensics. There are specific prompts that you should ask learners to reflect on to apply this concept to the real world scenario.
5 min	**Real world scenario:** Network Forensics	● 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.
5 min Break		
20 min	**Cyber Uncovered:** Log Analysis	● Define log analysis as the process of examining logs generated by computers, networks, and applications to extract insights, diagnose problems, or understand system behavior. ● Explain the importance of parsing, aggregating, and analyzing log data for identifying trends, detecting anomalies, and responding to security incidents. ● Discuss how logs are crucial in digital forensics for tracing and reconstructing events during a cybersecurity incident. ● Emphasize the role of logs in identifying the cause, extent, and perpetrators of incidents across all systems, applications, and devices. ● Introduce log classification based on source and depth, such as system logs, application logs, security logs, and audit logs. ● Explain the common practice of classifying logs by logging levels (Error, Warning, Debug, Information) and its relation to the amount of logged data. ● Describe the four components of a typical log structure: Timestamp, source identifier, event type or category, and detailed message. ● Highlight the significance of these components in log analysis for understanding events, severity levels, user IDs, and error codes. ● Explain the challenges of keeping logs separately at scale and introduce the concept of log forwarders for more manageable log collection. ● Emphasize the importance of correlating logs to piece together events from different sources, providing a comprehensive understanding of incidents. ● Discuss the role of the Network Time Protocol (NTP) in ensuring accurate and synchronized timestamps across systems for effective log correlation.

		● Provide information about the location of logs on Linux systems (/var/log) and their accessibility using preinstalled Linux utilities. ● List common logs relevant to forensic investigations, such as system logs, authentication logs, Secure Shell (SSH) logs, and DPKG logs. ● Introduce additional logs for specific applications like Apache, Nginx, and SQL servers, explaining their importance in investigating various issues. ● Describe the meticulous process of searching through logs, involving chronological correlation, keyword searches, and specialized tools. ● Introduce key Linux text processing utilities (grep, awk, sed, cut, sort, uniq) and explain their roles in improving log search and analysis. ● Walk through the example command 'grep 'Failed password' /var/log/auth.log' to detect failed login attempts. ● Introduce additional commands to extract usernames, attackers' IP addresses, count attempts per IP, and list brute-force attempt dates, showcasing the progression of log analysis. ● 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	**Real world scenario:** Log 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	**Lab:** Analyzing Linux Logs	● 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 Break		
20 min	**Cyber Uncovered:** Windows Logs	● Provide an overview of Windows Event Viewer as the logging system for Windows. ● Highlight the ways it differs from Linux logs, mentioning the specific binary format (.evtx) and the storage location. ● Explore the wide range of information recorded by the Windows Event Viewer. ● Discuss its role in monitoring, analyzing, and troubleshooting various aspects of the Windows operating system and installed applications. ● Discuss the role of a forensic investigator in examining the Windows Event Viewer. ● Emphasize the key signs they would look for, such as unauthorized access, failed login attempts, and evidence of tampering. ● Explore the indications of malware activity within the Event Viewer.

		● Discuss how repeated security alerts or antivirus error messages contribute to reconstructing the timeline and scope of a security incident. ● Introduce the process of searching through events using log filtering. ● Discuss the criteria for filtering logs, such as event level, sources, event IDs, and date ranges. ● Provide descriptions for key event IDs (4624, 4648, 1102, 4720, 4732, 4663, 4672). ● Explain how each event ID is relevant in a forensic context, emphasizing their significance in identifying specific events. ● Discuss the importance of event IDs related to processes (4688, 4946, 7001, 7022, 7045). ● Explore how these event IDs contribute to understanding application or malware execution, Windows Firewall changes, service start operations, service hangs, and service installations. ● Introduce alternative forensic suites, such as FTK and OSForensics. ● Discuss their role in importing .evtx files and providing additional filtering and viewing options for Windows 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.
20 min	**Lab:** Windows Event Viewer Investigation	● 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	**Real world scenario:** Windows Logs	● 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.
5 min	**Pulse Check**	● Before you launch the pulse check, explain each section clearly, and encourage the learners to participate in the survey. ● After administering the survey, share the poll results with learners and ask learners to provide feedback ● Encourage learners to attend office hours with the associate instructor.
5 min Break		
20 min	**Cyber Uncovered:** Timeline Analysis and Reporting	● Emphasize the primary objective of investigations: To reconstruct events and provide clear, factual insights. ● Highlight the importance of creating timelines and reports for legal and disciplinary proceedings. ● Explain how putting events in a timeline reveals unnoticed evidence and helps discover previously undetected events. ● Discuss the significance of chronological organization in identifying cause-and-effect relationships in various investigative contexts.

		● Define timeline creation and its role in arranging events in chronological order. ● Stress the importance of understanding the sequence and timing of activities during an incident, including high-level and minute details. ● Differentiate between Filesystem Timelines and Super Timelines in terms of definition, mechanism, difficulty, and use. ● Discuss the distinct applications of various types of timelines within investigative processes. ● Introduce forensic software such as Autopsy and dedicated tools like log2timeline for creating Super Timelines. ● Highlight the features of Autopsy, including its graphical interface and integration with other forensic functionalities. ● Discuss log2timeline's specialization in parsing logs and its command-line-based configuration for advanced users. ● Provide step-by-step instructions for creating a timeline using Autopsy, covering case creation, data source addition, and timeline analysis. ● Emphasize the application of filters in the Timeline tool for specific criteria and the importance of analyzing visual timelines for patterns or anomalies. ● Explain the concept of anti-forensics during an attack, focusing on adversaries deleting logs or modifying entries to conceal activities. ● Highlight the specific tampering methods on Windows (deleting logs) and Linux (editing files) mentioned in the text. ● Discuss the inconvenience of tampering and its potential as evidence in legal proceedings. ● Stress the importance of preconfiguring systems for remote logging or regular log backups to ensure data integrity, even in the face of tampering attempts. ● Be prepared to discuss the implication of the real world scenario presented at the beginning of class on Timeline Analysis and Reporting. There are specific prompts that you should ask learners to reflect on to apply this concept to the real world scenario.
25 min	**Real World Scenario:** Timeline Analysis and Reporting	● Break up learners into breakout rooms to discuss the scenario and brainstorm answers to the scenario task questions. ● Have learners come back together as a class and assign each group one of the tasks to review their suggestions and ideas.
15 min	**Lesson Closure**	● Encourage learners to read ahead of time ● Provide learners additional resources to read / practice and assign homework (e.g., future labs) before you demonstrate the labs during the next class ● Spend some time to highlight what are the key takeaways from today's lesson ● Important topics covered during the class includes ○ Highlight the key takeaway regarding Network Forensics:

		■ Network forensics involves the continuous monitoring and analysis of network traffic to identify suspicious activities and security breaches in real time. By capturing and analyzing data packets, investigators can reconstruct the sequence of events that led to an incident. ■ Evidence in network forensics is often dispersed across multiple components such as routers, servers, and endpoint devices. Each of these components may hold crucial information like IP addresses, logs, or session details that contribute to a comprehensive investigation ■ The complex flow of data through various nodes presents challenges due to the dynamic and often ephemeral nature of network traffic. Transient data may be difficult to capture and analyze, requiring advanced tools and techniques to ensure no critical information is missed ○ Highlight the key takeaway regarding Log Analysis: ■ Log analysis involves parsing and analyzing data to identify trends and anomalies ■ Logs are categorized based on the resources such as system, application, security, and levels such as error, warning, debug, and information ■ In Linux systems, logs are generally found under /var/log and there are various tools built-in Linux that aid that log analysis such as cat, grep, awk, sed, cut, sort, and uniq. ○ Highlight the key takeaway regarding Windows Log Analysis: ■ Windows Event Viewer stores logs in a binary format within *.evtx files. This format is efficient for storage and processing but requires specialized tools such as FTK and OSForensics for reading and analyzing the data ■ An investigator reviewing the Security log might focus on Event ID 4624, which records successful logins. By analyzing the timestamps and associated account names, they can detect unusual login patterns or unauthorized access attempts. ■ Forensic investigators utilize Event Viewer to search for indications of unauthorized

		access, system tampering, and malware activity. By examining these logs, they can trace suspicious behaviors, identify security breaches, and gather critical evidence for investigations ■ Logs in the Event Viewer are organized by Event IDs, timestamps, and categories to facilitate the identification of specific events. Investigators use these attributes to filter and pinpoint events of interest, allowing for precise analysis of system and application activities ○ Highlight the key takeaway regarding Timeline Analysis and Reporting: ■ The primary aim of forensic investigation is to reconstruct events and provide factual insights that can be used for legal or disciplinary purposes. This process involves collecting and analyzing digital evidence to support investigations with accurate, unbiased information. ■ Organizing events chronologically helps reveal previously undetected activities and establish cause-and-effect relationships. By analyzing the sequence of events, investigators can identify anomalies, trace the origin of incidents, and understand the broader context of an incident ■ A filesystem timeline tracks file activities, such as creation, modification, and deletion timestamps. A super timeline, on the other hand, combines these file activities with other system events, like network connections and user logins, to provide a comprehensive overview of system behavior. Tools like Autopsy and log2timeline are used to create these timelines, enabling forensic investigators to correlate data from multiple sources and derive meaningful insights
	Add Additional Time Filler	● Review using Kahoot or other similar platforms ● Conduct interview preparation conversations ● Continue discussions on real-world scenarios ● Demonstrate how to create users in Linux and grant them permissions ● Discuss different career paths in cybersecurity and highlight the roles that require Linux skills