TestOut®

TestOut Security Pro - English 7.0.x

COURSE OUTLINE

Modified 2020-11-17

Powered by LABSIM

TestOut Security Pro Outline - English 7.0.x

- Videos: 166 (17:20:42)
- Demonstrations: 126 (12:38:35)
- Simulations: 85
- Fact Sheets: 146
- Exams: 95

CONTENTS:

Copyright © 2020 TestOut Corporation. CompTIA, A+, Network+, Security+, Linux+, IT Fundamentals, Cybersecurity Analyst (CySA+), and related trademarks are the trademarks of CompTIA. Microsoft, MCITP, MSCA, MCTS, Office, and Windows are the trademarks of Microsoft. Cisco and CCNA are the trademarks of Cisco. Certified Ethical Hacker and CEH are the trademarks of the EC-Council. TestOut has no affiliation with these companies and the products and services advertised herein are not endorsed by any of them.

2.2 Malware

- 2.2.1 Malware (7:41)
- 2.2.2 Malware Facts
- 2.2.3 Malware Protection Facts
- 2.2.4 Implementing Malware Protections (5:05)
- 2.2.5 Use Windows Security (7:12)
- 2.2.6 Configure Microsoft Defender
- 2.2.7 Section Quiz

2.3 Social Engineering

- 2.3.1 Social Engineering Overview (4:47)
- 2.3.2 Social Engineering Overview Facts
- 2.3.3 Social Engineering Motivation (10:19)
- 2.3.4 Social Engineering Motivation Facts
- 2.3.5 Social Engineering Techniques (10:17)
- 2.3.6 Social Engineering Techniques Facts
- 2.3.7 Phishing and Internet-Based Techniques (5:00)
- 2.3.8 Phishing and Internet-Based Techniques Facts
- 2.3.9 Use the Social Engineer Toolkit (4:25)
- 2.3.10 Investigating a Social Engineering Attack (6:31)
- 2.3.11 Identify Social Engineering
- 2.3.12 Section Quiz

2.4 Vulnerability Concerns

- 2.4.1 Vulnerability Concerns (6:56)
- 2.4.2 Vulnerability Concerns Facts
- 2.4.3 Impact of Vulnerabilities (4:29)
- 2.4.4 Impact of Vulnerabilities Facts
- 2.4.5 Section Quiz

3.0 PHYSICAL

3.1 Physical Threats

- 3.1.1 Physical Security (6:26)
- 3.1.2 Physical Security Facts
- 3.1.3 Implement Physical Security
- 3.1.4 Section Quiz

3.2 Device and Network Protection

- 3.2.1 Hardware Security Guidelines (4:38)
- 3.2.2 Hardware Security Facts

Copyright © 2020 TestOut Corporation. CompTIA, A+, Network+, Security+, Linux+, IT Fundamentals, Cybersecurity Analyst (CySA+), and related trademarks are the trademarks of CompTIA. Microsoft, MCITP, MSCA, MCTS, Office, and Windows are the trademarks of Microsoft. Cisco and CCNA are the trademarks of Cisco. Certified Ethical Hacker and CEH are the trademarks of the EC-Council. TestOut has no affiliation with these companies and the products and services advertised herein are not endorsed by any of them.

- 3.2.3 Physical Network Protection (4:49)
- 3.2.4 Physical Network Protection Facts
- 3.2.5 Section Quiz

3.3 Environmental Controls

- 3.3.1 Environmental Controls (7:42)
- 3.3.2 Securing Environmental Systems (2:19)
- 3.3.3 Environmental Control Facts
- 3.3.4 Fire Protection Facts
- 3.3.5 Section Quiz

4.0 NETWORKS AND HOSTS DESIGN AND DIAGNOSIS

4.1 Manageable Network Plan

- 4.1.1 Manageable Network Plan (8:46)
- 4.1.2 Manageable Network Plan 2 (8:27)
- 4.1.3 Manageable Network Plan Facts
- 4.1.4 Section Quiz

4.2 Windows System Hardening

- 4.2.1 Operating System Hardening (7:58)
- 4.2.2 Hardening Facts
- 4.2.3 Hardening an Operating System (6:39)
- 4.2.4 Managing Automatic Updates (5:16)
- 4.2.5 Configure Automatic Updates
- 4.2.6 Configuring Microsoft Defender Firewall (6:42)
- 4.2.7 Configure Microsoft Defender Firewall
- 4.2.8 Configuring Windows Defender with Firewall Advanced Security (10:58)
- 4.2.9 Section Quiz

4.3 File Server Security

- 4.3.1 File Server Security (6:39)
- 4.3.2 File System Security Facts
- 4.3.3 File Permission Facts
- 4.3.4 Configuring NTFS Permissions (11:14)
- 4.3.5 Configure NTFS Permissions
- 4.3.6 Disable Inheritance
- 4.3.7 Section Quiz

4.4 Linux Host Security

- 4.4.1 Linux Host Security (14:12)
- 4.4.2 Removing Unnecessary Services (4:03)

Copyright © 2020 TestOut Corporation. CompTIA, A+, Network+, Security+, Linux+, IT Fundamentals, Cybersecurity Analyst (CySA+), and related trademarks are the trademarks of CompTIA. Microsoft, MCITP, MSCA, MCTS, Office, and Windows are the trademarks of Microsoft. Cisco and CCNA are the trademarks of Cisco. Certified Ethical Hacker and CEH are the trademarks of the EC-Council. TestOut has no affiliation with these companies and the products and services advertised herein are not endorsed by any of them.

- 4.4.3 Linux Host Security Facts
- 4.4.4 Configure iptables (4:03)
- 4.4.5 Configure iptables Facts
- 4.4.6 Section Quiz

5.0 DEVICES AND INFRASTRUCTURE

5.1 Security Appliances

- 5.1.1 Security Solutions (6:23)
- 5.1.2 Security Zones (6:31)
- 5.1.3 Security Zone Facts
- 5.1.4 All-In-One Security Appliances (4:14)
- 5.1.5 Security Solution Facts
- 5.1.6 Configuring Network Security Appliance Access (7:48)
- 5.1.7 Configure a Security Appliance
- 5.1.8 Configure Network Security Appliance Access
- 5.1.9 Configure QoS (7:39)
- 5.1.10 Configure QoS
- 5.1.11 Attack Deception (8:31)
- 5.1.12 Detect Malicious Network Traffic with a Honeypot (3:24)
- 5.1.13 Section Quiz

5.2 Demilitarized Zones

- 5.2.1 Demilitarized Zones (6:50)
- 5.2.2 Configuring a DMZ (3:26)
- 5.2.3 Configure a DMZ
- 5.2.4 DMZ Facts
- 5.2.5 Section Quiz

5.3 Firewalls

- 5.3.1 Firewalls (8:39)
- 5.3.2 Firewall Facts
- 5.3.3 Configuring Firewall Rules (6:50)
- 5.3.4 Configure Firewall Schedules (6:11)
- 5.3.5 Configure a Perimeter Firewall
- 5.3.6 Section Quiz

5.4 Network Address Translation

- 5.4.1 Network Address Translation (9:54)
- 5.4.2 Configure NAT (9:39)
- 5.4.3 Configure NAT

Copyright © 2020 TestOut Corporation. CompTIA, A+, Network+, Security+, Linux+, IT Fundamentals, Cybersecurity Analyst (CySA+), and related trademarks are the trademarks of CompTIA. Microsoft, MCITP, MSCA, MCTS, Office, and Windows are the trademarks of Microsoft. Cisco and CCNA are the trademarks of Cisco. Certified Ethical Hacker and CEH are the trademarks of the EC-Council. TestOut has no affiliation with these companies and the products and services advertised herein are not endorsed by any of them.

- 5.4.4 NAT Facts
- 5.4.5 Section Quiz

5.5 Virtual Private Networks

- 5.5.1 Virtual Private Networks (7:04)
- 5.5.2 Configuring a VPN (9:13)
- 5.5.3 Configuring a VPN Client (2:41)
- 5.5.4 Configure a Remote Access VPN
- 5.5.5 Configure a VPN Connection iPad
- 5.5.6 VPN Facts
- 5.5.7 VPN Protocol Facts
- 5.5.8 Section Quiz

5.6 Web Threat Protection

- 5.6.1 Web Threat Protection (6:15)
- 5.6.2 Configuring Web Threat Protection (7:24)
- 5.6.3 Configure URL Blocking
- 5.6.4 Web Threat Protection Facts
- 5.6.5 Section Quiz

5.7 Network Access Control

- 5.7.1 Network Access Control (6:32)
- 5.7.2 Network Access Control Facts
- 5.7.3 Section Quiz

5.8 Network Threats

- 5.8.1 Network Threats Overview (8:26)
- 5.8.2 Network Threats Facts
- 5.8.3 Section Quiz

5.9 Network Device Vulnerabilities

- 5.9.1 Device Vulnerabilities (6:57)
- 5.9.2 Device Vulnerability Facts
- 5.9.3 Searching for Default Passwords (2:56)
- 5.9.4 Unauthorized SSH Connection (4:21)
- 5.9.5 Securing a Switch (2:57)
- 5.9.6 Secure a Switch
- 5.9.7 Section Quiz

5.10 Network Applications

- 5.10.1 Network Application Security (4:59)
- 5.10.2 Configuring Application Control Software (7:48)

Copyright © 2020 TestOut Corporation. CompTIA, A+, Network+, Security+, Linux+, IT Fundamentals, Cybersecurity Analyst (CySA+), and related trademarks are the trademarks of CompTIA. Microsoft, MCITP, MSCA, MCTS, Office, and Windows are the trademarks of Microsoft. Cisco and CCNA are the trademarks of Cisco. Certified Ethical Hacker and CEH are the trademarks of the EC-Council. TestOut has no affiliation with these companies and the products and services advertised herein are not endorsed by any of them.

- 5.10.3 Network Application Facts
- 5.10.4 Section Quiz

5.11 Switch Security and Attacks

- 5.11.1 Switch Features (9:31)
- 5.11.2 Securing Network Switches (7:29)
- 5.11.3 Switch Security Facts
- 5.11.4 Switch Attacks (11:16)
- 5.11.5 Use SMAC to Spoof MAC Addresses (3:46)
- 5.11.6 Spoof MAC Addresses with SMAC
- 5.11.7 Switch Attack Facts
- 5.11.8 Hardening a Switch (10:38)
- 5.11.9 Harden a Switch
- 5.11.10 Secure Access to a Switch
- 5.11.11 Secure Access to a Switch 2
- 5.11.12 Section Quiz

5.12 Using VLANs

- 5.12.1 VLAN Overview (4:39)
- 5.12.2 VLAN Facts
- 5.12.3 Configuring VLANs (3:11)
- 5.12.4 Explore VLANs
- 5.12.5 Section Quiz

5.13 Router Security

- 5.13.1 Router Security (7:04)
- 5.13.2 Router ACLs (2:50)
- 5.13.3 Router Security Facts
- 5.13.4 Configuring ACLs (7:12)
- 5.13.5 Restrict Telnet and SSH Access
- 5.13.6 Permit Traffic
- 5.13.7 Block Source Hosts
- 5.13.8 Section Quiz

6.0 IDENTITY, ACCESS, AND ACCOUNT MANAGEMENT

6.1 Access Control Models

- 6.1.1 Identity and Access Management (6:01)
- 6.1.2 Authentication, Authorization, and Accounting (5:01)
- 6.1.3 Access Control Facts
- 6.1.4 Access Control Best Practices

Copyright © 2020 TestOut Corporation. CompTIA, A+, Network+, Security+, Linux+, IT Fundamentals, Cybersecurity Analyst (CySA+), and related trademarks are the trademarks of CompTIA. Microsoft, MCITP, MSCA, MCTS, Office, and Windows are the trademarks of Microsoft. Cisco and CCNA are the trademarks of Cisco. Certified Ethical Hacker and CEH are the trademarks of the EC-Council. TestOut has no affiliation with these companies and the products and services advertised herein are not endorsed by any of them.

- 6.1.5 Access Control Models (5:08)
- 6.1.6 Access Control Model Facts
- 6.1.7 Implementing Dynamic Access Control (8:12)
- 6.1.8 Section Quiz

6.2 Authentication

- 6.2.1 Authentication (5:23)
- 6.2.2 Authentication Methods (6:11)
- 6.2.3 Authentication Facts
- 6.2.4 Biometrics and Authentication Technologies (4:20)
- 6.2.5 Using a Biometric Scanner (2:48)
- 6.2.6 Using Single Sign-on (4:39)
- 6.2.7 Biometrics and Authentication Technologies Facts
- 6.2.8 Section Quiz

6.3 Authorization

- 6.3.1 Authorization (3:22)
- 6.3.2 Cumulative Access (3:03)
- 6.3.3 Authorization Facts
- 6.3.4 Examining the Access Token (7:52)
- 6.3.5 Section Quiz

6.4 Windows User Management

- 6.4.1 Windows Operating System Roles (12:29)
- 6.4.2 Windows Operating System Roles Facts
- 6.4.3 Using Local User Accounts for Sign-in (5:27)
- 6.4.4 Join a Workgroup (5:14)
- 6.4.5 Using Online User Accounts for Sign-in (4:32)
- 6.4.6 Using Domain User Accounts for Sign-in (4:38)
- 6.4.7 Using Azure AD User Accounts for Sign-in (3:46)
- 6.4.8 Windows User Management Facts
- 6.4.9 Section Quiz

6.5 Active Directory Overview

- 6.5.1 Active Directory Introduction (8:21)
- 6.5.2 Joining a Domain (7:49)
- 6.5.3 Managing Active Directory Objects (9:25)
- 6.5.4 Active Directory Facts
- 6.5.5 Create OUs
- 6.5.6 Delete OUs
- 6.5.7 Group Policy (8:51)

Copyright © 2020 TestOut Corporation. CompTIA, A+, Network+, Security+, Linux+, IT Fundamentals, Cybersecurity Analyst (CySA+), and related trademarks are the trademarks of CompTIA. Microsoft, MCITP, MSCA, MCTS, Office, and Windows are the trademarks of Microsoft. Cisco and CCNA are the trademarks of Cisco. Certified Ethical Hacker and CEH are the trademarks of the EC-Council. TestOut has no affiliation with these companies and the products and services advertised herein are not endorsed by any of them.

- 6.5.8 Using Group Policy (7:06)
- 6.5.9 Group Policy Facts
- 6.5.10 Create and Link a GPO
- 6.5.11 Create User Accounts
- 6.5.12 Manage User Accounts
- 6.5.13 Create a Group
- 6.5.14 Create Global Groups
- 6.5.15 Section Quiz

6.6 Hardening Authentication

- 6.6.1 Hardening Authentication (7:59)
- 6.6.2 Configuring User Account Restrictions (4:21)
- 6.6.3 Configuring Account Policies and UAC Settings (6:07)
- 6.6.4 Configure Account Password Policies
- 6.6.5 Hardening User Accounts (6:57)
- 6.6.6 Restrict Local Accounts
- 6.6.7 Secure Default Accounts
- 6.6.8 Enforce User Account Control
- 6.6.9 Hardening Authentication Facts
- 6.6.10 Configuring Smart Card Authentication (5:38)
- 6.6.11 Configure Smart Card Authentication
- 6.6.12 Smart Card Authentication Facts
- 6.6.13 Section Quiz

6.7 Linux Users

- 6.7.1 Linux User and Group Overview (11:14)
- 6.7.2 Managing Linux Users (8:00)
- 6.7.3 Linux User Commands and Files
- 6.7.4 Create a User Account
- 6.7.5 Rename a User Account
- 6.7.6 Delete a User
- 6.7.7 Change Your Password
- 6.7.8 Change a User's Password
- 6.7.9 Lock and Unlock User Accounts
- 6.7.10 Linux User Security and Restrictions (7:15)
- 6.7.11 Configuring Linux User Security and Restrictions (7:18)
- 6.7.12 Linux User Security and Restriction Facts
- 6.7.13 Section Quiz

6.8 Linux Groups

Copyright © 2020 TestOut Corporation. CompTIA, A+, Network+, Security+, Linux+, IT Fundamentals, Cybersecurity Analyst (CySA+), and related trademarks are the trademarks of CompTIA. Microsoft, MCITP, MSCA, MCTS, Office, and Windows are the trademarks of Microsoft. Cisco and CCNA are the trademarks of Cisco. Certified Ethical Hacker and CEH are the trademarks of the EC-Council. TestOut has no affiliation with these companies and the products and services advertised herein are not endorsed by any of them.

- 6.8.1 Managing Linux Groups (6:14)
- 6.8.2 Linux Group Commands
- 6.8.3 Rename and Create Groups
- 6.8.4 Add Users to a Group
- 6.8.5 Remove a User from a Group
- 6.8.6 Section Quiz

6.9 Remote Access

- 6.9.1 Remote Access (9:24)
- 6.9.2 Remote Access Facts
- 6.9.3 Configuring a RADIUS Solution (2:52)
- 6.9.4 RADIUS and TACACS+ Facts
- 6.9.5 Section Quiz

6.10 Network Authentication

- 6.10.1 Network Authentication Protocols (7:46)
- 6.10.2 Network Authentication Facts
- 6.10.3 LDAP Authentication (3:00)
- 6.10.4 Kerberos Authentication (5:20)
- 6.10.5 Controlling the Authentication Method (5:11)
- 6.10.6 Configure Kerberos Policy Settings
- 6.10.7 Credential Management (4:19)
- 6.10.8 Credential Management Facts
- 6.10.9 Section Quiz

7.0 CRYPTOGRAPHY AND PKI

7.1 Cryptography

- 7.1.1 Cryptography Concepts (7:03)
- 7.1.2 Cryptography Facts
- 7.1.3 Symmetric vs Asymmetric Encryption (10:47)
- 7.1.4 Cracking a Symmetric Encryption Key (4:49)
- 7.1.5 Symmetric and Asymmetric Encryption Facts
- 7.1.6 Cryptography Algorithm (9:23)
- 7.1.7 Cryptography Algorithms Facts
- 7.1.8 Blockchain (3:35)
- 7.1.9 Blockchain Facts
- 7.1.10 Use Steganography to Hide a File (3:21)
- 7.1.11 Hide Files with OpenStego
- 7.1.12 Cryptographic Attacks (4:32)

Copyright © 2020 TestOut Corporation. CompTIA, A+, Network+, Security+, Linux+, IT Fundamentals, Cybersecurity Analyst (CySA+), and related trademarks are the trademarks of CompTIA. Microsoft, MCITP, MSCA, MCTS, Office, and Windows are the trademarks of Microsoft. Cisco and CCNA are the trademarks of Cisco. Certified Ethical Hacker and CEH are the trademarks of the EC-Council. TestOut has no affiliation with these companies and the products and services advertised herein are not endorsed by any of them.

- 7.1.13 Cryptographic Attack Facts
- 7.1.14 Section Quiz

7.2 Cryptography Implementations

- 7.2.1 Cryptography Uses and Limitations (4:16)
- 7.2.2 Cryptography Uses and Limitations Facts
- 7.2.3 Combining Cryptographic Methods (4:44)
- 7.2.4 Hardware-Based Encryption Devices (3:16)
- 7.2.5 Cryptographic Implementation Facts
- 7.2.6 Section Quiz

7.3 Hashing

- 7.3.1 Hashing (5:36)
- 7.3.2 Hashing Algorithms (3:37)
- 7.3.3 Hashing Facts
- 7.3.4 Using Hashes (4:54)
- 7.3.5 Compare an MD5 Hash
- 7.3.6 Section Quiz

7.4 File Encryption

- 7.4.1 Encrypting File System (3:52)
- 7.4.2 Securing Files using EFS (8:14)
- 7.4.3 Encrypt Files with EFS
- 7.4.4 PGP and GPG (2:31)
- 7.4.5 Encrypting Files with GPG (3:28)
- 7.4.6 BitLocker and Database Encryption (5:31)
- 7.4.7 Configuring BitLocker (6:58)
- 7.4.8 Configure BitLocker with a TPM
- 7.4.9 File Encryption Facts
- 7.4.10 Section Quiz

7.5 Public Key Infrastructure

- 7.5.1 Public Key Infrastructure (5:16)
- 7.5.2 Public Key Infrastructure Facts
- 7.5.3 Certificate Types (4:10)
- 7.5.4 Certificate Types Facts
- 7.5.5 Manage Certificates (12:15)
- 7.5.6 Manage Certificates
- 7.5.7 Extended Validation (4:34)
- 7.5.8 Extended Validation Facts
- 7.5.9 Certificate Concepts (7:40)

Copyright © 2020 TestOut Corporation. CompTIA, A+, Network+, Security+, Linux+, IT Fundamentals, Cybersecurity Analyst (CySA+), and related trademarks are the trademarks of CompTIA. Microsoft, MCITP, MSCA, MCTS, Office, and Windows are the trademarks of Microsoft. Cisco and CCNA are the trademarks of Cisco. Certified Ethical Hacker and CEH are the trademarks of the EC-Council. TestOut has no affiliation with these companies and the products and services advertised herein are not endorsed by any of them.

- 7.5.10 Certificate Concepts Facts
- 7.5.11 Section Quiz

8.0 WIRELESS THREATS

8.1 Wireless Overview

- 8.1.1 Wireless Networking Overview (6:00)
- 8.1.2 Wireless Installation (3:26)
- 8.1.3 Wireless Networking Facts
- 8.1.4 Configuring a Wireless Connection (5:44)
- 8.1.5 Configure a Wireless Network
- 8.1.6 Section Quiz

8.2 Wireless Attacks

- 8.2.1 Wireless Attacks (7:39)
- 8.2.2 Wireless Attack Facts
- 8.2.3 Using Wireless Attack Tools (7:06)
- 8.2.4 Crack Wi-Fi Encryption with Aricrack-ng (5:41)
- 8.2.5 Detecting Rogue Hosts (3:46)
- 8.2.6 Configure Rogue Host Protection
- 8.2.7 Section Quiz

8.3 Wireless Defenses

- 8.3.1 Wireless Security (6:23)
- 8.3.2 Wireless Security Facts
- 8.3.3 Wireless Authentication and Access Methods (7:36)
- 8.3.4 Wireless Authentication and Access Methods Facts
- 8.3.5 Hardening a Wireless Access Point (7:50)
- 8.3.6 Harden a Wireless Network
- 8.3.7 Configure WIPS
- 8.3.8 Configuring a Captive Portal (6:21)
- 8.3.9 Configuring a Captive Portal
- 8.3.10 Section Quiz

9.0 VIRTUALIZATION, CLOUD SECURITY, AND SECURING MOBILE DEVICES

9.1 Host Virtualization

- 9.1.1 Host Virtualization Overview (10:11)
- 9.1.2 Load Balancing with Virtualization (6:11)
- 9.1.3 Virtualization Facts
- 9.1.4 Creating Virtual Machines (6:45)

Copyright © 2020 TestOut Corporation. CompTIA, A+, Network+, Security+, Linux+, IT Fundamentals, Cybersecurity Analyst (CySA+), and related trademarks are the trademarks of CompTIA. Microsoft, MCITP, MSCA, MCTS, Office, and Windows are the trademarks of Microsoft. Cisco and CCNA are the trademarks of Cisco. Certified Ethical Hacker and CEH are the trademarks of the EC-Council. TestOut has no affiliation with these companies and the products and services advertised herein are not endorsed by any of them.

- 9.1.5 Managing Virtual Machines (6:01)
- 9.1.6 Create Virtual Machines
- 9.1.7 Adding Virtual Network Adapters (3:47)
- 9.1.8 Section Quiz

9.2 Virtual Networking

- 9.2.1 Virtual Networking Overview (6:21)
- 9.2.2 Virtual Network Devices (4:14)
- 9.2.3 Configuring Virtual Network Devices (3:19)
- 9.2.4 Virtualization Implementation Facts
- 9.2.5 Virtual Networking Facts
- 9.2.6 Create Virtual Switches
- 9.2.7 Section Quiz

9.3 Software-Defined Networking

- 9.3.1 Software-Defined Networking Basics (3:34)
- 9.3.2 SDN Infrastructure and Architecture (2:38)
- 9.3.3 SDN Facts
- 9.3.4 Section Quiz

9.4 Cloud Services

- 9.4.1 Cloud Services Introduction (9:35)
- 9.4.2 Enhancing Cloud Performance (10:29)
- 9.4.3 Cloud Computing Security Issues (5:44)
- 9.4.4 Cloud Computing Facts
- 9.4.5 Cloud Storage Security Facts
- 9.4.6 Section Quiz

9.5 Cloud Security

- 9.5.1 Cloud Security Controls (Part 1) (5:25)
- 9.5.2 Cloud Security Controls (Part 2) (5:57)
- 9.5.3 Cloud Security Controls Facts
- 9.5.4 Cloud Security Solutions (6:16)
- 9.5.5 Cloud Security Solutions Facts
- 9.5.6 Section Quiz

9.6 Mobile Devices

- 9.6.1 Mobile Device Connection Methods (4:55)
- 9.6.2 Mobile Device Connection Facts
- 9.6.3 Enforcing Mobile Device Security (6:57)
- 9.6.4 Enforcing Mobile Device Security Facts

Copyright © 2020 TestOut Corporation. CompTIA, A+, Network+, Security+, Linux+, IT Fundamentals, Cybersecurity Analyst (CySA+), and related trademarks are the trademarks of CompTIA. Microsoft, MCITP, MSCA, MCTS, Office, and Windows are the trademarks of Microsoft. Cisco and CCNA are the trademarks of Cisco. Certified Ethical Hacker and CEH are the trademarks of the EC-Council. TestOut has no affiliation with these companies and the products and services advertised herein are not endorsed by any of them.

- 9.6.5 Enforcing Security Policies on Mobile Devices (3:02)
- 9.6.6 Sideload an App (6:45)
- 9.6.7 Section Quiz

9.7 Mobile Device Management

- 9.7.1 Mobile Device Management (4:46)
- 9.7.2 Mobile Device Management Facts
- 9.7.3 Enroll Devices and Perform a Remote Wipe (7:41)
- 9.7.4 Enrolling non-Windows Devices (2:27)
- 9.7.5 Mobile Application Management (4:03)
- 9.7.6 Mobile Application Management Facts
- 9.7.7 Section Quiz

9.8 BYOD Security

- 9.8.1 BYOD Security Issues (10:21)
- 9.8.2 BYOD Security Facts
- 9.8.3 Securing Mobile Devices (7:23)
- 9.8.4 Secure an iPad
- 9.8.5 Creating a Guest Network for BYOD (7:30)
- 9.8.6 Create a Guest Network for BYOD
- 9.8.7 Section Quiz

9.9 Embedded and Specialized Systems

- 9.9.1 Embedded and Specialized Systems (8:20)
- 9.9.2 Smart Home (7:03)
- 9.9.3 Constraints and Security of Embedded Devices (4:49)
- 9.9.4 Communication of Embedded Systems (6:33)
- 9.9.5 Embedded and Specialized Systems Facts
- 9.9.6 Section Quiz

10.0 SECURING DATA AND APPLICATIONS

10.1 Data Transmission Security

- 10.1.1 Secure Protocols (7:46)
- 10.1.2 Secure Protocols 2 (6:33)
- 10.1.3 Secure Protocol Facts
- 10.1.4 Adding SSL to a Website (6:00)
- 10.1.5 Allow SSL Connections
- 10.1.6 IPsec (6:08)
- 10.1.7 IPsec Facts
- 10.1.8 Requiring IPsec for Communications (11:57)

Copyright © 2020 TestOut Corporation. CompTIA, A+, Network+, Security+, Linux+, IT Fundamentals, Cybersecurity Analyst (CySA+), and related trademarks are the trademarks of CompTIA. Microsoft, MCITP, MSCA, MCTS, Office, and Windows are the trademarks of Microsoft. Cisco and CCNA are the trademarks of Cisco. Certified Ethical Hacker and CEH are the trademarks of the EC-Council. TestOut has no affiliation with these companies and the products and services advertised herein are not endorsed by any of them.

- 10.1.9 Section Quiz

10.2 Data Loss Prevention

- 10.2.1 Data Loss Prevention (6:52)
- 10.2.2 DLP Facts
- 10.2.3 Section Quiz

10.3 Web Application Attacks

- 10.3.1 Web Application Attacks 1 (7:18)
- 10.3.2 Web Application Attacks 2 (10:02)
- 10.3.3 XSS and CSRF Attacks (9:42)
- 10.3.4 Injection Attacks (4:01)
- 10.3.5 Header Manipulation (5:06)
- 10.3.6 Zero Day Application Attacks (3:19)
- 10.3.7 Client-Side Attacks (3:27)
- 10.3.8 Web Browser Threats (8:02)
- 10.3.9 Web Browser Security Facts
- 10.3.10 Clear the Browser Cache
- 10.3.11 Preventing Cross-Site Scripting (4:49)
- 10.3.12 SQL Injections (5:54)
- 10.3.13 Exploit SQL on a Web Page (3:58)
- 10.3.14 Web Application Attack Facts
- 10.3.15 Perform an SQL Injection Attack
- 10.3.16 Section Quiz

10.4 Application Development and Security

- 10.4.1 Development Life Cycle (6:35)
- 10.4.2 Automation and Scripting (6:42)
- 10.4.3 SDLC and Development Facts
- 10.4.4 Version Control Management (3:06)
- 10.4.5 Secure Coding Concepts (6:57)
- 10.4.6 Application Hardening (5:15)
- 10.4.7 Application Development Security Facts
- 10.4.8 Hardening Applications on Linux (4:31)
- 10.4.9 Implementing Application Whitelisting with AppLocker (7:21)
- 10.4.10 Implement Application Whitelisting with AppLocker
- 10.4.11 Implementing Data Execution Preventions (3:37)
- 10.4.12 Implement Data Execution Preventions
- 10.4.13 Hardening Applications Facts
- 10.4.14 Section Quiz

Copyright © 2020 TestOut Corporation. CompTIA, A+, Network+, Security+, Linux+, IT Fundamentals, Cybersecurity Analyst (CySA+), and related trademarks are the trademarks of CompTIA. Microsoft, MCITP, MSCA, MCTS, Office, and Windows are the trademarks of Microsoft. Cisco and CCNA are the trademarks of Cisco. Certified Ethical Hacker and CEH are the trademarks of the EC-Council. TestOut has no affiliation with these companies and the products and services advertised herein are not endorsed by any of them.

11.0 SECURITY ASSESSMENTS

11.1 Penetration Testing

- 11.1.1 Penetration Testing (8:35)
- 11.1.2 Penetration Testing Facts
- 11.1.3 Exploring Penetration Testing Tools (11:33)
- 11.1.4 Section Quiz

11.2 Monitoring and Reconnaissance

- 11.2.1 Network Monitoring (5:56)
- 11.2.2 Network Monitoring Facts
- 11.2.3 Performing Port and Ping Scans (4:47)
- 11.2.4 Reconnaissance (6:32)
- 11.2.5 Performing Reconnaissance (9:11)
- 11.2.6 Perform Reconnaissance with Nmap (4:14)
- 11.2.7 Perform Reconnaissance with the Harvester (4:52)
- 11.2.8 Reconnaissance Facts
- 11.2.9 Section Quiz

11.3 Intrusion Detection

- 11.3.1 Intrusion Detection (4:57)
- 11.3.2 IDS Facts
- 11.3.3 Use Squil and Squert (4:51)
- 11.3.4 Implement Intrusion Detection and Prevention (6:18)
- 11.3.5 Implement Intrusion Prevention
- 11.3.6 Section Quiz

11.4 Security Assessment Techniques

- 11.4.1 Vulnerability Assessment (6:59)
- 11.4.2 Vulnerability Assessment Facts
- 11.4.3 SIEM and SOAR (4:34)
- 11.4.4 SIEM and SOAR Facts
- 11.4.5 Conduct Vulnerability Scans (4:02)
- 11.4.6 Scanning a Network with Nessus (3:17)
- 11.4.7 Scan for Windows Vulnerabilities
- 11.4.8 Scan for Linux Vulnerabilities
- 11.4.9 Scan for Domain Controller Vulnerabilities
- 11.4.10 Scan for IoT Vulnerabilities
- 11.4.11 Scan for WAP Vulnerabilities
- 11.4.12 Section Quiz

Copyright © 2020 TestOut Corporation. CompTIA, A+, Network+, Security+, Linux+, IT Fundamentals, Cybersecurity Analyst (CySA+), and related trademarks are the trademarks of CompTIA. Microsoft, MCITP, MSCA, MCTS, Office, and Windows are the trademarks of Microsoft. Cisco and CCNA are the trademarks of Cisco. Certified Ethical Hacker and CEH are the trademarks of the EC-Council. TestOut has no affiliation with these companies and the products and services advertised herein are not endorsed by any of them.

11.5 Protocol Analyzers

- 11.5.1 Protocol Analyzers (3:46)
- 11.5.2 Protocol Analyzer Facts
- 11.5.3 Analyzing Network Traffic (6:47)
- 11.5.4 Section Quiz

11.6 Analyzing Network Attacks

- 11.6.1 Analyzing Network Attacks (7:51)
- 11.6.2 Analyzing Network Attacks Facts
- 11.6.3 Performing ARP Poisoning (5:15)
- 11.6.4 Poison ARP and Analyze with Wireshark
- 11.6.5 Performing DNS Poisoning (6:18)
- 11.6.6 Poison DNS
- 11.6.7 Performing a SYN Flood (6:20)
- 11.6.8 Perform and Analyze a SYN Flood
- 11.6.9 Examining DNS Attacks (11:57)
- 11.6.10 Malicious Code (7:09)
- 11.6.11 Malicious Code Facts
- 11.6.12 Section Quiz

11.7 Password Attacks

- 11.7.1 Password Attacks (7:26)
- 11.7.2 Password Attack Facts
- 11.7.3 Using Rainbow Tables (3:34)
- 11.7.4 Crack Password with Rainbow Tables
- 11.7.5 Crack Passwords (8:03)
- 11.7.6 Crack Password Protected Files (3:23)
- 11.7.7 Crack a Password with John the Ripper
- 11.7.8 Section Quiz

12.0 INCIDENT RESPONSE, FORENSICS, AND RECOVERY

12.1 Incident Response

- 12.1.1 Incident Response Process (4:58)
- 12.1.2 Incident Response Process Facts
- 12.1.3 Incident Response Frameworks and Management (3:28)
- 12.1.4 Incident Response Frameworks and Management Facts
- 12.1.5 Section Quiz

12.2 Mitigation of an Incident

- 12.2.1 Reconfigure and Protect Endpoints (4:17)

Copyright © 2020 TestOut Corporation. CompTIA, A+, Network+, Security+, Linux+, IT Fundamentals, Cybersecurity Analyst (CySA+), and related trademarks are the trademarks of CompTIA. Microsoft, MCITP, MSCA, MCTS, Office, and Windows are the trademarks of Microsoft. Cisco and CCNA are the trademarks of Cisco. Certified Ethical Hacker and CEH are the trademarks of the EC-Council. TestOut has no affiliation with these companies and the products and services advertised herein are not endorsed by any of them.

- 12.2.2 Reconfigure and Protect Endpoints Facts
- 12.2.3 Isolate and Containment (3:01)
- 12.2.4 Isolate and Containment Facts
- 12.2.5 Section Quiz

12.3 Log Management

- 12.3.1 Security Information and Event Management (3:35)
- 12.3.2 Log Management (6:50)
- 12.3.3 SIEM and Log Management Facts
- 12.3.4 Monitoring Data and Metadata (6:09)
- 12.3.5 Saving Captured Files with Wireshark (3:53)
- 12.3.6 Use Elasticsearch Logstash Kibana (4:43)
- 12.3.7 Use NetworkMiner (3:38)
- 12.3.8 Configuring Remote Logging on Linux (6:31)
- 12.3.9 Logging Events on pfSense (6:00)
- 12.3.10 Monitoring Data and Metadata Facts
- 12.3.11 Section Quiz

12.4 Windows Logging

- 12.4.1 Windows Event Subscriptions (5:48)
- 12.4.2 Configuring Collector-Initiated Subscriptions (6:01)
- 12.4.3 Configuring Source-Initiated Subscriptions (7:46)
- 12.4.4 Windows Event Subscriptions Facts
- 12.4.5 Logging Events with Event Viewer (5:17)
- 12.4.6 Section Quiz

12.5 Digital Forensics

- 12.5.1 Forensic Documentation and Evidence (7:33)
- 12.5.2 Forensic Acquisition of Data (5:43)
- 12.5.3 Forensic Tools (2:26)
- 12.5.4 Create a Forensic Drive Image with FTK (7:26)
- 12.5.5 Create a Forensic Drive Image with Guymager (5:27)
- 12.5.6 Create a Forensic Drive Image with DC3DD (6:03)
- 12.5.7 Examine a Forensic Drive Image with Autopsy (6:12)
- 12.5.8 Forensic Data Integrity and Preservation (4:42)
- 12.5.9 Forensic Investigation Facts
- 12.5.10 Section Quiz

12.6 File and Packet Manipulation

- 12.6.1 Manipulating Files (11:25)
- 12.6.2 Manipulating Files Facts

Copyright © 2020 TestOut Corporation. CompTIA, A+, Network+, Security+, Linux+, IT Fundamentals, Cybersecurity Analyst (CySA+), and related trademarks are the trademarks of CompTIA. Microsoft, MCITP, MSCA, MCTS, Office, and Windows are the trademarks of Microsoft. Cisco and CCNA are the trademarks of Cisco. Certified Ethical Hacker and CEH are the trademarks of the EC-Council. TestOut has no affiliation with these companies and the products and services advertised herein are not endorsed by any of them.

- 12.6.3 Shells and Scripting (9:00)
- 12.6.4 Shells and Scripting Facts
- 12.6.5 Packet Capture Manipulation (10:00)
- 12.6.6 Use TcpReplay (2:02)
- 12.6.7 Packet Capture Facts
- 12.6.8 Section Quiz

12.7 Redundancy

- 12.7.1 Redundancy (3:24)
- 12.7.2 Redundancy Facts
- 12.7.3 RAID (4:39)
- 12.7.4 Implementing RAID (6:54)
- 12.7.5 RAID Facts
- 12.7.6 Configure Fault-Tolerant Volumes
- 12.7.7 Hardware Clustering (7:53)
- 12.7.8 Clustering Facts
- 12.7.9 Section Quiz

12.8 Backup and Restore

- 12.8.1 Backup Types (10:16)
- 12.8.2 Backup Storage Options (3:23)
- 12.8.3 Configure Network Attached Storage (7:46)
- 12.8.4 Backup Types and Storage Facts
- 12.8.5 Implementing File Backups (7:42)
- 12.8.6 Back Up Files with File History
- 12.8.7 Demo Recovering Files (3:37)
- 12.8.8 Recover a File from File History
- 12.8.9 Backup a Domain Controller (3:04)
- 12.8.10 Backup a Domain Controller
- 12.8.11 Restoring Server Data from Backup (2:57)
- 12.8.12 Section Quiz

13.0 RISK MANAGEMENT

13.1 Organizational Security Policies

- 13.1.1 Personnel Policies (6:38)
- 13.1.2 Personnel Policy Facts
- 13.1.3 Managing Third Parties (5:27)
- 13.1.4 Managing Third Parties Facts
- 13.1.5 Data Protection and Policies (3:39)

Copyright © 2020 TestOut Corporation. CompTIA, A+, Network+, Security+, Linux+, IT Fundamentals, Cybersecurity Analyst (CySA+), and related trademarks are the trademarks of CompTIA. Microsoft, MCITP, MSCA, MCTS, Office, and Windows are the trademarks of Microsoft. Cisco and CCNA are the trademarks of Cisco. Certified Ethical Hacker and CEH are the trademarks of the EC-Council. TestOut has no affiliation with these companies and the products and services advertised herein are not endorsed by any of them.

- 13.1.6 Data Protection and Policies Facts
- 13.1.7 Credential and Organizational Policies (3:25)
- 13.1.8 Credential and Organizational Policies Facts
- 13.1.9 Section Quiz

13.2 Risk Management

- 13.2.1 Risk Types and Tolerance (4:48)
- 13.2.2 Risk Types and Tolerance Facts
- 13.2.3 Analyzing Risks (3:01)
- 13.2.4 Analyzing Risks Facts
- 13.2.5 Business Continuity Planning (5:06)
- 13.2.6 Business Continuity Planning Facts
- 13.2.7 Section Quiz

13.3 Email

- 13.3.1 Email Security (6:30)
- 13.3.2 Email Security Facts
- 13.3.3 Protecting a Client from Spam (4:01)
- 13.3.4 Securing an Email Server (2:53)
- 13.3.5 Configure Email Filters
- 13.3.6 Securing Accounts on an iPad (5:01)
- 13.3.7 Secure Email on iPad
- 13.3.8 Section Quiz

14.0 GOVERNANCE AND COMPLIANCE

14.1 Audits

- 14.1.1 Audits (4:35)
- 14.1.2 Audit Facts
- 14.1.3 Auditing the Windows Security Log (8:10)
- 14.1.4 Configure Advanced Audit Policy
- 14.1.5 Auditing Device Logs (3:57)
- 14.1.6 Enable Device Logs
- 14.1.7 Section Quiz

14.2 Controls and Frameworks

- 14.2.1 Control Categories and Types (4:44)
- 14.2.2 Control Categories and Types Facts
- 14.2.3 Security Frameworks (6:51)
- 14.2.4 Security Frameworks Facts
- 14.2.5 Section Quiz

Copyright © 2020 TestOut Corporation. CompTIA, A+, Network+, Security+, Linux+, IT Fundamentals, Cybersecurity Analyst (CySA+), and related trademarks are the trademarks of CompTIA. Microsoft, MCITP, MSCA, MCTS, Office, and Windows are the trademarks of Microsoft. Cisco and CCNA are the trademarks of Cisco. Certified Ethical Hacker and CEH are the trademarks of the EC-Council. TestOut has no affiliation with these companies and the products and services advertised herein are not endorsed by any of them.

14.3 Sensitive Data and Privacy

- 14.3.1 Consequences of Breaches (4:39)
- 14.3.2 Consequences of Breaches Facts
- 14.3.3 Information Classification (4:25)
- 14.3.4 Information Classification Facts
- 14.3.5 Privacy and Responsibility of Data (8:14)
- 14.3.6 Privacy and Responsibility of Data
- 14.3.7 Data Destruction (8:44)
- 14.3.8 Data Destruction Facts
- 14.3.9 File Shredding and Hard Drive Wiping (9:37)
- 14.3.10 Section Quiz

A.0 TESTOUT SECURITY PRO - PRACTICE EXAMS

A.1 Prepare for TestOut Security Pro Certification

- A.1.1 Pro Exam Objectives
- A.1.2 Pro Exam Objectives by Course Section
- A.1.3 How to take the Pro Exam
- A.1.4 Pro Exam FAQs

A.2 TestOut Security Pro Domain Review

- A.2.1 Pro Domain 1: Identity Management and Authentication
- A.2.2 Pro Domain 2: Physical and Network Security
- A.2.3 Pro Domain 3: Host and Application Defense
- A.2.4 Pro Domain 4: Data Security
- A.2.5 Pro Domain 5: Audit and Security Assessment

A.3 TestOut Security Pro Certification Practice Exam

B.0 COMPTIA SECURITY+ SY0-601 - PRACTICE EXAMS

B.1 Prepare for CompTIA Security+ SY0-601 Certification

- B.1.1 Security+ SY0-601 Exam Objectives
- B.1.2 Security+ SY0-601 Exam Objectives by Course Section
- B.1.3 How to take the Security+ SY0-601 Exam
- B.1.4 Security+ SY0-601 FAQs
- B.1.5 Hints and Tips for taking the Security+ SY0-601 Exam

B.2 CompTIA Security+ Domain Review (20 Questions)

- B.2.1 Security+ SY0-601 Domain 1: Attacks, Threats, and Vulnerabilities
- B.2.2 Security+ SY0-601 Domain 2: Architecture and Design
- B.2.3 Security+ SY0-601 Domain 3: Implementation

Copyright © 2020 TestOut Corporation. CompTIA, A+, Network+, Security+, Linux+, IT Fundamentals, Cybersecurity Analyst (CySA+), and related trademarks are the trademarks of CompTIA. Microsoft, MCITP, MSCA, MCTS, Office, and Windows are the trademarks of Microsoft. Cisco and CCNA are the trademarks of Cisco. Certified Ethical Hacker and CEH are the trademarks of the EC-Council. TestOut has no affiliation with these companies and the products and services advertised herein are not endorsed by any of them.

Copyright © 2020 TestOut Corporation. CompTIA, A+, Network+, Security+, Linux+, IT Fundamentals, Cybersecurity Analyst (CySA+), and related trademarks are the trademarks of CompTIA. Microsoft, MCITP, MSCA, MCTS, Office, and Windows are the trademarks of Microsoft. Cisco and CCNA are the trademarks of Cisco. Certified Ethical Hacker and CEH are the trademarks of the EC-Council. TestOut has no affiliation with these companies and the products and services advertised herein are not endorsed by any of them.