17.2 - Enterprise Services
- **17.2.1 - HTTP and HTTPSContains: *Text***
- **17.2.2 - Common HTTP ExploitsContains: *Text***
- **17.2.3 - EmailContains: *Text***
- **17.2.4 - Web-Exposed DatabasesContains: *Text***
- **17.2.5 - Client-side ScriptingContains: *Text***
- **17.2.6 - Lab - Attacking a MySQL DatabaseContains: *Text, Labs***
- **17.2.7 - Lab - Reading Server LogsContains: *Text, Labs***
- **17.2.8 - Check Your Understanding – Network Services AttacksContains: *Check Your Understandings***

17.3 - Attacking What We Do Summary
- **17.3.1 - What Did I Learn in this Module?Contains: *Text***
- **17.3.2 - Module 17: Attacking What We Do QuizContains: *Module Quiz***

18 - Understanding Defense

18.0 - Introduction
- **18.0.1 - Why Should I Take this Module?Contains: *Text***
- **18.0.2 - What Will I Learn in this Module?Contains: *Text***

18.1 - Defense-in-Depth
- **18.1.1 - Assets, Vulnerabilities, ThreatsContains: *Text***
- **18.1.2 - Identify AssetsContains: *Text***
- **18.1.3 - Identify VulnerabilitiesContains: *Text***
- **18.1.4 - Identify ThreatsContains: *Text***
- **18.1.5 - The Security Onion and The Security ArtichokeContains: *Text***

18.2 - Security Policies, Regulations, and Standards
- **18.2.1 - Business PoliciesContains: *Text***
- **18.2.2 - Security PolicyContains: *Text***
- **18.2.3 - BYOD PoliciesContains: *Text***
- **18.2.4 - Regulatory and Standards ComplianceContains: *Text***

18.3 - Understanding Defense Summary
- **18.3.1 - What Did I Learn in this Module?Contains: *Text***
- **18.3.2 - Module 18: Understanding Defense QuizContains: *Module Quiz***

19 - Access Control

19.0 - Introduction
- **19.0.1 - Why Should I Take this Module?Contains: *Text***
- **19.0.2 - What Will I Learn in this Module?Contains: *Text***

19.1 - Access Control Concepts
- **19.1.1 - Communications Security: CIAContains: *Text***
- **19.1.2 - Zero Trust SecurityContains: *Text***
- **19.1.3 - Access Control ModelsContains: *Text***
- **19.1.4 - Check Your Understanding - Identify the Access Control ModelContains: *Check Your Understandings***

19.2 - AAA Usage and Operation
- **19.2.1 - AAA OperationContains: *Text***
- **19.2.2 - AAA AuthenticationContains: *Text***
- **19.2.3 - AAA Accounting LogsContains: *Text***
- **19.2.4 - Check Your Understanding - Identify the Characteristic of AAAContains: *Interactive Activities***

19.3 - Access Control Summary

23 - Endpoint Vulnerability Assessment
23.0 - Introduction
- **23.0.1 - Why Should I Take this Module?Contains: *Text***
- **23.0.2 - What Will I Learn in this Module?Contains: *Text***

23.1 - Network and Server Profiling
- **23.1.1 - Network ProfilingContains: *Text***
- **23.1.2 - Server ProfilingContains: *Text***
- **23.1.3 - Network Anomaly DetectionContains: *Text***
- **23.1.4 - Network Vulnerability TestingContains: *Text***
- **23.1.5 - Check Your Understanding - Identify the Elements of Network ProfilingContains: *Check Your Understandings***

23.2 - Common Vulnerability Scoring System (CVSS)
- **23.2.1 - CVSS OverviewContains: *Text***
- **23.2.2 - CVSS Metric GroupsContains: *Text***
- **23.2.3 - CVSS Base Metric GroupContains: *Text***
- **23.2.4 - The CVSS ProcessContains: *Text***
- **23.2.5 - CVSS ReportsContains: *Text***
- **23.2.6 - Other Vulnerability Information SourcesContains: *Text***
- **23.2.7 - Check Your Understanding - Identify CVSS MetricsContains: *Check Your Understandings***

23.3 - Secure Device Management
- **23.3.1 - Risk ManagementContains: *Text***
- **23.3.2 - Check Your Understanding - Identify the Risk ResponseContains: *Check Your Understandings***
- **23.3.3 - Vulnerability ManagementContains: *Text***
- **23.3.4 - Asset ManagementContains: *Text***
- **23.3.5 - Mobile Device ManagementContains: *Text***
- **23.3.6 - Configuration ManagementContains: *Text***
- **23.3.7 - Enterprise Patch ManagementContains: *Text***
- **23.3.9 - Check Your Understanding - Identify Device Management ActivitiesContains: *Check Your Understandings***

23.4 - Information Security Management Systems
- **23.4.1 - Security Management SystemsContains: *Text***
- **23.4.2 - ISO-27001Contains: *Text***
- **23.4.3 - NIST Cybersecurity FrameworkContains: *Text***
- **23.4.4 - Check Your Understanding - Identify the Stages in the NIST Cybersecurity FrameworkContains: *Check Your Understandings***

23.5 - Endpoint Vulnerability Assessment Summary
- **23.5.1 - What Did I Learn in this Module?Contains: *Text***
- **23.5.2 - Module 23 - Endpoint Vulnerability QuizContains: *Text, Module Quiz***

24 - Technologies and Protocols
24.0 - Introduction
- **24.0.1 - Why Should I Take this Module?Contains: *Text***
- **24.0.2 - What Will I Learn in this Module?Contains: *Text***

24.1 - Monitoring Common Protocols
- **24.1.1 - Syslog and NTPContains: *Text***
- **24.1.2 - NTPContains: *Text***
- **24.1.3 - DNSContains: *Text***
- **24.1.4 - HTTP and HTTPSContains: *Text***

25.4 - Network Security Data Summary
- **25.4.1 - What Did I Learn in this Module?Contains: *Text***
- **25.4.2 - Module 25: Network Security Data QuizContains: *Module Quiz***

26 - Evaluating Alerts
26.0 - Introduction
- **26.0.1 - Why Should I Take this Module?Contains: *Text***
- **26.0.2 - What Will I Learn in this Module?Contains: *Text***

26.1 - Sources of Alerts
- **26.1.1 - Security OnionContains: *Text***
- **26.1.2 - Detection Tools for Collecting Alert DataContains: *Text***
- **26.1.3 - Analysis ToolsContains: *Text***
- **26.1.4 - Alert GenerationContains: *Text***
- **26.1.5 - Rules and AlertsContains: *Text***
- **26.1.6 - Snort Rule StructureContains: *Text***
- **26.1.7 - Lab - Snort and Firewall RulesContains: *Text, Labs***

26.2 - Overview of Alert Evaluation
- **26.2.1 - The Need for Alert EvaluationContains: *Text***
- **26.2.2 - Evaluating AlertsContains: *Text***
- **26.2.3 - Deterministic Analysis and Probabilistic AnalysisContains: *Text***
- **26.2.4 - Check your Understanding -- Identify Deterministic and Probabilistic ScenariosContains: *Interactive Activities***
- **26.2.5 - Check Your Understanding - Identify the Alert ClassificationContains: *Check Your Understandings***

26.3 - Evaluating Alerts Summary
- **26.3.1 - What did I learn in this module?Contains: *Text***
- **26.3.2 - Module 26: Evaluating Alerts QuizContains: *Module Quiz***

27 - Working with Network Security Data
27.0 - Introduction
- **27.0.1 - Why Should I Take this Module?Contains: *Text***
- **27.0.2 - What Will I Learn in this Module?Contains: *Text***

27.1 - A Common Data Platform
- **27.1.1 - ELKContains: *Text***
- **27.1.2 - Data ReductionContains: *Text***
- **27.1.3 - Data NormalizationContains: *Text***
- **27.1.4 - Data ArchivingContains: *Text***
- **27.1.5 - Lab - Convert Data into a Universal FormatContains: *Text, Labs***

27.2 - Investigating Network Data
- **27.2.1 - Working in SguilContains: *Text***
- **27.2.2 - Sguil QueriesContains: *Text***
- **27.2.3 - Pivoting from SguilContains: *Text***
- **27.2.4 - Event Handling in SguilContains: *Text***
- **27.2.5 - Working in ELKContains: *Text***
- **27.2.6 - Queries in ELKContains: *Text***
- **27.2.7 - Investigating Process or API CallsContains: *Text***
- **27.2.8 - Investigating File DetailsContains: *Text***
- **27.2.9 - Lab – Regular Expression TutorialContains: *Text, Labs***
- **27.2.10 - Lab - Extract an Executable from a PCAPContains: *Text, Labs***

28.4 - Incident Response

- **28.4.1 - Establishing an Incident Response CapabilityContains: *Text***
- **28.4.2 - Check Your Understanding - Identify the Incident Response Plan ElementsContains: *Check Your Understandings***
- **28.4.3 - Incident Response StakeholdersContains: *Text***
- **28.4.4 - NIST Incident Response Life CycleContains: *Text***
- **28.4.5 - PreparationContains: *Text***
- **28.4.6 - Detection and AnalysisContains: *Text***
- **28.4.7 - Containment, Eradication, and RecoveryContains: *Text***
- **28.4.8 - Post-Incident ActivitiesContains: *Text***
- **28.4.9 - Incident Data Collection and RetentionContains: *Text***
- **28.4.10 - Reporting Requirements and Information SharingContains: *Text***
- **28.4.11 - Check Your Understanding - Identify the Incident Handling TermContains: *Check Your Understandings***
- **28.4.12 - Lab - Incident HandlingContains: *Text, Labs***

28.5 - Digital Forensics and Incident Analysis and Response Summary

- **28.5.1 - What Did I Learn in this Module?Contains: *Text***
- **28.5.2 - Module 26: Evaluating Alerts QuizContains: *Module Quiz***

28.6 - Prepare for Your Exam and Launch Your Career!

- **28.6.1 - Certification Preparation and Discount VouchersContains: *Text***
- **28.6.2 - Career Resources and Employment OpportunitiesContains: *Text***