LearnKey

Domain 1 Lesson Plan

Domain 1 - Threats, Attacks and Vulnerabilities [approximately 14 hours of videos, labs, and projects]				
Lesson	**Lesson Topic and Subtopics**	**Objectives**	**Exercise Labs**	**Workbook Projects and Files**
Pre-Assessment Assessment time - 00:30:00	Threats, Attacks, and Vulnerabilities: Pre-Assessment			
Lesson 1 Video time - 00:09:22 Exercise Lab time - 00:08:00 Workbook time - 00:25:00	**Threats, Attacks, and Vulnerabilities Part 1** Social Engineering Techniques Smishing and Vishing Spam Types Dumpster Diving and Shoulder Surfing Pharming	1.1 Compare and contrast different types of social engineering techniques 1.1.1 Phishing 1.1.2 Smishing 1.1.3 Vishing 1.1.4 Spam 1.1.5 Spam over internet messaging (SPIM) 1.1.6 Spear phishing 1.1.7 Dumpster diving 1.1.8 Shoulder surfing 1.1.9 Pharming 1.1.12 Whaling 1.1.13 Prepending	Phishing with a Mobile Device Phishing in Instant Messaging	Types of Phishing and Spam – pg. 10 N/A Dumpster Diving, Shoulder Surfing, and Pharming – pg. 11 N/A
Lesson 2 Video time - 00:09:50 Exercise Lab time - 00:04:00 Workbook time - 00:30:00	**Threats, Attacks, and Vulnerabilities Part 2** Tailgating and Eliciting Information Identity Fraud and Invoice Scams Credential Harvesting and Reconnaissance Hoax and Impersonation Watering Hole Attack Typosquatting Influence Campaigns Reasons for Effectiveness	1.1.10 Tailgating 1.1.11 Eliciting information 1.1.14 Identity fraud 1.1.15 Invoice scams 1.1.16 Credential harvesting 1.1.17 Reconnaissance 1.1.18 Hoax 1.1.19 Impersonation 1.1.20 Watering hole attack 1.1.21 Typosquatting 1.1.22 Influence campaigns 1.1.22.1 Hybrid warfare 1.1.22.2 Social media 1.1.23 Principles (reasons for effectiveness) 1.1.23.1 Authority 1.1.23.2 Intimidation 1.1.23.3 Consensus 1.1.23.4 Scarcity 1.1.23.5 Familiarity 1.1.23.6 Trust 1.1.23.7 Urgency	Accessing Usernames	Stealing Credentials or Identities – pg. 14 N/A Social Engineering Online – pg. 15 N/A Reasons for Effectiveness – pg. 16 N/A
Lesson 3 Video time - 00:10:29 Exercise Lab time - 00:12:00	**Analyze Potential Indicators to Determine Attack Type** Ransomware and Crypto Malware Trojans and Worms	1.2 Given a scenario, analyze potential indicators to determine the type of attack 1.2.1 Malware 1.2.1.1 Ransomware 1.2.1.2 Trojans 1.2.1.3 Worms	Avoid PUPs View Pop-Ups Settings App Authentication	Malware – pg. 19 N/A Malware Attacks – pg. 20 N/A

Domain 1 - Threats, Attacks and Vulnerabilities [approximately 14 hours of videos, labs, and projects]				
Lesson	**Lesson Topic and Subtopics**	**Objectives**	**Exercise Labs**	**Workbook Projects and Files**
Workbook time - 00:25:00	Potentially Unwanted Programs (PUPs) Fileless Virus Bots and Logic Bombs Spyware Keyloggers and Rootkit Backdoor	1.2.1.4 Potentially unwanted programs (PUPs) 1.2.1.5 Fileless virus 1.2.1.6 Command and control 1.2.1.7 Bots 1.2.1.8 Crypto malware 1.2.1.9 Logic bombs 1.2.1.10 Spyware 1.2.1.11 Keyloggers 1.2.1.12 Remote access Trojan (RAT) 1.2.1.13 Rootkit 1.2.1.14 Backdoor		
Lesson 4 Video time - 00:06:33 Exercise Lab time - 00:04:00 Workbook time - 00:20:00	**Password Attacks** Spraying Password Guesses Rainbow Tables Plaintext and Unencrypted **Physical Attacks** Malicious Universal Serial Bus (USB) Cable Malicious Flash Drive Card Cloning and Skimming	1.2.2.1 Spraying 1.2.2.2 Dictionary 1.2.2.3 Brute force 1.2.2.3.1 Offline 1.2.2.3.2 Online 1.2.2.4 Rainbow tables 1.2.2.5 Plaintext/unencrypted 1.2.3 Physical attacks 1.2.3.1 Malicious universal serial bus (USB) cable 1.2.3.2 Malicious flash drive 1.2.3.3 Card cloning 1.2.3.4 Skimming	Malicious USB Cables	Password Attacks – pg. 23 N/A Physical Attacks – pg. 24 N/A
Lesson 5 Video time - 00:05:14 Exercise Lab time - 00:00:00 Workbook time - 00:20:00	**Adversarial Artificial Intelligence (AI)** Machine Learning Supply-Chain Attacks Cloud-Based vs. On-Premises Attacks **Cryptographic Attacks** Birthday, Collision, and Downgrade	1.2.4 Adversarial artificial intelligence (AI) 1.2.4.1 Tainted training data for machine learning (ML) 1.2.4.2 Security of machine learning algorithms 1.2.5 Supply-chain attack 1.2.6 Cloud-based vs. on-premises attacks 1.2.7 Cryptographic attacks 1.2.7.1 Birthday 1.2.7.2 Collision 1.2.7.3 Downgrade		Adversarial AI – pg. 27 N/A Cryptographic Attacks – pg. 28 N/A
Lesson 6 Video time - 00:09:51 Exercise Lab time - 00:12:00 Workbook time - 00:25:00	**Application Attack Indicators Part 1** Privilege Escalation Cross-Site Scripting Structured Query Language (SQL) Dynamic Link Library (DLL) Lightweight Directory Access Protocol (LDAP) Extensible Markup Language (XML) Pointer Object Dereference	1.3 Given a scenario, analyze potential indicators associated with application attacks 1.3.1 Privilege escalation 1.3.2 Cross-site scripting 1.3.3 Injections 1.3.3.1 Structured query language (SQL) 1.3.3.2 Dynamic link library (DLL) 1.3.3.3 Lightweight directory access protocol (LDAP) 1.3.3.4 Extensible markup language (XML) 1.3.4 Pointer/object dereference 1.3.5 Directory traversal 1.3.6 Buffer overflows	Buffer Overflow Locking Database Records Windows Device Dependencies	Application Attack Indicators – pg. 31 N/A Injections and Other Attacks – pg. 32 N/A

Domain 1 - Threats, Attacks and Vulnerabilities [approximately 14 hours of videos, labs, and projects]				
Lesson	**Lesson Topic and Subtopics**	**Objectives**	**Exercise Labs**	**Workbook Projects and Files**
	Directory Traversal Buffer Overflows Race Conditions and TOCTTOU Error Handling	1.3.7 Race conditions 1.3.7.1 Time of check/time of use 1.3.8 Error handling		
Lesson 7 Video time - 00:10:34 Exercise Lab time - 00:00:00 Workbook time - 00:30:00	**Application Attack Indicators Part 2** Improper Input Handling Replay Attack and Session Replays Integer Overflow Request Forgeries and Server-Side Client-Side and Cross-Site API Attacks Resource Exhaustion Memory Leak SSL Striping Shimming and Refactoring Pass the Hash	1.3.9 Improper input handling 1.3.10 Replay attack 1.3.10.1 Session replays 1.3.11 Integer overflow 1.3.12 Request forgeries 1.3.12.1 Server-side 1.3.12.2 Client-side 1.3.12.3 Cross-site 1.3.13 Application programming interface (API) attacks 1.3.14 Resource exhaustion 1.3.15 Memory leak 1.3.16 Secure sockets layer (SSL) stripping 1.3.17 Driver manipulation 1.3.17.1 Shimming 1.3.17.2 Refactoring 1.3.18 Pass the hash		Replay Attacks and Other Vulnerabilities – pg. 35 N/A Attacks on Resources – pg. 36 N/A
Lesson 8 Video time - 00:09:27 Exercise Lab time - 00:04:00 Workbook time - 00:25:00	**Potential Indicators Associated with Network Attacks Part 1** Rogue WAPs Bluejacking and Bluesnarfing Disassociation Jamming Radio-Frequency Identification (RFID) Near Field Communication (NFC) Initialization Vector (IV) Man in the Middle Man in the Browser Layer 2 Attacks and ARP Poisoning Media Access Control (MAC) Flooding MAC Cloning	1.4 Given a scenario, analyze potential indicators associated with network attacks 1.4.1 Wireless 1.4.1.1 Evil twin 1.4.1.2 Rogue access point 1.4.1.3 Bluesnarfing 1.4.1.4 Bluejacking 1.4.1.5 Disassociation 1.4.1.6 Jamming 1.4.1.7 Radio-frequency identification (RFID) 1.4.1.8 Near field communication (NFC) 1.4.1.9 Initialization vector (IV) 1.4.2 Man in the middle 1.4.3 Man in the browser 1.4.4 Layer 2 attacks 1.4.4.1 Address resolution protocol (ARP) poisoning 1.4.4.2 Media access control (MAC) flooding 1.4.4.3 MAC cloning	Run ARP Code	Wireless Attacks – pg. 39 N/A Layer 2 Attacks – pg. 40 N/A
Lesson 9 Video time - 00:08:59 Exercise Lab time - 00:12:00	**Potential Indicators Associated with Network Attacks Part 2** Domain Hijacking DNS Poisoning URL Redirection	1.4.5 Domain name system (DNS) 1.4.5.1 Domain hijacking 1.4.5.2 DNS poisoning 1.4.5.3 Universal resource locator (URL) redirection 1.4.5.4 Domain reputation	View a Host File View Domain Reputation Word Macros	DNS and DDoS Attacks – pg. 43 N/A Malicious Code – pg. 44 N/A

Domain 1 - Threats, Attacks and Vulnerabilities [approximately 14 hours of videos, labs, and projects]				
Lesson	**Lesson Topic and Subtopics**	**Objectives**	**Exercise Labs**	**Workbook Projects and Files**
Workbook time - 00:30:00	Domain Reputation Distributed Denial of Service (DDoS) Malicious Code and PowerShell Python Bash Macros and VBA	1.4.6 Distributed denial of service (DDoS) 1.4.6.1 Network 1.4.6.2 Application 1.4.6.3 Operational technology (OT) 1.4.7 Malicious code or script execution 1.4.7.1 PowerShell 1.4.7.2 Python 1.4.7.3 Bash 1.4.7.4 Macros 1.4.7.5 Visual Basic for Applications (VBA)		
Lesson 10 Video time - 00:10:38 Exercise Lab time - 00:04:00 Workbook time - 00:40:00	**Threat Actors, Vectors, and Intelligence Sources Part 1** Actors, Threats, and APT Insider Threats State Actors and Criminal Syndicates Hacktivists Script Kiddies Hackers and Their Hats Shadow IT Competitors Actor Attributes Level of Sophistication and Capability Resources, Funding, Intent, and Motivation	1.5 Explain different threat actors, vectors, and intelligence sources 1.5.1 Actors and threats 1.5.1.1 Advanced persistent threat (APT) 1.5.1.2 Insider threats 1.5.1.3 State actors 1.5.1.4 Hacktivists 1.5.1.5 Script kiddies 1.5.1.6 Criminal syndicates 1.5.1.7 Hackers 1.5.1.7.1 White hat 1.5.1.7.2 Black hat 1.5.1.7.3 Gray hat 1.5.1.8 Shadow IT 1.5.1.9 Competitors 1.5.2 Attributes of actors 1.5.2.1 Internal/external 1.5.2.2 Level of sophistication/capability 1.5.2.3 Resources/funding 1.5.2.4 Intent/motivation	Internal Threats	Types of Threats – pg. 47 N/A Hackers and Threat Actors – pg. 48 N/A Actor Attributes – pg. 49 N/A
Lesson 11 Video time - 00:09:15 Exercise Lab time - 00:16:00 Workbook time - 00:30:00	**Threat Actors, Vectors, and Intelligence Sources Part 2** Vectors Threat Intelligence Sources and OSINT Closed and Proprietary Vulnerability Databases Dark Web Indicators of Compromise Automated Indicator Sharing (AIS), STIX, and TAXII Predictive Analysis Threat Maps, File and Code Repositories	1.5.3 Vectors 1.5.3.1 Direct access 1.5.3.2 Wireless 1.5.3.3 Email 1.5.3.4 Supply chain 1.5.3.5 Social media 1.5.3.6 Removable media 1.5.3.7 Cloud 1.5.4 Threat intelligence sources 1.5.4.1 Open-source intelligence (OSINT) 1.5.4.2 Closed/proprietary 1.5.4.3 Vulnerability databases 1.5.4.4 Public/private information 1.5.4.5 Dark web 1.5.4.6 Indicators of compromise 1.5.4.7 Automated indicator sharing (AIS) 1.5.4.7.1 Structured threat information exchange (STIX)/Trusted automated exchange of indicator information (TAXII) 1.5.4.8 Predictive analysis	Types of Vectors Vulnerability Database Abnormal Network Activity Analyzing Files for Malicious Code	Vectors – pg. 52 N/A Threat Intelligence Sources – pg. 53 N/A

Domain 1 - Threats, Attacks and Vulnerabilities [approximately 14 hours of videos, labs, and projects]				
Lesson	**Lesson Topic and Subtopics**	**Objectives**	**Exercise Labs**	**Workbook Projects and Files**
		1.5.4.9 Threat maps 1.5.4.10 File/code repositories		
Lesson 12 Video time - 00:05:06 Exercise Lab time - 00:08:00 Workbook time - 00:20:00	**Threat Actors, Vectors, and Intelligence Sources Part 3** Research Sources and Vendor Websites Vulnerability Feeds and Threat Feeds Conferences Academic Journals Request for Comments (RFC) Local Industry Groups and Social Media Adversary TTP	1.5.5 Research sources 1.5.5.1 Vendor websites 1.5.5.2 Vulnerability feeds 1.5.5.3 Conferences 1.5.5.4 Academic journals 1.5.5.5 Request for comments (RFC) 1.5.5.6 Local industry groups 1.5.5.7 Social media 1.5.5.8 Threat feeds 1.5.5.9 Adversary tactics, techniques, and procedures (TTP)	Resource Source Websites Evaluating Web Standards	Research Sources – pg. 56 N/A
Lesson 13 Video time - 00:13:43 Exercise Lab time - 00:12:00 Workbook time - 00:20:00	**Security Concerns Associated with Vulnerability Types Part 1** Cloud vs. On-Premises Vulnerabilities Zero-Day Attack Open Permissions Unsecure Root Account Errors Weak Encryption Unsecure Protocols Default Settings Open Ports and Services	1.6 Explain the security concerns associated with various types of vulnerabilities 1.6.1 Cloud-based vs. on-premises vulnerabilities 1.6.2 Zero-day 1.6.3 Weak configurations 1.6.3.1 Open permissions 1.6.3.2 Unsecured root accounts 1.6.3.3 Errors 1.6.3.4 Weak encryption 1.6.3.5 Unsecure protocols 1.6.3.6 Default settings 1.6.3.7 Open ports and services	Shared Responsibility Model Open Permissions Disabling a Service	Vulnerabilities and Weak Configurations – pg. 59 N/A
Lesson 14 Video time - 00:10:32 Exercise Lab time - 00:04:00 Workbook time - 00:30:00	**Security Concerns Associated with Vulnerability Types Part 2** Third-Party and Vendor Risks Supply Chain Outsourced Code Development Data Storage Patch Management and Firmware Updates Legacy Platforms Impacts, Data Loss, and Availability Loss Data Breaches and Financial Data Exfiltration	1.6.4 Third-party risks 1.6.4.1 Vendor management 1.6.4.1.1 System integration 1.6.4.1.2 Lack of vendor support 1.6.4.2 Supply chain 1.6.4.3 Outsourced code development 1.6.4.4 Data storage 1.6.5 Improper or weak patch management 1.6.5.1 Firmware 1.6.5.2 Operating system (OS) 1.6.5.3 Applications 1.6.6 Legacy platforms 1.6.7 Impacts 1.6.7.1 Data loss 1.6.7.2 Data breaches 1.6.7.3 Data exfiltration 1.6.7.4 Identity theft 1.6.7.5 Financial	Application Patches	Third-Party Risks – pg. 62 N/A Impacts – pg. 63 N/A

Domain 1 - Threats, Attacks and Vulnerabilities [approximately 14 hours of videos, labs, and projects]				
Lesson	**Lesson Topic and Subtopics**	**Objectives**	**Exercise Labs**	**Workbook Projects and Files**
	Identity Theft Reputation	1.6.7.6 Reputation 1.6.7.7 Availability loss		
Lesson 15 Video time - 00:12:12 Exercise Lab time - 00:12:00 Workbook time - 00:25:00	**Security Assessment Techniques Part 1** Threat Hunting and Intelligence Fusion Threat Feeds, Advisories, and Bulletins Maneuvering Vulnerability Scans and False Positives False Negatives Log Reviews Credentialed vs. Non-Credentialed Intrusive vs. Non-Intrusive Application and Web Application Network CVE and CVSS Configuration Review	1.7 Summarize the techniques used in security assessments 1.7.1 Threat hunting 1.7.1.1 Intelligence fusion 1.7.1.2 Threat feeds 1.7.1.3 Advisories and bulletins 1.7.1.4 Maneuvering 1.7.2 Vulnerability scans 1.7.2.1 False positives 1.7.2.2 False negatives 1.7.2.3 Log reviews 1.7.2.4 Credentialed vs. non-credentialed 1.7.2.5 Intrusive vs. non-intrusive 1.7.2.6 Application 1.7.2.7 Web application 1.7.2.8 Network 1.7.2.9 Common Vulnerabilities and Exposures (CVE)/Common Vulnerability Scoring System (CVSS) 1.7.2.10 Configuration review	High Vulnerabilities Reading MSBA Scans Interpreting Scans	Threat Hunting – pg. 66 N/A Vulnerability Scans – pg. 67 N/A
Lesson 16 Video time - 00:07:10 Exercise Lab time - 00:08:00 Workbook time - 00:20:00	**Security Assessment Techniques Part 2** SIEM Packet Capture Data Inputs and User Behavior Analysis Sentiment Analysis Security Monitoring Log Aggregation and Log Collectors SOAR	1.7.3 Syslog/Security information and event management (SIEM) 1.7.3.1 Review reports 1.7.3.2 Packet capture 1.7.3.3 Data inputs 1.7.3.4 User behavior analysis 1.7.3.5 Sentiment analysis 1.7.3.6 Security monitoring 1.7.3.7 Log aggregation 1.7.3.8 Log collectors 1.7.4 Security orchestration, amount, response (SOAR)	Utilizing Azure Sentinel Interpreting Feedback	Characteristics of SIEM – pg. 70 N/A
Lesson 17 Video time - 00:11:56 Exercise Lab time - 00:08:00 Workbook time - 00:35:00	**Penetration Testing Techniques** White Box, Black Box, and Gray Box Rules of Engagement Lateral Movement Privilege Escalation and Boxes Persistence and Cleanup Bug Bounty Pivoting Reconnaissance and Drones War Flying and War Driving	1.8 Explain the techniques used in penetration testing 1.8.1 Penetration testing 1.8.1.1 White box 1.8.1.2 Black box 1.8.1.3 Gray box 1.8.1.4 Rules of engagement 1.8.1.5 Lateral movement 1.8.1.6 Privilege escalation 1.8.1.7 Persistence 1.8.1.8 Cleanup 1.8.1.9 Bug bounty 1.8.1.10 Pivoting 1.8.2 Passive and active reconnaissance 1.8.2.1 Drones/unmanned aerial vehicle	Bug Bounty Vulnerabilities OSINT Framework	Penetration Testing Tools – pg. 73 N/A Reconnaissance Tools – pg. 74 N/A

Domain 1 - Threats, Attacks and Vulnerabilities [approximately 14 hours of videos, labs, and projects]				
Lesson	**Lesson Topic and Subtopics**	**Objectives**	**Exercise Labs**	**Workbook Projects and Files**
	Footprinting OSINT Exercise Types	(UAV) 1.8.2.2 War flying 1.8.2.3 War driving 1.8.2.4 Footprinting 1.8.2.5 OSINT 1.8.3 Exercise types 1.8.3.1 Red team 1.8.3.2 Blue team 1.8.3.3 White team 1.8.3.4 Purple team		
Post-Assessment Assessment time - 01:00:00	Threats, Attacks and Vulnerabilities: Post-Assessment			