



TestOut CyberDefense Pro - English 1.0.x

COURSE OUTLINE

TestOut CyberDefense Pro Course Outline English - 1.0.x

- 📺 Videos: 131 (12:54:06)
- 💻 Demonstrations: 106 (9:17:29)
- 🕒 Simulations: 72
- 📄 Fact Sheets: 141
- 📝 Exams: 72

CONTENTS:

1.0 INTRODUCTION

1.1 Introduction to TestOut CyberDefense Pro

- 📺 1.1.1 TestOut CyberDefense Pro Overview (6:16)
- 💻 1.1.2 Use the Simulator (14:56)
- 💻 1.1.3 Explore the New Lab Features (10:19)







2.0 THREAT INTELLIGENCE

2.1 Penetration Testing and Threat Hunting






- 📺 2.1.1 Penetration Test Process and Types (5:17)
- 📄 2.1.2 Penetration Test Process and Types Facts
- 📺 2.1.3 Threat Data and Intelligence (3:20)
- 📄 2.1.4 Threat Data and Intelligence Facts
- 📺 2.1.5 Security Intelligence Cycle (3:06)
- 📄 2.1.6 Security Intelligence Cycle Facts
- 📺 2.1.7 Threat Hunting Overview (2:48)
- 📄 2.1.8 Threat Hunting Facts
- 📺 2.1.9 Threat Actor Types (3:42)
- 📄 2.1.10 Threat Actor Type Facts
- 📝 2.1.11 Section Quiz

2.2 Organizational Security

- 📺 2.2.1 Attack Frameworks (3:36)
- 📄 2.2.2 Attack Frameworks Facts
- 📺 2.2.3 Threat Research (2:50)




-  2.2.4 Threat Research Facts
-  2.2.5 Threat Modeling (4:31)
-  2.2.6 Threat Modeling Facts
-  2.2.7 Threat Intelligence Sharing (3:03)
-  2.2.8 Threat Intelligence Sharing
-  2.2.9 Section Quiz

2.3 Security Controls




-  2.3.1 Security Frameworks and Policies (4:42)
-  2.3.2 Security Frameworks and Policies Facts
-  2.3.3 Security Control Categories and Types (5:43)
-  2.3.4 Security Control Categories and Types Facts
-  2.3.5 Section Quiz

3.0 RISK MITIGATION




3.1 Risk Identification Process

-  3.1.1 Risk Identification Process Overview (5:48)
-  3.1.2 Risk Identification Process Facts
-  3.1.3 Section Quiz

3.2 Risk Calculation









-  3.2.1 Risk Calculation Overview (6:47)
-  3.2.2 Risk Calculation Facts
-  3.2.3 Section Quiz




3.3 Risk Communication and Training

-  3.3.1 Communication and Training Overview (5:01)
-  3.3.2 Communication and Training Facts
-  3.3.3 Section Quiz






4.0 SOCIAL AND PHYSICAL SECURITY

4.1 Social Engineering





-  4.1.1 Social Engineering Overview (4:47)
-  4.1.2 Social Engineering Overview Facts
-  4.1.3 Social Engineering Motivation (10:19)
-  4.1.4 Social Engineering Motivation Facts
-  4.1.5 Social Engineering Techniques (10:17)
-  4.1.6 Social Engineering Technique Facts
-  4.1.7 Phishing and Internet-Based Techniques (5:00)
-  4.1.8 Phishing and Internet-Based Technique Facts

-  4.1.9 Use the Social Engineer Toolkit (4:41)
-  4.1.10 Identify Social Engineering
-  4.1.11 Section Quiz

4.2 Physical Security









-  4.2.1 Physical Security Overview (11:24)
-  4.2.2 Physical Security Facts
-  4.2.3 Physical Security Attacks (6:33)
-  4.2.4 Physical Security Attack Facts
-  4.2.5 Section Quiz

4.3 Countermeasures and Prevention











-  4.3.1 Countermeasures and Prevention (8:15)
-  4.3.2 Countermeasures and Prevention Facts
-  4.3.3 Implement Physical Security Countermeasures
-  4.3.4 Section Quiz

5.0 RECONNAISSANCE

5.1 Reconnaissance Overview

-  5.1.1 Reconnaissance Processes (2:30)
-  5.1.2 Reconnaissance Process Facts
-  5.1.3 Reconnaissance Tool Facts
-  5.1.4 Google Hacking for Office Documents (4:21)
-  5.1.5 Reconnaissance with TheHarvester (4:51)
-  5.1.6 Reconnaissance with Nmap (4:15)
-  5.1.7 Perform Reconnaissance with Nmap
-  5.1.8 Section Quiz

5.2 Reconnaissance Countermeasures

-  5.2.1 Reconnaissance Countermeasures (3:02)
-  5.2.2 View Windows Services (5:12)
-  5.2.3 Disable Windows Services
-  5.2.4 View Linux Services (4:06)
-  5.2.5 Manage Linux Services
-  5.2.6 Enable and Disable Linux Services
-  5.2.7 Reconnaissance Countermeasure Facts
-  5.2.8 Disable IIS Banner Broadcasting (1:47)
-  5.2.9 Hide the IIS Banner Broadcast
-  5.2.10 Section Quiz

5.3 Scanning

- 📺 5.3.1 Scanning Processes (6:54)
- 📖 5.3.2 Scanning Process Facts
- 📖 5.3.3 Scanning Tool Facts
- 🔧 5.3.4 Troubleshoot Connectivity with ping/hping3
- 💻 5.3.5 Perform a Scan with Nmap (4:37)
- 🔧 5.3.6 Perform an Internal Scan with Nmap
- 🔧 5.3.7 Perform an External Scan Using Zenmap
- 💻 5.3.8 Perform a Scan with Nmap Scripts (4:39)
- 📺 5.3.9 Scanning Considerations (5:31)
- 📖 5.3.10 Scanning Considerations Facts
- 💻 5.3.11 Scanning and Terminating Processes (6:50)
- 🔧 5.3.12 Scan for Zombie Processes
- 📝 5.3.13 Section Quiz

6.0 ENUMERATION

6.1 Enumeration Overview





- 📺 6.1.1 Enumeration (5:56)
- 📺 6.1.2 Enumerate Operating Systems (6:46)
- 💻 6.1.3 Enumerate Windows (4:44)
- 💻 6.1.4 Enumerate a Linux System (6:57)
- 📖 6.1.5 Enumeration Facts
- 💻 6.1.6 Enumerate with NetBIOS Enumerator (2:54)
- 📖 6.1.7 Enumerate Ports and Services Facts
- 🔧 6.1.8 Perform Enumeration with Nmap
- 💻 6.1.9 Enumerate with SoftPerfect (3:48)
- 💻 6.1.10 Enumerate with Metasploit (5:48)
- 🔧 6.1.11 Perform Enumeration with Metasploit
- 🔧 6.1.12 Perform Enumeration of MSSQL with Metasploit
- 📝 6.1.13 Section Quiz

6.2 Enumeration Countermeasures






- 📺 6.2.1 Enumeration Countermeasures (4:17)
- 📖 6.2.2 Enumeration Countermeasure Facts
- 💻 6.2.3 Disable DNS Zone Transfers (12:00)
- 🔧 6.2.4 Prevent Zone Transfer
- 📝 6.2.5 Section Quiz

7.0 VULNERABILITY MANAGEMENT




7.1 Vulnerability Assessment

-  7.1.1 Vulnerability Assessment (9:28)
-  7.1.2 Vulnerability Assessment Facts
-  7.1.3 Conduct Vulnerability Scans (4:03)
-  7.1.4 Section Quiz










7.2 Vulnerability Management Life Cycle

-  7.2.1 Vulnerability Management Life Cycle (5:46)
-  7.2.2 Vulnerability Management Life Cycle Facts
-  7.2.3 Vulnerability Solutions (2:40)
-  7.2.4 Vulnerability Solution Facts
-  7.2.5 Section Quiz

7.3 Vulnerability Scoring Systems








-  7.3.1 Vulnerability Scoring Systems (5:54)
-  7.3.2 Vulnerability Scoring System Facts
-  7.3.3 Section Quiz

7.4 Vulnerability Analysis



-  7.4.1 Vulnerability Assessment Tools (7:24)
-  7.4.2 Vulnerability Assessment Tool Facts
-  7.4.3 Vulnerability Scan Analysis (4:31)
-  7.4.4 Configure a Nessus Scan (3:17)
-  7.4.5 Analyze Scan Results from a Nessus Report (2:59)
-  7.4.6 Vulnerability Scan Analysis Facts
-  7.4.7 Scan for Vulnerabilities on a Windows Workstation
-  7.4.8 Scan for Vulnerabilities on a Linux Server
-  7.4.9 Section Quiz










8.0 IDENTITY AND ACCESS MANAGEMENT SECURITY (IAM)

8.1 Identity and Access Management Security














-  8.1.1 Identity and Access Management (5:28)
-  8.1.2 Identity and Access Management Facts
-  8.1.3 Federation (3:50)
-  8.1.4 Federation Facts
-  8.1.5 Single Sign-On (4:12)
-  8.1.6 Single Sign-On Facts
-  8.1.7 Section Quiz

8.2 Privilege Escalation






-  8.2.1 Privilege Escalation in Windows (3:51)
-  8.2.2 Use Bootable Media to Modify User Accounts (6:31)

-  8.2.3 Crack the SAM Database (4:11)
-  8.2.4 Change a Windows Password (3:04)
-  8.2.5 Privilege Escalation in Windows Facts
-  8.2.6 Configure User Account Control (6:59)
-  8.2.7 Enforce User Account Control
-  8.2.8 Use Fail2Ban (4:01)
-  8.2.9 Escalate Privileges with Curl (2:54)
-  8.2.10 Explore Privilege Creep (4:14)
-  8.2.11 Section Quiz

8.3 Identity and Access Management Threats







-  8.3.1 Identity and Access Management Threats Overview (4:41)
-  8.3.2 Identity and Access Management Threats Facts
-  8.3.3 Keylogger Attack (5:19)
-  8.3.4 Analyze a USB Keylogger Attack
-  8.3.5 Use Rainbow Tables (3:34)
-  8.3.6 Analyze Passwords using Rainbow Tables
-  8.3.7 Crack Passwords (8:26)
-  8.3.8 Crack Password-Protected Files (3:30)
-  8.3.9 Crack a Router Password (6:37)
-  8.3.10 Use L0phtCrack to Audit Passwords (2:47)
-  8.3.11 Configure Password Policies (10:42)
-  8.3.12 Configure Account Password Policies
-  8.3.13 Section Quiz







8.4 Certificate Management

-  8.4.1 Certificate Types (4:12)
-  8.4.2 Certificate Types Facts
-  8.4.3 Manage Certificates (12:15)
-  8.4.4 Manage Certificates
-  8.4.5 Section Quiz















9.0 CYBERSECURITY THREATS

9.1 Malware

















-  9.1.1 Malware Overview (5:14)
-  9.1.2 Malware Overview Facts
-  9.1.3 Trojans and Backdoors (7:20)
-  9.1.4 Trojan and Backdoor Facts
-  9.1.5 Malware Concerns (6:36)
-  9.1.6 Malware Concern Facts

-  9.1.7 Malware Analysis (5:13)
-  9.1.8 Malware Analysis Facts
-  9.1.9 Create a Virus (2:41)
-  9.1.10 Create a HTTP Trojan (3:13)
-  9.1.11 Use ProRat to Create a Trojan (3:16)
-  9.1.12 Section Quiz

9.2 Combat Malware

-  9.2.1 Anti-Malware Software (4:08)
-  9.2.2 Scan for Open Ports with Netstat (3:03)
-  9.2.3 Track Port Usage with TCPView (2:32)
-  9.2.4 Anti-Malware Software Facts
-  9.2.5 Detect Open Ports with Nmap
-  9.2.6 View Open Ports with netstat
-  9.2.7 Scan for Open Ports from a Remote Computer
-  9.2.8 Counter Malware with Windows Defender
-  9.2.9 Reverse Engineering Overview (8:05)
-  9.2.10 Perform Reverse Engineering (5:04)
-  9.2.11 Inspect HTTP Requests with Tamper Data (3:12)
-  9.2.12 Navigate the DVWA Website (4:32)
-  9.2.13 Reverse Engineering Facts
-  9.2.14 Section Quiz

9.3 Sniffing

-  9.3.1 Sniffing (7:48)
-  9.3.2 Sniffer Facts
-  9.3.3 Sniff Network Traffic with Wireshark (6:51)
-  9.3.4 Sniff Network Traffic with TShark (2:57)
-  9.3.5 Capture Traffic with TCPDump (5:42)
-  9.3.6 Use SMAC to Spoof MAC Addresses (3:39)
-  9.3.7 Poison ARP (5:07)
-  9.3.8 Analyze ARP Poisoning with Wireshark
-  9.3.9 Poison DNS (6:20)
-  9.3.10 Analyze DNS Spoofing
-  9.3.11 Filter and Analyze Traffic with Wireshark
-  9.3.12 Analyze Email Traffic for Spoofed Addresses
-  9.3.13 Analyze Email Traffic for Sensitive Data
-  9.3.14 Sniffing Countermeasures and Detection (4:38)
-  9.3.15 Detect Promiscuous Mode (3:17)
-  9.3.16 Sniffing Countermeasure and Detection Facts

9.4 Session Hijacking




- 📺 9.4.1 Session Hijacking Overview (4:43)
- 📄 9.4.2 Session Hijacking Facts
- 📺 9.4.3 Client-Side and Network Attacks (8:16)
- 📄 9.4.4 Client-Side and Network Attack Facts
- 💻 9.4.5 Perform a Man-in-the-Middle DHCP Attack (6:55)
- 🔍 9.4.6 Analyze a DHCP Spoofing Man-in-the-Middle Attack
- 🔍 9.4.7 Analyze HTTP POST Packets with Wireshark
- 💻 9.4.8 Set Up a Web Session Hijack (3:39)
- 🔍 9.4.9 Hijack a Web Session
- 📺 9.4.10 Session Hijacking Countermeasures (3:56)
- 📄 9.4.11 Session Hijacking Countermeasure Facts
- 📄 9.4.12 Section Quiz

9.5 Denial of Service

- 📺 9.5.1 Denial of Service (DoS) Overview (5:45)
- 📄 9.5.2 Denial of Service (DoS) Facts
- 📺 9.5.3 DoS Attack Types (5:18)
- 📄 9.5.4 DoS Attack Type Facts
- 💻 9.5.5 Perform a SYN Flood (6:21)
- 🔍 9.5.6 Perform and Analyze a SYN Flood Attack
- 🔍 9.5.7 Analyze ICMP Traffic in Wireshark
- 💻 9.5.8 Launch a DoS and DDoS Attack (5:42)
- 🔍 9.5.9 Analyze a DoS Attack
- 🔍 9.5.10 Analyze a DDoS Attack
- 📺 9.5.11 DoS Countermeasures (4:39)
- 📄 9.5.12 DoS Countermeasure Facts
- 📄 9.5.13 Section Quiz











9.6 SQL Injections

- 📺 9.6.1 SQL Injection (7:19)
- 📄 9.6.2 SQL Injection Facts
- 📺 9.6.3 SQL Injection Attack Types (5:27)
- 📄 9.6.4 SQL Injection Attack Facts
- 💻 9.6.5 Exploit SQL on a Web Page (4:01)
- 🔍 9.6.6 Explore SQL Injection Flaws
- 📺 9.6.7 SQL Injection Countermeasures (3:43)
- 📄 9.6.8 SQL Injection Countermeasure Facts
- 💻 9.6.9 Find SQL Injection Flaws with sqlmap (4:22)















-  9.6.10 Test a Web Application with Burp Suite (7:06)
-  9.6.11 Detect SQL Injection Flaws with Burp Suite
-  9.6.12 Section Quiz

10.0 INFRASTRUCTURE SECURITY







10.1 Intrusion Detection Systems


-  10.1.1 Security Monitoring (6:39)
-  10.1.2 Security Monitoring Facts
-  10.1.3 Intrusion Detection System (IDS) (8:20)
-  10.1.4 Intrusion Detection System (IDS) Facts
-  10.1.5 Evade IDS (10:20)
-  10.1.6 Evade IDS Facts
-  10.1.7 Intrusion Detection and Prevention with Snort (6:18)
-  10.1.8 Intrusion Detection and Prevention with Suricata (3:23)
-  10.1.9 Implement Intrusion Prevention with pfSense
-  10.1.10 Section Quiz


10.2 Firewalls

-  10.2.1 Firewalls (10:33)
-  10.2.2 Firewall Facts
-  10.2.3 Evade Firewalls (7:16)
-  10.2.4 Evade Firewalls Facts
-  10.2.5 Configure a Perimeter Firewall (6:50)
-  10.2.6 Configure a Perimeter Firewall
-  10.2.7 Avoid Firewall Detection (5:22)
-  10.2.8 Perform a Decoy Scan
-  10.2.9 Bypass Windows Firewall with Metasploit (3:47)
-  10.2.10 Bypass Windows Firewall with Nmap
-  10.2.11 Configure NPS Remote Access (6:46)
-  10.2.12 Create a Remote Access Policy
-  10.2.13 Protect Remote Access with NPS
-  10.2.14 Section Quiz

10.3 Honeypots and DNS Sinkholes

-  10.3.1 Honeypots (4:41)
-  10.3.2 Honeypot Facts
-  10.3.3 Evade Honeypots (4:25)
-  10.3.4 Evade Honeypots Facts
-  10.3.5 Detect Malicious Network Traffic with a Honeypot (3:24)
-  10.3.6 Create a Honeypot with Pentbox

 10.3.7 Blackholing and DNS Sinkholing (4:14)

 10.3.8 DNS Sinkholes Facts

 10.3.9 Section Quiz

10.4 Web Servers

 10.4.1 Web Server Hacking (6:12)

 10.4.2 Web Server Hacking Facts


 10.4.3 Web Server Attacks (7:09)

 10.4.4 Web Server Attack Facts


 10.4.5 Mirror a Website with HTTrack (2:14)

 10.4.6 Extract Web Server Information (4:31)


 10.4.7 Extract Web Server Information with Nmap

 10.4.8 Analyze FTP Credentials with Wireshark


 10.4.9 Web Server Countermeasures (5:47)


 10.4.10 Web Server Countermeasures Facts


 10.4.11 Evaluate Webserver Security

 10.4.12 Section Quiz

10.5 Network Access

 10.5.1 Network Access Control (NAC) (7:31)

 10.5.2 Network Access Control (NAC) Facts

 10.5.3 Permissions (6:43)

 10.5.4 Permission Facts

 10.5.5 Change File Permissions with icacils (4:56)

 10.5.6 Section Quiz

10.6 Web Applications

 10.6.1 Web Applications (6:42)

 10.6.2 Web Application Facts

 10.6.3 Web Application Hacking (6:25)

 10.6.4 Web Application Hacking Facts


 10.6.5 Overflow Attacks (7:18)

 10.6.6 Overflow Attacks Facts

 10.6.7 Hidden Field Manipulation Attacks (2:28)

 10.6.8 Exploit Cross-Site Scripting Vulnerabilities (3:03)




 10.6.9 Test the Security of a Web Application 1

 10.6.10 Test the Security of a Web Application 2










 10.6.11 Web Application Countermeasures (6:44)

 10.6.12 Scan a Website with Acunetix (4:22)

 10.6.13 Web Application Countermeasure Facts


















-  10.6.14 Set Up URL Blocking (7:24)
-  10.6.15 Configure URL Blocking
-  10.6.16 Section Quiz

10.7 Specialized Technology





-  10.7.1 Embedded Systems (5:04)
-  10.7.2 Embedded Systems Facts
-  10.7.3 Controller Systems (5:14)
-  10.7.4 Controller Systems Facts
-  10.7.5 Premises and Automotive Systems (5:17)
-  10.7.6 Premises and Automotive Systems Facts
-  10.7.7 Use Windows Defender Application Control (5:38)
-  10.7.8 Configure Windows Defender Application Control
-  10.7.9 Section Quiz

11.0 WIRELESS AND IOT SECURITY











11.1 Wireless Security

-  11.1.1 Wireless Overview (7:44)
-  11.1.2 Wireless Facts
-  11.1.3 Wireless Encryption and Authentication (9:17)
-  11.1.4 Wireless Encryption and Authentication Facts
-  11.1.5 Wireless Hacking (9:26)
-  11.1.6 Wireless Hacking Facts
-  11.1.7 Wi-Fi Packet Analysis (5:35)
-  11.1.8 Crack Wi-Fi Encryption with Aircrack-ng (5:41)
-  11.1.9 Discover a Hidden Network
-  11.1.10 Wireless Hacking Countermeasures (9:12)
-  11.1.11 Wireless Hacking Countermeasure Facts
-  11.1.12 Detect a Rogue Device (5:54)
-  11.1.13 Discover a Rogue DHCP Server
-  11.1.14 Locate a Rogue Wireless Access Point
-  11.1.15 Set Up a Captive Portal (6:21)
-  11.1.16 Configure a Captive Portal
-  11.1.17 Section Quiz












11.2 Bluetooth Security

-  11.2.1 Bluetooth Threats (7:58)
-  11.2.2 Bluetooth Threats Facts
-  11.2.3 Discover Vulnerable Bluetooth Devices (4:10)
-  11.2.4 Discover Bluetooth Devices












11.3 Mobile Device Security

-  11.3.1 Mobile Device Attacks (6:05)
-  11.3.2 Mobile Device Attack Facts
-  11.3.3 Mobile Device Operating Systems (8:18)
-  11.3.4 Mobile Device Operating System Facts
-  11.3.5 Exploit Android with Binary Payloads (7:19)
-  11.3.6 Securing Mobile Devices (7:23)
-  11.3.7 Secure a Mobile Device
-  11.3.8 Mobile Device Defense (7:09)
-  11.3.9 Mobile Device Management Facts
-  11.3.10 Section Quiz











11.4 Cloud Security

-  11.4.1 Cloud Computing (9:40)
-  11.4.2 Cloud Computing Facts
-  11.4.3 Cloud Threats (7:11)
-  11.4.4 Cloud Threats Facts
-  11.4.5 Cloud Attacks (6:00)
-  11.4.6 Cloud Attacks Facts
-  11.4.7 Cloud Security (7:08)
-  11.4.8 Cloud Security Facts
-  11.4.9 Secure Files in the Cloud (3:54)
-  11.4.10 Use ScoutSuite to Analyze a Cloud Infrastructure (3:41)
-  11.4.11 Section Quiz












11.5 Internet of Things Security

-  11.5.1 Internet of Things (7:28)
-  11.5.2 Internet of Things Facts
-  11.5.3 IoT Technologies and Protocols (12:49)
-  11.5.4 IoT Technologies and Protocols Facts
-  11.5.5 IoT Security Challenges (7:52)
-  11.5.6 IoT Security Challenge Facts
-  11.5.7 IoT Security (5:50)
-  11.5.8 IoT Security Facts
-  11.5.9 Search for IoT with Shodan (4:39)
-  11.5.10 Scan for IoT with Nmap (3:24)
-  11.5.11 Scan for Vulnerabilities on IoT
-  11.5.12 Section Quiz














12.1 Hardware Analysis

-  12.1.1 Hardware Assurance (4:55)
-  12.1.2 Hardware Assurance Facts
-  12.1.3 Encrypt Data (4:33)
-  12.1.4 Encrypt a Hard Disk (6:27)
-  12.1.5 Encrypt a Hard Drive
-  12.1.6 Segmentation (4:28)
-  12.1.7 Segmentation Facts
-  12.1.8 Secure Processing (2:31)
-  12.1.9 Secure Processing Facts
-  12.1.10 Section Quiz


12.2 Security Information and Event Management (SIEM)

-  12.2.1 Security Information and Event Management (SIEM) Overview (4:05)
-  12.2.2 SIEM Review Facts
-  12.2.3 Set Up Security Appliance Access (7:48)
-  12.2.4 Configure a Security Appliance
-  12.2.5 Configure Security Appliance Access
-  12.2.6 Use Security Onion v2 – Hunter (6:52)
-  12.2.7 Use Security Onion v2 – Kibana (3:57)
-  12.2.8 Evaluate Network Security with Kibana
-  12.2.9 Evaluate Network Security with Hunter-1
-  12.2.10 Evaluate Network Security with Hunter-2
-  12.2.11 Section Quiz

12.3 Log Review

-  12.3.1 Log Review Overview (4:21)
-  12.3.2 Log Review Facts
-  12.3.3 Configure Centralized Logging with Cisco Devices (1:58)
-  12.3.4 Use pfSense to Log Events (6:00)
-  12.3.5 Evaluate Event Logs in pfSense (4:33)
-  12.3.6 Log Events with pfSense
-  12.3.7 Evaluate Event Logs in pfSense
-  12.3.8 Log Events with Event Viewer (5:17)
-  12.3.9 Windows Event Subscriptions (2:53)
-  12.3.10 Configure Collector-Initiated Subscriptions (6:01)
-  12.3.11 Configure Source-Initiated Subscriptions (7:46)
-  12.3.12 Windows Event Subscription Facts
-  12.3.13 Evaluate Windows Log Files

 12.3.14 Analyze Network Traffic with NetworkMiner (4:18)

 12.3.15 Section Quiz


12.4 Asset and Change Management


 12.4.1 Asset Management Overview (6:26)


 12.4.2 Asset Management Facts

 12.4.3 Supply Chain Overview (4:28)


 12.4.4 Supply Chain Facts


 12.4.5 Change Management Overview (2:55)

 12.4.6 Change Management Facts

 12.4.7 Section Quiz

12.5 Virtualization Management


 12.5.1 Virtualization Management Overview (7:04)

 12.5.2 Virtualization Management Facts

 12.5.3 Section Quiz

13.0 SOFTWARE ASSURANCE


13.1 Software Development Overview

 13.1.1 Software Development Life Cycle (SDLC) Integration (4:41)

 13.1.2 Software Development Life Cycle (SDLC) Integration Facts

 13.1.3 Service-Oriented Architectures (5:46)

 13.1.4 Service-Oriented Architectures Facts

 13.1.5 Assessment and Coding Practices (8:38)


 13.1.6 Assessment and Coding Practices Facts


 13.1.7 Section Quiz

13.2 Automation


 13.2.1 Automation Overview (5:26)

 13.2.2 Automation Facts

 13.2.3 Automation Technologies (5:43)


 13.2.4 Automation Technologies Facts

 13.2.5 REST API Facts

 13.2.6 Section Quiz








14.0 DATA ANALYSIS

14.1 Data Analysis and Protection







 14.1.1 Data Privacy Overview (11:15)

 14.1.2 Data Privacy Technical Controls (9:28)














 14.1.3 Data Privacy Facts

-  14.1.4 Data Loss Prevention (DLP) (4:33)
-  14.1.5 Data Loss Prevention (DLP) Facts
-  14.1.6 Data Monitoring Methods (8:13)
-  14.1.7 Data Monitoring Methods Facts
-  14.1.8 Rule and Query Writing (3:29)
-  14.1.9 Rule and Query Writing Facts
-  14.1.10 Section Quiz




14.2 Hashing

-  14.2.1 Hashing (3:56)
-  14.2.2 Hashing Algorithms (3:00)
-  14.2.3 Hashing Facts
-  14.2.4 Verify MD5 Hash Integrity (2:54)
-  14.2.5 Compare an MD5 Hash
-  14.2.6 Section Quiz

14.3 Digital Forensics



-  14.3.1 Digital Forensics Overview (6:32)
-  14.3.2 Digital Forensics Facts
-  14.3.3 Forensic Software (5:20)
-  14.3.4 Forensic Software Facts
-  14.3.5 Search Memory Dump for Malware (9:08)
-  14.3.6 Forensic Techniques Overview (5:27)
-  14.3.7 Forensic Techniques Facts
-  14.3.8 Create a Forensic Drive Image with FTK (7:26)
-  14.3.9 Create a Forensic Drive Image with Guymager (5:27)
-  14.3.10 Create a Forensic Drive Image with DC3DD (6:03)
-  14.3.11 Examine a Forensic Drive Image with Autopsy (6:13)
-  14.3.12 Examine a Forensic Drive Image
-  14.3.13 Section Quiz




14.4 Email Analysis

-  14.4.1 Email Analysis Overview (6:11)
-  14.4.2 Email Analysis Facts
-  14.4.3 Section Quiz








15.0 INCIDENT RESPONSE

15.1 Incident Response - Preparation











-  15.1.1 Incident Response Overview (3:27)
-  15.1.2 Incident Response Overview Facts

-  15.1.3 Incident Response Preparation (8:19)
-  15.1.4 Incident Response Preparation Facts
-  15.1.5 Section Quiz










15.2 Incident Response - Detection and Containment

-  15.2.1 Detection and Analysis (4:39)
-  15.2.2 Detection and Analysis Facts
-  15.2.3 Indicators of Compromise (2:49)
-  15.2.4 Indicators of Compromise Facts
-  15.2.5 Containment (3:49)
-  15.2.6 Containment Facts
-  15.2.7 Section Quiz

15.3 Incident Response - Eradication and Recovery



-  15.3.1 Eradication (4:13)
-  15.3.2 Eradication Facts
-  15.3.3 Wipe Disk Space (7:20)
-  15.3.4 Wipe an Entire Disk with Darik's Nuke (9:37)
-  15.3.5 Recovery (3:55)
-  15.3.6 Recovery Facts
-  15.3.7 Recover Deleted Files with Recuva (2:46)
-  15.3.8 Post-Incident Activities (4:38)
-  15.3.9 Post-Incident Activities Facts
-  15.3.10 Section Quiz

15.4 Indicators of Compromise

-  15.4.1 Network-Related Indicators of Compromise (5:14)
-  15.4.2 Network-Related Indicators of Compromise Facts
-  15.4.3 Create a DNS Tunnel with dnscat2 (4:58)
-  15.4.4 Host-Related Indicators of Compromise (7:42)
-  15.4.5 Host-Related Indicators of Compromise Facts
-  15.4.6 View Process Information
-  15.4.7 Application-Related Indicators of Compromise (3:50)
-  15.4.8 Application-Related Indicators of Compromise Facts
-  15.4.9 Section Quiz

A.0 TESTOUT CYBERDEFENSE PRO PRACTICE EXAMS

A.1 Prepare for TestOut CyberDefense Pro Certification

-  A.1.1 Pro Exam Objectives
-  A.1.2 Pro Objectives by Course Section

📖 A.1.3 How to take the Pro Exam

📖 A.1.4 Pro Exam FAQs

A.2 TestOut CyberDefense Pro Domain Review

📖 A.2.1 Pro Domain 1: Monitoring and Log Analysis

📖 A.2.2 Pro Domain 2: Threat Analysis and Detection

📖 A.2.3 Pro Domain 3: Risk Analysis and Mitigation

📖 A.2.4 Pro Domain 4: Incident Response

📖 A.2.5 Pro Domain 5: Audit and Compliance

📖 A.3 TestOut CyberDefense Pro Certification Practice Exam

B.0 COMPTIA CYSA+ CS0-002 - PRACTICE EXAMS

B.1 Prepare for CompTIA CySA+ Certification

📖 B.1.1 CompTIA CySA+ CS0-002 Exam Objectives

📖 B.1.2 CompTIA CySA+ CS0-002 Objectives by Course Section

📖 B.1.3 How to take the CySA+ CS0-002 Exam

📖 B.1.4 CySA+ CS0-002 Exam FAQs

📖 B.1.5 Hints and Tips for taking the CySA+ CS0-002 Exam

B.2 CompTIA CySA+ CS0-002 Practice Exams (20 Questions)

📖 B.2.1 CySA+ CS0-002 Domain 1: Threat and Vulnerability Management

📖 B.2.2 CySA+ CS0-002 Domain 2: Software and Systems Security

📖 B.2.3 CySA+ CS0-002 Domain 3: Security Operations and Monitoring

📖 B.2.4 CySA+ CS0-002 Domain 4: Incident Response

📖 B.2.5 CySA+ CS0-002 Domain 5: Compliance and Assessment

B.3 CompTIA CySA+ CS0-002 Practice Exams (All Questions)

📖 B.3.1 CySA+ CS0-002 Domain 1: Threat and Vulnerability Management

📖 B.3.2 CySA+ CS0-002 Domain 2: Software and Systems Security

📖 B.3.3 CySA+ CS0-002 Domain 3: Security Operations and Monitoring

📖 B.3.4 CySA+ CS0-002 Domain 4: Incident Response

📖 B.3.5 CySA+ CS0-002 Domain 5: Compliance and Assessment

📖 B.4 CompTIA CySA+ CS0-002 Certification Practice Exam