LESSON: Incident Handling

Primer

This module includes two short labs: the first lab focuses on Malware Analysis using Sysinternals, while the second labs are optional level up: Malware and Fileless Malware. 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

- Check-in with the students to see if they have any questions or need further clarification from any subject from the last class 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 discuss the crucial phases of incident response, focusing on containment, eradication, and recovery strategies. The initial steps in containment will be explored, emphasizing the delicate balance between isolating affected systems and maintaining normal business functions while preserving evidence and ensuring effective communication. The lesson will address the strategic decision-making process in incident response, weighing the "act or wait" dilemma and the benefits of waiting for threat intelligence and planning. Participants will gain insights into malware types, antivirus engines, and the utilization of tools like VirusTotal for comprehensive threat analysis. Techniques such as malware analysis, reverse engineering, and various analysis methods will be covered, along with the significance of static analysis in early incident detection. The use of specialized tools like hex viewers, Binwalk, and the Sysinternals Suite will be explored for visualizing and diagnosing Windows systems. The lesson will also touch on the risks associated with eradication, emphasizing collateral damage, reinfection risks, and data and evidence loss. The recovery process, including factors influencing its duration and the role of a disaster recovery plan (DRP), will be thoroughly examined. Learners will gain a comprehensive understanding of the recovery scope, covering data restoration, system repair, security updates, and thorough testing for complete incident resolution.

Objectives

- Describe the objective of the incident containment stage and its considerations.
- Explain the concept of the “act or wait” decision and the benefits of waiting before acting.
- Define the concept of indicators of compromise (IoCs) and their usage in incident handling.
- Review fundamental concepts about malware, including malware types and antivirus (AV) engines.
- Recognize the role of VirusTotal in malware identification when AV engines fail.
- Identify different types of malware investigation techniques and analysis methods.
- Describe static malware analysis techniques, including raw data visualization and magic bytes.
- Illustrate the use of malware analysis tools, including HxD, Binwalk, and the Sysinternals Suite.
- Identify the key steps and follow-up actions of the eradication stage.
- Describe potential risks during eradication.
- Identify the steps of the recovery stage.
- Define the concept of a disaster recovery plan (DRP).
- Explain the factors that define the recovery time and scope.

Lesson Activities and Teaching Strategies

Estimated Time	Lesson Portion	Directions
2 min	**Lesson Opener:** Incident Handling	● Introduce learners to the importance of incident handling in cybersecurity.
5 min	**Real World Scenario:** Incident Handling	● 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:** Incident Handling	● 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:** Containment Stage	● Emphasize the primary objective: Limiting the impact of a security breach. ● Highlight the importance of isolating affected systems and preventing further incident spread. ● Discuss immediate steps for isolating affected systems without disrupting critical business functions. ● Explore methods to maintain the integrity of logs and evidence during containment. ● Identify communication channels crucial for team coordination during the containment process. ● Stress the significance of proper planning in addressing containment considerations. ● Emphasize that effective planning can address critical questions in advance, streamlining the response. ● Explain the "act or wait" consideration and its impact on incident response. ● Discuss the risks and benefits associated with waiting and immediate intervention. ● Explore reasons for waiting, including gathering threat information and obtaining IoCs. ● Discuss how strategic planning during the waiting period can enhance response effectiveness. ● Define and elaborate on threat information and its role in understanding attacker tactics. ● Explain the concept of indicators of compromise (IoCs) and their significance in forensic data. ● Discuss practical uses of IoCs in incident response, including that they serve as warning signs and aid in threat identification. ● Explain how IoCs can be searched for in systems and networks for rapid detection during an incident. ● Introduce the concept of adversaries reusing techniques and tools. ● Highlight how cybersecurity incident response teams (CSIRTs) benefit from information gathered in other incidents. ● 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:** Containment Stage	● 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:**	● Explain the concept of malware, what it stands for, and its primary purpose.

	Basic Malware Analysis	● Highlight the diversity of malware families, mentioning viruses, ransomware, and spyware. ● Discuss various malware types, including ransomware, rootkits, Trojans, and worms. ● Emphasize the importance of understanding the distinct characteristics and objectives of each type. ● Explain how AV engines contribute to incident response by quickly identifying malware signatures. ● Discuss the importance of updated signatures in effectively containing and remediating attacks. ● Explore alternatives in cases where AV fails, introducing the use of VirusTotal. ● Highlight how VirusTotal aggregates multiple antivirus engines for a comprehensive threat overview. ● Emphasize the benefits of VirusTotal while cautioning against uploading sensitive files. ● Recommend safer actions, such as hash, name, or URL lookups, during the initial stages of an investigation. ● Introduce key techniques: Malware analysis and reverse engineering. ● Emphasize their association and independent applicability in understanding malicious behavior. ● Break down analysis methods, including basic static and dynamic analysis and advanced static and dynamic analysis. ● Highlight the specific information each method provides in uncovering malware behavior. ● Discuss the significance of static analysis without even executing malware. ● Explore tools such as hex viewers, strings, and Binwalk for static analysis purposes. ● Introduce the Sysinternals Suite as a valuable set of tools for managing, diagnosing, and monitoring Windows environments. ● Emphasize its role in inspecting system processes, file activities, and network traffic during incident response. ● Explain the purpose of the strings utility in identifying hard-coded strings in an executable. ● Introduce Sigcheck as a utility used to verify file version numbers, digital signatures, and timestamp information. ● Discuss Binwalk as a focused tool for identifying magic byte patterns and hidden files. ● Emphasize the importance of further investigation by cybersecurity experts for complex 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	**Real world scenario:** Basic Malware 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:** Malware Analysis Using Sysinternals	● 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**	● 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:** Eradication and Recovery	● Emphasize the importance of proper eradication in incident response to prevent the recurrence of security breaches. ● Explain the eradication process, highlighting actions such as systematically removing malware, applying security patches, and updating firewall rules. ● Discuss the significance of closely monitoring IoCs after an incident, addressing the potential for multiple threat actors and their ability to carry out an unlimited amount of attempts. ● Explore the risks associated with eradication, including collateral damage, reinfection risks, potential data loss, and the importance of preserving forensic evidence. ● Introduce the recovery process, covering steps like restoring systems from backups, patching vulnerabilities, and verifying system integrity and security. ● Discuss factors that influence the duration of the recovery process, such as organization size, system complexity, and incident response team preparedness. ● Explain the concept of a disaster recovery plan (DRP) and its role in minimizing the effects of unplanned incidents, enabling the organization to resume critical functions. ● Detail the steps of the recovery process, including activation, restoration, verification, and documentation, emphasizing the importance of capturing key learnings. ● Break down the recovery scope into key components—data restoration, system repair/rebuild, security updates, and testing—highlighting their significance in fully resolving incidents. ● 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:** Eradication and Recovery	● 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.
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 during the containment stage discussed in the class: ■ Main objectives of containment (i.e., limit the impact of the security breach) ■ Considerations such as systems isolations ■ Maintain the integrity of logs ■ Refrain from compromising the log integrity during the containment strategy ■ Advantages and disadvantages of "act or wait" ○ Highlight the key takeaway for basic malware analysis ■ Malware is a software designed for malicious intent such as disrupt business operations, steal user credentials ■ There are many types of malware such as rootkit, Trojan, keylogger, dropper ■ AV engines play critical role in identifying malware signature in an incident response ■ Malware analysis methods such as basic analysis and advanced dynamic analysis ○ Highlight the key takeaway for Eradication and Recovery Stage ■ Key action during this stage includes removal of the malware, applying patches, changing credentials on the compromised systems, and installing an update ■ After removal of malware, the affected system should be monitored to ensure that the malware is fully removed from the system
	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