LESSON: IoT and ICS

Before you Begin

This is the third week of this course. Instructors should be keeping pace with the lesson timings below. 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 and upcoming lessons, 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 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, 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.

Summary

In this lesson, learners will explore the multifaceted realm of the Internet of Things (IoT), understanding how it's used in smart homes, industries, agriculture, and healthcare. The five layers of IoT will be highlighted, emphasizing their unique roles in the IoT ecosystem. The focus will shift to the Industrial Internet of Things (IIoT), covering its components, devices, and the specialized search engine Shodan for enhanced threat intelligence. The lesson will address IoT security challenges, common attack vectors, and best practices. Moving into industrial control systems (ICS), learners will understand how they

manage machinery and critical infrastructure, with insights into IoT's role in streamlining operations. Examples of ICS protocols will be introduced. The lesson will conclude with an exploration of firmware, covering its functions, obtaining methods, embedded file systems, and security risks associated with hard-coded secrets. Additionally, some commonly used analysis tools will be introduced.

Objectives

- Define the concept, usage, and architecture of the Internet of Things (IoT).
- Describe the applications, key features, and components of the Industrial Internet of Things (IIoT).
- Recognize Shodan's application as an IoT search engine.
- Recognize the importance of IoT security.
- Identify the OWASP IoT Top 10 vulnerabilities.
- Describe different types of IoT attacks and their mitigation strategies.
- Differentiate between IoT attacks and traditional IT attacks.
- List IoT security best practices.
- Define the concept, components, and applications of industrial control systems (ICS).
- Recognize the importance of ICS security in an IoT-integrated environment.
- Identify different types of ICS protocols and recognize their importance in cybersecurity.
- Define the concept of firmware.
- Explain where firmware resides and how to obtain it.
- List popular embedded file systems used to manage and extract data from firmware.
- Recognize the risks associated with hard-coded secrets.
- Explain the motivations behind firmware attacks.
- Identify commonly used firmware examination tools.

Lesson Activities and Teaching Strategies

Estimated Time	Lesson Portion	Directions
< 2 min	**Lesson Opener:** IoT and ICS	● Introduce learners to the importance of IoT and ICS in cybersecurity.
< 5 min	**Real World Scenario:** IoT and ICS	● 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:** Introduction to IoT	● Start the lesson by defining the Internet of Things (IoT) as a network of interconnected devices embedded with sensors, software, and technology. ● Discuss the range of devices covered by IoT, from simple household items to advanced industrial machinery. Emphasize the integration of technology into daily life and industry.

		● Highlight how IoT enhances efficiency and safety across various sectors, providing examples of its use in consumer applications, agriculture, and industrial operations. ● Emphasize the current scale of IoT by mentioning the over 14 billion devices currently connected and the expectation of exponential growth. ● Explore the application of IoT in various fields, such as smart home devices, industrial sensors, agricultural management, and healthcare wearables. ● Introduce the five-layer architecture of IoT, explaining each layer's role: Perception, transmission, middleware, application, and business. ● Introduce the Industrial Internet of Things (IIoT) as the industrial application of IoT and outline its components: Sensors and devices, connectivity, data analysis and processing, and user interface. ● Break down the components of an IIoT system, covering edge components, smart gateways, connectors, data processing, and user interface. ● Provide examples of IIoT devices, such as traffic lights, surveillance cameras, engine and machine sensors, and centrifuges. Discuss their role in automation. ● Explain Shodan as a specialized search engine that conducts online scans of IoT devices. ● Highlight its advanced filtering capabilities and mention its role in providing threat intelligence. ● 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:** Searching Shodan	● 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:** IoT Security	● Define IoT security as the practice of safeguarding connected devices and networks in the Internet of Things from cyberthreats. ● Explore the key aspects of IoT security, including device vulnerability management, data privacy, network security, device authentication, and compliance and updates. ● Discuss the factors that contribute to insufficient security, such as lack of developer awareness, narrow perspective, supply chain vulnerabilities, and the use of insecure frameworks. ● Introduce the OWASP and its list of the top 10 vulnerabilities in the IoT domain. Discuss each vulnerability briefly.

		● Define an IoT attack as a malicious attempt to exploit vulnerabilities in internet-connected devices. Explain the potential consequences of such attacks. ● Explore the different attack vectors, including device hardware, web attacks on the user interface, unencrypted communication, and firmware updates. ● Discuss common IoT attacks, such as man-in-the-middle attacks, denial-of-service attacks, and replay attacks, on authentication messages. ● Introduce mitigation strategies for IoT attacks, including implementing strong encryption, employing robust authentication protocols, network segmentation, and regular firmware and software updates. ● Highlight the differences between IoT attacks and traditional IT attacks, focusing on limited security features, device diversity, physical consequences, and legacy device vulnerability. ● Conclude the lesson by presenting IoT security best practices, emphasizing the importance of research, investment, a comprehensive security plan, network segmentation, proper device management, and regular removal of end-of-life devices. ● 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		
25 min	**Cyber Uncovered:** Industrial Control Systems (ICS)	● Begin by defining ICS and explaining its role in overseeing and regulating industrial machinery, combining hardware, software, and network components. ● Explore the components of ICS, including programmable logic controllers (PLCs), SCADA systems, distributed control systems (DCS), Human Machine Interfaces (HMIs), and industrial communication networks. ● Explain their functions. ● Discuss how IoT technology contributes to industrial optimization in both IIoT and ICS environments. ● Highlight applications such as remote asset monitoring and predictive maintenance. ● Emphasize the importance of security in the integration of ICS and IoT technology. ● Discuss the risks associated with interconnected systems and the need for a robust security posture. ● Explain the significance of ICS protocols in ensuring reliable communication in industrial environments. ● Discuss how they standardize data transmission and control actions for operational efficiency. ● Introduce key ICS protocols, including Modbus, DNP3, Profibus, Controller Area Network (CAN), and EtherNet/IP.

		● Highlight their applications in different industrial settings. ● Discuss the pivotal role of ICS protocols in securing industrial control systems, especially in IoT-integrated environments. ● Explain their contribution to data integrity, system functionality, robust security measures, and continuous monitoring. ● 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:** Firmware	● Define firmware as semi-permanent software residing on dedicated board flash memory that instructs devices on interactions with hardware and software. ● Emphasize the importance of firmware in ensuring stable and reliable interactions within industrial control systems (ICS). ● Discuss the diverse range of electronic devices where firmware resides, including routers, computers, washing machines, televisions, and many other electronic devices. ● Highlight the ubiquity of firmware in electronic devices and its role as an essential software component. ● Explore various methods of obtaining firmware, such as downloading from vendors, extracting from device memory, capturing over-the-air (OTA) updates, reverse engineering, and exploring alternative options like OpenWrt. ● Discuss the significance of obtaining firmware updates from official sources for security and reliability. ● Stress the importance of comprehensive information gathering for effective firmware analysis. Introduce the concept of entropy as an analysis tool for detecting compressed or encrypted firmware data and explain how understanding compression and encryption is crucial for assessing firmware integrity and security. ● Define embedded systems and their role in performing dedicated functions within larger systems. ● Explore commonly used embedded file systems like SquashFS, Cramfs, JFFS2, YAFFS2, and ext2, emphasizing their use in conjunction with firmware for data storage and retrieval. ● Explain the concept of hard-coded secrets and its potential risks, including long-term vulnerabilities. ● Provide examples of hard-coded secrets such as URLs, encryption algorithms, authentication mechanisms, access tokens, credentials, local pathnames, environment details, API, and encryption keys. ● Discuss the motivation behind firmware attacks, highlighting the advantages they provide in terms of privileges, persistence, and bypassing security controls. ● Explore the ways attackers can create a path to firmware, including software-down methods (exploiting lack of updates) and hardware-up methods (injecting malicious firmware via USB).

		● Introduce tools used for examining firmware, including dd, Hexdump, Strings, Binwalk, and QEMU. ● Explain how these tools contribute to the analysis and extraction of data from binary firmware images. ● 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:** Analyzing Firmware	● 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 the understanding of IoT vs IIoT, security challenges with IoT and updates to industrial control systems. 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