OBJECTIVES/COMPETENCIES

Course Objectives	Competencies
Overview of the threat landscape	Characterize the Red Team/Blue Team roles for the security team Characterize common threat actors Characterize security assessment types Descibe the legal and ethical compliance requirements Characterize the special threats related to IoT devices
Scanning and Enumeration	Use tools to scan for networks and servers Use tools to scan the network for IoT devices Use tools to enumerate the devices on a network Use Shodan to search for exposed IoT devices
Vulnerability and System Hacking	Characterize the Vulnerability Management Life Cycle Describe vulnerability scoring systems & assesment tools Perform reconnaissance using operating system tools Obtain credentials using tools Escalate privileges Configure account policies and account controls Describe the process to analyze IoT device firmware
Sniffing network traffic & session hijacking	Perform passive online attacks Conduct a man-in-the middle attack Perform active sniffing of network traffic Mac address spoofing Characterize the techniques to hijack a web page Examine hidden web form fields Identify weaknesses in IoT embedded web servers

Security issues with WiFi, Bluetooth, mobile devices, and cloud	Characterize common WiFi attacks and DOS techniques Characterize common cell network protocols and connection hijacking Discover and enumerate wireless devices Characterize the security concerns with mobile devices
Cryptography	Ensure file integrity Implement disk and local file encryption Characterize PKI and security certificates