LESSON: Infrastructure Attacks

Before you Begin

This is the fifth lesson of this course. Students are at the half-way point of this course. Instructors may want to spin up the first lab of the module to get it ready and stable before doing it live when the lab slide comes up.

For this lesson, instructors are required to ensure the following activities are completed:

- 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.
- Ensure learners are given opportunities for breaks throughout the lesson. The pacing guide below provides recommended breaks. However, there are additional breaks added in the slide deck, please use them only if needed.
- 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, immediately 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. This is a must do. 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 open Q&A.

Summary

In this lesson, learners discuss enumeration, understanding the significance of identifying vulnerabilities within systems for potential exploitation. They will explore key tools and databases, such as Exploit-DB, CVE Details, and SearchSploit, essential for collating and analyzing known vulnerabilities and exploits. The lesson will guide them through the utilization of SearchSploit in Kali Linux for offline exploit searches, streamlining the process of vulnerability identification. Learners will gain a comprehensive understanding of crucial terminologies like vulnerability, payload, and exploit, using databases like CVE to discuss security risks within a standardized framework. The focus then shifts to the Metasploit framework, a potent tool for penetration testing, as learners explore its various modules, commands, and capabilities for effective ethical hacking and cybersecurity assessments. Additionally, they will grasp the methodologies of bind and reverse shells, differentiate between common shells like Telnet, SSH, and Netcat, and comprehend the functionalities of various interactive shell types within Metasploit. The

lesson culminates with insights into MSFvenom, emphasizing its role in generating shellcode and practical guidance on payload creation, delivery, listener setup, and post-exploitation activities. Finally, learners will understand the importance of awareness and endpoint protection measures to mitigate risks associated with payload-based attacks, ensuring a holistic approach to system security.

Objectives

- Describe the process of enumeration in cybersecurity.
- Explain enumeration terminology.
- Define the Common Vulnerabilities and Exposures (CVE).
- List the search engines.
- Describe how SearchSploit works.
- Describe Metasploit framework, tools, and module types.
- List Metasploit commands and module configurations.
- Define Metasploit scanning and search commands.
- Define shell, bind, and reverse shell.
- Describe the common shells and their uses.
- Explain the Metasploit shells.
- Define payload creation.
- Explain the Meterpreter listener process.
- Explain Meterpreter's post-exploitation modules.
- Compare and contrast the pros and cons of Metasploit.
- Describe the optional means of protection.

Lesson Activities and Teaching Strategies

Estimated Time	Lesson Portion	Directions
< 2 min	**Lesson Opener:** Infrastructure Attacks	● Introduce learners to cybersecurity infrastructure attacks.
< 5 min	**Real World Scenario:** Infrastructure Attacks	● 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:** Enumeration	• Emphasize the role of enumeration in cybersecurity, highlighting its importance in both offensive and defensive strategies. • Discuss how enumeration provides a deeper understanding of target systems and networks. • Define vulnerability, using the provided example. Discuss why identifying vulnerabilities is critical in cybersecurity. • Explore payload, referencing the text's example of a ransomware attack and its role in causing harm. • Explain the concept of exploits, drawing on the text's example of using a software bug to bypass security measures. • Introduce CVE and its function as a list of publicly known cybersecurity vulnerabilities and exposures. • Explain the unique identifiers assigned to each CVE for standardized reference and its role in aiding security professionals. • Discuss how the standardization provided by CVE facilitates data sharing across different platforms and tools. • Introduce CVE Details as an excellent website for documenting various CVEs, including severity, practicality, and an overview of affected products. • To better understand Common Vulnerabilities and Exposures (CVE), you can explore CVE Details for real world examples. Additionally, the official CVE website is an excellent resource for comprehensive information. • Introduce Exploit-DB as a vast archive gathering exploits, shellcodes, and security-related information. • Highlight NIST NVD as a U.S. government repository providing data on software vulnerabilities, misconfigurations, and impact metrics. • Explain SearchSploit as a tool providing portability to Exploit-DB, excluding the Google Hacking Database. • Mention that SearchSploit is pre-installed on Kali Linux and can be downloaded for Mac and Windows. • Provide step-by-step instructions for updating the SearchSploit database, searching for exploits, and downloading scripts. • Showcase the Kali Linux terminal view demonstrating the execution of the command 'searchsploit smb'. • Explain the significance of the demonstrated command and how it aligns with the functionality of the SearchSploit tool. • 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:** Enumeration	• 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:** Metasploit Framework	● Communicate the purpose of Metasploit and its intended audience. ● Highlight the integration of MSFconsole in Kali Linux and its significance. ● Explain the concept of Metasploit modules and how they contribute to the framework's flexibility. ● Emphasize the importance of running systemctl commands to prevent database-related issues. ● Define the role of exploits in Metasploit and their impact on targeted systems. ● Explain the function of payloads and the actions they define after a successful exploit. ● Clarify the purpose of auxiliaries, post modules, and Encoders in the Metasploit framework. ● Introduce essential Metasploit commands, such as "?," "show options," "show info," and "show targets." ● Demonstrate the usage of these commands within the Metasploit framework. ● Provide a step-by-step explanation of Metasploit module configurations using methods like "use [name]" and parameters like RHOST and LPORT. ● Guide learners through the execution of the "exploit" command. ● Conduct a demonstration of running the BlueKeep CVE auxiliary with Metasploit. ● Highlight the practical application of Metasploit in exploiting vulnerabilities. ● Explain the process of scanning in Metasploit, utilizing Nmap from MSFconsole. ● Showcase the variety of scanners available within MSFconsole. ● Emphasize the significance of saving scans for building the database. ● Describe the search functionality within Metasploit, covering the "search" option and its application across all modules. ● Clarify the use of "use" as a generic handler for an exploit and its specific application with "use [name]". ● 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:** Metasploit Framework Features	● 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:**	● Provide a clear definition of a shell in the context of cybersecurity.

	Bind and Reverse shells	● Explain the significance of a shell as a remote command interface for controlling compromised machines. ● Differentiate between a bind shell and a reverse shell, detailing how each establishes connections and facilitates command execution. ● Highlight the preference for reverse shells in bypassing common firewall rules, emphasizing the initiation of connections from the victim machine. ● Use the provided illustration of bind and reverse shells to visually reinforce the concepts. Encourage learners to identify the key components and understand the flow of connections. ● Introduce Telnet as a communication protocol, specifying its bidirectional, interactive, text-oriented communication features. ● Discuss the limitations of Telnet, particularly its lack of encryption and the associated security risks. ● Define SSH as a cryptographic network protocol, emphasizing its role in secure network services, remote administration, and file transfers. ● Share a demonstration of connecting to an SSH server from Kali Linux to provide a practical understanding. ● Describe Netcat as a versatile networking utility within the TCP/IP protocol, highlighting its "Swiss Army knife" functionality. ● Emphasize Netcat's port scanning capabilities, file transfers, and ability to create both cleartext and encrypted connections. ● Introduce Metasploit as a framework enabling the creation of interactive shells for engaging with compromised systems. ● Outline different shell types available in Metasploit, including Command Shell, Meterpreter Shell, Bash Shell, Python Shell, and PHP Shell. ● Dive deeper into Meterpreter as a robust shell within Metasploit, detailing its extensive functionalities, such as file system interaction and system data harvesting. ● Emphasize the importance of Meterpreter in post-exploitation activities. ● 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.
25 min	**Lab:** Common Metasploit Applications	● 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 (wait for ~75% respondent rate then close the poll)		
5 min Break		
20 min	**Cyber Uncovered:**	● Provide an overview of MSFvenom and its role in the Metasploit framework.

	Payload Creation and Usage	● Explain the key parameters involved in payload creation: -p, LHOST, LPORT, -f, -o. ● Conduct a live demonstration creating a reverse TCP Meterpreter shell. ● Highlight the significance of each parameter used in the demonstration. ● Emphasize the overall outcome of the command for creating the reverse shell. ● Explain the importance of a listener in establishing communication back to the attacker. ● Conduct a step-by-step demonstration of setting up a Meterpreter listener via MSFconsole. ● Discuss the role of MSFconsole, the handler exploit module, and the specified payload. ● Guide learners through launching MSFconsole, selecting the handler module, and configuring payload parameters. ● Illustrate initiating the listener and waiting for connections from the executed payload. ● Summarize the overall process demonstrated in intercepting a reverse TCP shell. ● Introduce essential Meterpreter post-exploitation commands: getuid, sysinfo, ipconfig, upload, download, and shell. ● Showcase a live demonstration of each command and explain their functionalities. ● Emphasize how these commands contribute to post-exploitation activities. ● Discuss the advantages and disadvantages of using Metasploit in cybersecurity. ● Engage students in a discussion about the modular and customizable nature of Metasploit, along with potential drawbacks. ● Highlight the importance of both CLI and GUI interfaces. ● Explain the significance of updating systems regularly for protection against automated tools. ● Discuss the role of endpoint protection measures and firewalls in preventing attacks. ● Emphasize the importance of being aware and detecting malicious activity early on to prevent further damage. ● 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.
25 min	**Lab:** Reverse Shell Creation and Execution	● 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 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 understanding vulnerabilities and exploiting them ethically as well as the tools for penetration testing and post-exploitation activities. 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
	Additional Time Filler (if needed)	● Kahoot ● Discuss interview prep and questioning ● Use breakout rooms for additional lab practice ● Continue Real World Scenario Conversation