LESSON: Social Engineering and OSINT

Before you Begin

This is the third 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. 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 will discuss open-source intelligence (OSINT), gaining a deep understanding of its crucial role in cybersecurity reconnaissance. The curriculum covers OSINT footprinting, information gathering, and people OSINT, equipping students with the skills required to map digital infrastructure and address cyberthreats. It delves into social networks in OSINT, Shodan.io, Google hacking, data leaks, SecurityTrails.com, Reverse Image Search, the OSINT framework, and Recon-ng. The lesson further extends to social engineering, unraveling psychological manipulation tactics—like phishing and impersonation—that pose threats to digital and physical security. Learners will gain practical insights into technologies like the fake ID generator, caller ID spoofing, email spoofing, short URL services, and SEToolkit, understanding their functionalities and potential risks. Emphasis is placed on the importance of awareness, education, and proactive measures for organizations to effectively safeguard against social engineering attacks through comprehensive training and robust security policies.

Objectives

- Define the use of OSINT in the cybersecurity domain.
- Describe the key aspects of OSINT footprinting.
- Explain the purpose and pivotal aspects of information gathering.
- List the objectives and methods of people OSINT and social networks.
- Explain the key features of Shodan.io.
- Explain the Google hacking technique.
- Describe the concerns that arise when data leaks occur.
- Describe the main goal of SecurityTrails.
- Explain the Reverse Image Search tool and how it can be used to assist investigators.
- Define the OSINT framework and the functionalities of Recon-ng.
- Describe social engineering.
- Explain social engineering attack methods and vectors.
- Explain the case study.
- List mitigation methods for social engineering attacks.
- Explain and describe social engineering tools.

Lesson Activities and Teaching Strategies

Estimated Time	Lesson Portion	Directions
< 2 min	**Lesson Opener:** Social Engineering and OSINT	● Introduce learners to the importance of social engineering and OSINT in cybersecurity.
< 5 min	**Real World Scenario:** Social Engineering and OSINT	● 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.
25 min	**Cyber Uncovered:** OSINT Introduction	● Explain the concept of OSINT (Open-Source Intelligence) and its significance in cybersecurity. ● Highlight that OSINT encompasses freely and legally obtainable information from public sources. ● Discuss the diverse media types covered by OSINT, including texts, images, videos, books, and television. ● Emphasize that OSINT extends beyond the internet and social networks. ● Introduce OSINT footprinting as a specific aspect within OSINT. ● Emphasize its role in gathering detailed information to build comprehensive target profiles. ● Discuss the importance of "pinpointing" in mapping the digital infrastructure of a target. ● Explore the significance of understanding the "business structure" for identifying potential vulnerabilities.

		● Explain how "social information" can provide human-centric insights, exposing additional cyberthreat vectors. ● Establish the foundational role of information gathering in cybersecurity endeavors. ● Highlight that information gathering is the initial phase in the cyber attack lifecycle. ● Explain the significance of "domain profiling" using tools like WHOIS lookup. ● Discuss "IP address analysis" and its importance in mapping network topology. ● Introduce "protocol examination" with a focus on identifying potential network vulnerabilities. ● Explore "security tracing" using Traceroute to illuminate packet paths and reveal network structure. ● Highlight the relevance of "personal data harvesting" through the analysis of publicly shared content on social media. ● Emphasize that information gathering lays bare the architecture, configurations, and potential vulnerabilities of the target environment. ● Discuss how insights gained from information gathering inform subsequent stages of security assessments or ethical hacking processes. ● 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		
20 min	**Cyber Uncovered:** OSINT Methods and Tools	● Define people OSINT and emphasize its importance in cybersecurity. ● Explain the goal of people OSINT in gathering information about individuals. ● Explore online searches as a method, including search engines and professional networking sites. ● Discuss the significance of exploring public records for information about an individual's past. ● Highlight the importance of social media analysis in gathering personal details and online behaviors. ● Introduce forum and blog analysis for insights into personal or professional discussions. ● Explain the use of specialized OSINT tools for automating data collection and analysis. ● Summarize the key points of OSINT and its critical role in identifying vulnerabilities. ● Emphasize the nuanced understanding of the human element in cybersecurity assessments. ● Discuss the emergence of social networks as a crucial source of OSINT data.

		● Present methods like profile analysis, connection mapping, content scrutiny, and automated data collection. ● Emphasize the role of social networks in understanding human behavior and organizational dynamics. ● Highlight the contribution of rich data from social networks to cybersecurity assessments. ● Introduce Shodan.io as a specialized search engine employed to identify online devices. ● Explain key features like device identification, service discovery, and vulnerability detection. ● Discuss use cases in cybersecurity assessments, research, and competitive intelligence. ● Define Google hacking and the role it plays in uncovering security loopholes. ● Introduce the Google Hacking Database (GHDB) and popular search terms. ● Provide examples of advanced search queries and their applications in cybersecurity. ● Present notable avenues where leaked data may surface, including search engines, whistleblower platforms, and web archives. ● Discuss the risks associated with leaked data and the importance of awareness and monitoring. ● Introduce SecurityTrails.com as a platform for cyber threat intelligence and domain data. ● Discuss its applications in cybersecurity assessments, investigative research, and domain analysis. ● Explain the significance of Reverse Image Search in the OSINT toolkit. ● Present popular platforms like Google Images and TinEye for Reverse Image Search. ● Discuss applications like identity verification, asset identification, and geolocation. ● Introduce the OSINT framework as an interactive, web-based platform. ● Explain core features, including resource aggregation, an interactive interface, and diverse categories. ● Highlight its role in simplifying the discovery process for OSINT resources and tools. ● Provide an overview of Recon-ng, emphasizing its role as an open-source intelligence (OSINT) tool designed for web reconnaissance in cybersecurity and digital investigations. ● Dive into the modular architecture of Recon-ng, explaining how the structure is based on modules, each serving specific reconnaissance tasks. Highlight the flexibility this approach provides for targeted data gathering. ● Cover the wide range of modules available in Recon-ng, including those for domain and host enumeration, contact information

		gathering, and social media analysis. Illustrate how learners can leverage these modules for various reconnaissance purposes. ● Discuss the scripting capabilities of Recon-ng, showcasing how learners can automate tasks. Emphasize the time-saving aspect, particularly in complex investigations, and highlight the importance of repeatability in workflows. ● Explore Recon-ng's integration with other tools and platforms. Illustrate how this integration enhances the tool's overall capabilities in terms of data collection and analysis. ● Provide concrete examples of Recon-ng's applications in OSINT, starting with its effectiveness in digital footprinting. Demonstrate how the tool identifies domains, subdomains, and related information. ● Explain how Recon-ng supports the collection of information crucial for social engineering campaigns. Showcase its role in gathering the data of potential targets to enhance the learners' understanding of its practical use. ● 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:** Working with Recon-ng	● 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		
25 min	**Cyber Uncovered:** Social Engineering	● Define social engineering as the manipulation of individuals to disclose confidential information. ● Emphasize the use of psychological tricks over technical hacking and the aim to exploit trust, fear, or curiosity. ● Discuss various attack methods, including phishing, pretexting, quid pro quo, baiting, tailgating, and impersonation. ● Provide examples and scenarios for each attack method to enhance understanding. ● Explore computer-based, phone-based, and physical attack vectors in social engineering. ● Discuss how each vector utilizes different channels to trick individuals or gain unauthorized access. ● Present a multi-faceted approach to protect against social engineering attacks, involving technical measures, policies, and user education. ● Highlight the importance of employee training, robust security policies, multi-factor authentication (MFA), security audits, incident response plans, and physical security measures. ● Introduce the background of ZenithCorp and the spear phishing attack on its financial department.

		● Break down the attack phases, including target identification and reconnaissance, crafting the spear phishing email, the malicious payload, credential harvesting, data breach, financial fraud, and the aftermath. ● Discuss the importance of employee training in recognizing and responding to spear phishing attempts. ● Highlight the role of multi-factor authentication (MFA) in reducing the risk of unauthorized access. ● Emphasize the significance of regularly updating and testing incident response plans. ● Stress the importance of continuously monitoring network activity for early detection and mitigation. ● 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:** Social Engineering and Case Study	● 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:** Social Engineering Tools	● Begin the lesson by introducing the overarching theme: Social engineering tools and their role in manipulating human interactions for information access. ● Emphasize the focus on functionality, cybersecurity roles, and impact on data security and system integrity. ● Introduce the fake ID generator, emphasizing its accessibility at fakenamegenerator.com and its purpose in creating synthetic identities. ● Discuss the potential uses and misuses of the fake ID generator, highlighting its implications for online verification processes. ● Move on to caller ID spoofing, exemplified by services like SpoofCard. Explain its function in masking phone numbers on the recipient's caller ID. ● Explore the legitimate uses of caller ID spoofing, such as privacy protection, and address potential misuses like prank calls and phishing. ● Transition to email spoofing, facilitated by services like Emkei.cz. Discuss its role in sending emails with altered header information and potential consequences. ● Highlight the benign and malicious ways which email spoofing can be used, emphasizing the complex challenge it poses in verifying sender identity. ● Discuss short URL services like Bit.ly and Shorturl.at, emphasizing their legitimate applications and their potential malicious uses in social engineering tactics.

		● Move on to the SEToolkit, an open-source framework for simulating social engineering attacks. Outline its features, including phishing attacks, pretexting scenarios, website cloning, payload delivery, mass mailer attacks, QR code attacks, SMS spoofing, and wireless access point attacks. ● Briefly introduce the SEToolkit and its primary features. ● Emphasize the significance of these features in assessing and improving security measures. ● Explain how SEToolkit facilitates the creation and deployment of phishing campaigns. ● Discuss the importance of understanding and simulating phishing attacks for security testing. ● Describe how SEToolkit allows for the design of pretexting techniques to assess responses. ● Highlight the role of pretexting in evaluating social engineering awareness. ● Discuss the website cloning tools provided by SEToolkit for credential harvesting exercises. ● Emphasize the importance of testing defenses against website cloning attacks. ● Explore how SEToolkit enables the delivery of payloads through various deceptive means. ● Discuss the implications of payload delivery on social engineering assessments. ● Explain the functionality of SEToolkit for mass email attacks with custom email templates. ● Discuss the relevance of mass mailer attacks in evaluating email security. ● Introduce the features of generating malicious QR codes and supporting SMS spoofing. ● Discuss the importance of assessing susceptibility to physical attacks via QR codes and SMS spoofing. ● Explain the tools provided by SEToolkit for creating malicious access points. ● Discuss the potential risks associated with wireless access point attacks. ● Introduce HiddenEye as a multifaceted tool in social engineering, emphasizing its open-source nature and target audience. ● Discuss how HiddenEye caters to ethical hackers, educators, and cybersecurity professionals. ● Detail the features of HiddenEye, such as phishing page creation, geolocation tracking, camera access, and credential harvesting. ● Discuss the integration capabilities of HiddenEye with other cybersecurity tools. ● Guide learners on installing HiddenEye on a compatible system, ensuring dependencies are met. ● Explain the process of choosing phishing campaign types, selecting or customizing templates, and deploying campaigns.

		● Discuss how HiddenEye collects data during and after the campaign. ● Emphasize the importance of analyzing the collected data to assess the effectiveness of phishing attempts. ● 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:** Social Engineering with HiddenEye	● 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 OSINT vs Social Engineering as well as the tools for mitigation. 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