LESSON: Web Anonymity

Before you Begin

This is the sixth lesson 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 will explore the layers of the internet, starting with the surface web, which is easily accessible through standard browsers, and extending to the deep web, which contains unindexed data like emails and electronic health records. The dark web, a small fraction of the internet, associated with illegal activities, will be introduced, requiring special tools like Tor or I2P for access. The focus then shifts to Tor, a primary tool for accessing the dark web, providing anonymity through volunteer-operated servers. Proxies, as intermediaries between clients and servers, will be discussed, covering caching proxies, anonymizing proxies, filtering proxies, and interception (transparent) proxies, each serving specific purposes. Anonymity VPNs will be explored for their excellence in providing online security and the lesson will delve into web proxy services, which offer varying levels of anonymity and security features. The role of VPNs, including site-to-site and remote access VPNs, in securing connections over less secure networks will be covered, along with a detailed examination of VPN protocols. The lesson concludes with a comprehensive understanding of Tor, its Onion routing

mechanism, hidden services, the Hidden Wiki, and the Tor Browser, empowering learners with insights into the diverse layers of the internet and tools for enhanced privacy and security.

Objectives

- Explain the three layers of the web: Surface web, deep web, and dark web.
- Define proxy servers and types.
- Explain the web proxy process.
- List the advantages and features of web proxies.
- List the free and paid web proxy services.
- Define virtual private networks (VPNs) and their basic types.
- Explain the anonymity VPN process, its advantages, and features.
- Compare and contrast VPNs and proxies.
- List and describe the VPN protocols.
- Define The Onion Router (Tor) and describe its three layers.
- Classify the nodes in the Tor network.
- Describe the Tor Browser and its features.
- Explain the Hidden Services of the Tor network and the Onion addresses used to access them.
- Explain the Hidden Wiki and its use.

Lesson Activities and Teaching Strategies

Estimated Time	Lesson Portion	Directions
< 2 min	**Lesson Opener:** Web Anonymity	● Introduce learners to the importance of SEH in cybersecurity.
< 5 min	**Real World Scenario:** Web Anonymity	● 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:** Web Levels	● Start by introducing the concept of the layered structure of the internet, emphasizing the diversity of content and accessibility. ● Utilize the provided illustration to visually represent the three web layers (Surface, Deep, Dark) and their characteristics. ● Discuss the surface web, highlighting its percentage of the total internet, accessibility via standard browsers, and indexing by search engines. ● Provide concrete examples of surface web content, such as news outlets, social media platforms, and online shopping sites. ● Transition to the deep web, emphasizing its vast percentage of the internet, lack of indexing, and the need for special tools or authorization for access. ● Illustrate the nature of deep web content, including personal emails, medical records, and confidential corporate information.

		● Move on to the dark web, discussing its limited percentage, the requirement for special tools, deliberate hiding, and its association with illegal activities. ● Provide specific examples of dark web content, such as black markets, dissident forums, and encrypted chat services. ● 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:** Surface, Deep, and Dark Web	● 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:** Proxy	● Emphasize the role of a proxy as an intermediary between a client and a server. ● Explain the diverse functionalities of proxies, including content filtering, data compression, and privacy enhancements. ● Discuss the characteristics and functions of caching proxies, highlighting their impact on web access speed, bandwidth usage, and server load. ● Explore anonymizing proxies, focusing on how they conceal user IP addresses and their applications in bypassing restrictions. ● Explain the purpose and use cases of filtering proxies, particularly in educational or corporate settings for enforcing internet usage policies. ● Introduce interception proxies, emphasizing their automatic communication interception in corporate networks and public Wi-Fi spots. ● Break down the web proxy process, explaining how a proxy server receives, processes, and forwards client requests, maintaining client anonymity. ● Utilize the provided illustration to visually reinforce the concept of the web proxy process. ● Highlight the advantages of using web proxies, such as anonymity, content filtering, and caching for improved web performance. ● Emphasize the role of web proxies in bypassing restrictions and their contribution to monitoring and logging for network administrators. ● Discuss security features provided by web proxies, including malware scanning, URL filtering, and data encryption. ● Showcase how web proxies contribute to bandwidth saving and improved speed through caching.

		● Introduce free web proxy services and discuss key features of each service, such as user-friendly interfaces, server locations, and data transfer limitations. ● Provide an overview of paid web proxy services, emphasizing the unique offerings of Oxylabs, Bright Data, Smartproxy, and NetNut. ● Highlight the distinctions between residential proxies, data center proxies, and rotating residential proxies offered by these services. ● Discuss specific features like proxy manager interfaces, browser extensions, and success rates for each paid service. ● 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		
25 min	**Cyber Uncovered:** VPN	● Introduce the concept of virtual private networks (VPNs) and their primary function. ● Explain how VPNs secure connections over less secure networks, emphasizing the masking of IP addresses and rerouting of traffic. ● Discuss site-to-site VPNs, focusing on their use in corporate settings and the secure communication they facilitate between branch offices. ● Explore remote access VPNs, highlighting their user-to-site configuration for secure remote access by employees. ● Explain anonymity VPNs, emphasizing their role in maintaining user anonymity and bypassing geographic restrictions. ● Break down the process of an anonymity VPN, detailing how the VPN client initiates a secure tunnel, encrypts data, and masks the user's IP address. ● Emphasize the VPN server's encryption and decryption stages, highlighting the protection of user data during transit. ● Instruct students to create a new illustration depicting the anonymity VPN connection versus a non-VPN connection to the internet. ● Emphasize the key stages in the VPN process, such as encryption, data routing, and IP masking. ● Discuss the advantages and features of anonymity VPNs, including IP masking, secure encryption, no-logs policy, bypassing geo-restrictions, and preventing ISP tracking. ● Emphasize how anonymity VPNs contribute to online anonymity and secure connections on public Wi-Fi networks. ● Compare VPNs and proxies based on key features, including anonymity level, security, geo-restrictions, speed, data encryption, and cost. ● Discuss scenarios where one might be preferable over the other, considering the specific needs of users. ● Introduce OpenVPN, highlighting its open-source nature, security features, encryption support, and ability to bypass network firewalls.

		● Explore IPSec, emphasizing its common use with other protocols for added encryption and its operation at the IP layer. ● Discuss L2TP, its encryption partnership with IPSec, and how it creates secure communication tunnels between connection points. ● Present PPTP, focusing on its historical significance, faster speed, and the caution associated with its use due to known security vulnerabilities. ● 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:** Web Proxy and VPN Usage	● 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:** Tor and Darknet	● Explain the concept of Tor and its objective of enhancing online privacy and freedom. ● Emphasize that Tor is a free software maintained by the non-profit Tor Project. ● Describe the Onion routing technique used by Tor, emphasizing data encryption in layers and transmission through volunteer-operated servers. ● Discuss how this process masks users' identities. ● Discuss the user base of Tor, including activists, journalists, and those in restrictive internet regions. ● Acknowledge the dual nature of Tor, providing anonymity but also enabling access to illegal activities. ● Introduce Tor as a platform for hidden services, extending anonymity to both users and service providers. ● Discuss the importance of hidden services in the Tor network. ● Explain the three layers of encryption in the Tor network. ● Describe the process of traffic traversal through random nodes and key exchanges. ● Introduce the entry (Guard) node and its role as the first point of contact. ● Explain the middle (Relay) node and its function in forwarding encrypted data. ● Describe the exit node and its role in decrypting data before it reaches its destination. ● Discuss the significance of the bridge node in overcoming network censorship. ● Introduce the Tor Browser as a modified version of Mozilla Firefox for anonymous browsing.

		● Highlight pre-configured security features and tools for managing proxy chains and blocking malicious scripts. ● Discuss the exclusive nature of hidden services in the Tor network and their role in ensuring anonymity. ● Explain Onion addresses, unique domain names ending in ".onion," and their function in protecting identities. ● Introduce the Hidden Wiki as a gateway to websites and services on the dark web. ● Discuss the content available on the Hidden Wiki and the associated risks, including links for malicious purposes. ● 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:** Tor Installation	● 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 the different layers of the internet and the tools for enhanced online privacy and security. 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