TestOut®

TestOut Security Pro - English 6.0.x

COURSE OUTLINE

Modified 2017-10-02

Powered by LABSIM

TestOut Security Pro Outline - English 6.0.0

🎞 Videos: 142 (14:33:02)

🖥 Demonstrations: 109 (12:43:48)

🖱 Simulations: 78

📄 Fact Sheets: 135

📝 Exams: 106

CONTENTS:

1.0 INTRODUCTION

1.1 Security Overview

- 🎞 1.1.1 The Security Landscape (3:50)
- 🎞 1.1.2 Security Concepts (4:14)
- 📄 1.1.3 Security Introduction
- 📝 1.1.4 Practice Questions

1.2 Using the Simulator

- 🖥 1.2.1 Using the Simulator (5:28)
- 🖱 1.2.2 Configure a Security Appliance
- 🖱 1.2.3 Install a Security Appliance

2.0 SECURITY BASICS

2.1 Understanding Attacks

- 🎞 2.1.1 Threat Actor Types (10:15)
- 📄 2.1.2 Threat Agents Overview
- 🎞 2.1.3 General Attack Strategy (6:06)
- 🎞 2.1.4 General Defense Strategy (7:50)
- 📄 2.1.5 Attack and Defense Strategy Overview
- 📝 2.1.6 Practice Questions

2.2 Defense Planning

- 🎞 2.2.1 The Layered Security Model (5:47)
- 🎞 2.2.2 User Education (2:33)
- 📄 2.2.3 Defense Planning Facts
- 📝 2.2.4 Practice Questions

Copyright © 2017 TestOut Corporation. CompTIA, A+, Network+, Security+, Linux+ and related trademarks and trade names 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. TestOut has no affiliation with any of these companies and the products and services advertised herein are not endorsed by any of them.

2.3 Access Control

- 2.3.1 Identity and Access Management (5:52)
- 2.3.2 Authentication, Authorization, and Accounting (4:29)
- 2.3.3 Access Control Best Practices
- 2.3.4 Practice Questions

2.4 Cryptography Basics

- 2.4.1 Cryptography Concepts (5:22)
- 2.4.2 Cryptography Facts
- 2.4.3 Practice Questions

2.5 Network Monitoring

- 2.5.1 Network Monitoring (2:40)
- 2.5.2 Network Monitoring Facts
- 2.5.3 Viewing Event Logs (9:39)
- 2.5.4 Practice Questions

2.6 Incident Response

- 2.6.1 First Responder (5:22)
- 2.6.2 Basic Forensic Procedures (10:56)
- 2.6.3 Using Forensic Tools (17:05)
- 2.6.4 Creating a Forensic Drive Image (10:02)
- 2.6.5 Incident Response Facts
- 2.6.6 Forensic Investigation Facts
- 2.6.7 Practice Questions

3.0 POLICIES, PROCEDURES, AND AWARENESS

3.1 Security Policies

- 3.1.1 Security Policies (11:50)
- 3.1.2 Data Privacy Laws (6:32)
- 3.1.3 Security Policy Facts
- 3.1.4 Security Documentation Facts
- 3.1.5 Security Management Facts
- 3.1.6 Data Retention Policies (4:54)
- 3.1.7 Data Retention Facts
- 3.1.8 Practice Questions

3.2 Risk Management

- 3.2.1 Risk Management (3:05)
- 3.2.2 Security Controls (2:41)

Copyright © 2017 TestOut Corporation. CompTIA, A+, Network+, Security+, Linux+ and related trademarks and trade names 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. TestOut has no affiliation with any of these companies and the products and services advertised herein are not endorsed by any of them.

- 3.2.3 Risk Management Facts
- 3.2.4 Practice Questions

3.3 Business Continuity

- 3.3.1 Business Continuity Planning (2:29)
- 3.3.2 Business Continuity Facts
- 3.3.3 Practice Questions

3.4 Manageable Network Plan

- 3.4.1 Manageable Network Plan (8:40)
- 3.4.2 Manageable Network Plan 2 (6:54)
- 3.4.3 Manageable Network Plan Facts
- 3.4.4 Practice Questions

3.5 Social Engineering

- 3.5.1 Social Engineering (10:13)
- 3.5.2 Phishing Variations (7:01)
- 3.5.3 Social Engineering Facts
- 3.5.4 Investigating a Social Engineering Attack (8:07)
- 3.5.5 Respond to Social Engineering
- 3.5.6 Practice Questions

3.6 App Development and Deployment

- 3.6.1 Development Life Cycle (5:10)
- 3.6.2 SDLC Facts
- 3.6.3 Software Development Models
- 3.6.4 Version Control Management (4:14)
- 3.6.5 Practice Questions

3.7 Employee Management

- 3.7.1 Employment Practices (8:12)
- 3.7.2 Employee Management Facts
- 3.7.3 Employee Documents Facts
- 3.7.4 Ethics Facts
- 3.7.5 Practice Questions

3.8 Mobile Devices

- 3.8.1 Mobile Device Management (10:20)
- 3.8.2 Mobile Device Security Facts
- 3.8.3 Practice Questions

3.9 Third-Party Integration

- 3.9.1 Third-Party Integration Security Issues (7:47)

Copyright © 2017 TestOut Corporation. CompTIA, A+, Network+, Security+, Linux+ and related trademarks and trade names 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. TestOut has no affiliation with any of these companies and the products and services advertised herein are not endorsed by any of them.

3.9.2 Third-Party Integration Security Facts
3.9.3 Practice Questions

4.0 PHYSICAL

4.1 Physical Threats
4.1.1 Physical Security (11:25)
4.1.2 Tailgating and Piggybacking (2:37)
4.1.3 Physical Security Facts
4.1.4 Implement Physical Security
4.1.5 Practice Questions

4.2 Device Protection
4.2.1 Hardware Security Guidelines (3:25)
4.2.2 Breaking into a System (4:55)
4.2.3 Hardware Security Facts
4.2.4 Practice Questions

4.3 Network Infrastructure Protection
4.3.1 Physical Network Protection (4:29)
4.3.2 Physical Network Protection Facts
4.3.3 Practice Questions

4.4 Environmental Controls
4.4.1 Environmental Controls (5:01)
4.4.2 Securing Environmental Systems (4:03)
4.4.3 Environmental Control Facts
4.4.4 Fire Protection Facts
4.4.5 Practice Questions

5.0 PERIMETER

5.1 Recon and Denial
5.1.1 Reconnaissance (6:41)
5.1.2 Performing Reconnaissance (9:09)
5.1.3 Reconnaissance Facts
5.1.4 Denial of Service (DoS) (4:45)
5.1.5 DoS Attack Facts
5.1.6 Performing a UDP Flood Attack (4:09)
5.1.7 Practice Questions

5.2 Spoofing and Poisoning

Copyright © 2017 TestOut Corporation. CompTIA, A+, Network+, Security+, Linux+ and related trademarks and trade names 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. TestOut has no affiliation with any of these companies and the products and services advertised herein are not endorsed by any of them.

- 5.2.1 Session and Spoofing Attacks (4:30)
- 5.2.2 Session-Based Attack Facts
- 5.2.3 Performing ARP Poisoning (7:42)
- 5.2.4 Spoofing Facts
- 5.2.5 DNS Attacks (6:09)
- 5.2.6 DNS Attack Facts
- 5.2.7 Examining DNS Attacks (13:48)
- 5.2.8 Prevent Zone Transfers
- 5.2.9 Practice Questions

5.3 Security Appliances

- 5.3.1 Security Solutions (4:46)
- 5.3.2 Security Zones (4:34)
- 5.3.3 Security Zone Facts
- 5.3.4 All-In-One Security Appliances (3:10)
- 5.3.5 Security Solution Facts
- 5.3.6 Configuring Network Security Appliance Access (5:40)
- 5.3.7 Configure Network Security Appliance Access
- 5.3.8 Practice Questions

5.4 Demilitarized Zones (DMZ)

- 5.4.1 Demilitarized Zones (6:49)
- 5.4.2 Configuring a DMZ (3:50)
- 5.4.3 Configure a DMZ
- 5.4.4 DMZ Facts
- 5.4.5 Practice Questions

5.5 Firewalls

- 5.5.1 Firewalls (6:24)
- 5.5.2 Firewall Facts
- 5.5.3 Configuring a Perimeter Firewall (7:54)
- 5.5.4 Configure a Perimeter Firewall
- 5.5.5 Practice Questions

5.6 Network Address Translation (NAT)

- 5.6.1 Network Address Translation (9:54)
- 5.6.2 Configuring NAT from the CLI (6:55)
- 5.6.3 Configuring NAT on an NSA (4:13)
- 5.6.4 NAT Facts
- 5.6.5 Practice Questions

Copyright © 2017 TestOut Corporation. CompTIA, A+, Network+, Security+, Linux+ and related trademarks and trade names 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. TestOut has no affiliation with any of these companies and the products and services advertised herein are not endorsed by any of them.

5.7 Virtual Private Networks (VPN)

- 5.7.1 Virtual Private Networks (VPNs) (7:03)
- 5.7.2 Configuring a VPN (2:34)
- 5.7.3 Configuring a VPN Client (10:36)
- 5.7.4 Configure a Remote Access VPN
- 5.7.5 Configure a VPN Connection iPad
- 5.7.6 VPN Facts
- 5.7.7 VPN Protocol Facts
- 5.7.8 Practice Questions

5.8 Web Threat Protection

- 5.8.1 Web Threat Protection (7:03)
- 5.8.2 Configuring Web Threat Protection (4:26)
- 5.8.3 Configure Web Threat Protection
- 5.8.4 Web Threat Protection Facts
- 5.8.5 Practice Questions

5.9 Network Access Protection

- 5.9.1 Network Access Protection (6:34)
- 5.9.2 Implementing NAC with DHCP Enforcement (14:04)
- 5.9.3 NAP Facts
- 5.9.4 Practice Questions

5.10 Wireless Overview

- 5.10.1 Wireless Networking Overview (5:58)
- 5.10.2 Wireless Antenna Types (5:01)
- 5.10.3 Wireless Networking Facts
- 5.10.4 Wireless Encryption (5:52)
- 5.10.5 Wireless Encryption Facts
- 5.10.6 Configuring a Wireless Connection (6:47)
- 5.10.7 Configure a Wireless Network
- 5.10.8 Practice Questions

5.11 Wireless Attacks

- 5.11.1 Wireless Attacks (6:21)
- 5.11.2 Wireless Attack Facts
- 5.11.3 Using Wireless Attack Tools (7:56)
- 5.11.4 Detecting Rogue Hosts (4:36)
- 5.11.5 Configure Rogue Host Protection
- 5.11.6 Practice Questions

Copyright © 2017 TestOut Corporation. CompTIA, A+, Network+, Security+, Linux+ and related trademarks and trade names 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. TestOut has no affiliation with any of these companies and the products and services advertised herein are not endorsed by any of them.

5.12 Wireless Defenses

- 🎞 5.12.1 Wireless Security Considerations (7:45)
- 🎞 5.12.2 Wireless Authentication (5:23)
- 🗎 5.12.3 Wireless Authentication Facts
- 🖥 5.12.4 Hardening a Wireless Access Point (6:39)
- 🖱 5.12.5 Harden a Wireless Network
- 🖱 5.12.6 Configure WIPS
- 🖥 5.12.7 Configuring a Captive Portal (4:15)
- 🗎 5.12.8 Wireless Security Facts
- 📝 5.12.9 Practice Questions

6.0 NETWORK

6.1 Network Threats

- 🎞 6.1.1 Network Threats Overview (8:34)
- 🗎 6.1.2 Network Threats Facts
- 📝 6.1.3 Practice Questions

6.2 Network Device Vulnerabilities

- 🎞 6.2.1 Device Vulnerabilities (6:55)
- 🗎 6.2.2 Device Vulnerability Facts
- 🖥 6.2.3 Searching defaultpasswords.com (2:18)
- 🖥 6.2.4 Securing a Switch (2:56)
- 🖱 6.2.5 Secure a Switch
- 📝 6.2.6 Practice Questions

6.3 Network Applications

- 🎞 6.3.1 Network Application Security (4:57)
- 🖥 6.3.2 Configuring Application Control Software (7:46)
- 🗎 6.3.3 Network Application Facts
- 📝 6.3.4 Practice Questions

6.4 Switch Attacks

- 🎞 6.4.1 Switch Attacks (5:42)
- 🗎 6.4.2 Switch Attack Facts
- 📝 6.4.3 Practice Questions

6.5 Switch Security

- 🎞 6.5.1 Switch Features (6:53)
- 🎞 6.5.2 Securing Network Switches (6:34)
- 🗎 6.5.3 Switch Security Facts

Copyright © 2017 TestOut Corporation. CompTIA, A+, Network+, Security+, Linux+ and related trademarks and trade names 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. TestOut has no affiliation with any of these companies and the products and services advertised herein are not endorsed by any of them.

- 🖥 6.5.4 Hardening a Switch (10:37)
- 🖱 6.5.5 Harden a Switch
- 🖱 6.5.6 Secure Access to a Switch
- 🖱 6.5.7 Secure Access to a Switch 2
- 📝 6.5.8 Practice Questions

6.6 Using VLANs

- 🎞 6.6.1 VLAN Overview (4:07)
- 🖥 6.6.2 Configuring VLANs from the CLI (4:39)
- 📄 6.6.3 VLAN Facts
- 🖱 6.6.4 Explore VLANs from the CLI
- 🖥 6.6.5 Configuring VLANs (3:09)
- 🖱 6.6.6 Explore VLANs
- 📝 6.6.7 Practice Questions

6.7 Router Security

- 🎞 6.7.1 Router Security (7:03)
- 🎞 6.7.2 Router ACLs (2:48)
- 📄 6.7.3 Router Security Facts
- 🖥 6.7.4 Configuring ACLs (7:10)
- 🖱 6.7.5 Restrict Telnet and SSH Access
- 🖱 6.7.6 Permit Traffic
- 🖱 6.7.7 Block Source Hosts
- 📝 6.7.8 Practice Questions

6.8 Intrusion Detection and Prevention

- 🎞 6.8.1 Intrusion Detection (6:30)
- 🎞 6.8.2 Detection vs. Prevention Controls (5:36)
- 📄 6.8.3 IDS Facts
- 🖥 6.8.4 Implementing Intrusion Monitoring (9:17)
- 🖥 6.8.5 Implementing Intrusion Prevention (5:58)
- 🖱 6.8.6 Implement Intrusion Prevention
- 📝 6.8.7 Practice Questions

6.9 Vulnerability Assessment

- 🎞 6.9.1 Vulnerability Assessment (4:23)
- 📄 6.9.2 Vulnerability Assessment Facts
- 🖥 6.9.3 Scanning a Network with Nessus (7:26)
- 🖥 6.9.4 Scanning a Network with Retina (7:16)
- 🖱 6.9.5 Scan for Vulnerabilities 1
- 🖱 6.9.6 Scan for Vulnerabilities 2

Copyright © 2017 TestOut Corporation. CompTIA, A+, Network+, Security+, Linux+ and related trademarks and trade names 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. TestOut has no affiliation with any of these companies and the products and services advertised herein are not endorsed by any of them.

- 6.9.7 Scan for Vulnerabilities 3
- 6.9.8 Scan for Vulnerabilities 4
- 6.9.9 Performing Port and Ping Scans (4:57)
- 6.9.10 Practice Questions

6.10 Protocol Analyzers

- 6.10.1 Protocol Analyzers (2:37)
- 6.10.2 Protocol Analyzer Facts
- 6.10.3 Analyzing Network Traffic (13:19)
- 6.10.4 Practice Questions

6.11 Remote Access

- 6.11.1 Remote Access (15:04)
- 6.11.2 Remote Access Facts
- 6.11.3 Configuring a RADIUS Solution (9:46)
- 6.11.4 RADIUS and TACACS+ Facts
- 6.11.5 Practice Questions

6.12 Network Authentication

- 6.12.1 Network Authentication Protocols (9:45)
- 6.12.2 Network Authentication Facts
- 6.12.3 LDAP Authentication (5:53)
- 6.12.4 Kerberos Authentication (5:04)
- 6.12.5 Controlling the Authentication Method (6:45)
- 6.12.6 Configure Kerberos Policy Settings
- 6.12.7 Credential Management (4:26)
- 6.12.8 Credential Management Facts
- 6.12.9 Practice Questions

6.13 Penetration Testing

- 6.13.1 Penetration Testing (2:38)
- 6.13.2 Penetration Testing Facts
- 6.13.3 Exploring Penetration Testing Tools (11:47)
- 6.13.4 Practice Questions

6.14 Virtual Networking

- 6.14.1 Virtual Networking Overview (6:04)
- 6.14.2 Virtual Network Devices (4:13)
- 6.14.3 Configuring Virtual Network Devices (3:13)
- 6.14.4 Virtualization Implementation Facts
- 6.14.5 Virtual Networking Facts

Copyright © 2017 TestOut Corporation. CompTIA, A+, Network+, Security+, Linux+ and related trademarks and trade names 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. TestOut has no affiliation with any of these companies and the products and services advertised herein are not endorsed by any of them.

- 6.14.6 Create Virtual Switches
- 6.14.7 Practice Questions

6.15 Software-Defined Networking (SDN)

- 6.15.1 Software-Defined Networking Basics (3:33)
- 6.15.2 SDN Infrastructure and Architecture (2:36)
- 6.15.3 SDN Facts
- 6.15.4 Practice Questions

6.16 Cloud Services

- 6.16.1 Cloud Services Introduction (9:34)
- 6.16.2 Cloud Computing Security Issues (5:43)
- 6.16.3 Cloud Computing Facts
- 6.16.4 Practice Questions

7.0 HOST

7.1 Malware

- 7.1.1 Malware (10:59)
- 7.1.2 Malware Facts
- 7.1.3 Malware Protection Facts
- 7.1.4 Implementing Malware Protections (6:17)
- 7.1.5 Using Windows Defender (7:18)
- 7.1.6 Configure Windows Defender
- 7.1.7 Practice Questions

7.2 Password Attacks

- 7.2.1 Password Attacks (6:28)
- 7.2.2 Password Attack Facts
- 7.2.3 Using Rainbow Tables (13:13)
- 7.2.4 Capturing Passwords (3:33)
- 7.2.5 Practice Questions

7.3 Windows System Hardening

- 7.3.1 Operating System Hardening (5:56)
- 7.3.2 Hardening Facts
- 7.3.3 Hardening an Operating System (6:49)
- 7.3.4 Managing Automatic Updates (4:42)
- 7.3.5 Configure Automatic Updates
- 7.3.6 Configuring Windows Firewall (6:13)
- 7.3.7 Configure Windows Firewall

Copyright © 2017 TestOut Corporation. CompTIA, A+, Network+, Security+, Linux+ and related trademarks and trade names 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. TestOut has no affiliation with any of these companies and the products and services advertised herein are not endorsed by any of them.

- 7.3.8 Configuring Windows Firewall Advanced Features (10:47)
- 7.3.9 Practice Questions

7.4 Hardening Enforcement

- 7.4.1 Hardening Enforcement with GPOs (2:21)
- 7.4.2 Using Security Templates and Group Policy (8:02)
- 7.4.3 Configuring GPOs to Enforce Security (11:31)
- 7.4.4 Hardening Enforcement Facts
- 7.4.5 Manage Services with Group Policy
- 7.4.6 Practice Questions

7.5 File Server Security

- 7.5.1 File Server Security (7:42)
- 7.5.2 File System Security Facts
- 7.5.3 File Permission Facts
- 7.5.4 Configuring NTFS Permissions (11:14)
- 7.5.5 Configure NTFS Permissions
- 7.5.6 Disable Inheritance
- 7.5.7 Practice Questions

7.6 Linux Host Security

- 7.6.1 Linux Host Security (14:44)
- 7.6.2 Removing Unnecessary Services and Scanning Ports (10:28)
- 7.6.3 Linux Host Security Facts
- 7.6.4 Practice Questions

7.7 Embedded Systems

- 7.7.1 SCADA and ICS Systems (5:52)
- 7.7.2 IoT Device Security (4:40)
- 7.7.3 Embedded Systems Security Facts
- 7.7.4 Practice Questions

7.8 Log Management

- 7.8.1 Log Management (5:06)
- 7.8.2 Log Facts
- 7.8.3 Logging Events with Event Viewer (5:15)
- 7.8.4 Windows Event Subscriptions (7:15)
- 7.8.5 Configuring Source-Initiated Subscriptions (5:26)
- 7.8.6 Configuring Remote Logging on Linux (8:30)
- 7.8.7 Remote Logging Facts
- 7.8.8 Practice Questions

Copyright © 2017 TestOut Corporation. CompTIA, A+, Network+, Security+, Linux+ and related trademarks and trade names 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. TestOut has no affiliation with any of these companies and the products and services advertised herein are not endorsed by any of them.

7.9 Audits

- 🎞 7.9.1 Audits (4:12)
- 📄 7.9.2 Audit Facts
- 🖥 7.9.3 Auditing the Windows Security Log (9:12)
- 🖱 7.9.4 Configure Advanced Audit Policy
- 🖥 7.9.5 Auditing Device Logs (1:50)
- 🖱 7.9.6 Enable Device Logs
- 📝 7.9.7 Practice Questions

7.10 Email

- 🎞 7.10.1 Email Security (6:29)
- 📄 7.10.2 Email Security Facts
- 🖥 7.10.3 Protecting a Client from Spam (5:49)
- 🖥 7.10.4 Securing an Email Server (2:51)
- 🖱 7.10.5 Configure Email Filters
- 🖥 7.10.6 Securing Email on iPad (5:22)
- 🖱 7.10.7 Secure Email on iPad
- 📝 7.10.8 Practice Questions

7.11 BYOD Security

- 🎞 7.11.1 BYOD Security Issues (10:20)
- 📄 7.11.2 BYOD Security Facts
- 🖥 7.11.3 Securing Mobile Devices (7:19)
- 🖱 7.11.4 Secure an iPad
- 📝 7.11.5 Practice Questions

7.12 Mobile Device Management

- 🎞 7.12.1 Mobile Device Considerations (4:54)
- 🎞 7.12.2 Mobile Application Security (6:56)
- 📄 7.12.3 Mobile Device Security Facts
- 🖥 7.12.4 Enforcing Security Policies on Mobile Devices (6:41)
- 🖥 7.12.5 Enrolling Devices and Performing a Remote Wipe (7:03)
- 📄 7.12.6 Mobile Device Enforcement Facts
- 🖥 7.12.7 Creating a Guest Network for BYOD (6:03)
- 🖱 7.12.8 Create a Guest Network for BYOD
- 📝 7.12.9 Practice Questions

7.13 Host Virtualization

- 🎞 7.13.1 Host Virtualization Overview (10:51)
- 🎞 7.13.2 Load Balancing with Virtualization (6:59)
- 📄 7.13.3 Virtualization Facts

Copyright © 2017 TestOut Corporation. CompTIA, A+, Network+, Security+, Linux+ and related trademarks and trade names 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. TestOut has no affiliation with any of these companies and the products and services advertised herein are not endorsed by any of them.

- 7.13.4 Creating Virtual Machines (6:51)
- 7.13.5 Managing Virtual Machines (5:22)
- 7.13.6 Create Virtual Machines
- 7.13.7 Adding Virtual Network Adapters (3:07)
- 7.13.8 Practice Questions

8.0 APPLICATION

8.1 Access Control Models

- 8.1.1 Access Control Models (4:59)
- 8.1.2 Access Control Facts
- 8.1.3 Access Control Model Facts
- 8.1.4 Implementing Discretionary Access Control (14:54)
- 8.1.5 Trusts and Transitive Access (4:55)
- 8.1.6 Trusts and Transitive Access Facts
- 8.1.7 Practice Questions

8.2 Authentication

- 8.2.1 Authentication (6:52)
- 8.2.2 Authentication Methods (4:08)
- 8.2.3 Authentication Facts
- 8.2.4 Using a Biometric Scanner (2:47)
- 8.2.5 Using Single Sign-on (4:23)
- 8.2.6 Single Sign-on Facts
- 8.2.7 Practice Questions

8.3 Authorization

- 8.3.1 Authorization (3:45)
- 8.3.2 Cumulative Access (6:21)
- 8.3.3 Authorization Facts
- 8.3.4 Examining the Access Token (9:15)
- 8.3.5 Practice Questions

8.4 Web Application Attacks

- 8.4.1 Web Application Attacks (2:39)
- 8.4.2 XSS and CSRF Attacks (9:41)
- 8.4.3 Injection Attacks (4:00)
- 8.4.4 Header Manipulation (4:18)
- 8.4.5 Zero Day Application Attacks (3:18)
- 8.4.6 Client-Side Attacks (3:19)
- 8.4.7 Web Application Attack Facts

Copyright © 2017 TestOut Corporation. CompTIA, A+, Network+, Security+, Linux+ and related trademarks and trade names 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. TestOut has no affiliation with any of these companies and the products and services advertised herein are not endorsed by any of them.

- 8.4.8 Preventing Cross-Site Scripting (4:08)
- 8.4.9 Practice Questions

8.5 Internet Browsers

- 8.5.1 Web Browser Threats (8:01)
- 8.5.2 Configuring Browser Security and Plugins (12:09)
- 8.5.3 Clearing the Browser Cache (4:56)
- 8.5.4 Clear the Browser Cache
- 8.5.5 Configure IE Pop-up Blocker
- 8.5.6 Internet Explorer Security Facts
- 8.5.7 Enforcing IE Settings Through GPO (3:31)
- 8.5.8 Enforce IE Settings Through GPO
- 8.5.9 Configure IE Preferences in a GPO
- 8.5.10 Practice Questions

8.6 Application Development

- 8.6.1 Secure Coding Concepts (9:58)
- 8.6.2 Application Hardening (7:53)
- 8.6.3 Application Development Security Facts
- 8.6.4 Hardening Applications on Linux (3:33)
- 8.6.5 Implementing Application Whitelisting with AppLocker (7:23)
- 8.6.6 Implement Application Whitelisting with AppLocker
- 8.6.7 Implementing Data Execution Preventions (DEP) (3:23)
- 8.6.8 Implement Data Execution Preventions (DEP)
- 8.6.9 Hardening Applications Facts
- 8.6.10 NoSQL Security (4:22)
- 8.6.11 NoSQL Security Facts
- 8.6.12 Practice Questions

8.7 Active Directory Overview

- 8.7.1 Active Directory Introduction (6:48)
- 8.7.2 Active Directory Structure (5:27)
- 8.7.3 Viewing Active Directory (8:11)
- 8.7.4 Active Directory Facts
- 8.7.5 Practice Questions

8.8 Windows Domain Users and Groups

- 8.8.1 Creating User Accounts (5:10)
- 8.8.2 Managing User Account Properties (8:30)
- 8.8.3 Create User Accounts

Copyright © 2017 TestOut Corporation. CompTIA, A+, Network+, Security+, Linux+ and related trademarks and trade names 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. TestOut has no affiliation with any of these companies and the products and services advertised herein are not endorsed by any of them.

- 🖱 8.8.4 Manage User Accounts
- 🖥 8.8.5 Managing Groups (4:58)
- 🖱 8.8.6 Create a Group
- 🖱 8.8.7 Create Global Groups
- 📄 8.8.8 User Account Management Facts
- 📝 8.8.9 Practice Questions

8.9 Linux Users

- 🎞 8.9.1 Linux User and Group Overview (11:00)
- 🖥 8.9.2 Managing Linux Users (8:40)
- 📄 8.9.3 Linux User Commands and Files
- 🖱 8.9.4 Create a User Account
- 🖱 8.9.5 Rename a User Account
- 🖱 8.9.6 Delete a User
- 🖱 8.9.7 Change Your Password
- 🖱 8.9.8 Change a User's Password
- 🖱 8.9.9 Lock and Unlock User Accounts
- 📝 8.9.10 Practice Questions

8.10 Linux Groups

- 🖥 8.10.1 Managing Linux Groups (7:49)
- 📄 8.10.2 Linux Group Commands
- 🖱 8.10.3 Rename and Create Groups
- 🖱 8.10.4 Add Users to a Group
- 🖱 8.10.5 Remove a User from a Group
- 📝 8.10.6 Practice Questions

8.11 Linux User Security

- 🎞 8.11.1 Linux User Security and Restrictions (7:14)
- 🖥 8.11.2 Configuring Linux User Security and Restrictions (7:51)
- 📄 8.11.3 Linux User Security and Restriction Facts
- 📝 8.11.4 Practice Questions

8.12 Group Policy Overview

- 🎞 8.12.1 Group Policy Overview (9:52)
- 🖥 8.12.2 Configuring Local Policies (11:28)
- 🖥 8.12.3 Creating and Linking Group Policy Objects (10:28)
- 📄 8.12.4 Group Policy Facts
- 🖱 8.12.5 Create and Link a GPO
- 📝 8.12.6 Practice Questions

Copyright © 2017 TestOut Corporation. CompTIA, A+, Network+, Security+, Linux+ and related trademarks and trade names 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. TestOut has no affiliation with any of these companies and the products and services advertised herein are not endorsed by any of them.

8.13 Hardening Authentication 1

- 8.13.1 Hardening Authentication (10:19)
- 8.13.2 Configuring User Account Restrictions (4:52)
- 8.13.3 Configure User Account Restrictions
- 8.13.4 Configuring Account Policies and UAC Settings (6:25)
- 8.13.5 Configure Account Policies
- 8.13.6 Hardening User Accounts (7:40)
- 8.13.7 Restrict Local Accounts
- 8.13.8 Secure Default Accounts
- 8.13.9 Enforce User Account Control
- 8.13.10 Hardening Authentication Facts
- 8.13.11 Practice Questions

8.14 Hardening Authentication 2

- 8.14.1 Configuring Smart Card Authentication (5:37)
- 8.14.2 Configure Smart Card Authentication
- 8.14.3 Smart Card Authentication Facts
- 8.14.4 Using Fine-Grained Password Policies (5:34)
- 8.14.5 Fine-Grained Password Policy Facts
- 8.14.6 Create a Fine-Grained Password Policy
- 8.14.7 Practice Questions

9.0 DATA

9.1 Data Management

- 9.1.1 Information Classification (2:54)
- 9.1.2 Information Classification Facts
- 9.1.3 Data Destruction (8:43)
- 9.1.4 File Shredding and Hard Drive Wiping (9:35)
- 9.1.5 Data Destruction Facts
- 9.1.6 Practice Questions

9.2 Advanced Cryptography

- 9.2.1 Advanced Cryptography Concepts (9:37)
- 9.2.2 Advanced Cryptography Facts
- 9.2.3 Cryptography Algorithms (2:58)
- 9.2.4 Cryptography Algorithms Facts
- 9.2.5 Practice Questions

9.3 Cryptography Implementations

- 9.3.1 Combining Cryptographic Methods (6:31)

Copyright © 2017 TestOut Corporation. CompTIA, A+, Network+, Security+, Linux+ and related trademarks and trade names 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. TestOut has no affiliation with any of these companies and the products and services advertised herein are not endorsed by any of them.

- 9.3.2 Hardware-Based Encryption Devices (5:49)
- 9.3.3 Cryptographic Implementation Facts
- 9.3.4 Practice Questions

9.4 Cryptographic Attacks

- 9.4.1 Cryptographic Attacks (10:27)
- 9.4.2 Cryptographic Attack Facts
- 9.4.3 Practice Questions

9.5 Symmetric Encryption

- 9.5.1 Symmetric Encryption (4:18)
- 9.5.2 Symmetric Encryption Facts
- 9.5.3 Cracking a Symmetric Encryption Key (4:47)
- 9.5.4 Practice Questions

9.6 Asymmetric Encryption

- 9.6.1 Asymmetric Encryption (5:40)
- 9.6.2 Asymmetric Encryption Facts
- 9.6.3 Practice Questions

9.7 File Encryption

- 9.7.1 Encrypting File System (EFS) (8:59)
- 9.7.2 Securing Files using EFS (8:17)
- 9.7.3 Encrypt Files with EFS
- 9.7.4 PGP and GPG (4:22)
- 9.7.5 Encrypting Files with GPG (5:46)
- 9.7.6 BitLocker and Database Encryption (4:39)
- 9.7.7 Configuring BitLocker (3:53)
- 9.7.8 Configure BitLocker with a TPM
- 9.7.9 File Encryption Facts
- 9.7.10 Practice Questions

9.8 Public Key Infrastructure (PKI)

- 9.8.1 Certificates (7:04)
- 9.8.2 Managing Certificates (10:34)
- 9.8.3 Manage Certificates
- 9.8.4 Certificate Lifecycle Facts
- 9.8.5 CA Implementation (5:34)
- 9.8.6 Configuring a Subordinate CA (10:08)
- 9.8.7 PKI Management Facts
- 9.8.8 Practice Questions

Copyright © 2017 TestOut Corporation. CompTIA, A+, Network+, Security+, Linux+ and related trademarks and trade names 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. TestOut has no affiliation with any of these companies and the products and services advertised herein are not endorsed by any of them.

9.9 Hashing

- 9.9.1 Hashing (4:06)
- 9.9.2 Hashing Algorithms (2:08)
- 9.9.3 Hashing Facts
- 9.9.4 Using Hashes (5:05)
- 9.9.5 Practice Questions

9.10 Data Transmission Security

- 9.10.1 Secure Protocols (6:22)
- 9.10.2 Secure Protocols 2 (7:50)
- 9.10.3 Secure Protocol Facts
- 9.10.4 Adding SSL to a Website (5:25)
- 9.10.5 Allow SSL Connections
- 9.10.6 IPsec (4:49)
- 9.10.7 IPsec Facts
- 9.10.8 Requiring IPsec for Communications (11:39)
- 9.10.9 Practice Questions

9.11 Data Loss Prevention (DLP)

- 9.11.1 Data Loss Prevention (DLP) (3:47)
- 9.11.2 DLP Facts
- 9.11.3 Practice Questions

9.12 Redundancy

- 9.12.1 Redundancy (3:23)
- 9.12.2 Redundancy Measurement Parameters (4:42)
- 9.12.3 Redundancy Facts
- 9.12.4 RAID (4:38)
- 9.12.5 Implementing RAID (7:18)
- 9.12.6 RAID Facts
- 9.12.7 Configure Fault-Tolerant Volumes
- 9.12.8 Clustering (7:06)
- 9.12.9 Clustering Facts
- 9.12.10 Practice Questions

9.13 Backup and Restore

- 9.13.1 Backup and Restore (9:13)
- 9.13.2 Backup and Restore Facts
- 9.13.3 Backup Management Facts
- 9.13.4 Backing Up Workstations (7:55)
- 9.13.5 Back Up a Workstation

Copyright © 2017 TestOut Corporation. CompTIA, A+, Network+, Security+, Linux+ and related trademarks and trade names 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. TestOut has no affiliation with any of these companies and the products and services advertised herein are not endorsed by any of them.

- 9.13.6 Restoring Workstation Data from Backup (4:04)
- 9.13.7 Backing Up a Domain Controller (2:45)
- 9.13.8 Back Up a Domain Controller
- 9.13.9 Restoring Server Data from Backup (3:00)
- 9.13.10 Practice Questions

9.14 Cloud Storage

- 9.14.1 Cloud Storage Security (2:44)
- 9.14.2 Cloud Storage Security Facts
- 9.14.3 Practice Questions

A.0 SECURITY PRO PRACTICE EXAMS

A.1 Preparing for Certification

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

- A.2 Security Pro Domain 1: Access Control and Identity Management
- A.3 Security Pro Domain 2: Policies, Procedures, Awareness
- A.4 Security Pro Domain 3: Physical Security
- A.5 Security Pro Domain 4: Perimeter Defenses
- A.6 Security Pro Domain 5: Network Defenses
- A.7 Security Pro Domain 6: Host Defenses
- A.8 Security Pro Domain 7: Application Defenses
- A.9 Security Pro Domain 8: Data Defenses
- A.10 Security Pro Domain 9: Audits and Assessments
- A.11 Security Pro Certification Practice Exam

B.0 COMPTIA SECURITY+ PRACTICE EXAMS

B.1 Preparing for Certification

- B.1.1 Security+ Exam Objectives
- B.1.2 Security+ Exam Objectives by Course Section
- B.1.3 Exam FAQs
- B.1.4 How to Register for an Exam
- B.1.5 Exam-taking Hints and Tips
- B.1.6 Why Certify?

- B.2 CompTIA Security+ Domain 1: Threats, Attacks and Vulnerabilities, All Questions
- B.3 CompTIA Security+ Domain 2: Technologies and Tools, All Questions

Copyright © 2017 TestOut Corporation. CompTIA, A+, Network+, Security+, Linux+ and related trademarks and trade names 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. TestOut has no affiliation with any of these companies and the products and services advertised herein are not endorsed by any of them.

- B.4 CompTIA Security+ Domain 3: Architecture and Design, All Questions
- B.5 CompTIA Security+ Domain 4: Identity and Access Management, All Questions
- B.6 CompTIA Security+ Domain 5: Risk Management, All Questions
- B.7 CompTIA Security+ Domain 6: Cryptography and PKI, All Questions
- B.8 CompTIA Security+ Certification Practice Exam

Copyright © 2017 TestOut Corporation. CompTIA, A+, Network+, Security+, Linux+ and related trademarks and trade names 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. TestOut has no affiliation with any of these companies and the products and services advertised herein are not endorsed by any of them.