

1 - The Danger

1.1 - Introduction

- 1.0.1 - First Time in This Course**Contains: *Text*
- 1.0.2 - Student Resources**Contains: *Text*
- 1.0.3 - Ethical Hacking Statement**Contains: *Text*
- 1.0.4 - Why Should I Take this Module?**Contains: *Text*
- 1.0.5 - What Will I Learn in this Module?**Contains: *Text*
- 1.0.6 - Class Activity - Top Hacker Shows Us How It's Done**Contains: *Text, Labs*

1.1 - War Stories

- 1.1.1 - Hijacked People**Contains: *Text*
- 1.1.2 - Ransomed Companies**Contains: *Text*
- 1.1.3 - Targeted Nations**Contains: *Text*
- 1.1.4 - Video - Anatomy of an Attack**Contains: *Text, Videos*
- 1.1.5 - Lab - Installing the Virtual Machines**Contains: *Text, Labs*
- 1.1.6 - Lab - Cybersecurity Case Studies**Contains: *Text, Labs*

1.2 - Threat Actors

- 1.2.1 - Threat Actors**Contains: *Text*
- 1.2.2 - How Secure is the Internet of Things?**Contains: *Text*
- 1.2.3 - Lab - Learning the Details of Attacks**Contains: *Text, Labs*

1.3 - Threat Impact

- 1.3.1 - PII, PHI, and PSIC**Contains: *Text*
- 1.3.2 - Lost Competitive Advantage**Contains: *Text*
- 1.3.3 - Politics and National Security**Contains: *Text*
- 1.3.4 - Lab - Visualizing the Black Hats**Contains: *Text, Labs*

1.4 - The Danger Summary

- 1.4.1 - What Did I Learn in this Module?**Contains: *Text*
- 1.4.2 - Module 1: The Danger Quiz**Contains: *Module Quiz*

2 - Fighters in the War Against Cybercrime

2.0 - Introduction

- 2.0.1 - Why Should I Take this Module?**Contains: *Text*
- 2.0.2 - What Will I Learn in this Module?**Contains: *Text*

2.1 - The Modern Security Operations Center

- 2.1.1 - Elements of a SOCC**Contains: *Text*
- 2.1.2 - People in the SOCC**Contains: *Text*
- 2.1.3 - Process in the SOCC**Contains: *Text*
- 2.1.4 - Technologies in the SOC: SIEM**Contains: *Text*
- 2.1.5 - Technologies in the SOC: SOAR**Contains: *Text*
- 2.1.6 - SOC Metrics**Contains: *Text*
- 2.1.7 - Enterprise and Managed Security**Contains: *Text*
- 2.1.8 - Security vs. Availability**Contains: *Text*
- 2.1.9 - Check Your Understanding – Identify the SOC Terminology**Contains: *Check Your Understandings*

2.2 - Becoming a Defender

- 2.2.1 - Certifications**Contains: *Text*
- 2.2.2 - Further Education**Contains: *Text*
- 2.2.3 - Sources of Career Information**Contains: *Text*
- 2.2.4 - Getting Experience**Contains: *Text*
- 2.2.5 - Lab – Becoming a Defender**Contains: *Text, Labs*

2.3 - Fighters in the War Against Cybercrime Summary

2.3.1 - What Did I Learn in this Module?Contains: *Text*

2.3.2 - Module 2: Fighters in the War Against Cybercrime QuizContains: *Module Quiz*

3 - The Windows Operating System

3.0 - Introduction

3.0.1 - Why Should I Take this Module?Contains: *Text*

3.0.2 - What Will I Learn in This Module?Contains: *Text*

3.0.3 - Class Activity - Identify Running ProcessesContains: *Text, Labs*

3.1 - Windows History

3.1.1 - Disk Operating SystemContains: *Text*

3.1.2 - Windows VersionsContains: *Text*

3.1.3 - Windows GUIContains: *Text*

3.1.4 - Operating System VulnerabilitiesContains: *Text*

3.2 - Windows Architecture and Operations

3.2.1 - Hardware Abstraction LayerContains: *Text*

3.2.2 - User Mode and Kernel ModeContains: *Text*

3.2.3 - Windows File SystemsContains: *Text*

3.2.4 - Alternate Data StreamsContains: *Text*

3.2.5 - Windows Boot ProcessContains: *Text*

3.2.6 - Windows StartupContains: *Text*

3.2.7 - Windows ShutdownContains: *Text*

3.2.8 - Processes, Threads, and ServicesContains: *Text*

3.2.9 - Memory Allocation and HandlesContains: *Text*

3.2.10 - The Windows RegistryContains: *Text*

3.2.11 - Lab - Exploring Processes, Threads, Handles, and Windows RegistryContains: *Text, Labs*

3.2.12 - Check Your Understanding - Identify the Windows Registry HiveContains: *Check Your Understandings*

3.3 - Windows Configuration and Monitoring

3.3.1 - Run as AdministratorContains: *Text*

3.3.2 - Local Users and DomainsContains: *Text*

3.3.3 - CLI and PowerShellContains: *Text*

3.3.4 - Windows Management InstrumentationContains: *Text*

3.3.5 - The net CommandContains: *Text*

3.3.6 - Task Manager and Resource MonitorContains: *Text*

3.3.7 - NetworkingContains: *Text*

3.3.8 - Accessing Network ResourcesContains: *Text*

3.3.9 - Windows ServerContains: *Text*

3.3.10 - Lab - Create User AccountsContains: *Text, Labs*

3.3.11 - Lab - Using Windows PowerShellContains: *Text, Labs*

3.3.12 - Lab - Windows Task ManagerContains: *Text, Labs*

3.3.13 - Lab - Monitor and Manage System Resources in WindowsContains: *Text, Labs*

3.4 - Windows Security

3.4.1 - The netstat CommandContains: *Text*

3.4.2 - Event ViewerContains: *Text*

3.4.3 - Windows Update ManagementContains: *Text*

3.4.4 - Local Security PolicyContains: *Text*

- 3.4.5 - Windows Defender Contains: *Text*
- 3.4.6 - Windows Defender Firewall Contains: *Text*
- 3.4.7 - Check Your Understanding - Identify the Windows Tool Contains: *Module Quiz*
- 3.5 - The Windows Operating System Summary
 - 3.5.1 - What Did I Learn in this Module? Contains: *Text*
 - 3.5.2 - Module 3: The Windows Operating System Quiz Contains: *Module Quiz*
- 4 - Linux Overview
 - 4.0 - Introduction
 - 4.0.1 - Why Should I Take this Module? Contains: *Text*
 - 4.0.2 - What Will I Learn in this Module? Contains: *Text*
 - 4.1 - Linux Basics
 - 4.1.1 - What is Linux? Contains: *Text*
 - 4.1.2 - The Value of Linux Contains: *Text*
 - 4.1.3 - Linux in the SOCC Contains: *Text*
 - 4.1.4 - Linux Tools Contains: *Text*
 - 4.2 - Working in the Linux Shell
 - 4.2.1 - The Linux Shell Contains: *Text*
 - 4.2.2 - Basic Commands Contains: *Text*
 - 4.2.3 - File and Directory Commands Contains: *Text*
 - 4.2.4 - Working with Text Files Contains: *Text*
 - 4.2.5 - The Importance of Text Files in Linux Contains: *Text*
 - 4.2.6 - Lab – Working with Text Files in the CLI Contains: *Text, Labs*
 - 4.2.7 - Lab – Getting Familiar with the Linux Shell Contains: *Text, Labs*
 - 4.3 - Linux Servers and Clients
 - 4.3.1 - An Introduction to Client-Server Communications Contains: *Text*
 - 4.3.2 - Servers, Services, and Their Ports Contains: *Text*
 - 4.3.3 - Clients Contains: *Text*
 - 4.3.4 - Lab - Linux Servers Contains: *Text, Labs*
 - 4.4 - Basic Server Administration
 - 4.4.1 - Service Configuration Files Contains: *Text*
 - 4.4.2 - Hardening Devices Contains: *Text*
 - 4.4.3 - Monitoring Service Logs Contains: *Text*
 - 4.4.4 - Lab – Locating Log Files Contains: *Text, Labs*
 - 4.5 - The Linux File System
 - 4.5.1 - The File System Types in Linux Contains: *Text*
 - 4.5.2 - Linux Roles and File Permissions Contains: *Text*
 - 4.5.3 - Hard Links and Symbolic Links Contains: *Text*
 - 4.5.4 - Lab - Navigating the Linux Filesystem and Permission Settings Contains: *Text, Labs*
 - 4.6 - Working with the Linux GUI
 - 4.6.1 - X Window System Contains: *Text*
 - 4.6.2 - The Linux GUI Contains: *Text*
 - 4.7 - Working on a Linux Host
 - 4.7.1 - Installing and Running Applications on a Linux Host Contains: *Text*
 - 4.7.2 - Keeping the System Up to Date Contains: *Text*
 - 4.7.3 - Processes and Forks Contains: *Text*
 - 4.7.4 - Malware on a Linux Host Contains: *Text*
 - 4.7.5 - Rootkit Check Contains: *Text*

- 4.7.6 - Piping CommandsContains: *Text*
- 4.7.7 - Video - Applications, Rootkits, and Piping CommandsContains: *Text, Videos*
- 4.8 - Linux Basics Summary
 - 4.8.1 - What Did I Learn in this Module?Contains: *Text*
 - 4.8.2 - Module 4: Linux Basics QuizContains: *Module Quiz*
- 5 - Network Protocols
 - 5.0 - Introduction
 - 5.0.1 - Why Should I Take this Module?Contains: *Text*
 - 5.0.2 - What Will I Learn in this Module?Contains: *Text*
 - 5.1 - Network Communications Process
 - 5.1.1 - Networks of Many SizesContains: *Text*
 - 5.1.2 - Client-Server CommunicationsContains: *Text*
 - 5.1.3 - Typical SessionsContains: *Text*
 - 5.1.4 - Tracing the PathContains: *Text*
 - 5.1.5 - Lab - Tracing a RouteContains: *Text, Labs*
 - 5.2 - Communications Protocols
 - 5.2.1 - What are Protocols?Contains: *Text*
 - 5.2.2 - Network ProtocolsContains: *Text*
 - 5.2.3 - The TCP/IP Protocol SuiteContains: *Text*
 - 5.2.4 - Message Formatting and EncapsulationContains: *Text, Animations*
 - 5.2.5 - Message SizeContains: *Text, Animations*
 - 5.2.6 - Message TimingContains: *Text, Animations*
 - 5.2.7 - Unicast, Multicast, and BroadcastContains: *Text, Animations*
 - 5.2.8 - The Benefits of Using a Layered ModelContains: *Text*
 - 5.2.9 - The OSI Reference ModelContains: *Text*
 - 5.2.10 - The TCP/IP Protocol ModelContains: *Text*
 - 5.3 - Data Encapsulation
 - 5.3.1 - Segmenting MessagesContains: *Text, Interactive Activities*
 - 5.3.2 - SequencingContains: *Text*
 - 5.3.3 - Protocol Data UnitsContains: *Text*
 - 5.3.4 - Three AddressesContains: *Text*
 - 5.3.5 - Encapsulation ExampleContains: *Text, Animations*
 - 5.3.6 - De-encapsulation ExampleContains: *Text, Animations*
 - 5.3.7 - Lab - Introduction to WiresharkContains: *Text, Labs*
 - 5.3.8 - Check Your Understanding - Data EncapsulationContains: *Check Your Understandings*
 - 5.4 - Network Protocols Summary
 - 5.4.1 - What Did I Learn in this Module?Contains: *Text*
 - 5.4.2 - Module 5: Network Protocols QuizContains: *Module Quiz*
- 6 - Ethernet and Internet Protocol (IP)
 - 6.0 - Introduction
 - 6.0.1 - Why Should I Take this Module?Contains: *Text*
 - 6.0.2 - What Will I Learn in this Module?Contains: *Text*
 - 6.1 - Ethernet
 - 6.1.1 - Ethernet EncapsulationContains: *Text*
 - 6.1.2 - Ethernet Frame FieldsContains: *Text*
 - 6.1.3 - MAC Address FormatContains: *Text*

- 6.1.4 - Check Your Understanding - Ethernet Frame FieldsContains: *Check Your Understandings*
- 6.2 - IPv4
 - 6.2.1 - The Network LayerContains: *Text, Animations*
 - 6.2.2 - IP EncapsulationContains: *Text*
 - 6.2.3 - Characteristics of IPContains: *Text*
 - 6.2.4 - ConnectionlessContains: *Text*
 - 6.2.5 - Best EffortContains: *Text*
 - 6.2.6 - Media IndependentContains: *Text*
 - 6.2.7 - Check Your Understanding - IP CharacteristicsContains: *Check Your Understandings*
 - 6.2.8 - IPv4 Packet HeaderContains: *Text*
 - 6.2.9 - IPv4 Packet Header FieldsContains: *Text*
 - 6.2.10 - Check Your Understanding - IPv4 PacketContains: *Check Your Understandings*
- 6.3 - IP Addressing Basics
 - 6.3.1 - Network and Host PortionsContains: *Text*
 - 6.3.2 - The Subnet MaskContains: *Text*
 - 6.3.3 - The Prefix LengthContains: *Text*
 - 6.3.4 - Determining the Network: Logical ANDContains: *Text*
 - 6.3.5 - Video – Network, Host, and Broadcast AddressesContains: *Videos*
 - 6.3.6 - Subnetting Broadcast DomainsContains: *Text*
 - 6.3.7 - Check Your Understanding - IPv4 Address StructureContains: *Check Your Understandings*
- 6.4 - Types of IPv4 Addresses
 - 6.4.1 - IPv4 Address Classes and Default Subnet MasksContains: *Text*
 - 6.4.2 - Reserved Private AddressesContains: *Text*
- 6.5 - The Default Gateway
 - 6.5.1 - Host Forwarding DecisionContains: *Text*
 - 6.5.2 - Default GatewayContains: *Text*
 - 6.5.3 - A Host Routes to the Default GatewayContains: *Text*
 - 6.5.4 - Host Routing TablesContains: *Text*
 - 6.5.5 - Check Your Understanding - How a Host RoutesContains: *Check Your Understandings*
- 6.6 - IPv6
 - 6.6.1 - Need for IPv6Contains: *Text*
 - 6.6.2 - IPv6 Addressing FormatsContains: *Text*
 - 6.6.3 - Rule 1 – Omit Leading ZerosContains: *Text*
 - 6.6.4 - Rule 2- Double ColonContains: *Text*
 - 6.6.5 - IPv6 Prefix LengthContains: *Text*
 - 6.6.6 - Video – Layer 2 and Layer 3 AddressingContains: *Text, Videos*
 - 6.6.7 - Check Your Understanding - IPv6 Address RepresentationContains: *Text, Interactive Activities*
- 6.7 - Ethernet and IP Protocol Summary
 - 6.7.1 - What Did I Learn in this Module?Contains: *Text*
 - 6.7.2 - Module 6: Ethernet and IP Protocol QuizContains: *Module Quiz*

7 - Connectivity Verification

7.0 - Introduction

7.0.1 - Why Should I Take this Module?Contains: *Text*

7.0.2 - What Will I Learn in this Module?Contains: *Text*

7.1 - ICMP

7.1.1 - ICMPv4 MessagesContains: *Text, Animations*

7.1.2 - ICMPv6 RS and RA MessagesContains: *Text*

7.2 - Ping and Traceroute Utilities

7.2.1 - Video - Network Testing and Verification with Windows CLI CommandsContains: *Videos*

7.2.2 - Ping - Test ConnectivityContains: *Text*

7.2.3 - Ping the LoopbackContains: *Text*

7.2.4 - Ping the Default GatewayContains: *Text*

7.2.5 - Ping a Remote HostContains: *Text, Animations*

7.2.6 - Traceroute - Test the PathContains: *Text, Animations*

7.2.7 - ICMP Packet FormatContains: *Text*

7.2.8 - Packet Tracer – Verify IPv4 and IPv6 AddressingContains: *Text, Packet Tracers*

7.3 - Connectivity Verification Summary

7.3.1 - What Did I Learn in this Module?Contains: *Text*

7.3.2 - Module 7: Connectivity Verification QuizContains: *Module Quiz*

8 - Address Resolution Protocol

8.0 - Introduction

8.0.1 - Why Should I Take this module?Contains: *Text*

8.0.2 - What Will I Learn in this Module?Contains: *Text*

8.1 - MAC and IP

8.1.1 - Destination on Same NetworkContains: *Text*

8.1.2 - Destination on Remote NetworkContains: *Text*

8.2 - ARP

8.2.1 - ARP OverviewContains: *Text*

8.2.2 - ARP FunctionsContains: *Text, Animations*

8.2.3 - Video - ARP Operation - ARP RequestContains: *Text, Videos*

8.2.4 - Video - ARP Operation - ARP ReplyContains: *Text, Videos*

8.2.5 - Video - ARP Role in Remote CommunicationContains: *Text, Videos*

8.2.6 - Removing Entries from an ARP TableContains: *Text*

8.2.7 - ARP Tables on Networking DevicesContains: *Text*

8.2.8 - Lab - Using Wireshark to Examine Ethernet FramesContains: *Text, Labs*

8.3 - ARP Issues

8.3.1 - ARP Issues - ARP Broadcasts and ARP SpoofingContains: *Text*

8.3.2 - Video - ARP SpoofingContains: *Text, Videos*

8.4 - Address Resolution Protocol Summary

8.4.1 - What Did I Learn in this Module?Contains: *Text*

8.4.2 - Module 8: Address Resolution Protocol QuizContains: *Module Quiz*

9 - The Transport Layer

9.0 - Introduction

9.0.1 - Why Should I Take this Module?Contains: *Text*

9.0.2 - What Will I Learn in this Module?Contains: *Text*

9.1 - Transport Layer Characteristics

- 9.1.1 - Role of the Transport LayerContains: *Text*
- 9.1.2 - Transport Layer ResponsibilitiesContains: *Text*
- 9.1.3 - Transport Layer ProtocolsContains: *Text*
- 9.1.4 - Transmission Control Protocol (TCP)Contains: *Text, Animations*
- 9.1.5 - TCP HeaderContains: *Text*
- 9.1.6 - TCP Header FieldsContains: *Text*
- 9.1.7 - User Datagram Protocol (UDP)Contains: *Text, Animations*
- 9.1.8 - UDP HeaderContains: *Text*
- 9.1.9 - UDP Header FieldsContains: *Text*
- 9.1.10 - Socket PairsContains: *Text*
- 9.1.11 - Check Your Understanding – Compare TCP and UDP CharacteristicsContains: *Interactive Activities*
- 9.2 - Transport Layer Session Establishment
 - 9.2.1 - TCP Server ProcessesContains: *Text*
 - 9.2.2 - TCP Connection EstablishmentContains: *Text*
 - 9.2.3 - Session TerminationContains: *Text*
 - 9.2.4 - TCP Three-way Handshake AnalysisContains: *Text*
 - 9.2.5 - Video – TCP 3-Way HandshakeContains: *Text, Videos*
 - 9.2.6 - Lab – Using Wireshark to Observe the TCP 3-Way HandshakeContains: *Text, Labs*
 - 9.2.7 - Check Your Understanding – TCP Connection and Termination ProcessContains: *Interactive Activities*
- 9.3 - Transport Layer Reliability
 - 9.3.1 - TCP Reliability - Guaranteed and Ordered DeliveryContains: *Text*
 - 9.3.2 - Video - TCP Reliability – Sequence Numbers and AcknowledgementsContains: *Text, Videos*
 - 9.3.3 - TCP Reliability - Data Loss and RetransmissionContains: *Text*
 - 9.3.4 - Video - TCP Reliability – Data Loss and RetransmissionContains: *Text, Videos*
 - 9.3.5 - TCP Flow Control - Window Size and AcknowledgmentsContains: *Text*
 - 9.3.6 - TCP Flow Control - Maximum Segment Size (MSS)Contains: *Text*
 - 9.3.7 - TCP Flow Control - Congestion AvoidanceContains: *Text*
 - 9.3.8 - Lab - Exploring NmapContains: *Text, Labs*
 - 9.3.9 - Check Your Understanding - Reliability and Flow ControlContains: *Check Your Understandings*
- 9.4 - The Transport Layer Summary
 - 9.4.1 - What Did I Learn in this Module?Contains: *Text*
 - 9.4.2 - Module 9: The Transport Layer QuizContains: *Module Quiz*
- 10 - Network Services
 - 10.0 - Introduction
 - 10.0.1 - Why Should I Take this Module?Contains: *Text*
 - 10.0.2 - What Will I Learn in this Module?Contains: *Text*
 - 10.1 - DHCP
 - 10.1.1 - Dynamic Host Configuration ProtocolContains: *Text*
 - 10.1.2 - DHCP OperationContains: *Text*
 - 10.1.3 - DHCP Message FormatContains: *Text*
 - 10.1.4 - Check Your Understanding - DHCPContains: *Check Your Understandings*
 - 10.2 - DNS

- 10.2.1 - DNS OverviewContains: *Text*
- 10.2.2 - The DNS Domain HierarchyContains: *Text*
- 10.2.3 - The DNS Lookup ProcessContains: *Text*
- 10.2.4 - DNS Message FormatContains: *Text*
- 10.2.5 - Dynamic DNSContains: *Text*
- 10.2.6 - The WHOIS ProtocolContains: *Text*
- 10.2.7 - Lab - Using Wireshark to Examine a UDP DNS CaptureContains: *Text, Labs*
- 10.3 - NAT
 - 10.3.1 - IPv4 Private Address SpaceContains: *Text*
 - 10.3.2 - What is NAT?Contains: *Text*
 - 10.3.3 - How NAT WorksContains: *Text, Animations*
 - 10.3.4 - Port Address TranslationContains: *Text, Animations*
- 10.4 - File Transfer and Sharing Services
 - 10.4.1 - FTP and TFTPContains: *Text*
 - 10.4.2 - SMBContains: *Text*
 - 10.4.3 - Lab - Using Wireshark to Examine TCP and UDP CapturesContains: *Text, Labs*
- 10.5 - Email
 - 10.5.1 - Email ProtocolsContains: *Text*
 - 10.5.2 - SMTPContains: *Text*
 - 10.5.3 - POP3Contains: *Text*
 - 10.5.4 - IMAPContains: *Text*
- 10.6 - HTTP
 - 10.6.1 - Hypertext Transfer Protocol and Hypertext Markup LanguageContains: *Text*
 - 10.6.2 - The HTTP URLContains: *Text*
 - 10.6.3 - HTTP OperationContains: *Text*
 - 10.6.4 - HTTP Status CodesContains: *Text*
 - 10.6.5 - HTTP/2Contains: *Text*
 - 10.6.6 - Securing HTTP – HTTPSContains: *Text*
 - 10.6.7 - Lab - Using Wireshark to Examine HTTP and HTTPS TrafficContains: *Text, Labs*
- 10.7 - Network Services Summary
 - 10.7.1 - What Did I Learn in this Module?Contains: *Text*
 - 10.7.2 - Module 10: Network Services QuizContains: *Module Quiz*
- 11 - Network Communication Devices
 - 11.0 - Introduction
 - 11.0.1 - Why Should I Take this Module?Contains: *Text*
 - 11.0.2 - What Will I Learn in this Module?Contains: *Text*
 - 11.1 - Network Devices
 - 11.1.1 - End DevicesContains: *Text, Animations*
 - 11.1.2 - Video - End DevicesContains: *Text, Videos*
 - 11.1.3 - RoutersContains: *Text, Animations*
 - 11.1.4 - Check Your Understanding - Match Layer 2 and Layer 3 AddressingContains: *Interactive Activities*
 - 11.1.5 - Packet Forwarding Decision ProcessContains: *Text*
 - 11.1.6 - Routing InformationContains: *Text*
 - 11.1.7 - End-to-End Packet ForwardingContains: *Text, Animations*

- 11.1.8 - Video - Static and Dynamic RoutingContains: *Text, Videos*
- 11.1.9 - Hubs, Bridges, LAN SwitchesContains: *Text*
- 11.1.10 - Switching OperationContains: *Text*
- 11.1.11 - Video - MAC Address Tables on Connected SwitchesContains: *Text, Videos*
- 11.1.12 - VLANsContains: *Text*
- 11.1.13 - STPContains: *Text*
- 11.1.14 - Multilayer SwitchingContains: *Text*
- 11.2 - Wireless Communications
 - 11.2.1 - Video - Wireless CommunicationsContains: *Text, Videos*
 - 11.2.2 - Wireless versus Wired LANsContains: *Text*
 - 11.2.3 - 802.11 Frame StructureContains: *Text*
 - 11.2.4 - CSMA/CAContains: *Text*
 - 11.2.5 - Wireless Client and AP AssociationContains: *Text*
 - 11.2.6 - Passive and Active Discover ModeContains: *Text*
 - 11.2.7 - Check Your Understanding – Steps in the Client and AP ProcessContains: *Check Your Understandings*
 - 11.2.8 - Wireless Devices -AP, LWAP, and WLCContains: *Text*
 - 11.2.9 - Check Your Understanding - Identify the LAN DeviceContains: *Check Your Understandings*
- 11.3 - Network Communication Devices Summary
 - 11.3.1 - What Did I Learn in this Module?Contains: *Text*
 - 11.3.2 - Module 11: Network Communication Devices QuizContains: *Module Quiz*
- 12 - Network Security Infrastructure
 - 12.0 - Introduction
 - 12.0.1 - Why Should I Take this Module?Contains: *Text*
 - 12.0.2 - What Will I Learn in this Module?Contains: *Text*
 - 12.1 - Network Topologies
 - 12.1.1 - Network RepresentationsContains: *Text*
 - 12.1.2 - Topology DiagramsContains: *Text*
 - 12.1.3 - Networks of Many SizesContains: *Text*
 - 12.1.4 - LANs and WANsContains: *Text*
 - 12.1.5 - The Three-Layer Network Design ModelContains: *Text*
 - 12.1.6 - Video - Three-Layer Network DesignContains: *Text, Videos*
 - 12.1.7 - Common Security ArchitecturesContains: *Text*
 - 12.1.8 - Check your Understanding - Identify the Network TopologyContains: *Check Your Understandings*
 - 12.1.9 - Packet Tracer - Identify Packet FlowContains: *Text, Packet Tracers*
 - 12.2 - Security Devices
 - 12.2.1 - Video - Security DevicesContains: *Text, Videos*
 - 12.2.2 - FirewallsContains: *Text, Animations*
 - 12.2.3 - Firewall Type DescriptionsContains: *Text*
 - 12.2.4 - Check Your Understanding - Identify the Type of FirewallContains: *Check Your Understandings*
 - 12.2.5 - Intrusion Prevention and Detection DevicesContains: *Text*
 - 12.2.6 - Advantages and Disadvantages of IDS and IPSContains: *Text*
 - 12.2.7 - Types of IPSContains: *Text*
 - 12.2.8 - Specialized Security AppliancesContains: *Text*

12.2.9 - Check Your Understanding - Compare IDS and IPS CharacteristicsContains: *Interactive Activities*

12.3 - Security Services

12.3.1 - Video - Security ServicesContains: *Text, Videos*

12.3.2 - Traffic Control with ACLsContains: *Text*

12.3.3 - ACLs: Important FeaturesContains: *Text*

12.3.4 - Packet Tracer - ACL DemonstrationContains: *Text, Packet Tracers*

12.3.5 - SNMPContains: *Text*

12.3.6 - NetFlowContains: *Text*

12.3.7 - Port MirroringContains: *Text*

12.3.8 - Syslog ServersContains: *Text*

12.3.9 - NTPContains: *Text*

12.3.10 - AAA ServersContains: *Text*

12.3.11 - VPNContains: *Text*

12.3.12 - Check Your Understanding - Identify the Network Security Device or ServiceContains: *Check Your Understandings*

12.4 - Network Security Infrastructure Summary

12.4.1 - What Did I Learn in this Module?Contains: *Text*

12.4.2 - Module 12: Network Security Infrastructure QuizContains: *Module Quiz*

13 - Attackers and Their Tools

13.0 - Introduction

13.0.1 - Why Should I Take this Module?Contains: *Text*

13.0.2 - What Will I Learn in this Module?Contains: *Text*

13.1 - Who is Attacking Our Network?

13.1.1 - Threat, Vulnerability, and RiskContains: *Text*

13.1.2 - Hacker vs. Threat ActorContains: *Text*

13.1.3 - Evolution of Threat ActorsContains: *Text*

13.1.4 - CybercriminalsContains: *Text*

13.1.5 - Cybersecurity TasksContains: *Text*

13.1.6 - Cyber Threat IndicatorsContains: *Text*

13.1.7 - Threat Sharing and Building Cybersecurity AwarenessContains: *Text*

13.1.8 - Check Your Understanding – What Color is my Hat?Contains: *Interactive Activities*

13.2 - Threat Actor Tools

13.2.1 - Introduction of Attack ToolsContains: *Text, Interactive Activities*

13.2.2 - Evolution of Security ToolsContains: *Text*

13.2.3 - Categories of AttacksContains: *Text*

13.2.4 - Check Your Understanding - Classify Cyber AttacksContains: *Check Your Understandings*

13.3 - Attackers and Their Tools Summary

13.3.1 - What Did I Learn in this Module?Contains: *Text*

13.3.2 - Module 13: Attackers and Their Tools QuizContains: *Module Quiz*

14 - Common Threats and Attacks

14.0 - Introduction

14.0.1 - Why Should I Take this Module?Contains: *Text*

14.0.2 - What Will I Learn in this Module?Contains: *Text*

14.1 - Malware

14.1.1 - Types of MalwareContains: *Text, Animations*

- 14.1.2 - VirusesContains: *Text*
- 14.1.3 - Trojan HorsesContains: *Text*
- 14.1.4 - Trojan Horse ClassificationContains: *Text*
- 14.1.5 - WormsContains: *Text*
- 14.1.6 - Worm ComponentsContains: *Text, Animations*
- 14.1.7 - RansomwareContains: *Text*
- 14.1.8 - Other MalwareContains: *Text*
- 14.1.9 - Common Malware BehaviorsContains: *Text*
- 14.1.10 - Check Your Understanding - MalwareContains: *Check Your Understandings*
- 14.1.11 - Lab - Anatomy of MalwareContains: *Text, Labs*
- 14.2 - Common Network Attacks - Reconnaissance, Access, and Social Engineering
 - 14.2.1 - Types of Network AttacksContains: *Text*
 - 14.2.2 - Reconnaissance AttacksContains: *Text, Animations*
 - 14.2.3 - Video - Reconnaissance AttacksContains: *Videos*
 - 14.2.4 - Access AttacksContains: *Text, Animations*
 - 14.2.5 - Video – Access and Social Engineering AttacksContains: *Text, Videos*
 - 14.2.6 - Social Engineering AttacksContains: *Text*
 - 14.2.7 - Strengthening the Weakest LinkContains: *Text*
 - 14.2.8 - Lab – Social EngineeringContains: *Text, Labs*
- 14.3 - Network Attacks - Denial of Service, Buffer Overflows, and Evasion
 - 14.3.1 - Video - Denial of Service AttacksContains: *Text, Videos*
 - 14.3.2 - DoS and DDoS AttacksContains: *Text, Animations*
 - 14.3.3 - Components of DDoS AttacksContains: *Text*
 - 14.3.4 - Video – Mirai BotnetContains: *Text, Videos*
 - 14.3.5 - Buffer Overflow AttackContains: *Text*
 - 14.3.6 - Evasion MethodsContains: *Text*
 - 14.3.7 - Check Your Understanding - Identify the Types of Network AttacksContains: *Check Your Understandings*
- 14.4 - Common Threats and Attacks Summary
 - 14.4.1 - What Did I Learn in this Module?Contains: *Text*
 - 14.4.2 - Module 14: Common Threats and Attacks QuizContains: *Module Quiz*
- 15 - Network Monitoring and Tools
 - 15.0 - Introduction
 - 15.0.1 - Why Should I Take this Module?Contains: *Text*
 - 15.0.2 - What Will I Learn in this Module?Contains: *Text*
 - 15.0.3 - Class Activity – What’s Going On?Contains: *Text, Labs*
 - 15.1 - Introduction to Network Monitoring
 - 15.1.1 - Network Security TopologyContains: *Text*
 - 15.1.2 - Network Monitoring MethodsContains: *Text*
 - 15.1.3 - Network TapsContains: *Text*
 - 15.1.4 - Traffic Mirroring and SPANContains: *Text*
 - 15.2 - Introduction to Network Monitoring Tools
 - 15.2.1 - Network Security Monitoring ToolsContains: *Text*
 - 15.2.2 - Network Protocol AnalyzersContains: *Text*
 - 15.2.3 - NetFlowContains: *Text*
 - 15.2.4 - SIEM and SOARContains: *Text*
 - 15.2.5 - SIEM SystemsContains: *Text*

- 15.2.6 - Check Your Understanding - Identify the Network Monitoring ToolContains: *Check Your Understandings*
- 15.2.7 - Packet Tracer - Logging Network ActivityContains: *Text, Packet Tracers*
- 15.3 - Network Monitoring and Tools Summary
 - 15.3.1 - What Did I Learn in this Module?Contains: *Text*
 - 15.3.2 - Module 15: Network Monitoring and Tools QuizContains: *Module Quiz*

- 16 - Attacking the Foundation
 - 16.0 - Introduction
 - 16.0.1 - Why Should I Take this Module?Contains: *Text*
 - 16.0.2 - What Will I Learn in this Module?Contains: *Text*
 - 16.1 - IP PDU Details
 - 16.1.1 - IPv4 and IPv6Contains: *Text*
 - 16.1.2 - The IPv4 Packet HeaderContains: *Text*
 - 16.1.3 - Video - Sample IPv4 Headers in WiresharkContains: *Text, Videos*
 - 16.1.4 - The IPv6 Packet HeaderContains: *Text*
 - 16.1.5 - Video - Sample IPv6 Headers in WiresharkContains: *Text, Videos*
 - 16.2 - IP Vulnerabilities
 - 16.2.1 - IP VulnerabilitiesContains: *Text*
 - 16.2.2 - ICMP AttacksContains: *Text*
 - 16.2.3 - Video - Amplification, Reflection, and Spoofing AttacksContains: *Text, Videos*
 - 16.2.4 - Amplification and Reflection AttacksContains: *Text*
 - 16.2.5 - Address Spoofing AttacksContains: *Text*
 - 16.2.6 - Check Your Understanding - IP Vulnerabilities and ThreatsContains: *Check Your Understandings*
 - 16.3 - TCP and UDP Vulnerabilities
 - 16.3.1 - TCP Segment HeaderContains: *Text*
 - 16.3.2 - TCP ServicesContains: *Text*
 - 16.3.3 - TCP AttacksContains: *Text*
 - 16.3.4 - UDP Segment Header and OperationContains: *Text*
 - 16.3.5 - UDP AttacksContains: *Text*
 - 16.3.6 - Check Your Understanding - TCP and UDP VulnerabilitiesContains: *Check Your Understandings*
 - 16.4 - Attacking the Foundation Summary
 - 16.4.1 - What Did I Learn in this Module?Contains: *Text*
 - 16.4.2 - Module 16: Attacking the Foundation QuizContains: *Module Quiz*

- 17 - Attacking What We Do
 - 17.0 - Introduction
 - 17.0.1 - Why Should I Take this Module?Contains: *Text*
 - 17.0.2 - What Will I Learn in this Module?Contains: *Text*
 - 17.1 - IP Services
 - 17.1.1 - ARP VulnerabilitiesContains: *Text, Animations*
 - 17.1.2 - ARP Cache PoisoningContains: *Text*
 - 17.1.3 - DNS AttacksContains: *Text*
 - 17.1.4 - DNS TunnelingContains: *Text*
 - 17.1.5 - DHCPContains: *Text*
 - 17.1.6 - DHCP AttacksContains: *Text*
 - 17.1.7 - Lab - Exploring DNS TrafficContains: *Text, Labs*

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

- 19.3.1 - What Did I Learn in this Module?Contains: *Text*
- 19.3.2 - Module 19: Access Control QuizContains: *Module Quiz*

20 - Threat Intelligence

20.0 - Introduction

- 20.0.1 - Why Should I Take this Module?Contains: *Text*
- 20.0.2 - What Will I Learn in this Module?Contains: *Text*

20.1 - Information Sources

- 20.1.1 - Network Intelligence CommunitiesContains: *Text*
- 20.1.2 - Cisco Cybersecurity ReportsContains: *Text*
- 20.1.3 - Security Blogs and PodcastsContains: *Text*

20.2 - Threat Intelligence Services

- 20.2.1 - Cisco TalosContains: *Text*
- 20.2.2 - FireEyeContains: *Text*
- 20.2.3 - Automated Indicator SharingContains: *Text*
- 20.2.4 - Common Vulnerabilities and Exposures (CVE) DatabaseContains: *Text*
- 20.2.5 - Threat Intelligence Communication StandardsContains: *Text*
- 20.2.6 - Threat Intelligence PlatformsContains: *Text*
- 20.2.7 - Check Your Understanding - Identify the Threat Intelligence Information SourceContains: *Check Your Understandings*

20.3 - Threat Intelligence Summary

- 20.3.1 - What Did I Learn in this Module?Contains: *Text*
- 20.3.2 - Module 20: Threat Intelligence QuizContains: *Module Quiz*

21 - Cryptography

21.0 - Introduction

- 21.0.1 - Why Should I Take this module?Contains: *Text*
- 21.0.2 - What Will I Learn in this Module?Contains: *Text*
- 21.0.3 - Class Activity - Creating CodesContains: *Text, Labs*

21.1 - Integrity and Authenticity

- 21.1.1 - Securing CommunicationsContains: *Text*
- 21.1.2 - Cryptographic Hash FunctionsContains: *Text*
- 21.1.3 - Cryptographic Hash OperationContains: *Text*
- 21.1.4 - MD5 and SHAContains: *Text*
- 21.1.5 - Origin AuthenticationContains: *Text*
- 21.1.6 - Lab – Hashing Things OutContains: *Text, Labs*

21.2 - Confidentiality

- 21.2.1 - Data ConfidentialityContains: *Text*
- 21.2.2 - Symmetric EncryptionContains: *Text*
- 21.2.3 - Asymmetric EncryptionContains: *Text*
- 21.2.4 - Asymmetric Encryption - ConfidentialityContains: *Text*
- 21.2.5 - Asymmetric Encryption - AuthenticationContains: *Text*
- 21.2.6 - Asymmetric Encryption - IntegrityContains: *Text*
- 21.2.7 - Diffie-HellmanContains: *Text*
- 21.2.8 - Video - CryptographyContains: *Text, Videos*
- 21.2.9 - Check Your Understanding - Classify the Encryption AlgorithmsContains: *Check Your Understandings*
- 21.2.10 - Lab - Encrypting and Decrypting Data Using OpenSSLContains: *Text, Labs*

- 21.2.11 - Lab - Encrypting and Decrypting Data Using a Hacker
ToolContains: *Text, Labs*
- 21.2.12 - Lab - Examining Telnet and SSH in WiresharkContains: *Text, Labs*
- 21.3 - Public Key Cryptography
 - 21.3.1 - Using Digital SignaturesContains: *Text*
 - 21.3.2 - Digital Signatures for Code SigningContains: *Text*
 - 21.3.3 - Digital Signatures for Digital CertificatesContains: *Text*
- 21.4 - Authorities and the PKI Trust System
 - 21.4.1 - Public Key ManagementContains: *Text*
 - 21.4.2 - The Public Key InfrastructureContains: *Text*
 - 21.4.3 - The PKI Authorities SystemContains: *Text*
 - 21.4.4 - The PKI Trust SystemContains: *Text*
 - 21.4.5 - Interoperability of Different PKI VendorsContains: *Text*
 - 21.4.6 - Certificate Enrollment, Authentication, and RevocationContains: *Text*
 - 21.4.7 - Lab – Certificate Authority StoresContains: *Text, Labs*
- 21.5 - Applications and Impacts of Cryptography
 - 21.5.1 - PKI ApplicationsContains: *Text*
 - 21.5.2 - Encrypted Network TransactionsContains: *Text*
 - 21.5.3 - Encryption and Security MonitoringContains: *Text*
- 21.6 - Cryptography Summary
 - 21.6.1 - What Did I Learn in this Module?Contains: *Text*
 - 21.6.2 - Module 21: Public Key Cryptography QuizContains: *Module Quiz*

- 22 - Endpoint Protection
- 22.0 - Introduction
 - 22.0.1 - Why Should I Take this Module?Contains: *Text*
 - 22.0.2 - What Will I Learn in this Module?Contains: *Text*
- 22.1 - Antimalware Protection
 - 22.1.1 - Endpoint ThreatsContains: *Text*
 - 22.1.2 - Endpoint SecurityContains: *Text*
 - 22.1.3 - Host-Based Malware ProtectionContains: *Text*
 - 22.1.4 - Network-Based Malware ProtectionContains: *Text*
 - 22.1.5 - Check Your Understanding - Identify Antimalware Terms and ConceptsContains: *Check Your Understandings*
- 22.2 - Host-Based Intrusion Prevention
 - 22.2.1 - Host-Based FirewallsContains: *Text*
 - 22.2.2 - Host-Based Intrusion DetectionContains: *Text*
 - 22.2.3 - HIDS OperationContains: *Text*
 - 22.2.4 - HIDS ProductsContains: *Text*
 - 22.2.5 - Check your Understanding - Identify the Host-Based Intrusion Protection TerminologyContains: *Check Your Understandings*
- 22.3 - Application Security
 - 22.3.1 - Attack SurfaceContains: *Text*
 - 22.3.2 - Application Block Listing and Allow ListingContains: *Text*
 - 22.3.3 - System-Based SandboxingContains: *Text*
 - 22.3.4 - Video - Using a Sandbox to Launch MalwareContains: *Text, Videos*
- 22.4 - Endpoint Protection Summary
 - 22.4.1 - What Did I Learn in this Module?Contains: *Text*
 - 22.4.2 - Module 22: Endpoint Protection QuizContains: *Module Quiz*

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*

- 24.1.5 - Email ProtocolsContains: *Text*
- 24.1.6 - ICMPContains: *Text*
- 24.1.7 - Check Your Understanding - Identify the Monitored ProtocolContains: *Check Your Understandings*
- 24.2 - Security Technologies
 - 24.2.1 - ACLsContains: *Text*
 - 24.2.2 - NAT and PATContains: *Text*
 - 24.2.3 - Encryption, Encapsulation, and TunnelingContains: *Text*
 - 24.2.4 - Peer-to-Peer Networking and TorContains: *Text*
 - 24.2.5 - Load BalancingContains: *Text*
 - 24.2.6 - Check Your Understanding - Identify the Impact of the Technology on Security and MonitoringContains: *Check Your Understandings*
- 24.3 - Technologies and Protocols Summary
 - 24.3.1 - What Did I Learn in this Module?Contains: *Text*
 - 24.3.2 - Module 24: Technologies and Protocols QuizContains: *Module Quiz*
- 25 - Network Security Data
 - 25.0 - Introduction
 - 25.0.1 - Why Should I Take this Module?Contains: *Text*
 - 25.0.2 - What Will I Learn in this Module?Contains: *Text*
 - 25.1 - Types of Security Data
 - 25.1.1 - Alert DataContains: *Text*
 - 25.1.2 - Session and Transaction DataContains: *Text*
 - 25.1.3 - Full Packet CapturesContains: *Text*
 - 25.1.4 - Statistical DataContains: *Text*
 - 25.1.5 - Check Your Understanding - Identify Types of Network Monitoring DataContains: *Check Your Understandings*
 - 25.2 - End Device Logs
 - 25.2.1 - Host LogsContains: *Text*
 - 25.2.2 - SyslogContains: *Text*
 - 25.2.3 - Server LogsContains: *Text*
 - 25.2.4 - SIEM and Log CollectionContains: *Text*
 - 25.2.5 - Check Your Understanding - Identify Windows Event Security LevelsContains: *Check Your Understandings*
 - 25.3 - Network Logs
 - 25.3.1 - TcpcdumpContains: *Text*
 - 25.3.2 - NetFlowContains: *Text*
 - 25.3.3 - Application Visibility and ControlContains: *Text*
 - 25.3.4 - Content Filter LogsContains: *Text*
 - 25.3.5 - Logging from Cisco DevicesContains: *Text*
 - 25.3.6 - Proxy LogsContains: *Text*
 - 25.3.7 - Next-Generation FirewallsContains: *Text*
 - 25.3.8 - Check Your Understanding - Identify the Security Technology from the Data DescriptionContains: *Check Your Understandings*
 - 25.3.9 - Check Your Understanding - Identify the NextGen Firewall Event TypesContains: *Check Your Understandings*
 - 25.3.10 - Packet Tracer - Explore a NetFlow ImplementationContains: *Text, Packet Tracers*
 - 25.3.11 - Packet Tracer - Logging from Multiple SourcesContains: *Text, Packet Tracers*

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*

- 27.2.11 - Video - Interpret HTTP and DNS Data to Isolate Threat ActorContains: *Text, Videos*
- 27.2.12 - Lab - Interpret HTTP and DNS Data to Isolate Threat ActorContains: *Text, Labs*
- 27.2.13 - Video - Isolate Compromised Host Using 5-TupleContains: *Text, Videos*
- 27.2.14 - Lab - Isolate Compromised Host Using 5-TupleContains: *Text, Labs*
- 27.2.15 - Lab - Investigate a Malware ExploitContains: *Text, Labs*
- 27.2.16 - Lab - Investigating an Attack on a Windows HostContains: *Text, Labs*
- 27.3 - Enhancing the Work of the Cybersecurity Analyst
 - 27.3.1 - Dashboards and VisualizationsContains: *Text*
 - 27.3.2 - Workflow ManagementContains: *Text*
- 27.4 - Working with Network Security Data Summary
 - 27.4.1 - What Did I Learn in this Module?Contains: *Text*
 - 27.4.2 - Module 27: Working with Network Security Data QuizContains: *Module Quiz*

- 28 - Digital Forensics and Incident Analysis and Response
 - 28.0 - Introduction
 - 28.0.1 - Why Should I Take this Module?Contains: *Text*
 - 28.0.2 - What Will I Learn in this Module?Contains: *Text*
 - 28.1 - Evidence Handling and Attack Attribution
 - 28.1.1 - Digital ForensicsContains: *Text*
 - 28.1.2 - The Digital Forensics ProcessContains: *Text*
 - 28.1.3 - Check Your Understanding - Identify the Steps in the Digital Forensics ProcessContains: *Check Your Understandings*
 - 28.1.4 - Types of EvidenceContains: *Text*
 - 28.1.5 - Check Your Understanding - Identify the Type of EvidenceContains: *Check Your Understandings*
 - 28.1.6 - Evidence Collection OrderContains: *Text*
 - 28.1.7 - Chain of CustodyContains: *Text*
 - 28.1.8 - Data Integrity and PreservationContains: *Text*
 - 28.1.9 - Attack AttributionContains: *Text*
 - 28.1.10 - The MITRE ATT&CK FrameworkContains: *Text*
 - 28.2 - The Cyber Kill Chain
 - 28.2.1 - Steps of the Cyber Kill ChainContains: *Text*
 - 28.2.2 - ReconnaissanceContains: *Text*
 - 28.2.3 - WeaponizationContains: *Text*
 - 28.2.4 - DeliveryContains: *Text*
 - 28.2.5 - ExploitationContains: *Text*
 - 28.2.6 - InstallationContains: *Text*
 - 28.2.7 - Command and ControlContains: *Text*
 - 28.2.8 - Actions on ObjectivesContains: *Text*
 - 28.2.9 - Check Your Understanding - Identify the Kill Chain StepContains: *Check Your Understandings*
 - 28.3 - The Diamond Model of Intrusion Analysis
 - 28.3.1 - Diamond Model OverviewContains: *Text*
 - 28.3.2 - Pivoting Across the Diamond ModelContains: *Text*
 - 28.3.3 - The Diamond Model and the Cyber Kill ChainContains: *Text*
 - 28.3.4 - Check Your Understanding - Identify the Diamond Model FeaturesContains: *Check Your Understandings*

28.4 - Incident Response

- 28.4.1 - Establishing an Incident Response Capability**Contains: *Text*
 - 28.4.2 - Check Your Understanding - Identify the Incident Response Plan Elements**Contains: *Check Your Understandings*
 - 28.4.3 - Incident Response Stakeholders**Contains: *Text*
 - 28.4.4 - NIST Incident Response Life Cycle**Contains: *Text*
 - 28.4.5 - Preparation**Contains: *Text*
 - 28.4.6 - Detection and Analysis**Contains: *Text*
 - 28.4.7 - Containment, Eradication, and Recovery**Contains: *Text*
 - 28.4.8 - Post-Incident Activities**Contains: *Text*
 - 28.4.9 - Incident Data Collection and Retention**Contains: *Text*
 - 28.4.10 - Reporting Requirements and Information Sharing**Contains: *Text*
 - 28.4.11 - Check Your Understanding - Identify the Incident Handling Term**Contains: *Check Your Understandings*
 - 28.4.12 - Lab - Incident Handling**Contains: *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 Quiz**Contains: *Module Quiz*
- ## **28.6 - Prepare for Your Exam and Launch Your Career!**
- 28.6.1 - Certification Preparation and Discount Vouchers**Contains: *Text*
 - 28.6.2 - Career Resources and Employment Opportunities**Contains: *Text*