Cybersecurity Training Course

Time:
Written Content—15:04 hrs
Videos—3:12 hrs
Quizzes—5:50 hrs (will be updated within the outline)
Labs—25:00 hrs (lab time is based off an average estimate)
Estimated Completion Time—50:00 hrs

Outline:

I. Course Introduction
   A. Intro Video (Video – 5:47)
   B. Getting Started
   C. About the Course
   D. Course Outcomes
   E. Using Practice Labs (Video – 5:14)

II. Module 1 – Threat Appraisal and Management
   A. Cybersecurity Analysts
      i. Cybersecurity Analysts (Video – 9:40)
      ii. Responsibilities and Functions of a Cybersecurity Analyst
      iii. Basis of an Effective Information Security Approach
      iv. Fundamentals of Risk Evaluation
   B. Security Policy
      i. The Basis of Security Policy
      ii. Password and Account Management Policies
      iii. Acceptable Use Policy
      iv. Data Classification Policies
      v. Data Ownership Policies
      vi. Data Retention Policies
      vii. Classification of Security Measures
C. Frameworks
   i. NIST
   ii. ISO/IEC 27001
   iii. COBIT
   iv. SABSA
   v. TOGAF
   vi. ITIL

CI. Information Security Practices
   i. Information Security Practices (Video – 5:22)

E. Risk Assessment
   i. Two Types of Analysis
      1. Quantitative Analysis
      2. Qualitative Analysis
   ii. Technical Control View
   iii. Operational Control View
   iv. Technical Impact and Likelihood

F. Environmental Reconnaissance Techniques
   i. Environmental Reconnaissance Techniques (Video – 7:25)
   ii. Procedures/Common Tasks
      1. Topology Discovery
      2. OS Fingerprinting
         a. Passive OS Fingerprinting
         b. Active OS Fingerprinting
      3. Service Discovery
      4. Packet Capture
      5. Log Review
      6. Router/Firewall ACLs Review
      7. Email Harvesting
      8. Social Media Profiling
      9. Social Engineering
     10. DNS Harvesting (Video – 9:52)
     11. Phishing
   iii. Variables
      1. Wired vs. Wireless
      2. Virtual vs. Physical
      3. Internal vs. External
      4. Cloud vs. On-premise (Video – 8:09)
   iv. Tools
      1. Nmap
      2. Host Scanning
      3. Network Mapping
      4. NETSTAT
      5. Packet Analyzer
      6. IDS/IPS
      7. HIDS/NIDS
      8. Firewall Rule-based and Logs
      9. Syslog
      10. Vulnerability Scanner

Social Engineering Reconnaissance (Lab – 60:00)
III. Module 2 – Threat Management

A. Security Practices
   i. Threat Management (Video – 9:40)
   ii. Penetration Testing
   iii. Rules of Engagement
      1. Timing
      2. Scope
      3. Authorization
      4. Exploitation
      5. Communication
      6. Reporting
   iv. Reverse Engineering (Video – 8:17)
   v. Sandboxing/Isolation
   vi. Hardware
   vii. Software/Malware
   viii. Fingerprinting/Hashing
   ix. Decomposition
   x. Training and Exercises

B. Data Analysis (Video – 5:36)
   i. Point-In-Time-Analysis
      1. Packet Analysis
      2. Protocol Analysis
      3. Traffic Analysis
      4. Netflow Analysis
      5. Wireless Analysis
   ii. Data Correlation and Analytics
      1. Anomaly Analysis
      2. Availability Analysis
      3. Trend Analysis
      4. Heuristic Analysis
      5. Behavioral Analysis
   iii. Data Output (Video – 7:5)
      1. Firewall Logs
      2. Packet Capture
      3. Event Logs
      4. Syslogs
      5. IDS Report
   iv. Tools
      1. SIEM
      2. Packet Analyzer/Packet Sniffer
      3. IDS
      4. Resource Monitoring Tool
      5. Netflow Analyzer

Topology Discovery Part 1 (Lab – 60:00)
Topology Discovery Part 2 (Lab – 60:00)
DNS Harvesting (60:00)
Alienvault Monitoring – SIEM and NetFlow (Lab – 60:00)

v. Network Segmentation
   1. Implementing a Countermeasure (Video – 13:23)
   2. System Isolation
   3. Jump Box

vi. Honeypot

vii. Endpoint Security

viii. Group Policy
      1. ACLs
      2. Sinkhole
ix. Hardening Authentication
   1. Mandatory Access Control (MAC)
   2. Compensating Controls
   3. Blocking Unused Ports/Services
   4. Patching
   5. Network Access Control (NAC)
IPv4 Access Lists for Traffic Filtering (Lab – 60:00) Configure Verify and Troubleshoot Port Security (Lab – 60:00)

IV. Module 3 – Vulnerability Management (Video – 4:57)
   A. Implementing a Vulnerability Management Process
      i. Identification of Requirements
         1. Regulatory Environments
         2. Corporate Policy
         3. Data Classification (Video – 3:54)
         4. Asset Inventory
      ii. Establish Scanning Frequencies (Video – 5:57)
         1. Risk Appetite
         2. Regulatory Requirements
         3. Technical Constraints
         4. Workflow
      iii. Configure Tools to Perform Scans According to Specification
         1. Determining Scanning Criteria
         2. Tool Updates/Plug-ins
         3. Permissions and Access
      iv. Execute Scanning (Video – 6:23)
      v. Generate Reports
         1. Automated
      vi. Remediation
         1. Prioritizing
         2. Communication/Change Control
         3. Sandboxing/Testing
         4. Inhibitors to Remediation
      vii. Ongoing Scanning and Continuous Monitoring
   B. Output Analysis (Video – 4:04)
      i. Analyze Reports from a Vulnerability Scan
      ii. Validate Results and Correlate Other Data Points
Alienvault Monitoring – Threats, Vulnerabilities, and Reporting (Lab – 60:00)

V. Module 4 – Vulnerability Mitigation and Incident Response
   A. Common Vulnerabilities (Video – 6:28)
      i. Host Infrastructure
         1. Servers
         2. Endpoints, Including Mobile Devices
         3. SCADA Devices and Industrial Control Systems (ICSs)
      ii. Network Infrastructure
         1. Network Appliances
         2. Physical Infrastructure
         3. Interconnected Networks
         4. Virtual Private Networks (VPNs)
      iii. Virtual Infrastructure
         1. Virtual Hosts
         2. Virtual Networks
         3. Management Interface
Vulnerability Scanner MBSA (Lab – 60:00)

Configure Verify and Troubleshoot GRE Tunnel Connectivity (Lab – 60:00)

B. Incident Impact and Investigation (Video – 5:18)
   i. Threat Classification
      1. Known Threats vs. Unknown Threats
      2. Zero-day
      3. Advanced Persistent Threat (ATP)
   ii. Factors Contributing to Incident Severity and Prioritization
      1. Incident Severity and Recovery (Video – 7:49)
      2. Scope of Impact
      3. Types of Data

Packet Sniffing (Lab – 60:00)
   iii. Forensics Kit
      1. Documentation (Video – 2:05)
      2. Digital Forensics Workstation
      3. Write Blockers
      4. Cables
      5. Drive Adapters
      6. Wiped Removable Media
      7. Cameras
      8. Crime Tape
      9. Tamper-Proof Seals
     10. Documentation/Forms
   iv. Forensic Investigation Suite (Video – 5:26)
      1. Hashing Utilities
      2. Imaging Utilities
      3. Analysis Utilities
      4. Chain of Custody
      5. OS and Process Analysis
      6. Mobile Device Forensics
      7. Password Crackers
      8. Cryptography Tools
      9. Log Viewer
     10. Registry Viewer
     11. Application Viewer
     12. USB Viewer
     13. User Account Viewer

Vulnerability Scanner Nessus (Lab – 60:00)
VI. Module 5 – Incident Response and Security Procedures (Video – 5:15)

A. Incident Communication Management and Symptom Analysis
   i. Communication
   ii. Stakeholders
      1. HR
      2. Legal
      3. Marketing
      4. Management
   iii. Purpose of Communication Processes
      1. Limit Communication to Trusted Parties
      2. Disclosure
         a. Regulatory Requirements
         b. Legislative Requirements
      3. Prevent Inadvertent Release of Information
      4. Secure Method of Communication
   iv. Role-Based Responsibilities
      1. Technical
      2. Management
      3. Law Enforcement
      4. Public Relations
      5. Retain Incident Response Provider
   v. Common Network-Related Symptoms (Video – 5:08)
      1. Bandwidth Consumption
      2. Beaconing
      3. Irregular Peer-to-Peer Communication
      4. Rogue Devices on the Network
      5. Scan Sweeps
      6. Unusual Traffic Spikes
   vi. Common Host-Related Symptoms
      1. Process Consumption
      2. Memory Consumption
      3. Drive Capacity Consumption
      4. Unauthorized Software
      5. Malicious Processes (Video – 4:35)
      6. Unauthorized Changes and Privileges
      7. Data Exfiltration
   vii. Common Application-Related Symptoms
      1. Anomalous Activity
      2. Introduction of New Accounts
      3. Unexpected Output
      4. Service Interruption
      5. Memory Overflows

B. Incident Remediation and Security Procedures (Video – 5:53)
   i. Containment Techniques
      1. Segmentation
      2. Isolation
      3. Removal
      4. Reverse Engineering
   ii. Eradication Techniques
      1. Reconstruction/Reimage
      2. Sanitization
      3. Secure Disposal
   iii. Validation
      1. Patching
      2. Permissions
      3. Scanning
      4. Verify Logging/Communication to Security Monitoring
iv. Corrective Actions
   1. Lessons Learned Report
   2. Change Control Process
   3. Update Incident Response Plan

v. Incident Summary Report

Implement IOS Features to Mitigate Threats (Lab – 60:00)

vi. Procedures
   1. Continuous Monitoring
   2. Evidence Production
   3. Patching
   4. Compensating Control Development
   5. Control Testing Procedures
   6. Manage Exceptions
   7. Remediation Plans

vii. Verifications and Quality Control
   1. Audits
   2. Evaluations
   3. Assessments
   4. Maturity Model
   5. Certification

VII. Module 6 – Security Architecture

A. Identify and Access Management and Compensating Controls
   i. Types of Security Issues (Video – 4:40)
   ii. Security Issues Associated with Context-Based Authentication
       1. Time
       2. Location
       3. Frequency
       4. Behavioral
   iii. Security Issues Associated with Identities
       1. Personnel
       2. Endpoints and Servers
       3. Services and Applications
       4. Roles
   iv. Security Issues Associated with Identity Repositories
       1. Directory Services
       2. Authentication, Authorization, Auditing (AAA) Services
   v. Security Issues Associated with Federation and Single Sign-On
       1. Federation and Single Sign-On Authentication (Video – 5:20)
       3. Self-Service Password Reset
   vi. Exploits
       1. Impersonation
       2. Man-in-the-Middle
       3. Session Hijack
       4. Cross-site Scripting
       5. Privilege Escalation
       6. Rootkit
Compliance Patching (Lab – 60:00)

Forensics – Email and Social Media Investigation (Lab – 60:00)

Understanding Digital Forensics Profession and Investigations (Lab – 60:00)

vii. Security Data Analytics
   1. Security Architecture and Compensating Controls (Video – 4:13)
   2. Data Aggregation
   3. Trend Analysis
   4. Historical Analysis

viii. Manual Review
   1. Firewall Logs
   2. Syslog
   3. Defense in Depth

ix. Personnel
   1. Personnel Security Strategy (Video – 4:52)
   2. Training
   3. Dual Control
   4. Separation of Duties
   5. Third Party/Consultants
   6. Cross Training
   7. Mandatory Vacation
   8. Succession Planning

x. Processes
   1. Continual Improvement
   2. Scheduled Reviews
   3. Retirement of Processes

xi. Technologies
   1. Automated Reporting
   2. Security Appliances
   3. Security Suites
   4. Outsourcing
   5. Security as a Service
   6. Cryptography

xii. Other Security Concepts/Network Design

Passive Topology Discovery (Lab – 60:00)

Monitoring Servers (Lab – 60:00)

Securing the Management Plane on Cisco Routers (Lab – 60:00)
B. Application Security Best Practices and Cybersecurity Tools
   ii. Best Practices During Software Development
       1. Security Requirements Definition
       2. Security Testing Phases
       3. Manual Peer Reviews
       4. User Acceptance Testing
       5. Stress Test Application
       7. Input Validation
   iii. Secure Coding Best Practices
       1. OWASP
       2. SANS
       3. Center for Internet Security
       DVWA – Manual SQL Injection and Password Cracking (Lab – 60:00)
   iv. Preventative
       1. IPS
       2. HIPS
       3. Firewall
       4. Antivirus or Anti-malware
       5. EMET
       6. Web Proxy
       7. Web Application Firewall (WAF)
   v. Collective
       1. SIEM Tools
       2. Network Scanning (NMAP)
       3. Vulnerability Scanning
   vi. Packet Capture
       1. Command Line/IP Utilities
       2. IDS/HIDS
   vii. Analytical
       1. Monitoring Tools
       2. Interception Proxy
       3. Exploit Framework
       4. Fuzzers
   viii. Forensics
       1. Forensic Suites
       2. Hashing
       3. Password Cracking
       4. Imaging

Windows Command Line Tools (Lab – 60:00)
Encryption and Hashing (Lab – 60:00)
Introduction to Syslog (Lab – 60:00)
Implement SSL VPN using ASA Device Manager (Lab – 60:00)
Implement the Cisco Adaptive Security Appliance (Lab – 60:00)