LESSON: Network Scanning

Before you Begin

This is the second lesson of this course. Instructors should not spend any time explaining how to access TDX Arena or how to navigate Canvas. 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. 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 explore the foundational role of network scanning in cybersecurity, gaining insights into the network's structure, active hosts, and services. The TCP 3-way handshake and TCP flags are examined for secure connections, with a focus on Nmap, a key open-source tool for identifying active devices, open ports, and network characteristics. Key features of Nmap, including host discovery, port scanning, version detection, and OS detection, are highlighted, along with its scriptable interactions for advanced automation. The lesson covers various scanning types and command flags, providing flexibility and control. Fingerprinting in Nmap, covering OS and service/version fingerprinting, offers crucial information for network understanding and preparation. The lesson concludes with host discovery in Nmap, introducing learners to the Nmap Scripting Engine (NSE) for custom tasks and evasion techniques, ensuring stealthier scans and nuanced security assessments.

Objectives

- Define the concept of network scanning.
- Identify the different types of network scanning discoveries.
- Explain the TCP 3-way handshake process.
- Describe the TCP flags and their main role.
- Define Nmap and list its key features.
- Explain Nmap scanning types.
- Explain the basic Nmap command structure and flags.
- Describe Nmap fingerprinting types.
- List and describe TCP and UDP scans.
- Define host discovery and list its flags.
- Describe the Nmap Scripting Engine and its key points.
- Explain firewall and IDS evasion and their key points.

Lesson Activities and Teaching Strategies

Estimated Time	Lesson Portion	Directions
< 2 min	**Lesson Opener:** Network Scanning	● Introduce learners to the importance of network scanning in cybersecurity.
< 5 min	**Real World Scenario:** Network Scanning	● 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.
30 min	**Cyber Uncovered:** Introduction to Network Scanning	● Begin the lesson by emphasizing the significance of network scanning in cybersecurity assessments. ● Explain its role in understanding network structure, discovering active hosts, and identifying services. ● Provide an overview of various tools used for network scanning. ● Discuss the main aspects, including mapping the network structure, collecting crucial information, and identifying devices. ● Use the "Discoveries of Network Scanning" slide to engage learners. ● Walk through the discoveries of network scanning, emphasizing network layout, services, hosts, fingerprints, and open ports. ● Facilitate a discussion about how an attacker can leverage network discoveries. ● Explore the importance of understanding network layout, services, hosts, fingerprints, and open ports for targeted attacks or defenses. ● Explain the TCP 3-way handshake as a fundamental process for establishing connections. ● Use the provided illustration to visually guide learners through the steps of the handshake.

		● Break down the purpose of each TCP flag. ● Discuss their role in controlling the state and flow of a TCP connection. ● Engage learners with an interactive session using the TCP 3-way handshake illustration. ● Encourage questions and discussions to ensure a clear understanding. ● Relate TCP flags to real world scenarios, showcasing their significance in different stages of data transfer. ● Provide examples of when each flag might be employed. ● 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 Break		
30 min	**Lab:** Network Scanning with TCP	● 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		
30 min	**Cyber Uncovered:** Nmap Basics	● Begin by introducing Nmap as a versatile and open-source tool for network discovery and security auditing. ● Highlight the key features of Nmap, emphasizing its role in host discovery, port scanning, version detection, OS detection, scriptable interactions, and vulnerability detection. ● Discuss the varied usage of Nmap by IT professionals, ethical hackers, and cyber defenders for tasks like network inventory, service upgrade schedules, monitoring host uptime, and vulnerability assessments. ● Introduce different Nmap scanning types, such as SYN scan, TCP (Connect) scan, and mention other types like UDP scan, FIN scan, and Xmas scan, each with its use case and flag. ● Explore the basic command structure and flags in Nmap, covering options like specifying ports, skipping host discovery, using fast mode, setting timing templates, increasing verbosity level, and controlling output format. ● Dive into Nmap fingerprinting, explaining the significance of OS and service/version fingerprinting using the -O and -sV flags, respectively. ● Use the provided example of service/version fingerprinting to illustrate the practical application of flags and to showcase scan results on a target host. ● Cover TCP scans, focusing on SYN scan (-sS) and Connect scan (-sT), explaining their characteristics, use cases, and providing examples for better comprehension.

		● Conclude with UDP scan (-sU), detailing its purpose, mentioning its connectionless protocol, and providing an example scan on a target host. ● **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.
5 min Pulse Check (wait for ~75% respondent rate then close the poll)		
5 min Break		
30 min	**Cyber Uncovered:** Advanced Nmap Features	● Begin by emphasizing the importance of host discovery as a crucial preliminary step in network scanning, providing a foundation for more detailed scans while optimizing time and resources. ● Introduce the flags for host discovery, explaining each one's purpose, such as -sn for disabling port scan and options like -PE, -PS, -PA, and -PU for sending ICMP echo, TCP SYN, TCP ACK, and UDP packets, respectively. ● Use the provided example to illustrate the practical application of host discovery flags, emphasizing the command structure and the insights gained from identifying live hosts and open ports. ● Transition to the Nmap Scripting Engine (NSE) overview, highlighting its role in automating networking tasks and its script categories, such as default, discovery, vulnerability, and exploit. ● Emphasize the versatility of pre-written scripts available in the /usr/share/nmap/scripts/ directory, encouraging learners to explore and use them in their current format or as a basis for custom script development. ● Guide learners on running scripts using the --script flag, providing an example like --script=vuln to run vulnerability scripts, showcasing the relevance of scripting in Nmap scans. ● Introduce the significance of firewall and IDS evasion in ethical hacking and penetration testing, detailing key points such as fragmentation, decoy scanning, timing adjustments, source port manipulation, and idle scan. ● Use the provided example of a fragmented scan with decoy IPs to illustrate evasion techniques and highlight how these methods contribute to a more accurate assessment of the network's security posture. ● 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.
30 min	**Lab:** Nmap Port Scanning	● 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 network scanning fundamentals and Nmap's advanced capabilities like NSE. 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