TestOut Security Pro - English 6.0.x

LESSON PLAN
# Table of Contents

**Introduction**
- Section 1.1: Security Overview ................................................................. 5
- Section 1.2: Using the Simulator ................................................................. 6

**Security Basics**
- Section 2.1: Understanding Attacks ............................................................... 7
- Section 2.2: Defense Planning ........................................................................ 8
- Section 2.3: Access Control ........................................................................... 9
- Section 2.4: Cryptography Basics ................................................................. 10
- Section 2.5: Network Monitoring ................................................................. 11
- Section 2.6: Incident Response ................................................................... 12

**Policies, Procedures, and Awareness**
- Section 3.1: Security Policies ....................................................................... 14
- Section 3.2: Risk Management ....................................................................... 16
- Section 3.3: Business Continuity .................................................................. 18
- Section 3.4: Manageable Network Plan ..................................................... 20
- Section 3.5: Social Engineering .................................................................... 21
- Section 3.6: App Development and Deployment ........................................... 23
- Section 3.7: Employee Management ............................................................ 24
- Section 3.8: Mobile Devices ......................................................................... 26
- Section 3.9: Third-Party Integration .............................................................. 27

**Physical**
- Section 4.1: Physical Threats ....................................................................... 28
- Section 4.2: Device Protection ....................................................................... 30
- Section 4.3: Network Infrastructure Protection ........................................... 31
- Section 4.4: Environmental Controls ............................................................ 32

**Perimeter**
- Section 5.1: Recon and Denial ..................................................................... 34
- Section 5.2: Spoofing and Poisoning ............................................................. 35
- Section 5.3: Security Appliances .................................................................. 37
- Section 5.4: Demilitarized Zones (DMZ) ..................................................... 39
- Section 5.5: Firewalls .................................................................................... 40
- Section 5.6: Network Address Translation (NAT) ....................................... 42
- Section 5.7: Virtual Private Networks (VPN) ............................................... 43
- Section 5.8: Web Threat Protection ............................................................... 45
- Section 5.9: Network Access Protection ...................................................... 47
- Section 5.10: Wireless Overview ................................................................. 48
- Section 5.11: Wireless Attacks .................................................................... 50
- Section 5.12: Wireless Defenses ................................................................. 52

**Network**
- Section 6.1: Network Threats ..................................................................... 55
- Section 6.2: Network Device Vulnerabilities ............................................. 56
- Section 6.3: Network Applications ............................................................... 58
- Section 6.4: Switch Attacks ......................................................................... 59
- Section 6.5: Switch Security ......................................................................... 60
- Section 6.6: Using VLANs ........................................................................... 62
- Section 6.7: Router Security ......................................................................... 63
- Section 6.8: Intrusion Detection and Prevention ........................................... 65
- Section 6.9: Vulnerability Assessment ........................................................... 67

Copyright © 2017 TestOut Corporation. CompTIA, A+, Network+, Security+, Linux+ and related trademarks and trade names are the trademarks of CompTIA. Microsoft, MCITP, MScA, MCTS, Windows, and Office 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.
Practice Exams
Practice Exams ........................................................................................................... 153

Appendices
Appendix A: Security Pro Exam Objectives .................................................................. 154
Appendix B: CompTIA Security+ Exam Objectives ...................................................... 160
Appendix C: Approximate Time for the Course .............................................................. 185
1.1: Security Overview

The TestOut Security Pro Certification exam measures not just what you know, but what you can do. This exam measures your ability to implement processes to protect an organization's assets against danger, damage, loss, and criminal activity.

Lecture Focus Questions:

- What challenges does a security professional face?
- What is the difference between integrity and non-repudiation?
- What are the three main goals of the CIA of Security?
- What are the key components of risk management?
- What are three types of threat agents?

Video/Demo

- 1.1.1 The Security Landscape 3:50
- 1.1.2 Security Concepts 4:14

Total Video Time 8:04

Fact Sheets

- 1.1.3 Security Introduction

Number of Exam Questions

10 questions

Total Time

About 24 minutes
1.2: Using the Simulator

Summary

In this section, you will learn to:

- Read simulated component documentation and view components to make appropriate choices to meet the scenario.
- Add and remove simulated computer components.
- Change views and add simulated components.
- Use the zoom feature to view additional image details.
- Attach simulated cables.
- Use the simulation interface to identify where simulated cables connect to the computer.
- Configure a security appliance
- Install a security appliance

Video/Demo

<table>
<thead>
<tr>
<th>Video/Demo</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.2.1 Using the Simulator</td>
<td>5:28</td>
</tr>
</tbody>
</table>

Total Video Time 5:28

Lab/Activity

- 1.2.2 Configure a Security Appliance
- 1.2.3 Install a Security Appliance

Total Time

About 16 minutes
2.1: Understanding Attacks

Lecture Focus Questions:

- How do persistent and non-persistent threats differ?
- What protections can you implement against organized crime threat actors?
- Which method is used to access an application or operating system for troubleshooting?
- Which five methodologies can be used to defend your network?

This section covers the following Security+ certification exam objectives:
1.3 Explain threat actor types and attributes

- Types of actors
  - Script kiddies
  - Hacktivist
  - Organized crime
  - Nation states/APT
  - Insiders
  - Competitors

- Attributes of actors
  - Internal/external
  - Level of sophistication
  - Resources/funding
  - Intent/motivation

- Use of open-source intelligence

1.4 Explain penetration testing concepts

- Active reconnaissance
- Passive reconnaissance
- Pivot

**Video/Demo**

<table>
<thead>
<tr>
<th>Title</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1.1 Threat Actor Types</td>
<td>10:15</td>
</tr>
<tr>
<td>2.1.3 General Attack Strategy</td>
<td>6:06</td>
</tr>
<tr>
<td>2.1.4 General Defense Strategy</td>
<td>7:50</td>
</tr>
</tbody>
</table>

**Total Video Time** 24:11

**Fact Sheets**

- 2.1.2 Threat Agents Overview
- 2.1.5 Attack and Defense Strategy Overview

**Number of Exam Questions**
6 questions

**Total Time**

*About 41 minutes*
2.2: Defense Planning

Lecture Focus Questions:

- What is layered security?
- What are the seven layers in layered security?
- What is a countermeasure?
- How can countermeasures reduce the risk of a threat agent being able to exploit a vulnerability?

This section covers the following Security+ certification exam objective:
3.1 Explain use cases and purpose for frameworks, best practices and secure configuration guides

- Defense-in-depth/layered security
  - Vendor diversity
  - Control diversity
    - Administrative
    - Technical
  - User training

**Video/Demo**

<table>
<thead>
<tr>
<th>Video/Demo</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.2.1 The Layered Security Model</td>
<td>5:47</td>
</tr>
<tr>
<td>2.2.2 User Education</td>
<td>2:33</td>
</tr>
</tbody>
</table>

**Total Video Time** 8:20

**Fact Sheets**

- 2.2.3 Defense Planning Facts

**Number of Exam Questions**

5 questions

**Total Time**

*About 19 minutes*
2.3: Access Control

Lecture Focus Questions:

- How do separation of duties and job rotation differ?
- Why is defense-in-depth important?
- Which authentication type requires you to prove your identity?
- What allows authenticated users access to resources in different domains?
- What is AAA?

This section covers the following Security+ certification exam objectives:

4.1 Compare and contrast identity and access management concepts

- Identification, authentication, authorization and accounting (AAA)
- Multifactor authentication
  - Something you are
  - Something you have
  - Something you know
  - Somewhere you are
  - Something you do
- Transitive trust

4.4 Given a scenario, differentiate common account management practices

- General Concepts
  - Least privilege

5.1 Explain the importance of policies, plans and procedures related to organizational security

- Personnel management
  - Job rotation
  - Separation of duties

Video/Demo

<table>
<thead>
<tr>
<th>Video/Demo</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.3.1 Identity and Access Management</td>
<td>5:52</td>
</tr>
<tr>
<td>2.3.2 Authentication, Authorization, and Accounting</td>
<td>4:29</td>
</tr>
<tr>
<td><strong>Total Video Time</strong></td>
<td><strong>10:21</strong></td>
</tr>
</tbody>
</table>

Fact Sheets

- 2.3.3 Access Control Best Practices

Number of Exam Questions

- 12 questions

Total Time

About 28 minutes
2.4: Cryptography Basics

Lecture Focus Questions:

- What is a legitimate use for cryptanalysis?
- How is the strength of a cryptosystem related to the length of the key?
- Which of the following is typically kept secret, the encryption algorithm or the key (or both)?
- What is the difference between a transposition cipher and a substitution cipher?
- What is a legitimate use for steganography?

This section covers the following Security+ certification exam objective:
6.1 Compare and contrast basic concepts of cryptography.

- Steganography

Video/Demo

<table>
<thead>
<tr>
<th>Video/Demo</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.4.1 Cryptography Concepts</td>
<td>5:22</td>
</tr>
<tr>
<td>Total Video Time</td>
<td>5:22</td>
</tr>
</tbody>
</table>

Fact Sheets

- 2.4.2 Cryptography Facts

Number of Exam Questions

6 questions

Total Time

About 17 minutes
2.5: Network Monitoring

Lecture Focus Questions:

- What does a protocol analyzer do?
- Why is network monitoring important?
- What type of information can be gained from network monitoring?
- How does a throughput tester differ from a load tester?

In this section, you will learn to:

- View event logs

This section covers the following Security+ certification exam objective:
2.2 Given a scenario, use appropriate software tools to assess the security posture of an organization

- Protocol analyzer
- Network scanners

Video/Demo

<table>
<thead>
<tr>
<th>Video/Demo</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.5.1 Network Monitoring</td>
<td>2:40</td>
</tr>
<tr>
<td>2.5.3 Viewing Event Logs</td>
<td>9:39</td>
</tr>
<tr>
<td><strong>Total Video Time</strong></td>
<td><strong>12:19</strong></td>
</tr>
</tbody>
</table>

Fact Sheets

- 2.5.2 Network Monitoring Facts

Number of Exam Questions
5 questions

Total Time
About 23 minutes
2.6: Incident Response

Lecture Focus Questions:

- What actions should take place when an incident occurs?
- What types of things would a computer forensic investigator want to analyze if he selected a live analysis over a dead analysis?
- What methods can be used to save the contents of memory as part of a forensic investigation?
- How should you ensure the integrity of collected digital evidence?
- Why is chain of custody so important with forensic investigations?

This section teaches you to:

- Gather and authenticate forensic information from a system using a computer forensic tool.
- Analyze and record forensic evidence.

This section covers the following Security+ certification exam objective:

5.4 Given a scenario, follow incident response procedures.

- Incident response plan
  - Documented incident types/category definitions
  - Roles and responsibilities
  - Reporting requirements/escalation
  - Cyber-incident response teams
  - Exercise

- Incident response process
  - Preparation
  - Identification
  - Containment
  - Eradication
  - Recovery
  - Lessons learned

5.5 Summarize basic concepts of forensics.

- Order of volatility
- Chain of custody
- Legal hold
- Data acquisition
  - Capture system image
  - Network traffic and logs
  - Capture video
  - Record time offset
  - Take hashes
• Screenshots
  • Witness interviews
• Preservation
• Recovery
• Strategic intelligence/counterintelligence gathering
  • Active logging
• Track man-hours

**Video/Demo**

<table>
<thead>
<tr>
<th>Video/Demo</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.6.1 First Responder</td>
<td>5:22</td>
</tr>
<tr>
<td>2.6.2 Basic Forensic Procedures</td>
<td>10:56</td>
</tr>
<tr>
<td>2.6.3 Using Forensic Tools</td>
<td>17:05</td>
</tr>
<tr>
<td>2.6.4 Creating a Forensic Drive Image</td>
<td>10:02</td>
</tr>
<tr>
<td><strong>Total Video Time</strong></td>
<td><strong>43:25</strong></td>
</tr>
</tbody>
</table>

**Fact Sheets**

- 2.6.5 Incident Response Facts
- 2.6.6 Forensic Investigation Facts

**Number of Exam Questions**

13 questions

**Total Time**

*About 67 minutes*
3.1: Security Policies

Lecture Focus Questions:

- What is the difference between a regulation and a guideline?
- What are the main reasons to implement security policies within an organization?
- How is due diligence different from due process?
- How can a code escrow agreement provide security for an organization?
- When a new security plan is distributed, why is it important to destroy all copies of the old version?
- What are the characteristics of a strong password policy?

This section covers the following Security+ certification exam objectives:

4.4 Given a scenario, differentiate common account management practices

- Account policy enforcement
  - Password complexity

5.1 Explain the importance of policies, plans and procedures related to organizational security

- Agreement types
  - SLA
- Personnel management
  - Mandatory vacations
  - Job rotation
  - Background checks
  - Exit interviews
  - Continuing education
  - Acceptable use policy/rules of behavior
  - Adverse actions
- General security policies
  - Personal email

5.2 Summarize business impact analysis concepts

- MTBF
- MTTR
- Impact
  - Life
  - Property
  - Safety
  - Finance
  - Reputation
- Privacy impact assessment
- Privacy threshold assessment
5.3 Explain risk management processes and concepts

- Change management

5.8 Given a scenario, carry out data security and privacy practices

- Data sensitivity labeling and handling
  - PII
- Data retention
- Legal and compliance

**Video/Demo**

<table>
<thead>
<tr>
<th>Video/Demo</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1.1 Security Policies</td>
<td>11:50</td>
</tr>
<tr>
<td>3.1.2 Data Privacy Laws</td>
<td>6:32</td>
</tr>
<tr>
<td>3.1.6 Data Retention Policies</td>
<td>4:54</td>
</tr>
</tbody>
</table>

**Total Video Time** 23:16

**Fact Sheets**

- 3.1.3 Security Policy Facts
- 3.1.4 Security Documentation Facts
- 3.1.5 Security Management Facts
- 3.1.7 Data Retention Facts

**Number of Exam Questions**

15 questions

**Total Time**

*About 59 minutes*
3.2: Risk Management

Lecture Focus Questions:

- What kinds of components are *tangible* assets?
- How can an asset have both a tangible and intangible value?
- Why is it important that organizations determine their assets’ value?
- How is *quantitative* analysis different from *qualitative* analysis?
- What components are used to measure risk quantitatively?
- What method is typically deployed in risk *transference*?
- Why is risk *rejection* not a wise risk response?

This section covers the following TestOut Security Pro certification exam objective:

- 2.2 Evaluate Information Risk
  - Perform risk calculation
  - Risk avoidance, transference, acceptance, mitigation, and deterrence

This section covers the following Security+ certification exam objective:

5.3 Explain risk management processes and concepts.

- Threat assessment
  - Environmental
  - Manmade
  - Internal vs. external

- Risk assessment
  - SLE
  - ALE
  - ARO
  - Asset value
  - Risk register
  - Likelihood of occurrence
  - Supply chain assessment
  - Impact
  - Quantitative
  - Qualitative
  - Testing
    - Penetration testing authorization
    - Vulnerability testing authorization
  - Risk response techniques
    - Accept
    - Transfer
    - Avoid
    - Mitigate

**Video/Demo**

<table>
<thead>
<tr>
<th></th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.2.1</td>
<td>3:05</td>
</tr>
<tr>
<td>3.2.2</td>
<td>2:41</td>
</tr>
</tbody>
</table>

**Total Video Time**: 5:46
Fact Sheets

3.2.3 Risk Management Facts

Number of Exam Questions
15 questions

Total Time
About 26 minutes
3.3: Business Continuity

Lecture Focus Questions:

- When is the best time to start planning for disaster recovery?
- How is the Disaster Recovery Plan (DRP) related to the Business Continuity Plan (BCP)?
- What is the top priority when planning for a disaster?
- How does a Business Impact Analysis (BIA) help to improve the security of an organization?
- In addition to planning for how to keep operations going in the event of an incident, what else should a disaster recovery plan include?
- How does succession planning differ from replacement planning?

This section covers the following TestOut Security Pro certification exam objective:

- 2.2 Evaluate Information Risk
  - Perform Risk calculation
  - Risk avoidance, transference, acceptance, mitigation, and deterrence

This section covers the following Security+ certification exam objectives:
5.3 Explain risk management processes and concepts.

- Risk assessment
  - Risk response techniques
    - Accept
    - Transfer
    - Avoid
    - Mitigate

5.6 Explain disaster recovery and continuity of operation concepts.

- Recovery sites
  - Hot site
  - Warm site
  - Cold site
- Order of restoration
- Backup concepts
  - Differential
  - Incremental
  - Snapshots
  - Full
- Geographic considerations
  - Off-site backups
  - Distance
  - Location selection
- Legal implications
- Data sovereignty
- Continuity of operation planning
  - Exercises/tabletop
  - After-action reports
  - Failover
  - Alternate processing sites
  - Alternate business practices

**Video/Demo**

- 3.3.1 Business Continuity Planning 2:29
  - Total Video Time 2:29

**Fact Sheets**

- 3.3.2 Business Continuity Facts

**Number of Exam Questions**

6 questions

**Total Time**

*About 14 minutes*
3.4: Manageable Network Plan

Lecture Focus Questions:

- When you develop a manageable network plan, what should you keep in mind as you prepare to document your network?
- Which elements of the network are identified when you map your network?
- What steps should you perform to protect your network?
- How can you ensure that all of the devices in the network have access, but still maintain security?
- What must you keep in mind to control user access and ensure network security?

This section covers the following Security+ certification exam objectives:
3.3 Given a scenario, implement secure systems design

- Operating systems
  - Patch management
- 2.3 Maintain Hardware and Software Inventory

Video/Demo

<table>
<thead>
<tr>
<th>Video/Demo</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.4.1 Manageable Network Plan</td>
<td>8:40</td>
</tr>
<tr>
<td>3.4.2 Manageable Network Plan 2</td>
<td>6:54</td>
</tr>
</tbody>
</table>

Total Video Time 15:34

Fact Sheets

- 3.4.3 Manageable Network Plan Facts

Number of Exam Questions

5 questions

Total Time

About 26 minutes
3.5: Social Engineering

Lecture Focus Questions:

• How is passive social engineering different from active social engineering?
• What methods do attackers use to make an interaction appear legitimate?
• How is employee awareness training the most effective countermeasure for social engineering?
• What specific countermeasures should be implemented to mitigate social engineering?
• How is tailgating different from piggybacking?
• What is a watering hole attack?

This section teaches you to:

• Identify and ignore email hoaxes to protect system resources.
• Train users to identify phishing scams.

This section covers the following TestOut Security Pro certification exam objective:

• 2.1 Promote Information Security Awareness
  o Using email best practices

This section covers the following Security+ certification exam objective:
1.2 Compare and contrast types of attacks.

• Social engineering
  o Phishing
  o Spear phishing
  o Whaling
  o Vishing
  o Tailgating
  o Impersonation
  o Dumpster diving
  o Shoulder surfing
  o Hoax
  o Watering hole attack
  o Principles (reasons for effectiveness)
    ▪ Authority
    ▪ Intimidation
    ▪ Consensus
    ▪ Scarcity
    ▪ Familiarity
    ▪ Trust
    ▪ Urgency
Video/Demo

<p>| | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>3.5.1 Social Engineering</td>
<td>10:13</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>3.5.2 Phishing Variations</td>
<td>7:01</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>3.5.4 Investigating a Social Engineering Attack</td>
<td>8:07</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total Video Time</td>
<td></td>
<td>25:21</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Lab/Activity

- 3.5.5 Respond to Social Engineering

Fact Sheets

- 3.5.3 Social Engineering Facts

Number of Exam Questions

15 questions

Total Time

About 51 minutes
3.6: App Development and Deployment

Lecture Focus Questions:

- How does the spiral model combine the waterfall model and the prototype model?
- What are at least three of the different software development standardized models?
- How should security be employed in the different stages of development?
- What does functional design entail?
- What are some of the early steps taken during the initial phases of the system development life cycle?
- When is change control necessary?
- What are the responsibilities of developers after a product is released?

This section covers the following Security+ certification exam objective:
3.6 Summarize secure application development and deployment concepts.

- Development life-cycle models
  - Waterfall vs. Agile

Video/Demo

<table>
<thead>
<tr>
<th>Video/Demo</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.6.1 Development Life Cycle</td>
<td>5:10</td>
</tr>
<tr>
<td>3.6.4 Version Control Management</td>
<td>4:14</td>
</tr>
</tbody>
</table>

Total Video Time 9:24

Fact Sheets

- 3.6.2 SDLC Facts
- 3.6.3 Software Development Models

Number of Exam Questions

7 questions

Total Time

About 27 minutes
3.7: Employee Management

Lecture Focus Questions:

- How can pre-employment processing improve the security of an organization?
- What is the role of the policy handbook regarding security?
- What guidelines must be considered when monitoring employees?
- Why should employees be required to sign employment agreements?
- Why shouldn't an organization target and monitor specific employees?
- What are three examples of agreements an employee should be required to sign?
- How are separation of duties and two-man control different?
- How can collusion be avoided?
- What is the importance of a clear job description?
- What are some of the steps of a termination process?
- Why is it important to conduct an exit interview?

This section covers the following Security+ certification exam objective:

5.1 Explain the importance of policies, plans and procedures related to organizational security.

- Standard operating procedure
- Personnel management
  - Mandatory vacations
  - Job rotation
  - Separation of duties
  - Clean desk
  - Background checks
  - Exit interviews
  - Role-based awareness training
    - Data owner
    - System administrator
    - System owner
    - User
    - Privileged user
    - Executive user
  - NDA
  - Onboarding
  - Continuing education
  - Acceptable use policy/rules of behavior
  - Adverse actions
- General security policies
  - Social media networks/applications
  - Personal email

Video/Demo

3.7.1 Employment Practices  

Time 8:12

Total Video Time 8:12

Copyright © 2017 TestOut Corporation. CompTIA, A+, Network+, Security+, Linux+ and related trademarks and trade names are the trademarks of CompTIA. Microsoft, MCITP, MSCA, MCTS, Windows, and Office 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.
Fact Sheets
- 3.7.2 Employee Management Facts
- 3.7.3 Employee Documents Facts
- 3.7.4 Ethics Facts

Number of Exam Questions
15 questions

Total Time
About 39 minutes
3.8: Mobile Devices

Lecture Focus Questions:

- What does Wi-Fi triangulation do?
- How do Wi-Fi triangulation and cell phone tower triangulation differ?
- Why would you use storage segmentation?
- When would you use remote wipe?

This section covers the following TestOut Security Pro certification exam objectives:

- 2.1 Promote Information Security Awareness
  - Traveling with Personal Mobile Devices
- 3.2 Harden Mobile Devices (iPad)
  - Apply updates
  - Set Autolock
  - Enable passcodes
  - Configure network security settings

This section covers the following Security+ certification exam objective:
2.5 Given a scenario, deploy mobile devices securely

- Mobile device management concepts
  - Remote wipe
  - Screen locks
  - Passwords and pins
  - Storage segmentation
  - Full device encryption

**Video/Demo**

<table>
<thead>
<tr>
<th>Video/Demo</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.8.1 Mobile Device Management</td>
<td>10:20</td>
</tr>
</tbody>
</table>

**Total Video Time** 10:20

**Fact Sheets**

- 3.8.2 Mobile Device Security Facts

**Number of Exam Questions**
6 questions

**Total Time**
*About 22 minutes*
3.9: Third-Party Integration

Lecture Focus Questions:

- What security issues must be identified and addressed during the onboarding phase of a third-party relationship?
- What are the key documents that are included in an Interoperability Agreement (IA)?
- What is the role of the Service Level Agreement (SLA)?
- During the ongoing phase of the relationship, how do you ensure that security has not been compromised?
- Which items need to be disabled or reset during the off-boarding phase of the relationship?

This section covers the following Security+ certification exam objectives:

4.4 Given a scenario, differentiate common account management practices.

- General Concepts
  - Onboarding/offboarding

5.1 Explain the importance of policies, plans and procedures related to organizational security.

- Agreement types
  - BPA
  - SLA
  - ISA
  - MOU/MOA
- Personnel management
  - Onboarding

Video/Demo

3.9.1 Third-Party Integration Security Issues

Total Video Time 7:47

Fact Sheets

3.9.2 Third-Party Integration Security Facts

Number of Exam Questions

5 questions

Total Time

About 18 minutes
4.1: Physical Threats

Lecture Focus Questions:

• What types of physical controls can be implemented to protect the perimeter of a building?
• What is the difference between a mantrap and a double-entry door?
• What types of doors are effective deterrents to piggybacking?
• How does an anti-passback system work?
• What types of devices are best suited for interior motion detection? Perimeter motion detection?
• How do physical access logs help to increase facility security?

In this section, you will learn to:

• Implement physical security

This section covers the following TestOut Security Pro certification exam objective:

• 3.1 Harden Data Center Physical Access
  o Implement access rosters
  o Use visitor identification and control
  o Protect doors and windows
  o Implement physical intrusion detection systems

This section covers the following Security+ certification exam objectives:
2.7 Compare and contrast physical security and environmental controls

• Physical security
  o Hardware locks
  o Mantraps
  o Video Surveillance
  o Fencing
  o Proximity readers
  o Access list
  o Proper lighting
  o Signs
  o Guards
  o Barricades
  o Biometrics
  o Protected distribution (cabling)
  o Alarms
  o Motion detection

• Control types
  o Deterrent
  o Preventive
3.9 Explain the importance of physical security controls.

- Lighting
- Signs
- Fencing/gate/cage
- Security guards
- Alarms
- Safe
- Secure cabinets/enclosures
- Protected distribution/Protected cabling
- Mantrap
- Lock types
- Biometrics
- Barricades/bollards
- Tokens/cards
- Cameras
- Motion detection
- Logs
- Infrared detection
- Key management

**Video/Demo**

- 4.1.1 Physical Security 11:25
- 4.1.2 Tailgating and Piggybacking 2:37

**Total Video Time** 14:02

**Lab/Activity**

- 4.1.4 Implement Physical Security

**Fact Sheets**

- 4.1.3 Physical Security Facts

**Number of Exam Questions**

15 questions

**Total Time**

*About 40 minutes*
4.2: Device Protection

Lecture Focus Questions:

- How can you protect computers that are placed in cubicles?
- What are the security guidelines you should implement to protect servers in your organization?
- How can you ensure that the memory and hard disks cannot be removed from a computer that is bolted to a desk?
- What types of details should a hardware checkout policy include?

In this section, you will learn to:

- Break into a system

This section covers the following TestOut Security Pro certification exam objective:

- 2.3 Maintain Hardware and Software Inventory

This section covers the following Security+ certification exam objective: 2.7 Compare and contrast physical security and environmental controls

- Physical security
  - Hardware locks
  - Proximity readers
  - Protected distribution (cabling)
  - Alarms
  - Motion detection

Video/Demo

<table>
<thead>
<tr>
<th>Video/Demo</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.1 Hardware Security Guidelines</td>
<td>3:25</td>
</tr>
<tr>
<td>4.2.2 Breaking into a System</td>
<td>4:55</td>
</tr>
<tr>
<td><strong>Total Video Time</strong></td>
<td><strong>8:20</strong></td>
</tr>
</tbody>
</table>

Fact Sheets

- 4.2.3 Hardware Security Facts

Number of Exam Questions

5 questions

Total Time

*About 19 minutes*
4.3: Network Infrastructure Protection

Lecture Focus Questions:

- What are the three layers inside the SDN layered architecture?
- How does DNS poisoning work?
- How does domain hijacking work?
- How does man-in-the-browser work?

This section covers the following Security+ certification exam objectives:

1.2 Compare and contrast types of attacks

- Application/service attacks
  - DNS poisoning
  - Domain hijacking
  - Man-in-the-browser

3.2 Given a scenario, implement secure network architecture concepts

Video/Demo

<table>
<thead>
<tr>
<th>Video/Demo</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3.1 Physical Network Protection</td>
<td>4:29</td>
</tr>
</tbody>
</table>

Total Video Time 4:29

Fact Sheets

- 4.3.2 Physical Network Protection Facts

Number of Exam Questions

5 questions

Total Time

About 15 minutes
4.4: Environmental Controls

Lecture Focus Questions:

- What temperature range protects equipment from overheating?
- What is a good HVAC practice to help prevent electrostatic discharge?
- What is the difference between a positive pressure system and a negative pressure system? Which is best to use in a server room?
- What is the difference between a sag and a brownout?
- How does a deluge sprinkler function differently than a wet pipe system?
- What should you do first in the event of a fire?
- When using a portable fire extinguisher, it is recommended that you use the PASS system to administer the fire suppressant. How does the PASS system work?
- What is the recommended range for extinguishing a small fire using a fire extinguisher?
- What are the advantages of using a gas as a fire suppressant? Disadvantages?

This section covers the following Security+ certification exam objectives:

2.7 Compare and contrast physical security and environmental controls

- Environmental controls
  - HVAC
  - Fire suppression
  - EMI shielding
  - Hot and cold aisles
  - Environmental monitoring
  - Temperature and humidity controls

3.9 Explain the importance of physical security controls.

- Airgap
- Environmental controls
  - HVAC
  - Hot and cold aisles
  - Fire suppression

Video/Demo

| 4.4.1 Environmental Controls | 5:01 |
| 4.4.2 Securing Environmental Systems | 4:03 |
| **Total Video Time** | **9:04** |

Fact Sheets

- 4.4.3 Environmental Control Facts
- 4.4.4 Fire Protection Facts
Number of Exam Questions
10 questions

Total Time
About 30 minutes
5.1: Recon and Denial

Lecture Focus Questions:

- How does organizational reconnaissance differ from technical reconnaissance?
- What types of resources make organizational reconnaissance readily available?
- How is footprinting used to determine the operating system of the recipient?
- How does a distributed reflective denial of service (DRDoS) increase the severity of a DoS attack?
- What countermeasures help mitigate DoS and DDoS attacks?

In this section, you will learn to:

- Perform reconnaissance
- Perform a UDP flood attack

This section covers the following Security+ certification exam objectives:

1.2 Compare and contrast types of attacks

- Application/service attacks
  - DoS
  - DDoS

1.4 Explain penetration testing concepts

- Active reconnaissance
- Passive reconnaissance
- Pivot
- Initial exploitation
- Ports
- Persistence
- Escalation of privilege
- Black box
- White box
- Gray box
- Pen testing vs. vulnerability scanning

Video/Demo

<table>
<thead>
<tr>
<th>Video/Demo</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1.1 Reconnaissance</td>
<td>6:41</td>
</tr>
<tr>
<td>5.1.2 Performing Reconnaissance</td>
<td>9:09</td>
</tr>
<tr>
<td>5.1.4 Denial of Service (DoS)</td>
<td>4:45</td>
</tr>
<tr>
<td>5.1.6 Performing a UDP Flood Attack</td>
<td>4:09</td>
</tr>
</tbody>
</table>

Total Video Time: 24:44

Fact Sheets

- 5.1.3 Reconnaissance Facts
- 5.1.5 DoS Attack Facts

Number of Exam Questions

15 questions

Total Time

About 50 minutes
5.2: Spoofing and Poisoning

Lecture Focus Questions:

- Why is a man-in-the-middle attack so dangerous to the victim?
- What countermeasures can you use to control TCP/IP hijacking?
- What methods should you employ to prevent a replay attack?
- What countermeasures can help prevent spoofing?
- What is the difference between primary and secondary DNS servers?
- How does domain name kiting work?
- In what ways can the HOSTS file be used to improve security?

In this section, you will learn to:

- Perform ARP poisoning
- Examine DNS attacks
- Prevent zone transfers

This section covers the following TestOut Security Pro certification exam objective:

- 4.1 Harden the Network Perimeter (using a Cisco Network Security Appliance)
  - Implement web threat protection

This section covers the following Security+ certification exam objective:

1.2 Compare and contrast types of attacks

- Application/service attacks
  - Man-in-the-middle
  - ARP poisoning
  - DNS poisoning
  - Domain hijacking
  - Replay
  - Hijacking and related attacks
    - Session hijacking
  - MAC spoofing
  - IP spoofing

Video/Demo

<table>
<thead>
<tr>
<th>Video/Demo</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.2.1 Session and Spoofing Attacks</td>
<td>4:30</td>
</tr>
<tr>
<td>5.2.3 Performing ARP Poisoning</td>
<td>7:42</td>
</tr>
<tr>
<td>5.2.5 DNS Attacks</td>
<td>6:09</td>
</tr>
<tr>
<td>5.2.7 Examining DNS Attacks</td>
<td>13:48</td>
</tr>
<tr>
<td><strong>Total Video Time</strong></td>
<td><strong>32:09</strong></td>
</tr>
</tbody>
</table>

Lab/Activity

- 5.2.8 Prevent Zone Transfers
Fact Sheets
- 5.2.2 Session-Based Attack Facts
- 5.2.4 Spoofing Facts
- 5.2.6 DNS Attack Facts

Number of Exam Questions
15 questions

Total Time
About 68 minutes
5.3: Security Appliances

Lecture Focus Questions:

- What are the benefits and risks of using proxy servers?
- What is the purpose of a content filtering server?
- How can Network Access Controls (NAC) improve a network’s security?
- What is the difference between the intranet and the internet?
- What are the uses of a DMZ?
- Why is a Honeynet useful?
- What are the features of an all-in-one security appliance?
- What size organization should employ an all-in-one security appliance?

In this section, you will learn to:

- Configure Network Security Appliance access

This section covers the following TestOut Security Pro certification exam objective:

- 5.2 Implement Intrusion Detection/Prevention (Using a Cisco Network Security Appliance)
  - Enable IPS protection for a LAN and DMZ
  - Apply IPS signature updates
  - Configure IPS policy

This section covers the following Security+ certification exam objectives:

2.1 Install and configure network components, both hardware- and software-based, to support organizational security

- Proxy
- NAC
- Mail gateway
  - Spam filter

3.2 Given a scenario, implement secure network architecture concepts

- Zones/topologies
  - DMZ
  - Extranet
  - Intranet
  - Wireless
  - Guest
  - Honeynets
  - Ad hoc
- Security device/technology placement
  - Filters
  - Proxies
Video/Demo

- 5.3.1 Security Solutions 4:46
- 5.3.2 Security Zones 4:34
- 5.3.4 All-In-One Security Appliances 3:10
- 5.3.6 Configuring Network Security Appliance Access 5:40

Total Video Time 18:10

Lab/Activity

- 5.3.7 Configure Network Security Appliance Access

Fact Sheets

- 5.3.3 Security Zone Facts
- 5.3.5 Security Solution Facts

Number of Exam Questions

5 questions

Total Time

About 39 minutes
5.4: Demilitarized Zones (DMZ)

Lecture Focus Questions:
- How is a honeypot used to increase network security?
- How is a gateway different from a router?
- What is the typical configuration for a DMZ configured as a dual-homed gateway?
- A screened subnet uses two firewalls. What are the functions of each firewall?
- What type of computer might exist inside of a demilitarized zone (DMZ)?
- What makes bastion hosts vulnerable to attack? What should you do to harden bastion hosts?

In this section, you will learn to:
- Configure a DMZ

This section covers the following TestOut Security Pro certification exam objective:
- 4.1 Harden the Network Perimeter (using a Cisco Network Security Appliance)
  - Create a DMZ
- 8.2 Protect Data Transmissions Across Open, Public Networks
  - Encrypt data communications

This section covers the following Security+ certification exam objective:
3.2 Given a scenario, implement secure network architecture concepts
- Zones/topologies
  - DMZ

Video/Demo
- 5.4.1 Demilitarized Zones 6:49
- 5.4.2 Configuring a DMZ 3:50
Total Video Time 10:39

Lab/Activity
- 5.4.3 Configure a DMZ

Fact Sheets
- 5.4.4 DMZ Facts

Number of Exam Questions
6 questions

Total Time
About 27 minutes
5.5: Firewalls

Lecture Focus Questions:

- What is the difference between a network-based firewall and an application/host-based firewall?
- When would you choose to implement a host-based firewall?
- What traffic characteristics can be specified in a filtering rule for a packet filtering firewall?
- How does a packet filtering firewall differ from a circuit-level gateway?
- Where should a network-based firewall be placed?

In this section, you will learn to:

- Configure a perimeter firewall

This section covers the following TestOut Security Pro certification exam objective:

- 4.1 Harden the Network Perimeter (using a Cisco Network Security Appliance)
  - Configure a firewall
  - Implement web threat protection

This section covers the following Security+ certification exam objectives:

2.1 Install and configure network components, both hardware- and software-based, to support organizational security.

- Firewall
  - ACL
  - Application-based vs. network-based
  - Stateful vs. stateless
  - Implicit deny

2.3 Given a scenario, troubleshoot common security issues

- Misconfigured devices
  - Firewall

2.4 Given a scenario, analyze and interpret output from security technologies

- Host-based firewall

3.2 Given a scenario, implement secure network architecture concepts

- Security device/technology placement
  - Filters
  - Proxies
  - Firewalls
Video/Demo

- 5.5.1 Firewalls  
- 5.5.3 Configuring a Perimeter Firewall  

**Total Video Time** 14:18

Lab/Activity

- 5.5.4 Configure a Perimeter Firewall

Fact Sheets

- 5.5.2 Firewall Facts

Number of Exam Questions

15 questions

Total Time

*About 40 minutes*
5.6: Network Address Translation (NAT)

Lecture Focus Questions:

- How has NAT extended the use of IPv4?
- How does a NAT router associate a port number with a request from a private host?
- What are the three ways NAT can be implemented?
- Where is NAT typically implemented?
- Why do private networks have a limited range of IP addresses?

In this section, you will learn to:

- Install and configure the Network Address Translation (NAT) IP routing protocol on a router
- Configure the NAT router to act as a DHCP server
- Configure the NAT router to act as a DNS proxy
- Configure NAT from the CLI
- Configure NAT on an NSA

This section covers the following TestOut Security Pro certification exam objective:

- 4.1 Harden the Network Perimeter (using a Cisco Network Security Appliance)
- Configure NAT

This section covers the following Security+ certification exam objective:

3.2 Given a scenario, implement secure network architecture concepts

- Zones/topologies
  - NAT

Video/Demo

- 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

Total Video Time 21:02

Fact Sheets

- 5.6.4 NAT Facts

Number of Exam Questions

6 questions

Total Time

About 33 minutes
5.7: Virtual Private Networks (VPN)

Lecture Focus Questions:

- What are three ways a VPN can be implemented?
- What is a VPN concentrator?
- What function do VPN endpoints provide?
- What is the difference between full tunnel and split tunnel?
- What are three types of protocols used by a VPN?
- What is inverse split tunneling?

In this section, you will learn to:

- Configure a remote access VPN
- Configure a VPN connection iPad

This section covers the following TestOut Security Pro certification exam objective:

- 4.1 Harden the Network Perimeter (using a Cisco Network Security Appliance)
  - Configure VPN

This section covers the following Security+ certification exam objectives:

2.1 Install and configure network components, both hardware- and software-based, to support organizational security

- VPN concentrator
  - Remote access vs. site-to-site
  - IPSec
    - Tunnel mode
    - Transport mode
    - AH
    - ESP
  - Split tunnel vs. full tunnel
  - TLS
  - Always-on VPN

3.2 Given a scenario, implement secure network architecture concepts

- Tunneling/VPN
  - Site-to-site
  - Remote access
- Security device/technology placement
  - VPN concentrators
Video/Demo

<table>
<thead>
<tr>
<th>Topic</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.7.1 Virtual Private Networks (VPNs)</td>
<td>7:03</td>
</tr>
<tr>
<td>5.7.2 Configuring a VPN</td>
<td>2:34</td>
</tr>
<tr>
<td>5.7.3 Configuring a VPN Client</td>
<td>10:36</td>
</tr>
<tr>
<td><strong>Total Video Time</strong></td>
<td><strong>20:13</strong></td>
</tr>
</tbody>
</table>

Lab/Activity

- 5.7.4 Configure a Remote Access VPN
- 5.7.5 Configure a VPN Connection iPad

Fact Sheets

- 5.7.6 VPN Facts
- 5.7.7 VPN Protocol Facts

Number of Exam Questions
10 questions

Total Time

*About 51 minutes*
5.8: Web Threat Protection

Lecture Focus Questions:

- What is the difference between a web filter and web threat filtering?
- Which web threat protections prevent a user from visiting restricted websites?
- Where are SPAM filters normally located on your network?
- What are the pros and cons of using an all-in-one device?
- How can proxies be used for web threat protection?

In this section, you will learn to:

- Configure web threat protection

This section covers the following TestOut Security Pro certification exam objective:

- 4.1 Harden the Network Perimeter (using a Cisco Network Security Appliance)
  - Implement web threat protection

This section covers the following Security+ certification exam objectives:

2.1 Install and configure network components, both hardware- and software-based, to support organizational security.

- Proxy
  - Forward and reverse proxy
  - Transparent
  - Application/multipurpose
- Mail gateway
  - Spam filter
  - DLP
  - Encryption

2.3 Given a scenario, troubleshoot common security issues

- Misconfigured devices
  - Content filter

3.2 Given a scenario, implement secure network architecture concepts

- Security device/technology placement
  - Filters
  - Proxies

Video/Demo Time

- 5.8.1 Web Threat Protection 7:03
- 5.8.2 Configuring Web Threat Protection 4:26

Total Video Time 11:29
Lab/Activity
- 5.8.3 Configure Web Threat Protection

Fact Sheets
- 5.8.4 Web Threat Protection Facts

Number of Exam Questions
5 questions

Total Time
About 27 minutes
5.9: Network Access Protection

Lecture Focus Questions:

- How do remediation servers and auto-remediation help clients become compliant?
- Which server role service do you add to configure a server as an enforcement point for NAP?
- How do you define the quarantine network when using 802.1x enforcement?
- Which enforcement method uses a Health Registration Authority (HRA)?
- What type of communication occurs in the boundary network when using IPsec enforcement?
- What is an agent?

In this section, you will learn to:

- Implement NAC with DHCP enforcement

This section covers the following TestOut Security Pro certification exam objective:

- 1.2 Harden Authentication
  - Configure secure remote access

This section covers the following Security+ certification exam objective:

2.1 Install and configure network components, both hardware- and software-based, to support organizational security

- NAC
  - Dissolvable vs. permanent
  - Host health checks
  - Agent vs. agentless

Video/Demo

<table>
<thead>
<tr>
<th></th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.9.1 Network Access Protection</td>
<td>6:34</td>
</tr>
<tr>
<td>5.9.2 Implementing NAC with DHCP Enforcement</td>
<td>14:04</td>
</tr>
<tr>
<td>Total Video Time</td>
<td>20:38</td>
</tr>
</tbody>
</table>

Fact Sheets

|   | 5.9.3 NAP Facts |

Number of Exam Questions

5 questions

Total Time

About 31 minutes
5.10: Wireless Overview

Lecture Focus Questions:

- What is the role of a wireless access point (WAP)?
- What is the difference in functionality between an omnidirectional antenna and a directional antenna?
- Which two methods are available for configuring a wireless network?
- What is the purpose of a wireless LAN controller?
- What is the difference between a fat WAP and a thin WAP?
- How does WPA2 differ from WPA?

In this section, you will learn to:

- Configure a wireless network

This section covers the following TestOut Security Pro certification exam objective:

- 4.2 Secure Wireless Devices and Clients
  - Implement WPA2
  - Configure enhanced security
    - MAC filtering
    - SSID cloaking
    - Power control
  - Disable Network Discovery

This section covers the following Security+ certification exam objectives:

2.1 Install and configure network components, both hardware- and software-based, to support organizational security

- Access point
  - SSID
  - MAC filtering
  - Signal strength
  - Band selection/width
  - Antenna types and placement
  - Fat vs. thin
  - Controller-based vs. standalone

- Bridge

3.2 Given a scenario, implement secure network architecture concepts

- Zones/topologies
  - Wireless
  - Ad hoc
6.3 Given a scenario, install and configure wireless security settings

- Cryptographic protocols
  - WPA
  - WPA2
  - CCMP
  - TKIP
- Authentication protocols
  - EAP
  - PEAP
  - EAP-FAST
  - EAP-TLS
  - EAP-TTLS
  - IEEE 802.1x
  - RADIUS Federation
- Methods
  - PSK vs. Enterprise vs. Open
  - WPS
  - Captive portals

Video/Demo
- 5.10.1 Wireless Networking Overview  5:58
- 5.10.2 Wireless Antenna Types  5:01
- 5.10.4 Wireless Encryption  5:52
- 5.10.6 Configuring a Wireless Connection  6:47

Total Video Time  23:38

Lab/Activity
- 5.10.7 Configure a Wireless Network

Fact Sheets
- 5.10.3 Wireless Networking Facts
- 5.10.5 Wireless Encryption Facts

Number of Exam Questions
15 questions

Total Time
About 54 minutes
5.11: Wireless Attacks

Lecture Focus Questions:

- What is the difference between bluejacking and bluesnarfing?
- Why is a successful bluebugging attack more dangerous to the victim than a bluesnarfing attack?
- What is the best method for protecting against attacks directed towards Bluetooth capabilities?
- What is the difference between a rogue access point and an evil twin?
- How can you protect your network against rogue access points?

In this section, you will learn to:

- Use wireless attack tools
- Detect rogue hosts
- Configure rogue host protection

This section covers the following Security+ certification exam objective:

1.2 Compare and contrast types of attacks.

- Wireless attacks
  - Replay
  - IV
  - Evil twin
  - Rogue AP
  - Jamming
  - WPS
  - Bluejacking
  - Bluesnarfing
  - RFID
  - NFC
  - Disassociation

Video/Demo

<table>
<thead>
<tr>
<th></th>
<th></th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>🔥 5.11.1 Wireless Attacks</td>
<td></td>
<td>6:21</td>
</tr>
<tr>
<td>🎬 5.11.3 Using Wireless Attack Tools</td>
<td></td>
<td>7:56</td>
</tr>
<tr>
<td>🎬 5.11.4 Detecting Rogue Hosts</td>
<td></td>
<td>4:36</td>
</tr>
<tr>
<td><strong>Total Video Time</strong></td>
<td></td>
<td><strong>18:53</strong></td>
</tr>
</tbody>
</table>

Lab/Activity

- 5.11.5 Configure Rogue Host Protection

Fact Sheets

- 5.11.2 Wireless Attack Facts
Number of Exam Questions
15 questions

Total Time
About 44 minutes
5.12: Wireless Defenses

Lecture Focus Questions:

- How does turning off the SSID broadcast help secure the wireless network?
- What methods can you use to secure a wireless network from data emanation?
- What does open authentication use for authenticating a device? Why isn’t this solution very secure?
- Which two additional components are required to implement 802.1x authentication?
- What does WEP use for the encryption key? Why does this present a security problem?
- Why should you not use shared key authentication with WEP?
- What is the difference between WPA Personal and WPA Enterprise?
- You have an access point that currently supports only WEP. What would you typically need to do to support WPA2?
- Which encryption methods are used with WPA and WPA2?
- What is the difference between 2.4 Ghz frequencies and 5 GHz frequencies?

In this section, you will learn to:

- Harden a wireless network
- Configure WIPS
- Configure a captive portal

This section covers the following TestOut Security Pro certification exam objectives:

- 4.2 Secure Wireless Devices and Clients
  - Change the default user name, password, and administration limits
  - Implement WPA2
  - Configure enhanced security
    - MAC filtering
    - SSID cloaking
    - Power control
- 5.1 Harden Network Devices (Using a Cisco Small Business Switch)
  - Remove unsecure protocols (FTP, telnet, rlogin, rsh)
- 8.1 Protect and Maintain the Integrity of Data Files
  - Implement encryption technologies
- 8.2 Protect Data Transmissions Across Open, Public Networks
  - Encrypt data communications
  - Implement secure protocols
  - Remove unsecure protocols

This section covers the following Security+ certification exam objectives:

1.6 Explain the impact associated with types of vulnerabilities.
- Misconfiguration/weak configuration
- Default configuration

2.1 Install and configure network components, both hardware- and software-based, to support organizational security.

- Access point
  - SSID
  - MAC filtering
  - Signal strength
  - Band selection/width
  - Antenna types and placement
  - Fat vs. thin
  - Controller-based vs. standalone

2.3 Given a scenario, troubleshoot common security issues.

- Misconfigured devices
  - Access points

6.3 Given a scenario, install and configure wireless security settings.

- Authentication protocols
  - EAP
  - PEAP
  - EAP-FAST
  - EAP-TLS
  - EAP-TTLS
  - IEEE 802.1x
  - RADIUS Federation
- Methods
  - PSK vs. Enterprise vs. Open
  - WPS
  - Captive portals

### Video/Demo

<table>
<thead>
<tr>
<th>Video/Demo</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.12.1 Wireless Security Considerations</td>
<td>7:45</td>
</tr>
<tr>
<td>5.12.2 Wireless Authentication</td>
<td>5:23</td>
</tr>
<tr>
<td>5.12.4 Hardening a Wireless Access Point</td>
<td>6:39</td>
</tr>
<tr>
<td>5.12.7 Configuring a Captive Portal</td>
<td>4:15</td>
</tr>
</tbody>
</table>

**Total Video Time** 24:02

### Lab/Activity

- 5.12.5 Harden a Wireless Network
- 5.12.6 Configure WIPS

---

Copyright © 2017 TestOut Corporation. CompTIA, A+, Network+, Security+, Linux+ and related trademarks and trade names are the trademarks of CompTIA. Microsoft, MCITP, MSCA, MCTS, Windows, and Office 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.
Fact Sheets
- 5.12.3 Wireless Authentication Facts
- 5.12.8 Wireless Security Facts

Number of Exam Questions
15 questions

Total Time
*About 60 minutes*
6.1: Network Threats

Lecture Focus Questions:

- How does a passive attack differ from an active attack?
- How does educating and training users maintain a secure network environment?
- Which areas of your network should you focus on to best understand it?
- How does segmenting your network increase network security?

This section covers the following Security+ certification exam objectives:

1.6 Explain the impact associated with types of vulnerabilities

- Untrained users

3.2 Given a scenario, implement secure network architecture concepts

- Segregation/segmentation/isolation
  - Physical
  - Logical (VLAN)

5.3 Explain risk management processes and concepts

- Threat assessment
  - Internal vs. external

Video/Demo

<table>
<thead>
<tr>
<th>Video/Demo</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1.1 Network Threats Overview</td>
<td>8:34</td>
</tr>
</tbody>
</table>

Total Video Time 8:34

Fact Sheets

6.1.2 Network Threats Facts

Number of Exam Questions

5 questions

Total Time

About 19 minutes
6.2: Network Device Vulnerabilities

Lecture Focus Questions:

- For security considerations, what is the first thing you should do when new hardware and software is turned on for the first time?
- What are the characteristics of a complex password?
- Why is it important to apply new firmware or patches for devices within your organization?
- What are some major risks of hard-coded passwords on devices throughout the enterprise?
- What are some resources that you can use to keep track of existing vulnerabilities for the technology you may use throughout your organization?

In this section, you will learn to:

- Search defaultpasswords.com.
- Secure a switch

This section covers the following TestOut Security Pro certification exam objectives:

- 4.1 Harden the Network Perimeter (using a Cisco Network Security Appliance)
  - Change the default user name and password
- 5.1 Harden Network Devices (Using a Cisco Small Business Switch)
  - Change the default user name and password on network devices
  - Use secure passwords

This section covers the following Security+ certification exam objectives:

1.1 Given a scenario, analyze indicators of compromise and determine the type of malware

- Backdoor

1.2 Compare and contrast types of attacks

- Application/service attacks
  - Privilege escalation

3.3 Given a scenario, implement secure systems design

- Operating systems
  - Disable default accounts/passwords

Given a scenario, differentiate common account management practices

- Account policy enforcement
  - Password complexity
Video/Demo
- 6.2.1 Device Vulnerabilities 6:55
- 6.2.3 Searching defaultpasswords.com 2:18
- 6.2.4 Securing a Switch 2:56

Total Video Time 12:09

Lab/Activity
- 6.2.5 Secure a Switch

Fact Sheets
- 6.2.2 Device Vulnerability Facts

Number of Exam Questions
5 questions

Total Time
About 28 minutes
6.3: Network Applications

Lecture Focus Questions:

- What kinds of security problems might you have with P2P software?
- Which types of malware are commonly spread through instant messaging (IM)?
- What security concerns should you be aware of when using instant messaging software?
- What security measures should you incorporate to control the use of networking software?

In this section, you will learn to:

- Configure application control software

This section covers the following TestOut Security Pro certification exam objective:

- 7.1 Implement Application Defenses
  - Configure a GPO for application whitelisting
  - Configure parental controls to enforce web content filtering

This section covers the following Security+ certification exam objective:

3.3 Given a scenario, implement secure systems design

- Operating systems
  - Disabling unnecessary ports and services

Video/Demo

<table>
<thead>
<tr>
<th>Video/Demo</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.3.1 Network Application Security</td>
<td>4:57</td>
</tr>
<tr>
<td>6.3.2 Configuring Application Control Software</td>
<td>7:46</td>
</tr>
<tr>
<td><strong>Total Video Time</strong></td>
<td><strong>12:43</strong></td>
</tr>
</tbody>
</table>

Fact Sheets

- 6.3.3 Network Application Facts

Number of Exam Questions

5 questions

Total Time

About 23 minutes
6.4: Switch Attacks

Lecture Focus Questions:

- What types of attacks are commonly perpetrated against switches?
- How does MAC flooding make a switch function as a hub? What is this state called?
- How are switches indirectly involved in ARP poisoning?
- How does the attacker hide his identity when performing MAC spoofing?

This section covers the following Security+ certification exam objective:
1.2 Compare and contrast types of attacks

- Application/service attacks
  - ARP poisoning
  - MAC spoofing

Video/Demo

Video/Demo 6.4.1 Switch Attacks Time 5:42
Total Video Time 5:42

Fact Sheets

Fact Sheets 6.4.2 Switch Attack Facts

Number of Exam Questions

5 questions

Total Time

About 16 minutes
6.5: Switch Security

Lecture Focus Questions:

- How does a switch identify devices that are in different VLANs?
- What is the function of a trunk port?
- When trunking is used, how is the receiving switch able to identify which VLAN the frame belongs to?
- What is required for devices to communicate between VLANs?
- How is port security different from port filtering?

In this section, you will learn to:

- Harden a switch
- Secure access to a switch

This section covers the following TestOut Security Pro certification exam objectives:

- 5.1 Harden Network Devices (Using a Cisco Small Business Switch)
  - Implement port security
  - Remove unsecure protocols (FTP, telnet, rlogin, rsh)
  - Run latest iOS version
  - Segment traffic using VLANs
- 7.1 Implement Application Defenses
  - Configure virtual machines and switches

This section covers the following Security+ certification exam objectives:

2.1 Install and configure network components, both hardware- and software-based, to support organizational security.

- Switch
  - Port security
  - Layer 2 vs. Layer 3
  - Loop prevention
  - Flood guard
- Access point
  - MAC filtering

3.2 Given a scenario, implement secure network architecture concepts.

- Segregation/segmentation/isolation
  - Logical (VLAN)
- Security device/technology placement
  - Filters
  - Aggregation switches
Video/Demo

<table>
<thead>
<tr>
<th>Feature</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.5.1 Switch Features</td>
<td>6:53</td>
</tr>
<tr>
<td>6.5.2 Securing Network Switches</td>
<td>6:34</td>
</tr>
<tr>
<td>6.5.4 Hardening a Switch</td>
<td>10:37</td>
</tr>
<tr>
<td><strong>Total Video Time</strong></td>
<td><strong>24:04</strong></td>
</tr>
</tbody>
</table>

Lab/Activity

- 6.5.5 Harden a Switch
- 6.5.6 Secure Access to a Switch
- 6.5.7 Secure Access to a Switch 2

Fact Sheets

- 6.5.3 Switch Security Facts

Number of Exam Questions

15 questions

Total Time

*About 60 minutes*
6.6: Using VLANs

Lecture Focus Questions:

- What are two advantages to creating VLANs on your network?
- You have two VLANs configured on a single switch. How many broadcast domains are there? How many collision domains are there?
- What happens if two devices on the same switch are assigned to different VLANs?

In this section, you will learn to:

- Configure VLANs from the CLI
- Configure VLANs

This section covers the following TestOut Security Pro certification exam objective:

- 5.1 Harden Network Devices (Using a Cisco Small Business Switch)
  - Segment traffic using VLANs

This section covers the following Security+ certification exam objective:

3.2 Given a scenario, implement secure network architecture concepts

- Segregation/segmentation/isolation
  - Logical (VLAN)

Video/Demo

<table>
<thead>
<tr>
<th>6.6.1 VLAN Overview</th>
<th>4:07</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.6.2 Configuring VLANs from the CLI</td>
<td>4:39</td>
</tr>
<tr>
<td>6.6.5 Configuring VLANs</td>
<td>3:09</td>
</tr>
</tbody>
</table>

Total Video Time 11:55

Lab/Activity

- 6.6.4 Explore VLANs from the CLI
- 6.6.6 Explore VLANs

Fact Sheets

- 6.6.3 VLAN Facts

Number of Exam Questions

5 questions

Total Time

About 32 minutes
6.7: Router Security

Lecture Focus Questions:

- Why should you change router defaults on new routers?
- Which secure protocols should you use to remotely manage a router?
- What type of actions can be used to ensure the physical security of network devices?
- Why should you update router firmware?
- How do ACLs work on a router?

In this section, you will learn to:

- Restrict Telnet and SSH access
- Permit traffic
- Block source hosts

This section covers the following TestOut Security Pro certification exam objectives:

- 3.1 Harden Data Center Physical Access
  - Implement access rosters
  - Protect doors and windows
- 5.1 Harden Network Devices (Using a Cisco Small Business Switch)
  - Implement access lists, deny everything else

This section covers the following Security+ certification exam objectives:

1.6 Explain the impact associated with types of vulnerabilities

- Misconfiguration/weak configuration
- Default configuration

2.1 Install and configure network components, both hardware- and software-based, to support organizational security

- Router
  - ACLs
  - Antispoofing

**Video/Demo**

<table>
<thead>
<tr>
<th>Video/Demo</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.7.1 Router Security</td>
<td>7:03</td>
</tr>
<tr>
<td>6.7.2 Router ACLs</td>
<td>2:48</td>
</tr>
<tr>
<td>6.7.4 Configuring ACLs</td>
<td>7:10</td>
</tr>
</tbody>
</table>

**Total Video Time** 17:01
Lab/Activity
- 6.7.5 Restrict Telnet and SSH Access
- 6.7.6 Permit Traffic
- 6.7.7 Block Source Hosts

Fact Sheets
- 6.7.3 Router Security Facts

Number of Exam Questions
5 questions

Total Time
About 43 minutes
6.8: Intrusion Detection and Prevention

Lecture Focus Questions:

- What does it mean when traffic is labeled as a false negative?
- What data sources does an IDS system use to gather information that it will analyze to find attacks?
- How does an IPS differ from an IDS?
- What type of recognition method is used by most virus scanning software?
- What is the advantage of using a network-based IDS instead of a host-based IDS?
- What are the security reasons for using a honeypot or honeynet?
- After an attack, what types of data should you back up to retain information about the attack for future investigations?

In this section, you will learn to:

- Implement intrusion monitoring
- Implement intrusion prevention

This section covers the following TestOut Security Pro certification exam objective:

- 4.1 Harden the Network Perimeter (using a Cisco Network Security Appliance)
  - Implement web threat protection

This section covers the following Security+ certification exam objective:

2.1 Install and configure network components, both hardware- and software-based, to support organizational security

- NIPS/NIDS
  - Signature-based
  - Heuristic/behavioral
  - Anomaly
  - Inline vs. passive
  - In-band vs. out-of-band
  - Rules
  - Analytics
  - False positive
  - False negative

Video/Demo

<table>
<thead>
<tr>
<th>Video/Demo</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.8.1 Intrusion Detection</td>
<td>6:30</td>
</tr>
<tr>
<td>6.8.2 Detection vs. Prevention Controls</td>
<td>5:36</td>
</tr>
<tr>
<td>6.8.4 Implementing Intrusion Monitoring</td>
<td>9:17</td>
</tr>
<tr>
<td>6.8.5 Implementing Intrusion Prevention</td>
<td>5:58</td>
</tr>
<tr>
<td><strong>Total Video Time</strong></td>
<td>27:21</td>
</tr>
</tbody>
</table>
Lab/Activity
  - 6.8.6 Implement Intrusion Prevention

Fact Sheets
  - 6.8.3 IDS Facts

Number of Exam Questions
15 questions

Total Time
About 53 minutes
6.9: Vulnerability Assessment

Lecture Focus Questions:

- Why should an administrator perform a vulnerability assessment on a system?
- What is the most important step to perform before running a vulnerability scan? Why?
- How does a port scanner identify devices with ports that are in a listening state?
- How can a port scanner be used maliciously?
- What types of items does OVAL identify as a definition?

In this section, you will learn to:

- Scan a network with Nessus
- Scan a network with Retina
- Scan for vulnerabilities
- Perform port and ping scans

This section covers the following TestOut Security Pro certification exam objective:

- 5.1 Harden Network Devices (Using a Cisco Small Business Switch)
  - Shut down unnecessary services and ports
  - Implement port security

This section covers the following Security+ certification exam objectives:

1.4 Explain penetration testing concepts

- Ports

1.5 Explain vulnerability scanning concepts

- Passively test security controls
- Identify vulnerability
- Identify lack of security controls
- Identify common misconfigurations
- Intrusive vs. non-intrusive
- Credentialed vs. non-credentialed
- False positive

2.1 Install and configure network components, both hardware- and software-based, to support organizational security

- Switch
  - Port security
2.2 Given a scenario, use appropriate software tools to assess the security posture of an organization

- Network scanners
  - Rogue system detection
  - Network mapping
- Wireless scanners/cracker
- Password cracker
- Vulnerability scanner
- Command line tools
  - ping

3.3 Given a scenario, implement secure systems design

- Operating systems
  - Disabling unnecessary ports and services
  - Secure configurations

### Video/Demo

<table>
<thead>
<tr>
<th>Video/Demo</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.9.1 Vulnerability Assessment</td>
<td>4:23</td>
</tr>
<tr>
<td>6.9.3 Scanning a Network with Nessus</td>
<td>7:26</td>
</tr>
<tr>
<td>6.9.4 Scanning a Network with Retina</td>
<td>7:16</td>
</tr>
<tr>
<td>6.9.9 Performing Port and Ping Scans</td>
<td>4:57</td>
</tr>
<tr>
<td><strong>Total Video Time</strong></td>
<td><strong>24:02</strong></td>
</tr>
</tbody>
</table>

### Lab/Activity

- 6.9.5 Scan for Vulnerabilities 1
- 6.9.6 Scan for Vulnerabilities 2
- 6.9.7 Scan for Vulnerabilities 3
- 6.9.8 Scan for Vulnerabilities 4

### Fact Sheets

- 6.9.2 Vulnerability Assessment Facts

### Number of Exam Questions

14 questions

### Total Time

*About 64 minutes*
**6.10: Protocol Analyzers**

**Lecture Focus Questions:**

- What types of information can a protocol analyzer provide?
- When using a protocol analyzer, why is it necessary to configure the NIC in *promiscuous* mode?
- When running a protocol analyzer on a switch, how does *port mirroring* work?
- What are some common protocol analyzers?

In this section, you will learn to:

- Analyze network traffic

This section covers the following TestOut Security Pro certification exam objective:

- 7.1 Implement Application Defenses
  - Configure virtual machines and switches

This section covers the following Security+ certification exam objective:

2.2 Given a scenario, use appropriate software tools to assess the security posture of an organization

- Protocol analyzer

**Video/Demo**

<table>
<thead>
<tr>
<th>Video/Demo</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.10.1 Protocol Analyzers</td>
<td>2:37</td>
</tr>
<tr>
<td>6.10.3 Analyzing Network Traffic</td>
<td>13:19</td>
</tr>
<tr>
<td><strong>Total Video Time</strong></td>
<td><strong>15:56</strong></td>
</tr>
</tbody>
</table>

**Fact Sheets**

- 6.10.2 Protocol Analyzer Facts

**Number of Exam Questions**

8 questions

**Total Time**

*About 29 minutes*
6.11: Remote Access

Lecture Focus Questions:

- How does EAP differ from CHAP or MS-CHAP?
- What is the difference between authentication and authorization?
- What is PPPoE? What is it used for?
- What are examples of criteria used to restrict remote access?
- Why is PSTN uncommon?
- What types of attacks are remote access servers vulnerable to?

In this section, you will learn to:

- Configure a RADIUS solution

This section covers the following TestOut Security Pro certification exam objective:

- 1.2 Harden Authentication
  - Configure secure remote access

This section covers the following Security+ certification exam objectives:

2.6 Given a scenario, implement secure protocols.

- Protocols
  - SNMPv3
  - SSL/TLS
- Use cases
  - Remote access

4.2 Given a scenario, install and configure identity and access services.

- TACACS+
- CHAP
- PAP
- MSCHAP
- RADIUS

Video/Demo Time

- ▶ 6.11.1 Remote Access 15:04
- ▶ 6.11.3 Configuring a RADIUS Solution 9:46

Total Video Time 24:50

Fact Sheets

- ▶ 6.11.2 Remote Access Facts
- ▶ 6.11.4 RADIUS and TACACS+ Facts
Number of Exam Questions
15 questions

Total Time
About 50 minutes
6.12: Network Authentication

Lecture Focus Questions:

- Using a challenge/response process, what information is exchanged over the network during logon? How does this provide security for logon credentials?
- What is the difference between authentication with LAN Manager and NT LAN Manager?
- What security vulnerabilities should an administrator be aware of when using Kerberos for authentication?
- Which two entities are combined to make up the KDC?
- Why does Kerberos require clock synchronization between devices?

After finishing this section, you should be able to complete the following tasks:

- Control the authentication method
- Configure kerberos policy settings
- Use credential management

This section covers the following Security+ certification exam objective:

4.2 Given a scenario, install and configure identity and access services.

- LDAP
- Kerberos
- SAML
- OpenID Connect
- OAUTH
- Shibboleth
- Secure token
- NTLM

**Video/Demo**

<table>
<thead>
<tr>
<th>Video/Demo</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.12.1 Network Authentication Protocols</td>
<td>9:45</td>
</tr>
<tr>
<td>6.12.3 LDAP Authentication</td>
<td>5:53</td>
</tr>
<tr>
<td>6.12.4 Kerberos Authentication</td>
<td>5:04</td>
</tr>
<tr>
<td>6.12.5 Controlling the Authentication Method</td>
<td>6:45</td>
</tr>
<tr>
<td>6.12.7 Credential Management</td>
<td>4:26</td>
</tr>
<tr>
<td><strong>Total Video Time</strong></td>
<td><strong>31:53</strong></td>
</tr>
</tbody>
</table>

**Lab/Activity**

- 6.12.6 Configure Kerberos Policy Settings

**Fact Sheets**

- 6.12.2 Network Authentication Facts
- 6.12.8 Credential Management Facts
Number of Exam Questions
15 questions

Total Time
*About 62 minutes*
6.13: Penetration Testing

**Lecture Focus Questions:**

- What is the main goal of penetration testing?
- What type of tools or methods does a penetration test use?
- Why should you be careful in the methods you deploy?
- What should you do before performing a penetration test?
- How does a penetration test differ from a vulnerability assessment or scan?
- What types of details do the rules of engagement identify?
- What security function does the Open Source Security Testing Methodology Manual (OSSTMM) provide?

In this section, you will learn to:

- Use penetration testing tools

This section covers the following Security+ certification exam objectives:

1.4 Explain penetration testing concepts.

- Active reconnaissance
- Passive reconnaissance
- Pivot
- Initial exploitation
- Ports
- Persistence
- Escalation of privilege
- Black box
- White box
- Gray box
- Pen testing vs. vulnerability scanning

5.3 Explain risk management processes and concepts.

- Risk assessment
  - Testing
    - Penetration testing authorization
    - Vulnerability testing authorization

**Video/Demo**

| 6.13.1 Penetration Testing | 2:38 |
| 6.13.3 Exploring Penetration Testing Tools | 11:47 |

**Total Video Time** 14:25

**Fact Sheets**

6.13.2 Penetration Testing Facts
Number of Exam Questions
12 questions

Total Time
About 32 minutes
6.14: Virtual Networking

Lecture Focus Questions:

- How does a virtual network differ from a physical network?
- What is a VPN?
- What is a virtual machine?
- What are some virtualization terms and what do they mean?
- What is a Dynamic Host Configuration Protocol (DHCP)?
- How can physical devices become virtual ones?
- What is at least one example of the network virtualization service providers?

In this section, you will learn to:

- Configure virtual network devices
- Create virtual switches

This section covers the following TestOut Security Pro certification exam objective:

- 7.1 Implement Application Defenses
  - Configure virtual machines and switches

This section covers the following Security+ certification exam objectives:

3.2 Given a scenario, implement secure network architecture concepts.

- Segregation/segmentation/isolation
  - Virtualization

3.7 Summarize cloud and virtualization concepts.

- Hypervisor
  - Type I
  - Type II
  - Application cells/containers
- VM sprawl avoidance
- VM escape protection
- VDI/VDE

**Video/Demo**

<table>
<thead>
<tr>
<th>Video/Demo</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.14.1 Virtual Networking Overview</td>
<td>6:04</td>
</tr>
<tr>
<td>6.14.3 Configuring Virtual Network Devices</td>
<td>3:13</td>
</tr>
<tr>
<td><strong>Total Video Time</strong></td>
<td><strong>13:30</strong></td>
</tr>
</tbody>
</table>

**Lab/Activity**

- 6.14.6 Create Virtual Switches
Fact Sheets
- 6.14.4 Virtualization Implementation Facts
- 6.14.5 Virtual Networking Facts

Number of Exam Questions
5 questions

Total Time
About 34 minutes
6.15: Software-Defined Networking (SDN)

Lecture Focus Questions:

- Which three layers exist in the SDN architecture?
- What is the function of the controller?
- Which technology allows network and security professionals to manage, control, and make changes to a network?
- What are the advantages of SDN?
- What are the disadvantages of SDN?

This section covers the following Security+ certification exam objective:
3.2 Given a scenario, implement secure network architecture concepts.

- SDN

Video/Demo

<table>
<thead>
<tr>
<th>Duration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>6:09</td>
<td>Total Video Time</td>
</tr>
<tr>
<td>3:33</td>
<td>6.15.1 Software-Defined Networking Basics</td>
</tr>
<tr>
<td>2:36</td>
<td>6.15.2 SDN Infrastructure and Architecture</td>
</tr>
</tbody>
</table>

Fact Sheets

- 6.15.3 SDN Facts

Number of Exam Questions

5 questions

Total Time

About 17 minutes
6.16: Cloud Services

Lecture Focus Questions:

- What is the difference between a hybrid cloud and a community cloud?
- What is the difference between IaaS and PaaS?
- Which two implementations are available for SaaS?
- What services does cloud computing provide?
- Which cloud computing model allows the client to run software without purchasing servers, data center space, or network equipment?

This section covers the following Security+ certification exam objective:
3.7 Summarize cloud and virtualization concepts.

- Cloud storage
- Cloud deployment models
  - SaaS
  - PaaS
  - IaaS
  - Private
  - Public
  - Hybrid
  - Community
- On-premise vs. hosted vs. cloud
- VDI/VDE
- Cloud access security broker
- Security as a Service

Video/Demo

<table>
<thead>
<tr>
<th>Video/Demo</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.16.1 Cloud Services Introduction</td>
<td>9:34</td>
</tr>
<tr>
<td>6.16.2 Cloud Computing Security Issues</td>
<td>5:43</td>
</tr>
</tbody>
</table>

Total Video Time 15:17

Fact Sheets

- 6.16.3 Cloud Computing Facts

Number of Exam Questions

5 questions

Total Time

About 26 minutes

Copyright © 2017 TestOut Corporation. CompTIA, A+, Network+, Security+, Linux+ and related trademarks and trade names are the trademarks of CompTIA. Microsoft, MCITP, MSCA, MCTS, Windows, and Office 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.
7.1: Malware

Lecture Focus Questions:

- What is the difference between a virus and a worm?
- Which types of malware can be spread through email?
- How are Trojans and botnets related?
- What does it mean for software to be quarantined?
- Why is it a good practice to show file extensions?
- In addition to implementing virus scanning software, what must you do to ensure that you are protected from the latest virus variations?

After finishing this section, you should be able to complete the following tasks:

- Implement malware protections
- Configure Windows Defender protections to secure a network from malware

This section covers the following Security+ certification exam objective:
1.1 Given a scenario, analyze indicators of compromise and determine the type of malware.

- Viruses
- Crypto-malware
- Ransomware
- Worm
- Trojan
- Rootkit
- Keylogger
- Adware
- Spyware
- Bots
- RAT
- Logic bomb
- Backdoor

Video/Demo

<table>
<thead>
<tr>
<th>Video/Demo</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.1.1 Malware</td>
<td>10:59</td>
</tr>
<tr>
<td>7.1.4 Implementing Malware Protections</td>
<td>6:17</td>
</tr>
<tr>
<td>7.1.5 Using Windows Defender</td>
<td>7:18</td>
</tr>
</tbody>
</table>

Total Video Time 24:34

Lab/Activity

- 7.1.6 Configure Windows Defender
Fact Sheets
- 7.1.2 Malware Facts
- 7.1.3 Malware Protection Facts

Number of Exam Questions
15 questions

Total Time
About 55 minutes
7.2: Password Attacks

Lecture Focus Questions:

- How are attackers able to recover passwords?
- What are the characteristics of a complex password?
- What are the differences between brute force and dictionary attacks?
- How does account lockout help secure an account?
- What technique mitigates rainbow table attacks?

In this section, you will learn to:

- Use rainbow tables
- Capture passwords

This section covers the following TestOut Security Pro certification exam objective:

- 5.1 Harden Network Devices (Using a Cisco Small Business Switch)
  - Use secure passwords

This section covers the following Security+ certification exam objectives:

1.2 Compare and contrast types of attacks.

- Cryptographic attacks
  - Birthday
  - Known plaintext/cipher text
  - Rainbow tables
  - Dictionary
  - Brute force
    - Online vs offline
  - Collision
  - Downgrade
  - Replay
  - Weak implementations

2.2 Given a scenario, use appropriate software tools to assess the security posture of an organization.

- Protocol analyzer
- Network scanners
  - Rogue system detection
  - Network mapping
- Wireless scanners/cracker
- Password cracker

4.4 Given a scenario, differentiate common account management practices.

- Account policy enforcement
  - Password complexity
Video/Demo

- 7.2.1 Password Attacks 6:28
- 7.2.3 Using Rainbow Tables 13:13
- 7.2.4 Capturing Passwords 3:33

Total Video Time 23:14

Fact Sheets

- 7.2.2 Password Attack Facts

Number of Exam Questions

5 questions

Total Time

About 34 minutes
7.3: Windows System Hardening

Lecture Focus Questions:

- What is hardening? How does it benefit security?
- How do you reduce the attack surface of a device?
- Why should you only install software that you need?
- What is a security baseline?
- What is the difference between a hotfix and a patch? Why would you use one or the other?

In this section, you will learn to:

- Harden an operating system
- Manage automatic updates
- Configure automatic updates
- Configure Windows Firewall
- Configure Windows Firewall advanced features

This section covers the following TestOut Security Pro certification exam objectives:

- 6.1 Harden Computer Systems Against Attack
  - Configure Domain GPO to enforce Windows Firewall use
- 6.2 Implement Patch Management/System Updates
  - Configure Windows Update
- 7.2 Implement Patch Management/Software Updates
  - Configure Microsoft Update

This section covers the following Security+ certification exam objectives:

2.4 Given a scenario, analyze and interpret output from security technologies

- Patch management tools
- Web application firewall

3.2 Given a scenario, implement secure network architecture concepts

- Security device/technology placement
  - Firewalls

3.3 Given a scenario, implement secure systems design

- Operating systems
  - Patch management
  - Trusted operating system
### Video/Demo

<table>
<thead>
<tr>
<th>Topic</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.3.1 Operating System Hardening</td>
<td>5:56</td>
</tr>
<tr>
<td>7.3.3 Hardening an Operating System</td>
<td>6:49</td>
</tr>
<tr>
<td>7.3.4 Managing Automatic Updates</td>
<td>4:42</td>
</tr>
<tr>
<td>7.3.6 Configuring Windows Firewall</td>
<td>6:13</td>
</tr>
<tr>
<td>7.3.8 Configuring Windows Firewall Advanced Features</td>
<td>10:47</td>
</tr>
</tbody>
</table>

**Total Video Time**

34:27

### Lab/Activity

- 7.3.5 Configure Automatic Updates
- 7.3.7 Configure Windows Firewall

### Fact Sheets

- 7.3.2 Hardening Facts

### Number of Exam Questions

10 questions

### Total Time

*About 60 minutes*
7.4: Hardening Enforcement

Lecture Focus Questions:

- How do GPOs ensure the consistent application of controls?
- Which hardening tasks can be implemented using a GPO?
- How can GPOs be used to harden the physical security of a workstation?
- How can you determine that the security controls implemented are still enforced?
- What are security templates, and how are they used?
- What is the easiest way to set controls on a Windows system, according to the NSA?

In this section, you will learn to:

- Use security templates and Group Policy
- Configuring GPOs to enforce security
- Manage services with Group Policy

This section covers the following TestOut Security Pro certification exam objectives:

- 6.1 Harden Computer Systems Against Attack
  - Configure a GPO to enforce workstation/server security settings
  - Configure Domain GPO to enforce Windows Firewall use
  - Configure Domain Servers GPO to remove unneeded services (such as file and printer sharing)
  - Protect against spyware and unwanted software using Windows Defender
  - Configure NTFS permissions for secure file sharing
- 7.1 Implement Application Defenses
  - Configure a GPO to enforce Internet Explorer settings
  - Configure web application security
  - Configure parental controls to enforce web content filtering
  - Configure secure browser settings
  - Configure secure email settings
  - Configure virtual machines and switches

This section covers the following Security+ certification exam objectives:

3.3 Given a scenario, implement secure systems design

- Operating systems
  - Secure configurations

4.4 Given a scenario, differentiate common account management practices

- General Concepts
  - Group-based access control
- Account policy enforcement
  - Group policy
Video/Demo
- 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
Total Video Time 21:54

Lab/Activity
- 7.4.5 Manage Services with Group Policy

Fact Sheets
- 7.4.4 Hardening Enforcement Facts

Number of Exam Questions
5 questions

Total Time
About 37 minutes
7.5: File Server Security

Lecture Focus Questions:

- How can you identify if a permission has been inherited?
- How do Share and NTFS permissions differ?
- Which elements can NTFS permissions be set on?
- How can you view the users that have permissions for a particular drive?

In this section, you will learn to:

- Configure NTFS permissions
- Disable inheritance

This section covers the following TestOut Security Pro certification exam objectives:

- 5.1 Harden Network Devices (Using a Cisco Small Business Switch)
  - Shut down unnecessary services and ports
- 6.1 Harden Computer Systems Against Attack
  - Configure NTFS permissions for secure file sharing

This section covers the following Security+ certification exam objectives:

- 3.3 Given a scenario, implement secure systems design
  - Operating systems
    - Disabling unnecessary ports and services
    - Least functionality
- 4.4 Given a scenario, differentiate common account management practices
  - General Concepts
    - Least privilege

Video/Demo

<table>
<thead>
<tr>
<th>Video/Demo</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.5.1 File Server Security</td>
<td>7:42</td>
</tr>
<tr>
<td>7.5.4 Configuring NTFS Permissions</td>
<td>11:14</td>
</tr>
<tr>
<td><strong>Total Video Time</strong></td>
<td><strong>18:56</strong></td>
</tr>
</tbody>
</table>

Lab/Activity

- 7.5.5 Configure NTFS Permissions
- 7.5.6 Disable Inheritance

Fact Sheets

- 7.5.2 File System Security Facts
- 7.5.3 File Permission Facts
Number of Exam Questions
13 questions

Total Time
About 52 minutes
7.6: Linux Host Security

Lecture Focus Questions:

- What is a socket?
- Which utility scans for all listening and non-listening sockets?
- Which utility identifies open ports on the Linux system?
- Which commands should you use to disable unneeded daemons?

In this section, you will learn to:

- Remove unnecessary services and scan ports

This section covers the following TestOut Security Pro certification exam objective:

- 5.1 Harden Network Devices (Using a Cisco Small Business Switch)
  - Shut down unnecessary services and ports
  - Implement port security

This section covers the following Security+ certification exam objectives:

1.4 Explain penetration testing concepts

- Ports

2.1 Install and configure network components, both hardware- and software-based, to support organizational security.

- Switch
  - Port security

3.3 Given a scenario, implement secure systems design

- Operating systems
  - Disabling unnecessary ports and services

Video/Demo

<table>
<thead>
<tr>
<th>Video/Demo</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>[✔️] 7.6.1 Linux Host Security</td>
<td>14:44</td>
</tr>
<tr>
<td>[☐] 7.6.2 Removing Unnecessary Services and Scanning Ports</td>
<td>10:28</td>
</tr>
<tr>
<td><strong>Total Video Time</strong></td>
<td><strong>25:12</strong></td>
</tr>
</tbody>
</table>

Fact Sheets

- [☐] 7.6.3 Linux Host Security Facts

Number of Exam Questions

5 questions

Total Time

*About 36 minutes*
7.7: Embedded Systems

Lecture Focus Questions:

- What is an SoC?
- For devices that cannot be manually updated, how can you minimize the amount of damage if they are compromised?
- What are common static environments within the Internet of Things?

This section covers the following Security+ certification exam objectives:

1.6 Explain the impact associated with types of vulnerabilities.

- Vulnerabilities due to:
  - Embedded systems

3.5 Explain the security implications of embedded systems

- SCADA/ICS
- Smart devices/IoT
  - Wearable technology
  - Home automation
- HVAC
- SoC
- RTOS
- Printers/MFDs
- Camera systems
- Special purpose
  - Medical devices
  - Vehicles
  - Aircraft/UAV

Video/Demo

<table>
<thead>
<tr>
<th>Video/Demo</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.7.1 SCADA and ICS Systems</td>
<td>5:52</td>
</tr>
<tr>
<td>7.7.2 IoT Device Security</td>
<td>4:40</td>
</tr>
</tbody>
</table>

Total Video Time 10:32

Fact Sheets

- 7.7.3 Embedded Systems Security Facts

Number of Exam Questions

5 questions

Total Time

*About 21 minutes*
7.8: Log Management

Lecture Focus Questions:

- What is the purpose of SIEM?
- How can rules in the correlation process help reduce the use of system resources?
- How can alerts and triggers aid administrators as they resolve threats or issues?
- Why does time synchronization matter for SIEM?

In this section, you will learn to:

- Log events with Event Viewer
- Configure source-initiated subscriptions
- Configuring remote logging on Linux

This section covers the following TestOut Security Pro certification exam objectives:

- 9.1 Implement Logging and Auditing
  - Configure Domain GPO audit policy
  - Configure Domain GPO for event logging
- 9.2 Review Security Logs and Violation Reports, Implement Remediation

This section covers the following Security+ certification exam objectives:

2.1 Install and configure network components, both hardware- and software-based, to support organizational security.

- SIEM
  - Aggregation
  - Correlation
  - Automated alerting and triggers
  - Time synchronization
  - Event deduplication
  - Logs/WORM

2.3 Given a scenario, troubleshoot common security issues.

- Logs and events anomalies

Video/Demo

<table>
<thead>
<tr>
<th>Video/Demo</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.8.1 Log Management</td>
<td>5:06</td>
</tr>
<tr>
<td>7.8.3 Logging Events with Event Viewer</td>
<td>5:15</td>
</tr>
<tr>
<td>7.8.4 Windows Event Subscriptions</td>
<td>7:15</td>
</tr>
<tr>
<td>7.8.5 Configuring Source-Initiated Subscriptions</td>
<td>5:26</td>
</tr>
<tr>
<td>7.8.6 Configuring Remote Logging on Linux</td>
<td>8:30</td>
</tr>
</tbody>
</table>

Total Video Time: 31:32
Fact Sheets
- 7.8.2 Log Facts
- 7.8.7 Remote Logging Facts

Number of Exam Questions
15 questions

Total Time
*About 57 minutes*
7.9: Audits

Lecture Focus Questions:

- When would you choose an external auditor instead of an internal auditor?
- What is the difference between privilege auditing and usage auditing?
- How can escalation auditing help to secure a system?
- What is an SOX audit? Who is required to have SOX audits?
- How does PCI compliance affect an organization’s audits?

In this section, you will learn to:

- Configure advanced audit policy
- Enable device logs

This section covers the following TestOut Security Pro certification exam objectives:

- 5.1 Harden Network Devices (Using a Cisco Small Business Switch)
  - Turn on logging with timestamps
- 9.1 Implement Logging and Auditing
  - Configure Domain GPO audit policy
  - Configure Domain GPO for event logging
- 9.2 Review Security Logs and Violation Reports, Implement Remediation
- 9.3 Review Audit Reports, Implement Remediation
- 9.4 Review Vulnerability Reports, Implement Remediation

This section covers the following Security+ certification exam objective:
4.4 Given a scenario, differentiate common account management practices

- General Concepts
  - Permission auditing and review
  - Usage auditing and review

<table>
<thead>
<tr>
<th>Video/Demo</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.9.1 Audits</td>
<td>4:12</td>
</tr>
<tr>
<td>7.9.3 Auditing the Windows Security Log</td>
<td>9:12</td>
</tr>
<tr>
<td>7.9.5 Auditing Device Logs</td>
<td>1:50</td>
</tr>
<tr>
<td><strong>Total Video Time</strong></td>
<td><strong>15:14</strong></td>
</tr>
</tbody>
</table>

Lab/Activity

- 7.9.4 Configure Advanced Audit Policy
- 7.9.6 Enable Device Logs

Fact Sheets

- 7.9.2 Audit Facts
Number of Exam Questions
5 questions

Total Time
About 36 minutes
7.10: Email

Lecture Focus Questions:

- How does spam filtering help end users?
- In what format are emails sent?
- Why is it important to add multiple layers of security?
- Why would you only encrypt email coming from outside your network?
- What is S/MIME?
- What is the difference between POP3 and IMAP?

In this section, you will learn to:

- Protect a client from spam
- Secure an email server
- Configure email filters
- Secure email on iPad

This section covers the following TestOut Security Pro certification exam objectives:

- 2.1 Promote Information Security Awareness
  - Using email best practices
- 7.1 Implement Application Defenses
  - Configure secure email settings

This section covers the following Security+ certification exam objectives:

- 5.1 Explain the importance of policies, plans and procedures related to organizational security
  - General security policies
    - Personal email
- 6.4 Given a scenario, implement public key infrastructure
  - Types of certificates
    - Email

**Video/Demo**

<table>
<thead>
<tr>
<th>Video/Demo</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.10.1 Email Security</td>
<td>6:29</td>
</tr>
<tr>
<td>7.10.3 Protecting a Client from Spam</td>
<td>5:49</td>
</tr>
<tr>
<td>7.10.4 Securing an Email Server</td>
<td>2:51</td>
</tr>
<tr>
<td>7.10.6 Securing Email on iPad</td>
<td>5:22</td>
</tr>
</tbody>
</table>

**Total Video Time** 20:31

**Lab/Activity**

- 7.10.5 Configure Email Filters
- 7.10.7 Secure Email on iPad
Fact Sheets

7.10.2 Email Security Facts

Number of Exam Questions
10 questions

Total Time
About 46 minutes
7.11: BYOD Security

Lecture Focus Questions:

- How would you remediate a tablet or phone infected with malware?
- What is an AUP? How does it benefit mobile security?
- How does VDI provide enhanced security and better data protection?
- What is the difference between CYOD and COPE?
- How can you prevent malicious insider attacks?

In this section, you will learn to:

- Secure mobile devices
- Secure an iPad

This section covers the following TestOut Security Pro certification exam objective:

- 2.1 Promote Information Security Awareness
  - Traveling with Personal Mobile Devices
  - Exchanging content between home and work
  - Storing personal information on the internet
  - Using social networking sites
  - Using SSL encryption
  - Using email best practices
  - Password management
  - Photo/GPS integration
  - Information security
  - Auto-lock and passcode lock

This section covers the following Security+ certification exam objective:

2.5 Given a scenario, deploy mobile devices securely

- Deployment models
  - BYOD
  - COPE
  - CYOD
  - Corporate-owned
  - VDI

Video/Demo

<table>
<thead>
<tr>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.11.1</td>
</tr>
<tr>
<td>7.11.3</td>
</tr>
</tbody>
</table>

Total Video Time 17:39

Lab/Activity

- 7.11.4 Secure an iPad

Copyright © 2017 TestOut Corporation. CompTIA, A+, Network+, Security+, Linux+ and related trademarks and trade names are the trademarks of CompTIA. Microsoft, MCITP, MSCP, MCTS, Windows, and Office 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.
Fact Sheets

7.11.2 BYOD Security Facts

Number of Exam Questions
5 questions

Total Time
About 33 minutes
7.12: Mobile Device Management

Lecture Focus Questions:

- Which process allows you to define specific apps that users are allowed to have on their mobile devices?
- Which two configurations can be used to deploy Windows Intune?
- What does a mobile device management (MDM) solution allow you to do?
- How do jailbreaking and sideloading differ?

In this section, you will learn to:

- Enforce security policies on mobile devices
- Enroll devices and perform a remote wipe
- Create a guest network for BYOD

This section covers the following TestOut Security Pro certification exam objectives:

- 3.2 Harden Mobile Devices (iPad)
  - Set Autolock
  - Configure network security settings
- 3.3 Harden Mobile Devices (Laptop)
  - Implement full disk encryption

This section covers the following Security+ certification exam objectives:

- 2.5 Given a scenario, deploy mobile devices securely

  - Connection methods
    - Cellular
    - WiFi
    - SATCOM
    - Bluetooth
    - NFC
    - ANT
    - Infrared
    - USB
  - Mobile device management concepts
    - Application management
    - Content management
    - Remote wipe
    - Geofencing
    - Geolocation
    - Screen locks
    - Push notification services
    - Passwords and pins
    - Biometrics
    - Context-aware authentication
    - Containerization
    - Storage segmentation
    - Full device encryption

  - Enforcement and monitoring for:
- Third-party app stores
- Rooting/jailbreaking
- Sideloadung
- Custom firmware
- Carrier unlocking
- Firmware OTA updates
- Camera use
- SMS/MMS
- External media
- USB OTG
- Recording microphone
- GPS tagging
- WiFi direct/ad hoc
- Tethering
- Payment methods
  - Deployment models
    - BYOD

3.3 Given a scenario, implement secure systems design

- Operating systems
  - Types
    - Mobile OS

**Video/Demo**

- 7.12.1 Mobile Device Considerations 4:54
- 7.12.2 Mobile Application Security 6:56
- 7.12.5 Enrolling Devices and Performing a Remote Wipe 7:03
- 7.12.7 Creating a Guest Network for BYOD 6:03

**Total Video Time** 31:37

**Lab/Activity**

- 7.12.8 Create a Guest Network for BYOD

**Fact Sheets**

- 7.12.3 Mobile Device Security Facts
- 7.12.6 Mobile Device Enforcement Facts

**Number of Exam Questions**

8 questions

**Total Time**

*About 55 minutes*
7.13: Host Virtualization

Lecture Focus Questions:
- What is virtualization?
- What is the difference between a virtual machine and a hypervisor?
- What are the advantages of virtualization?
- What are the disadvantages of virtualization?

In this section, you will learn to:
- Create virtual machines
- Add virtual network adapters
- Manage virtual machines

This section covers the following TestOut Security Pro certification exam objective:
- 7.1 Implement Application Defenses
  - Configure virtual machines and switches

This section covers the following Security+ certification exam objective:
3.7 Summarize cloud and virtualization concepts
- Hypervisor
  - Type I
  - Type II
  - Application cells/containers
- VDI/VDE

Video/Demo

<table>
<thead>
<tr>
<th>Video/Demo</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.13.1 Host Virtualization Overview</td>
<td>10:51</td>
</tr>
<tr>
<td>7.13.2 Load Balancing with Virtualization</td>
<td>6:59</td>
</tr>
<tr>
<td>7.13.4 Creating Virtual Machines</td>
<td>6:51</td>
</tr>
<tr>
<td>7.13.5 Managing Virtual Machines</td>
<td>5:22</td>
</tr>
<tr>
<td>7.13.7 Adding Virtual Network Adapters</td>
<td>3:07</td>
</tr>
</tbody>
</table>

Total Video Time 33:10

Lab/Activity
- 7.13.6 Create Virtual Machines

Fact Sheets
- 7.13.3 Virtualization Facts

Number of Exam Questions
6 questions

Total Time
About 50 minutes
8.1: Access Control Models

Lecture Focus Questions:

- What is access control? Why is it important?
- How does discretionary access control (DAC) provide access control?
- What is the difference between a transitive trust and a non-transitive trust?
- What type of entries does the Discretionary Access Control List (DACL) contain?
- What is the function of each of the two types of labels used by the Mandatory Access Control (MAC) access model?
- How are rule-based access control and mandatory access control (MAC) similar?
- How does role-based access control differ from rule-based access control?
- How does the Clark-Wilson model differ from the Biba model?

In this section, you will learn to:

- Implement DAC

This section covers the following TestOut Security Pro exam objective:

- 5.1 Harden Computer Systems Against Attack
  - Configure a GPO to enforce workstation/server security settings
  - Configure Domain GPO to enforce Windows Firewall use
  - Configure Domain Servers GPO to remove unneeded services (such as file and printer sharing)

This section covers the following Security+ certification exam objectives:

4.1 Compare and contrast identity and access management concepts

- Transitive trust

4.3 Given a scenario, implement identity and access management controls

- Access control models
  - MAC
  - DAC
  - ABAC
  - Role-based access control
  - Rule-based access control

Video/Demo

<table>
<thead>
<tr>
<th>Video/Demo</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1 Access Control Models</td>
<td>4:59</td>
</tr>
<tr>
<td>8.1.4 Implementing Discretionary Access Control</td>
<td>14:54</td>
</tr>
<tr>
<td>8.1.5 Trusts and Transitive Access</td>
<td>4:55</td>
</tr>
</tbody>
</table>

Total Video Time 24:48
Fact Sheets
- 8.1.2 Access Control Facts
- 8.1.3 Access Control Model Facts
- 8.1.6 Trusts and Transitive Access Facts

Number of Exam Questions
15 questions

Total Time
About 55 minutes
8.2: Authentication

Lecture Focus Questions:

- What is the difference between authentication and identification?
- Which authentication type is the most common?
- What are some characteristics of the "something you are" authentication type?
- What are some characteristics of the "something you have" authentication type?
- What are some characteristics of the "something you know" authentication type?
- Which form of authentication is generally considered the strongest?
- What is the difference between synchronous and asynchronous token devices?
- Which type of biometric processing error is more serious, a false positive or a false negative? Why?
- What is the difference between strong authentication, two-factor authentication, and multi-factor authentication?
- What are the main advantages of SSO authentication? Disadvantages?
- What are examples of authentication services beside SSO?

In this section, you will learn to:

- Use a biometric scanner
- Use single sign-on

This section covers the following TestOut Security Pro certification exam objective:

- 1.2 Harden Authentication
  - Implement centralized authentication

This section covers the following Security+ certification exam objectives:

4.1 Compare and contrast identity and access management concepts

- Multifactor authentication
  - Something you are
  - Something you have
  - Something you know
  - Somewhere you are
  - Something you do

- Single sign-on

4.3 Given a scenario, implement identity and access management controls

- Biometric factors
  - Fingerprint scanner
  - Retinal scanner
  - Iris scanner
  - Voice recognition

Copyright © 2017 TestOut Corporation. CompTIA, A+, Network+, Security+, Linux+ and related trademarks and trade names are the trademarks of CompTIA. Microsoft, MCITP, MSCA, MCTS, Windows, and Office 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.
- Facial recognition
- False acceptance rate
- False rejection rate
- Crossover error rate

**Video/Demo**

<table>
<thead>
<tr>
<th>Video/Demo</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.2.1 Authentication</td>
<td>6:52</td>
</tr>
<tr>
<td>8.2.2 Authentication Methods</td>
<td>4:08</td>
</tr>
<tr>
<td>8.2.4 Using a Biometric Scanner</td>
<td>2:47</td>
</tr>
<tr>
<td>8.2.5 Using Single Sign-on</td>
<td>4:23</td>
</tr>
</tbody>
</table>

**Total Video Time** 18:10

**Fact Sheets**

- 8.2.3 Authentication Facts
- 8.2.6 Single Sign-on Facts

**Number of Exam Questions**
15 questions

**Total Time**
*About 44 minutes*
8.3: Authorization

Lecture Focus Questions:

- What three types of information make up an access token?
- On a Microsoft system, when is the access token generated?
- What types of objects are considered security principals?
- What is the difference between a discretionary access control list (DACL) and a system access control list (SACL)?

In this section, you will learn to:

- Examine the elements of an access token

This section covers the following TestOut Security Pro certification exam objectives:

- 1.1 Create, Modify, and Delete User Profiles
  - Restrict use of common access accounts
- 5.1 Harden Network Devices (Using a Cisco Small Business Switch)
  - Implement access lists, deny everything else

This section covers the following Security+ certification exam objectives:

- 4.3 Given a scenario, implement identity and access management controls
  - File system security
- 4.4 Given a scenario, differentiate common account management practices
  - General Concepts
    - Group-based access control

<table>
<thead>
<tr>
<th>Video/Demo</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.3.1 Authorization</td>
<td>3:45</td>
</tr>
<tr>
<td>8.3.2 Cumulative Access</td>
<td>6:21</td>
</tr>
<tr>
<td>8.3.4 Examining the Access Token</td>
<td>9:15</td>
</tr>
</tbody>
</table>

**Total Video Time** 19:21

Fact Sheets

- 8.3.3 Authorization Facts

Number of Exam Questions
5 questions

Total Time
About 30 minutes

Copyright © 2017 TestOut Corporation. CompTIA, A+, Network+, Security+, Linux+ and related trademarks and trade names are the trademarks of CompTIA. Microsoft, MCITP, MSCP, MCTS, Windows, and Office 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: Web Application Attacks

Lecture Focus Questions:

- What are two ways that drive-by download attacks occur?
- Which countermeasures can be used to eliminate buffer overflow attacks?
- How can cross-site scripting (XSS) be used to breach the security of a web user?
- What is the best method for preventing SQL injection attacks?
- What are some types of header manipulation?
- Which mitigation practices help to protect internet-based activities from web application attacks?

In this section, you will learn to:

- Prevent cross-site scripting

This section covers the following TestOut Security Pro certification exam objective:

- 4.1 Harden the Network Perimeter (using a Cisco Network Security Appliance)
  - Implement web threat protection

This section covers the following Security+ certification exam objectives:

1.2 Compare and contrast types of attacks

- Application/service attacks
  - Buffer overflow
  - Injection
  - Cross-site scripting
  - Cross-site request forgery
  - Zero day
  - Hijacking and related attacks
    - Clickjacking
    - Session hijacking
    - URL hijacking
    - Typo squatting
  - Driver manipulation
    - Shimming
    - Refactoring

1.6 Explain the impact associated with types of vulnerabilities

- Memory/buffer vulnerability
  - Integer overflow
  - Buffer overflow
  - DLL injection
- New threats/zero day
Video/Demo

- 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
- 8.4.8 Preventing Cross-Site Scripting 4:08

Total Video Time 31:23

Fact Sheets

- 8.4.7 Web Application Attack Facts

Number of Exam Questions

15 questions

Total Time

About 52 minutes
8.5: Internet Browsers

Lecture Focus Questions:

- What types of information do cookies store? Why could this be a security concern?
- What steps should you take to secure the browser from add-ons that are not appropriate for your environment?
- For security’s sake, what should you do whenever you use a public computer to access the internet and retrieve personal data?
- What elements might indicate an unsecured connection or an attack?
- Why should you turn off the remember search and form history feature?

In this section, you will learn to:

- Clear the browser cache
- Configure IE pop-up blocker
- Enforce IE settings through GPOs
- Configure IE preferences in a GPO

This section covers the following TestOut Security Pro certification exam objectives:

- 6.1 Harden Computer Systems Against Attack
  - Configure a GPO to enforce workstation/server security settings
- 7.1 Implement Application Defenses
  - Configure a GPO to enforce Internet Explorer settings
  - Configure web application security
  - Configure parental controls to enforce web content filtering
  - Configure secure browser settings
- 8.2 Protect Data Transmissions Across Open, Public Networks
  - Encrypt data communications

Video/Demo

<table>
<thead>
<tr>
<th>Video/Demo</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.5.1 Web Browser Threats</td>
<td>8:01</td>
</tr>
<tr>
<td>8.5.2 Configuring Browser Security and Plugins</td>
<td>12:09</td>
</tr>
<tr>
<td>8.5.3 Clearing the Browser Cache</td>
<td>4:56</td>
</tr>
<tr>
<td>8.5.7 Enforcing IE Settings Through GPO</td>
<td>3:31</td>
</tr>
<tr>
<td><strong>Total Video Time</strong></td>
<td><strong>28:37</strong></td>
</tr>
</tbody>
</table>

Lab/Activity

- 8.5.4 Clear the Browser Cache
- 8.5.5 Configure IE Pop-up Blocker
- 8.5.8 Enforce IE Settings Through GPO
- 8.5.9 Configure IE Preferences in a GPO
Fact Sheets

8.5.6 Internet Explorer Security Facts

Number of Exam Questions
8 questions

Total Time
About 62 minutes
8.6: Application Development

Lecture Focus Questions:

- What is the purpose of fuzzing?
- What does input validation ensure?
- What are the basic techniques for application hardening?
- When should you update applications with the latest patches?

In this section, you will learn to:

- Harden applications on Linux
- Implement application whitelisting with AppLocker
- Implement Data Execution Preventions (DEP)

This section covers the following TestOut Security Pro exam objective:

- 7.1 Implement Application Defenses.
  - Configure a GPO for Application Whitelisting
  - Enable Data Execution Prevention (DEP)

This section covers the following Security+ certification exam objectives:

2.4 Given a scenario, analyze and interpret output from security technologies.

- Application whitelisting
- Data execution prevention

3.3 Given a scenario, implement secure systems design.

- Operating systems
  - Disabling unnecessary ports and services
  - Least functionality
  - Secure configurations
  - Application whitelisting/blacklisting

3.4 Explain the importance of secure staging deployment concepts.

- Sandboxing
- Environment
  - Development
  - Test
  - Staging
  - Production
- Secure baseline
- Integrity measurement
3.6 Summarize secure application development and deployment concepts.

- Secure DevOps
  - Security automation
  - Continuous integration
  - Baselining
  - Immutable systems
  - Infrastructure as code
- Secure coding techniques
  - Proper error handling
  - Proper input validation
  - Normalization
  - Stored procedures
  - Code signing
  - Encryption
  - Obfuscation/camouflage
  - Code reuse/dead code
  - Server-side vs. client-side execution and validation
  - Memory management
  - Use of third-party libraries and SDKs
  - Data exposure
- Code quality and testing
  - Static code analyzers
  - Dynamic analysis (e.g., fuzzing)
  - Stress testing
  - Sandboxing
  - Model verification

**Video/Demo**

- 8.6.1 Secure Coding Concepts  
  Time: 9:58
- 8.6.2 Application Hardening  
  Time: 7:53
- 8.6.4 Hardening Applications on Linux  
  Time: 3:33
- 8.6.5 Implementing Application Whitelisting with AppLocker  
  Time: 7:23
- 8.6.7 Implementing Data Execution Preventions (DEP)  
  Time: 3:23
- 8.6.10 NoSQL Security  
  Time: 4:22

**Total Video Time**: 36:32

**Lab/Activity**

- 8.6.6 Implement Application Whitelisting with AppLocker
- 8.6.8 Implement Data Execution Preventions (DEP)

**Fact Sheets**

- 8.6.3 Application Development Security Facts
- 8.6.9 Hardening Applications Facts
- 8.6.11 NoSQL Security Facts
Number of Exam Questions
6 questions

Total Time
About 68 minutes
8.7: Active Directory Overview

Lecture Focus Questions:

- What is the purpose of a domain?
- What is the difference between a tree and a forest?
- How do Organizational Units (OUs) simplify security administration?
- What are the advantages of a hierarchical directory database over a flat file database?

Video/Demo

<table>
<thead>
<tr>
<th>Video/Demo</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.7.1 Active Directory Introduction</td>
<td>6:48</td>
</tr>
<tr>
<td>8.7.2 Active Directory Structure</td>
<td>5:27</td>
</tr>
<tr>
<td>8.7.3 Viewing Active Directory</td>
<td>8:11</td>
</tr>
<tr>
<td><strong>Total Video Time</strong></td>
<td><strong>20:26</strong></td>
</tr>
</tbody>
</table>

Fact Sheets

- 8.7.4 Active Directory Facts

Number of Exam Questions

5 questions

Total Time

*About 31 minutes*
8.8: Windows Domain Users and Groups

Lecture Focus Questions:

- What are the differences between disabled, locked out, and expired user accounts?
- What is the best way to handle a user’s account when an employee quits and will be replaced by a new employee in the near future?
- What are the recommendations for using a template user account?
- Which properties of a user account are not duplicated when you copy the user?

In this section, you will learn to:

- Create user accounts
- Manage user accounts
- Create a group
- Create global groups

This section covers the following TestOut Security Pro certification exam objective:

- 1.1 Create, Modify, and Delete User Profiles
  - Manage Windows Domain Users and Groups
    - Create, rename, and delete users and groups
    - Assign users to appropriate groups
    - Lock and unlock user accounts
    - Change a user’s password
  - Manage Windows Local Users and Groups
    - Restrict use of local user accounts
  - Restrict use of common access accounts

This section covers the following Security+ certification exam objective:

4.4 Given a scenario, differentiate common account management practices

- Account types
  - User account
  - Shared and generic accounts/credentials
  - Guest accounts
  - Service accounts
  - Privileged accounts

Video/Demo

<table>
<thead>
<tr>
<th>Video/Demo</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.8.1 Creating User Accounts</td>
<td>5:10</td>
</tr>
<tr>
<td>8.8.2 Managing User Account Properties</td>
<td>8:30</td>
</tr>
<tr>
<td>8.8.5 Managing Groups</td>
<td>4:58</td>
</tr>
</tbody>
</table>

Total Video Time 18:38
Lab/Activity
- 8.8.3 Create User Accounts
- 8.8.4 Manage User Accounts
- 8.8.6 Create a Group
- 8.8.7 Create Global Groups

Fact Sheets
- 8.8.8 User Account Management Facts

Number of Exam Questions
5 questions

Total Time
About 49 minutes
8.9: Linux Users

Lecture Focus Questions:

- Which directory contains configuration file templates that are copied into a new user’s home directory?
- When using `useradd` to create a new user account, what type of default values create the user account?
- How can you view all the default values in the `/etc/default/useradd` file?
- How do you create a user with `useradd` that does not receive the default values in `/etc/default/useradd` file?
- Which command deletes a user and their home directory at the same time?

In this section, you will learn to:

- Create a user account
- Rename a user account
- Delete a user
- Change your password
- Change a user’s password
- Lock and unlock user accounts

This section covers the following TestOut Security Pro certification exam objective:

- 1.1 Create, Modify, and Delete User Profiles
  - Manage Linux Users and Groups
    - Create, rename, and delete users and groups
    - Assign users to appropriate groups
    - Lock and unlock user accounts
    - Change a user’s password
    - Configure password aging

This section covers the following Security+ certification exam objective:

4.4 Given a scenario, differentiate common account management practices

- Account types
  - User account
  - Shared and generic accounts/credentials
  - Guest accounts
  - Service accounts
  - Privileged accounts

Video/Demo

<table>
<thead>
<tr>
<th>Video/Demo</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.9.1 Linux User and Group Overview</td>
<td>11:00</td>
</tr>
<tr>
<td>8.9.2 Managing Linux Users</td>
<td>8:40</td>
</tr>
<tr>
<td><strong>Total Video Time</strong></td>
<td><strong>19:40</strong></td>
</tr>
</tbody>
</table>
Lab/Activity
- 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

Fact Sheets
- 8.9.3 Linux User Commands and Files

Number of Exam Questions
7 questions

Total Time
About 62 minutes
8.10: Linux Groups

Lecture Focus Questions:

- Which `usermod` option changes the secondary group membership?
- Which command removes all secondary group memberships for specific user accounts?
- Which `groupmod` option changes the name of a group?

In this section, you will learn to:

- Rename and create groups
- Add users to a group
- Remove a user from a group

This section covers the following TestOut Security Pro certification exam objective:

- 1.1 Create, Modify, and Delete User Profiles
  - Manage Linux Users and Groups
    - Create, rename, and delete users and groups
    - Assign users to appropriate groups

**Video/Demo**  
- 8.10.1 Managing Linux Groups  
  **Time**  
  7:49  
  **Total Video Time**  
  7:49

**Lab/Activity**  
- 8.10.3 Rename and Create Groups  
- 8.10.4 Add Users to a Group  
- 8.10.5 Remove a User from a Group

**Fact Sheets**  
- 8.10.2 Linux Group Commands

**Number of Exam Questions**  
5 questions

**Total Time**  
*About 33 minutes*
8.11: Linux User Security

Lecture Focus Questions:

- When using `chage` to set an expiration date for user passwords, which option sets the number of days for the password warning message?
- What is the difference between hard and soft limits?
- When using `ulimit` to limit computer resources used for applications launched from the shell, which option displays the current limits?
- What command removes all restrictions for process memory usage?
- Why shouldn’t passwords expire too frequently?

In this section, you will learn to:

- Configuring Linux user security and restrictions

This section covers the following TestOut Security Pro certification exam objectives:

- 1.1 Create, Modify, and Delete User Profiles
  - Manage Linux Users and Groups
    - Change a user’s password
    - Configure password aging
- 5.1 Harden Network Devices (Using a Cisco Small Business Switch)
  - Change the default user name and password on network devices
  - Use secure passwords

This section covers the following Security+ certification exam objective:

4.4 Given a scenario, differentiate common account management practices

- Account policy enforcement
  - Password complexity
  - Expiration
  - Password history
  - Password reuse
  - Password length

Video/Demo

- 8.11.1 Linux User Security and Restrictions 7:14
- 8.11.2 Configuring Linux User Security and Restrictions 7:51
  
Total Video Time 15:05

Fact Sheets

- 8.11.3 Linux User Security and Restriction Facts

Number of Exam Questions

5 questions

Total Time

About 26 minutes

Copyright © 2017 TestOut Corporation. CompTIA, A+, Network+, Security+, Linux+ and related trademarks and trade names are the trademarks of CompTIA. Microsoft, MCITP, MSCA, MCTS, Windows, and Office 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.
8.12: Group Policy Overview

Lecture Focus Questions:

- When are user policies applied?
- How do computer policies differ from user policies?
- How do GPOs applied to an OU differ from GPOs applied to a domain?
- What is the order in which GPOs are applied?
- If a setting is undefined in one GPO and defined in another, which setting is used?
- If a setting is defined in two GPOs, which setting is applied?

In this section, you will learn to:

- Create a GPO
- Link a GPO

This section covers the following Security Pro exam objectives:

- 1.1 Create, modify, and delete user profiles
  - Manage Windows Local Users and Groups
    - Restrict use of local user accounts
  - Restrict use of common access accounts
- 1.2 Harden authentication
  - Configure Domain GPO Account Policy to enforce a robust password policy
  - Configure the Domain GPO to control local administrator group membership and administrator password
- 6.1 Harden Computer Systems Against Attack
  - Configure a GPO to enforce workstation/server security settings
  - Configure Domain Servers GPO to remove unneeded services (such as file and printer sharing)

This section covers the following Security+ certification exam objective:
4.4 Given a scenario, differentiate common account management practices

- General Concepts
  - Group-based access control
- Account policy enforcement
  - Group policy

**Video/Demo**

- **8.12.1 Group Policy Overview**
  - Time: 9:52
- **8.12.2 Configuring Local Policies**
  - Time: 11:28
- **8.12.3 Creating and Linking Group Policy Objects**
  - Time: 10:28

**Total Video Time: 31:48**
Lab/Activity

- 8.12.5 Create and Link a GPO

Fact Sheets

- 8.12.4 Group Policy Facts

Number of Exam Questions

5 questions

Total Time

About 47 minutes
8.13: Hardening Authentication 1

Lecture Focus Questions:

- On a Microsoft system, which characteristics typically define a complex password?
- What does the minimum password age setting prevent?
- What is a drawback to account lockout for failed password attempts?
- What are the advantages of a self-service password reset management system?

In this section, you will learn to:

- Configure user account restrictions
- Configure account policies
- Restrict local accounts
- Secure default accounts
- Enforce user account control

This section covers the following TestOut Security Pro certification exam objectives:

- 1.1 Create, Modify, and Delete User Profiles
  - Manage Windows Domain Users and Groups
    - Lock and unlock user accounts
    - Change a user’s password
  - Manage Windows Local Users and Groups
    - Restrict use of local user accounts
  - Restrict use of common access accounts
- 1.2 Harden Authentication
  - Configure Domain GPO Account Policy to enforce a robust password policy
  - Configure the Domain GPO to control local administrator group membership and administrator password
  - Disable or rename default accounts, such as Guest and Administrator
  - Configure the Domain GPO to enforce User Account Control
- 5.1 Harden Network Devices (Using a Cisco Small Business Switch)
  - Use secure passwords

This section covers the following Security+ certification exam objective:
4.4 Given a scenario, differentiate common account management practices

- General Concepts
  - Group-based access control
- Account policy enforcement
  - Group policy
  - Password complexity
  - Expiration
Video/Demo
- 8.13.1 Hardening Authentication 10:19
- 8.13.2 Configuring User Account Restrictions 4:52
- 8.13.4 Configuring Account Policies and UAC Settings 6:25
- 8.13.6 Hardening User Accounts 7:40

Total Video Time 29:16

Lab/Activity
- 8.13.3 Configure User Account Restrictions
- 8.13.5 Configure Account Policies
- 8.13.7 Restrict Local Accounts
- 8.13.8 Secure Default Accounts
- 8.13.9 Enforce User Account Control

Fact Sheets
- 8.13.10 Hardening Authentication Facts

Number of Exam Questions
11 questions

Total Time
About 71 minutes
8.14: Hardening Authentication 2

Lecture Focus Questions:

- What are the two categories of smart cards, and how they are read by a smart card reader?
- What are the advantages and disadvantages of using smart cards?
- When would you choose to use fine-grained password policies?
- How does a contactless smart card differ from a contact smart card?

In this section, you will learn to:

- Configure authentication for a smart card
- Create a fine-grained password policy

This section covers the following TestOut Security Pro certification exam objectives:

- 1.1 Create, Modify, and Delete User Profiles
  - Manage Windows Local Users and Groups
    - Restrict use of local user accounts
  - Restrict use of common access accounts
- 1.2 Harden Authentication
  - Configure a GPO for smart card authentication for sensitive resources

This section covers the following Security+ certification exam objectives:

- 3.9 Explain the importance of physical security controls
- 4.3 Given a scenario, implement identity and access management controls

Physical access control
  - Smart cards
- Certificate-based authentication
  - PIV/CAC/smart card

Video/Demo

- 8.14.1 Configuring Smart Card Authentication 5:37
- Total Video Time 11:11

Lab/Activity

- 8.14.2 Configure Smart Card Authentication
- 8.14.6 Create a Fine-Grained Password Policy
Fact Sheets
- 8.14.3 Smart Card Authentication Facts
- 8.14.5 Fine-Grained Password Policy Facts

Number of Exam Questions
6 questions

Total Time
*About 38 minutes*
9.1: Data Management

Lecture Focus Questions:

- Who is responsible for properly destroying data?
- Which governmental regulations should be followed when destroying data?
- How does wiping differ from degaussing?
- What is the difference between private internal and private restricted?

This section teaches you to:

- File shredding
- Hard drive wiping

This section covers the following Security+ certification exam objective:

2.2 Given a scenario, use appropriate software tools to assess the security posture of an organization.

- Data sanitization tools

5.8 Given a scenario, carry out data security and privacy practices.

- Data destruction and media sanitization
  - Burning
  - Shredding
  - Pulping
  - Pulverizing
  - Degaussing
  - Purging
  - Wiping
- Data sensitivity labeling and handling
  - Confidential
  - Private
  - Public
  - Proprietary
  - PII
  - PHI
- Data roles
  - Owner
  - Steward/custodian
  - Privacy officer
- Data retention
- Legal and compliance
Video/Demo

- 9.1.1 Information Classification 2:54
- 9.1.3 Data Destruction 8:43
- 9.1.4 File Shredding and Hard Drive Wiping 9:35

Total Video Time 21:12

Fact Sheets

- 9.1.2 Information Classification Facts
- 9.1.5 Data Destruction Facts

Number of Exam Questions
6 questions

Total Time
About 38 minutes
9.2: Advanced Cryptography

Lecture Focus Questions:

- What is the difference between a symmetric key and an asymmetric key?
- What are some of the modes of operation?
- How do low-power devices affect which encryption you choose to employ?
- What happens at the output stage of encryption?

This section covers the following TestOut Security Pro certification exam objectives:

- **8.1 Protect and Maintain the Integrity of Data Files**
  - Implement encryption technologies
  - Perform data backups and recovery
  - Implement redundancy and failover mechanisms
- **8.2 Protect Data Transmissions Across Open, Public Networks**
  - Encrypt data communications
  - Implement secure protocols
  - Remove unsecure protocols

This section covers the following Security+ certification exam objective:

6.1 Compare and contrast basic concepts of cryptography.

- Symmetric algorithms
- Modes of operation
- Asymmetric algorithms
- Hashing
- Salt, IV, nonce
- Elliptic curve
- Weak/deprecated algorithms
- Key exchange
- Digital signatures
- Diffusion
- Confusion
- Collision
- Steganography
- Obfuscation
- Stream vs. block
- Key strength
- Session keys
- Ephemeral key
- Secret algorithm
- Data-in-transit
- Data-at-rest
- Data-in-use
- Random/pseudo-random number generation
- Key stretching
- Implementation vs. algorithm selection
  - Crypt service provider
  - Crypt modules
- Perfect forward secrecy
- Security through obscurity
- Common use cases
  - Low power devices
  - Low latency
  - High resiliency
  - Supporting confidentiality
  - Supporting integrity
  - Supporting obfuscation
  - Supporting authentication
  - Supporting non-repudiation
  - Resource vs. security constraints

**Video/Demo**

<table>
<thead>
<tr>
<th>Video/Demo</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.2.1 Advanced Cryptography Concepts</td>
<td>9:37</td>
</tr>
<tr>
<td>9.2.3 Cryptography Algorithms</td>
<td>2:58</td>
</tr>
</tbody>
</table>

**Total Video Time** 12:35

**Fact Sheets**

<table>
<thead>
<tr>
<th>Fact Sheets</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.2.2 Advanced Cryptography Facts</td>
</tr>
<tr>
<td>9.2.4 Cryptography Algorithms Facts</td>
</tr>
</tbody>
</table>

**Number of Exam Questions**

5 questions

**Total Time**

About 28 minutes
9.3: Cryptography Implementations

Lecture Focus Questions:

- What advantages does asymmetric encryption when compared with symmetric encryption? What are the disadvantages?
- What is the difference between digital signatures and digital envelopes?
- How does the protection offered by BitLocker differ from EFS?
- How does TPM work? Where is it located on a computer?
- What is the difference between TPM and an HSM?
- Which types of traffic can SSL protect?

This section covers the following TestOut Security Pro certification exam objectives:

- 2.1 Promote Information Security Awareness
  - Traveling with Personal Mobile Devices
  - Exchanging content between home and work
  - Storing personal information on the internet
  - Using social networking sites
  - Using SSL encryption
  - Using email best practices
- 7.1 Implement Application Defenses
  - Configure secure browser settings
  - Configure secure email settings
- 8.1 Protect and Maintain the Integrity of Data Files
  - Implement encryption technologies
- 8.2 Protect Data Transmissions Across Open, Public Networks
  - Encrypt data communications
  - Implement secure protocols
  - Remove unsecure protocols

This section covers the following Security+ certification exam objectives:

- 3.3 Given a scenario, implement secure systems design.
  - Hardware/firmware security
    - TPM
    - HSM

- 5.1 Explain the importance of policies, plans and procedures related to organizational security.
  - General security policies
    - Social media networks/applications
    - Personal email

- 6.1 Compare and contrast basic concepts of cryptography.
• Digital signatures

6.2 Explain cryptography algorithms and their basic characteristics.

• Asymmetric algorithms
  o PGP/GPG

6.4 Given a scenario, implement public key infrastructure.

• Types of certificates
  o Email
• Certificate formats
  o PEM

**Video/Demo**

<table>
<thead>
<tr>
<th>Video/Demo</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.3.1 Combining Cryptographic Methods</td>
<td>6:31</td>
</tr>
<tr>
<td>9.3.2 Hardware-Based Encryption Devices</td>
<td>5:49</td>
</tr>
</tbody>
</table>

**Total Video Time** 12:20

**Fact Sheets**

- 9.3.3 Cryptographic Implementation Facts

**Number of Exam Questions**

6 questions

**Total Time**

*About 24 minutes*
9.4: Cryptographic Attacks

Lecture Focus Questions:

- What is cryptanalysis? Why is it important?
- How does a brute force attack work?
- How can you protect yourself from a dictionary attack?
- What is a man in the middle attack?
- What are some countermeasures you can use to strengthen your cryptosystem?

This section covers the following TestOut Security Pro certification exam objectives:

- 8.1 Protect and Maintain the Integrity of Data Files
  - Implement encryption technologies
- 8.2 Protect Data Transmissions Across Open, Public Networks
  - Encrypt data communications
  - Implement secure protocols
  - Remove unsecure protocols

This section covers the following Security+ certification exam objective:

1.2 Compare and contrast types of attacks

- Application/service attacks
  - Man-in-the-middle
  - Replay
- Cryptographic attacks
  - Birthday
  - Known plain text/cipher text
  - Dictionary
  - Brute force
    - Online vs. offline
  - Replay
  - Weak implementations

Video/Demo

<table>
<thead>
<tr>
<th>Video/Demo</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.4.1 Cryptographic Attacks</td>
<td>10:27</td>
</tr>
</tbody>
</table>

Total Video Time 10:27

Fact Sheets

- 9.4.2Cryptographic Attack Facts

Number of Exam Questions

14 questions

Total Time

About 30 minutes

Copyright © 2017 TestOut Corporation. CompTIA, A+, Network+, Security+, Linux+ and related trademarks and trade names are the trademarks of CompTIA. Microsoft, MCITP, MSCA, MCTS, Windows, and Office 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.
9.5: Symmetric Encryption

Lecture Focus Questions:

- A user needs to communicate securely with five other users using symmetric key encryption. How many keys are required?
- How are symmetric keys typically exchanged between communication partners?
- What is an advantage of increasing the number of bits in the key? What is a disadvantage?
- Why are symmetric key stream ciphers considered to be slower than symmetric key block ciphers?
- Considering symmetric key stream ciphers and block ciphers, which would you select to process large amounts of data? Why?
- How does 3DES differ from DES?

In this section, you will learn to:

- Crack a symmetric encryption key

This section covers the following TestOut Security Pro certification exam objectives:

- 8.1 Protect and Maintain the Integrity of Data Files
  - Implement encryption technologies
- 8.2 Protect Data Transmissions Across Open, Public Networks
  - Encrypt data communications
  - Implement secure protocols
  - Remove unsecure protocols

This section covers the following Security+ certification exam objectives:

6.1 Compare and contrast basic concepts of cryptography

- Symmetric algorithms
- Modes of operation
- Hashing
- Salt, IV, nonce
- Weak/deprecated algorithms
- Stream vs. block
- Key strength
- Secret algorithm
- Key stretching

6.2 Explain cryptography algorithms and their basic characteristics

- Symmetric algorithms
  - AES
  - DES
- 3DES
- RC4
- Blowfish/Twofish

- Cipher modes
  - CBC
  - ECB
  - Stream vs. block

- Hashing algorithms
  - MD5
  - SHA
  - HMAC
  - RIPEMD

- Key stretching algorithms
  - BCRYPT
  - PBKDF2

**Video/Demo**

- [ 9.5.1 Symmetric Encryption ] 4:18
- [ 9.5.3 Cracking a Symmetric Encryption Key ] 4:47

**Total Video Time** 9:05

**Fact Sheets**

- [ 9.5.2 Symmetric Encryption Facts ]

**Number of Exam Questions**

15 questions

**Total Time**

*About 30 minutes*
9.6: Asymmetric Encryption

Lecture Focus Questions:

- How do public keys differ from private keys? What is the relationship between the two?
- For which type of environment is asymmetric cryptography best suited?
- Why does asymmetric encryption require fewer keys than symmetric encryption?
- What services are provided by the cryptographic service provider (CSP)?
- What is the main use for the Diffie-Hellman protocol?

This section covers the following TestOut Security Pro certification exam objectives:

- 8.1 Protect and Maintain the Integrity of Data Files
  - Implement encryption technologies
- 8.2 Protect Data Transmissions Across Open, Public Networks
  - Encrypt data communications
  - Implement secure protocols
  - Remove unsecure protocols

This section covers the following Security+ certification exam objectives:
6.1 Compare and contrast basic concepts of cryptography.

- Modes of operation
- Asymmetric algorithms
- Elliptic curve
- Weak/deprecated algorithms
- Key exchange
- Digital signatures
- Key strength
- Session keys
- Ephemeral key
- Secret algorithm
- Data-in-transit
- Data-at-rest
- Data-in-use
- Perfect forward secrecy
- Common use cases
  - Supporting confidentiality
  - Supporting integrity
  - Supporting authentication
  - Supporting non-repudiation
  - Resource vs. security constraints

6.2 Explain cryptography algorithms and their basic characteristics.
- Asymmetric algorithms
  - RSA
  - DSA
  - Diffie-Hellman
    - Groups
    - DHE
    - ECDHE
  - Elliptic curve
  - PGP/GPG

**Video/Demo**

- 9.6.1 Asymmetric Encryption

  **Time**
  - Total Video Time 5:40

**Fact Sheets**

- 9.6.2 Asymmetric Encryption Facts

**Number of Exam Questions**

12 questions

**Total Time**

*About 23 minutes*
9.7: File Encryption

Lecture Focus Questions:

- On which computers should you implement EFS?
- What is the FEK? How is it used?
- Under what conditions can EFS encryption be compromised?
- Once a system encrypted with Bitlocker boots, who is able to access files?
- How is Bitlocker different from EFS?
- What can you encrypt with GPG?

In this section, you will learn to:

- Encrypt Files with EFS
- Encrypt Files with GPG
- Configure BitLocker with a TPM

This section covers the following TestOut Security Pro certification exam objectives:

- 8.1 Protect and Maintain the Integrity of Data Files
  o Implement encryption technologies
- 8.2 Protect Data Transmissions Across Open, Public Networks
  o Encrypt data communications

This section covers the following Security+ certification exam objective:
6.2 Explain cryptography algorithms and their basic characteristics

- Symmetric algorithms
  o AES
  o DES
  o 3DES
- Asymmetric algorithms
  o RSA
  o DSA
  o Elliptic curve
  o PGP/GPG

Video/Demo

<table>
<thead>
<tr>
<th>Video/Demo</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.7.1 Encrypting File System (EFS)</td>
<td>8:59</td>
</tr>
<tr>
<td>9.7.2 Securing Files using EFS</td>
<td>8:17</td>
</tr>
<tr>
<td>9.7.4 PGP and GPG</td>
<td>4:22</td>
</tr>
<tr>
<td>9.7.5 Encrypting Files with GPG</td>
<td>5:46</td>
</tr>
<tr>
<td>9.7.6 BitLocker and Database Encryption</td>
<td>4:39</td>
</tr>
<tr>
<td>9.7.7 Configuring BitLocker</td>
<td>3:53</td>
</tr>
</tbody>
</table>

Total Video Time 35:56
Lab/Activity
- 9.7.3 Encrypt Files with EFS
- 9.7.8 Configure BitLocker with a TPM

Fact Sheets
- 9.7.9 File Encryption Facts

Number of Exam Questions
8 questions

Total Time
About 59 minutes
9.8: Public Key Infrastructure (PKI)

**Lecture Focus Questions:**

- Who authorizes subordinate CAs? Why is this important?
- What does the issuance policy on a CA control?
- How does a client verify the information in an SSL certificate to determine if it trusts the certificate?
- What is the difference between key archival and key escrow?
- How are revoked certificates identified? Under what circumstances would a certificate be revoked?
- What security advantage do dual key pairs provide?

In this section, you will learn to:

- Manage certificates
- Configure a subordinate CA

This section covers the following TestOut Security Pro certification exam objective:

- 1.3 Manage Certificates
  - Approve, deny, and revoke certificate requests

This section covers the following Security+ certification exam objective:

6.4 Given a scenario, implement public key infrastructure

- Components
  - CA
  - CRL
  - OCSP
  - CSR
  - Certificate
  - Public key
  - Private key
- Concepts
  - Online vs. offline CA
  - Key escrow

**Video/Demo**

<table>
<thead>
<tr>
<th>Time</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>7:04</td>
<td>9.8.1 Certificates</td>
</tr>
<tr>
<td>10:34</td>
<td>9.8.2 Managing Certificates</td>
</tr>
<tr>
<td>5:34</td>
<td>9.8.5 CA Implementation</td>
</tr>
<tr>
<td>10:08</td>
<td>9.8.6 Configuring a Subordinate CA</td>
</tr>
<tr>
<td><strong>Total Video Time</strong></td>
<td><strong>33:20</strong></td>
</tr>
</tbody>
</table>
Lab/Activity
- 9.8.3 Manage Certificates

Fact Sheets
- 9.8.4 Certificate Lifecycle Facts
- 9.8.7 PKI Management Facts

Number of Exam Questions
15 questions

Total Time
About 64 minutes
9.9: Hashing

Lecture Focus Questions:

- What security goal or function is provided by hashes?
- Why doesn't a hash provide message encryption?
- What is the hash value output named?
- What does it mean when the message sender and receiver have different hashes?
- When comparing MD5 and SHA-1, which method provides greater security? Why?
- What is a collision? Why is this condition undesirable in a hashing algorithm?
- Why is high amplification an indicator of a good hashing algorithm?

In this section, you will learn to:

- Use hashes

This section covers the following TestOut Security Pro certification exam objectives:

- 8.1 Protect and Maintain the Integrity of Data Files
  - Implement encryption technologies
- 8.2 Protect Data Transmissions Across Open, Public Networks
  - Encrypt data communications

This section covers the following Security+ certification exam objectives:

- 6.1 Compare and contrast basic concepts of cryptography.
  - Hashing
  - Collision

6.2 Explain cryptography algorithms and their basic characteristics.

- Hashing algorithms
  - MD5
  - SHA
  - HMAC
  - RIPEMD

Video/Demo

<table>
<thead>
<tr>
<th>Video/Demo</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.9.1 Hashing</td>
<td>4:06</td>
</tr>
<tr>
<td>9.9.2 Hashing Algorithms</td>
<td>2:08</td>
</tr>
<tr>
<td>9.9.4 Using Hashes</td>
<td>5:05</td>
</tr>
<tr>
<td><strong>Total Video Time</strong></td>
<td><strong>11:19</strong></td>
</tr>
</tbody>
</table>
Fact Sheets

- 9.9.3 Hashing Facts

Number of Exam Questions
10 questions

Total Time
About 27 minutes
9.10: Data Transmission Security

Lecture Focus Questions:

- How does SSL verify authentication credentials?
- What protocol is the successor to SSL 3.0?
- How can you tell that a session with a web server is using SSL?
- What is the difference between HTTPS and S-HTTP?
- What does it mean when HTTPS is stateful?
- What is the difference between IPsec tunnel mode and transport mode?

In this section, you will learn to:

- Add SSL to a website
- Allow SSL connections
- Require IPsec for communications

This section covers the following TestOut Security Pro certification exam objectives:

- 2.1 Promote Information Security Awareness
  - Using SSL encryption
- 8.2 Protect Data Transmissions Across Open, Public Networks
  - Implement secure protocols

This section covers the following Security+ certification exam objectives:

2.1 Install and configure network components, both hardware- and software-based, to support organizational security

- VPN concentrator
  - IPSec
    - Tunnel mode
    - Transport mode
    - AH
    - ESP
  - TLS

2.6 Given a scenario, implement secure protocols

- Protocols
  - SSH
  - LDAPS
  - FTPS
  - SSL/TLS
  - HTTPS
- Use cases
  - Email and web
- File transfer
- Directory services

**Video/Demo**

<table>
<thead>
<tr>
<th>#</th>
<th>Description</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10.1</td>
<td>Secure Protocols</td>
<td>6:22</td>
</tr>
<tr>
<td>9.10.2</td>
<td>Secure Protocols 2</td>
<td>7:50</td>
</tr>
<tr>
<td>9.10.4</td>
<td>Adding SSL to a Website</td>
<td>5:25</td>
</tr>
<tr>
<td>9.10.6</td>
<td>IPsec</td>
<td>4:49</td>
</tr>
<tr>
<td>9.10.8</td>
<td>Requiring IPsec for Communications</td>
<td>11:39</td>
</tr>
</tbody>
</table>

**Total Video Time**: 36:05

**Lab/Activity**

- 9.10.5 Allow SSL Connections

**Fact Sheets**

- 9.10.3 Secure Protocol Facts
- 9.10.7 IPsec Facts

**Number of Exam Questions**

15 questions

**Total Time**

*About 67 minutes*
9.11: Data Loss Prevention (DLP)

Lecture Focus Questions:

- What is the purpose of a DLP system?
- How can DLP be implemented?
- Why is endpoint DLP important?
- What is an example of file-level DLP?

This section covers the following Security+ certification exam objectives:
2.1 Install and configure network components, both hardware- and software-based, to support organizational security

- DLP
  - USB blocking
  - Cloud-based
  - Email

2.3 Given a scenario, troubleshoot common security issues

- Data exfiltration

2.4 Given a scenario, analyze and interpret output from security technologies

- DLP

Video/Demo

9.11.1 Data Loss Prevention (DLP)    Time

3:47

Total Video Time 3:47

Fact Sheets

9.11.2 DLP Facts

Number of Exam Questions

5 questions

Total Time

About 14 minutes
9.12: Redundancy

Lecture Focus Questions:

- What is the usual activation goal time for a hot site? How does it differ from the goal time for a warm site?
- Why is a hot site so much more expensive to operate than a warm site?
- Why is it important that two companies with a reciprocal agreement should not be located too closely to each other?
- Of the three redundancy solutions, which is the most common redundant site type? Why is it the most common?
- What is data sovereignty?
- Why should you locate redundant sites at least 25 miles from the primary site?
- What is the main advantage of RAID 0? Disadvantage?
- What is the difference between RAID 0+1 and RAID 1+0?

In this section, you will learn to:

- Implement RAID
- Configure fault-tolerant volumes

This section covers the following TestOut Security Pro certification exam objective:

- 8.1 Protect and Maintain the Integrity of Data Files
  - Implement redundancy and failover mechanisms

This section covers the following Security+ certification exam objectives:

- 3.8 Explain how resiliency and automation strategies reduce risk
  - Elasticity
  - Scalability
  - Distributive allocation
  - Redundancy
  - Fault tolerance
  - High availability
  - RAID

- 5.2 Summarize business impact analysis concepts
  - RTO/RPO
  - MTBF
  - MTTR
  - Mission-essential functions
  - Identification of critical systems
  - Single point of failure
5.6 Explain disaster recovery and continuity of operation concepts

- Recovery sites
  - Hot site
  - Warm site
  - Cold site
- Order of restoration
- Geographic considerations
  - Off-site backups
  - Distance
  - Location selection
  - Legal implications
  - Data sovereignty

**Video/Demo**

<table>
<thead>
<tr>
<th>Video/Demo</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.12.1 Redundancy</td>
<td>3:23</td>
</tr>
<tr>
<td>9.12.2 Redundancy Measurement Params</td>
<td>4:42</td>
</tr>
<tr>
<td>9.12.4 RAID</td>
<td>4:38</td>
</tr>
<tr>
<td>9.12.5 Implementing RAID</td>
<td>7:18</td>
</tr>
<tr>
<td>9.12.8 Clustering</td>
<td>7:06</td>
</tr>
</tbody>
</table>

**Total Video Time** 27:07

**Lab/Activity**

- 9.12.7 Configure Fault-Tolerant Volumes

**Fact Sheets**

- 9.12.3 Redundancy Facts
- 9.12.6 RAID Facts
- 9.12.9 Clustering Facts

**Number of Exam Questions**

15 questions

**Total Time**

*About 63 minutes*
9.13: Backup and Restore

Lecture Focus Questions:

- How is an incremental backup different from a differential backup?
- When is the archive bit set? Which backup types reset the archive bit?
- What is the advantage of the Full + Incremental backup strategy? What is the disadvantage?
- Why should backup tapes be stored offsite?
- What are common types of backup media rotation systems used to provide protection to adequately restore data?
- How do you back up Active Directory?
- What should you regularly do to make sure your backup strategy is working properly?

In this section, you will learn to:

- Back up a workstation
- Restore workstation data from backup
- Back up a domain controller
- Restore server data from backup

This section covers the following TestOut Security Pro certification exam objectives:

- 6.3 Perform System Backups and Recovery
- 8.1 Protect and Maintain the Integrity of Data Files
  - Perform data backups and recovery

This section covers the following Security+ certification exam objectives:
3.8 Explain how resiliency and automation strategies reduce risk

- Templates
- Master image
- Non-persistence
  - Snapshots
  - Revert to known state
  - Rollback to known configuration
  - Live boot media

5.6 Explain disaster recovery and continuity of operation concepts

- Backup concepts
  - Differential
  - Incremental
  - Snapshots
  - Full
Video/Demo

<table>
<thead>
<tr>
<th>Task</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.13.1 Backup and Restore</td>
<td>9:13</td>
</tr>
<tr>
<td>9.13.4 Backing Up Workstations</td>
<td>7:55</td>
</tr>
<tr>
<td>9.13.6 Restoring Workstation Data from Backup</td>
<td>4:04</td>
</tr>
<tr>
<td>9.13.7 Backing Up a Domain Controller</td>
<td>2:45</td>
</tr>
<tr>
<td>9.13.9 Restoring Server Data from Backup</td>
<td>3:00</td>
</tr>
</tbody>
</table>

Total Video Time 26:57

Lab/Activity

- 9.13.5 Back Up a Workstation
- 9.13.8 Back Up a Domain Controller

Fact Sheets

- 9.13.2 Backup and Restore Facts
- 9.13.3 Backup Management Facts

Number of Exam Questions
14 questions

Total Time
About 61 minutes
9.14: Cloud Storage

Lecture Focus Questions:

- What is cloud storage?
- What is a Cloud Access Security Broker (CASB)?
- What is one example of a cloud storage provider?
- What are some advantages of using cloud storage?
- What are some security measures to use when implementing cloud storage?

This section covers the following Security+ certification exam objective:
3.7 Summarize cloud and virtualization concepts

- Cloud access security broker

Video/Demo

<table>
<thead>
<tr>
<th>9.14.1 Cloud Storage Security</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2:44</td>
</tr>
</tbody>
</table>

Total Video Time 2:44

Fact Sheets


Number of Exam Questions

5 questions

Total Time

About 13 minutes
Practice Exams

A.0: Security Pro Practice Exams
Security Pro Domain 1: Access Control and Identity Management (24 questions)
Security Pro Domain 2: Policies, Procedures, Awareness (2 questions)
Security Pro Domain 3: Physical Security (2 questions)
Security Pro Domain 4: Perimeter Defenses (9 questions)
Security Pro Domain 5: Network Defenses (7 questions)
Security Pro Domain 6: Host Defenses (7 questions)
Security Pro Domain 7: Application Defenses (10 questions)
Security Pro Domain 8: Data Defenses (6 questions)
Security Pro Domain 9: Audits and Assessments (2 questions)
Security Pro Certification Practice Exam (15 questions)

B.0: CompTIA Security+ Practice Exams
CompTIA Security+ Domain 1: Threats, Attacks and Vulnerabilities, All Questions (177 questions)
CompTIA Security+ Domain 2: Technologies and Tools, All Questions (147 questions)
CompTIA Security+ Domain 3: Architecture and Design, All Questions (236 questions)
CompTIA Security+ Domain 4: Identity and Access Management, All Questions (154 questions)
CompTIA Security+ Domain 5: Risk Management, All Questions (123 questions)
CompTIA Security+ Domain 6: Cryptography and PKI, All Questions (95 questions)
CompTIA Security+ Certification Practice Exam (100 questions)
Appendix A: Security Pro Exam Objectives

The TestOut Security Pro course and certification exam cover the following objectives:

<table>
<thead>
<tr>
<th>#</th>
<th>Domain</th>
<th>Module, Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Access Control and Identity Management</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Create, Modify, and Delete User Profiles</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Manage Windows Domain Users and Groups</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Create, rename, and delete users and groups</td>
<td>8.3, 8.8, 8.9, 8.10, 8.12, 8.13, 8.14</td>
</tr>
<tr>
<td></td>
<td>- Assign users to appropriate groups</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Lock and unlock user accounts</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Change a user's password</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Manage Linux Users and Groups</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Create, rename, and delete users and groups</td>
<td>8.3, 8.8, 8.9, 8.10, 8.12, 8.13, 8.14</td>
</tr>
<tr>
<td></td>
<td>- Assign users to appropriate groups</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Lock and unlock user accounts</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Change a user's password</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Configure password aging</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Manage Windows Local Users and Groups</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Restrict use of local user accounts</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Restrict use of common access accounts</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Harden Authentication</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Configure Domain GPO Account Policy</td>
<td>5.9, 6.11, 8.2, 8.12, 8.13, 8.14</td>
</tr>
<tr>
<td></td>
<td>to enforce a robust password policy</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Configure the Domain GPO to control local administrator group membership and administrator password</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>1.3</td>
<td>Manage Certificates</td>
<td>9.8</td>
</tr>
<tr>
<td></td>
<td>• Approve, deny, and revoke certificate requests</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Configure Domain GPO Kerberos settings</td>
<td></td>
</tr>
<tr>
<td>2.0</td>
<td>Policies, Procedures, and Awareness</td>
<td></td>
</tr>
<tr>
<td>2.1</td>
<td>Promote Information Security Awareness</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Traveling with Personal Mobile Devices</td>
<td>3.5, 3.8</td>
</tr>
<tr>
<td></td>
<td>• Exchanging content between home and work</td>
<td>5.4</td>
</tr>
<tr>
<td></td>
<td>• Storing personal information on the internet</td>
<td>7.10, 7.11</td>
</tr>
<tr>
<td></td>
<td>• Using social networking sites</td>
<td>9.3, 9.10</td>
</tr>
<tr>
<td></td>
<td>• Using SSL encryption</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Using email best practices</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Password management</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Photo/GPS integration</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Information security</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Auto-lock and passcode lock</td>
<td></td>
</tr>
<tr>
<td>2.2</td>
<td>Evaluate Information Risk</td>
<td>3.2, 3.3</td>
</tr>
<tr>
<td></td>
<td>• Perform risk calculation</td>
<td>4.3</td>
</tr>
<tr>
<td></td>
<td>• Risk avoidance, transference, acceptance, mitigation, and deterrence</td>
<td></td>
</tr>
<tr>
<td>Section</td>
<td>Topic</td>
<td>Notes</td>
</tr>
<tr>
<td>---------</td>
<td>-------</td>
<td>-------</td>
</tr>
<tr>
<td>2.3</td>
<td>Maintain Hardware and Software Inventory</td>
<td>4.2</td>
</tr>
<tr>
<td>3.0</td>
<td><strong>Physical Security</strong></td>
<td></td>
</tr>
<tr>
<td>3.1</td>
<td>Harden Data Center Physical Access</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Implement access rosters</td>
<td>4.1</td>
</tr>
<tr>
<td></td>
<td>• Use visitor identification and control</td>
<td>6.7</td>
</tr>
<tr>
<td></td>
<td>• Protect doors and windows</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Implement physical intrusion detection systems</td>
<td></td>
</tr>
<tr>
<td>3.2</td>
<td>Harden Mobile Devices (iPad)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Apply updates</td>
<td>3.8</td>
</tr>
<tr>
<td></td>
<td>• Set Autolock</td>
<td>5.5</td>
</tr>
<tr>
<td></td>
<td>• Enable passcodes</td>
<td>7.12</td>
</tr>
<tr>
<td></td>
<td>• Configure network security settings</td>
<td></td>
</tr>
<tr>
<td>3.3</td>
<td>Harden Mobile Devices (Laptop)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Set a BIOS password</td>
<td>5.5</td>
</tr>
<tr>
<td></td>
<td>• Set a login password</td>
<td>7.12</td>
</tr>
<tr>
<td></td>
<td>• Implement full disk encryption</td>
<td></td>
</tr>
<tr>
<td>4.0</td>
<td><strong>Perimeter Defenses</strong></td>
<td></td>
</tr>
<tr>
<td>4.1</td>
<td>Harden the Network Perimeter (using a Cisco Network Security Appliance)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Change the default user name and password</td>
<td>5.2, 5.4, 5.5, 5.6, 5.7, 5.8</td>
</tr>
<tr>
<td></td>
<td>• Configure a firewall</td>
<td>6.2</td>
</tr>
<tr>
<td></td>
<td>• Create a DMZ</td>
<td>8.4</td>
</tr>
<tr>
<td></td>
<td>• Configure NAT</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Configure VPN</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Implement web threat protection</td>
<td></td>
</tr>
<tr>
<td>4.2</td>
<td>Secure Wireless Devices and Clients</td>
<td>5.10, 5.12</td>
</tr>
</tbody>
</table>
- Change the default user name, password, and administration limits
- Implement WPA2
- Configure enhanced security
  - MAC filtering
  - SSID cloaking
  - Power control
- Disable Network Discovery

### 5.0 Network Defenses

#### 5.1 Harden Network Devices (Using a Cisco Small Business Switch)

- Change the default user name and password on network devices
- Use secure passwords
- Shut down unnecessary services and ports
- Implement port security
- Remove unsecure protocols (FTP, telnet, rlogin, rsh)
- Implement access lists, deny everything else
- Run latest iOS version
- Turn on logging with timestamps
- Segment traffic using VLANs

<table>
<thead>
<tr>
<th>2.11</th>
<th>5.12</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2, 6.5, 6.6, 6.7, 6.9</td>
<td>7.2, 7.5, 7.6, 7.9</td>
</tr>
<tr>
<td>8.3, 8.11, 8.13</td>
<td></td>
</tr>
</tbody>
</table>

#### 5.2 Implement Intrusion Detection/Prevention (Using a Cisco Network Security Appliance)

- Enable IPS protection for a LAN and DMZ
- Apply IPS signature updates
- Configure IPS policy

<table>
<thead>
<tr>
<th>5.3</th>
</tr>
</thead>
</table>

### 6.0 Host Defenses

#### 6.1 Harden Computer Systems Against Attack

| 7.3, 7.4, 7.5 |
| 8.12 |

---

Copyright © 2017 TestOut Corporation. CompTIA, A+, Network+, Security+, Linux+ and related trademarks and trade names are the trademarks of CompTIA. Microsoft, MCITP, MUSCA, MCTS, Windows, and Office 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.
- Configure a GPO to enforce workstation/server security settings
- Configure Domain GPO to enforce Windows Firewall use
- Configure Domain Servers GPO to remove unneeded services (such as file and printer sharing)
- Protect against spyware and unwanted software using Windows Defender
- Configure NTFS permissions for secure file sharing

<table>
<thead>
<tr>
<th>6.2</th>
<th>Implement Patch Management/System Updates</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Configure Windows Update</td>
</tr>
<tr>
<td></td>
<td>• Apply the latest Apple software updates</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>6.3</th>
<th>Perform System Backups and Recovery</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>9.13</td>
</tr>
</tbody>
</table>

### 7.0 Application Defenses

<table>
<thead>
<tr>
<th>7.1</th>
<th>Implement Application Defenses</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Configure a GPO to enforce Internet Explorer settings</td>
</tr>
<tr>
<td></td>
<td>• Configure a GPO for application whitelisting</td>
</tr>
<tr>
<td></td>
<td>• Enable Data Execution Prevention (DEP)</td>
</tr>
<tr>
<td></td>
<td>• Configure web application security</td>
</tr>
<tr>
<td></td>
<td>• Configure parental controls to enforce web content filtering</td>
</tr>
<tr>
<td></td>
<td>• Configure secure browser settings</td>
</tr>
<tr>
<td></td>
<td>• Configure secure email settings</td>
</tr>
<tr>
<td></td>
<td>• Configure virtual machines and switches</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>7.2</th>
<th>Implement Patch Management/Software Updates</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>7.3</td>
</tr>
</tbody>
</table>
- Configure Microsoft Update

<table>
<thead>
<tr>
<th>8.0</th>
<th>Data Defenses</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1</td>
<td>Protect and Maintain the Integrity of Data Files</td>
</tr>
<tr>
<td></td>
<td>- Implement encryption technologies</td>
</tr>
<tr>
<td></td>
<td>- Perform data backups and recovery</td>
</tr>
<tr>
<td></td>
<td>- Implement redundancy and failover mechanisms</td>
</tr>
<tr>
<td>8.2</td>
<td>Protect Data Transmissions Across Open, Public Networks</td>
</tr>
<tr>
<td></td>
<td>- Encrypt data communications</td>
</tr>
<tr>
<td></td>
<td>- Implement secure protocols</td>
</tr>
<tr>
<td></td>
<td>- Remove unsecure protocols</td>
</tr>
<tr>
<td></td>
<td>5.4, 5.12, 7.4, 8.5, 9.2, 9.3, 9.4, 9.5, 9.6, 9.7, 9.10</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>9.0</th>
<th>Audits and Assessments</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.1</td>
<td>Implement Logging and Auditing</td>
</tr>
<tr>
<td></td>
<td>- Configure Domain GPO audit policy</td>
</tr>
<tr>
<td></td>
<td>- Configure Domain GPO for event logging</td>
</tr>
<tr>
<td></td>
<td>7.8, 7.9</td>
</tr>
<tr>
<td>9.2</td>
<td>Review Security Logs and Violation Reports, Implement Remediation</td>
</tr>
<tr>
<td></td>
<td>7.8, 7.9, 8.1</td>
</tr>
<tr>
<td>9.3</td>
<td>Review Audit Reports, Implement Remediation</td>
</tr>
<tr>
<td></td>
<td>7.9</td>
</tr>
<tr>
<td>9.4</td>
<td>Review Vulnerability Reports, Implement Remediation</td>
</tr>
<tr>
<td></td>
<td>7.9</td>
</tr>
</tbody>
</table>
## Appendix B: CompTIA Security+ Exam Objectives

### Exam: SY0-501: CompTIA Security+

The Security+ exam tests general knowledge of security concepts, threats, and tools. The exam covers the following topics.

<table>
<thead>
<tr>
<th>#</th>
<th>Objective</th>
<th>Module. Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td><strong>Threats, Attacks and Vulnerabilities</strong></td>
<td></td>
</tr>
<tr>
<td>1.1</td>
<td>Given a scenario, analyze indicators of compromise and determine the type of malware.</td>
<td>6.2</td>
</tr>
<tr>
<td></td>
<td>• Viruses</td>
<td>7.1</td>
</tr>
<tr>
<td></td>
<td>• Crypto-malware</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Ransomware</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Worm</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Trojan</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Rootkit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Keylogger</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Adware</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Spyware</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Bots</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• RAT</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Logic bomb</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Backdoor</td>
<td></td>
</tr>
</tbody>
</table>

| 1.2 | Compare and contrast types of attacks.                                    |                 |
|     | • Social engineering:                                                     |                 |
|     |   o Phishing                                                              |                 |
|     |   o Spear phishing                                                       |                 |
|     |   o Whaling                                                               |                 |
|     |   o Vishing                                                              |                 |
|     |   o Tailgating                                                            |                 |
|     |   o Impersonation                                                        |                 |
|     |   o Dumpster diving                                                       |                 |
|     |   o Shoulder surfing                                                      |                 |
|     |   o Hoax                                                                  |                 |
|     |   o Watering hole attack                                                 |                 |
|     |   o Principles (reasons for effectiveness)                               |                 |
|     |     ▪ Authority                                                           |                 |

Copyright © 2017 TestOut Corporation. CompTIA, A+, Network+, Security+, Linux+ and related trademarks and trade names are the trademarks of CompTIA. Microsoft, MCITP, MScA, MCTS, Windows, and Office 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.
- Intimidation
- Consensus
- Scarcity
- Familiarity
- Trust
- Urgency

- Application/service attacks
  - DoS
  - DDoS
  - Man-in-the-middle
  - Buffer overflow
  - Injection
  - Cross-site scripting
  - Cross-site request forgery
  - Privilege escalation
  - ARP poisoning
  - Amplification
  - DNS poisoning
  - Domain hijacking
  - Man-in-the-browser
  - Zero day
  - Replay
  - Pass the hash
  - Hijacking and related attacks
    - Clickjacking
    - Session hijacking
    - URL hijacking
    - Typo squatting
  - Driver manipulation
    - Shimming
    - Refactoring
  - MAC spoofing
  - IP spoofing

- Wireless attacks
  - Replay
  - IV
  - Evil twin
  - Rogue AP
  - Jamming
  - WPS
  - Bluejacking
  - Bluesnarfing
  - RFID
  - NFC
  - Disassociation
### 1.3 Explain threat actor types and attributes.

<table>
<thead>
<tr>
<th>Types of actors</th>
<th>Attributes of actors</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Script kiddies</td>
<td>- Internal/external</td>
</tr>
<tr>
<td>- Hacktivist</td>
<td>- Level of sophistication</td>
</tr>
<tr>
<td>- Organized crime</td>
<td>- Resources/funding</td>
</tr>
<tr>
<td>- Nation states/APT</td>
<td>- Intent/motivation</td>
</tr>
<tr>
<td>- Insiders</td>
<td>- Use of open-source intelligence</td>
</tr>
<tr>
<td>- Competitors</td>
<td></td>
</tr>
</tbody>
</table>

### 1.4 Explain penetration testing concepts.

<table>
<thead>
<tr>
<th>Concepts</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Active reconnaissance</td>
</tr>
<tr>
<td>- Passive reconnaissance</td>
</tr>
<tr>
<td>- Pivot</td>
</tr>
<tr>
<td>- Initial exploitation</td>
</tr>
<tr>
<td>- Ports</td>
</tr>
<tr>
<td>- Persistence</td>
</tr>
<tr>
<td>- Escalation of privilege</td>
</tr>
<tr>
<td>- Black box</td>
</tr>
<tr>
<td>- White box</td>
</tr>
<tr>
<td>- Gray box</td>
</tr>
<tr>
<td>- Pen testing vs. vulnerability scanning</td>
</tr>
</tbody>
</table>

### 1.5 Explain vulnerability scanning concepts.

- Passively test security controls
<table>
<thead>
<tr>
<th>1.6</th>
<th>Explain the impact associated with types of vulnerabilities.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Race conditions</td>
</tr>
<tr>
<td></td>
<td>• Vulnerabilities due to:</td>
</tr>
<tr>
<td></td>
<td>○ End-of-life systems</td>
</tr>
<tr>
<td></td>
<td>○ Embedded systems</td>
</tr>
<tr>
<td></td>
<td>○ Lack of vendor support</td>
</tr>
<tr>
<td></td>
<td>• Improper input handling</td>
</tr>
<tr>
<td></td>
<td>• Improper error handling</td>
</tr>
<tr>
<td></td>
<td>• Misconfiguration/weak configuration</td>
</tr>
<tr>
<td></td>
<td>• Default configuration</td>
</tr>
<tr>
<td></td>
<td>• Resource exhaustion</td>
</tr>
<tr>
<td></td>
<td>• Untrained users</td>
</tr>
<tr>
<td></td>
<td>• Improperly configured accounts</td>
</tr>
<tr>
<td></td>
<td>• Vulnerable business processes</td>
</tr>
<tr>
<td></td>
<td>• Weak cipher suites and implementations</td>
</tr>
<tr>
<td></td>
<td>• Memory/buffer vulnerability</td>
</tr>
<tr>
<td></td>
<td>○ Memory leak</td>
</tr>
<tr>
<td></td>
<td>○ Integer overflow</td>
</tr>
<tr>
<td></td>
<td>○ Buffer overflow</td>
</tr>
<tr>
<td></td>
<td>○ Pointer dereference</td>
</tr>
<tr>
<td></td>
<td>○ DLL injection</td>
</tr>
<tr>
<td></td>
<td>• System sprawl/undocumented assets</td>
</tr>
<tr>
<td></td>
<td>• Architecture/design weaknesses</td>
</tr>
<tr>
<td></td>
<td>• New threats/zero day</td>
</tr>
<tr>
<td></td>
<td>• Improper certificate and key management</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2.0</th>
<th>Technologies and Tools</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>Install and configure network components, both hardware- and software-based, to support organizational security.</td>
</tr>
<tr>
<td></td>
<td>• Firewall</td>
</tr>
<tr>
<td></td>
<td>○ ACL</td>
</tr>
</tbody>
</table>
• Application-based vs. network-based
• Stateful vs. stateless
• Implicit deny

• VPN concentrator
  o Remote access vs. site-to-site
  o IPSec
    ▪ Tunnel mode
    ▪ Transport mode
    ▪ AH
    ▪ ESP
  o Split tunnel vs. full tunnel
  o TLS
  o Always-on VPN

• NIPS/NIDS
  o Signature-based
  o Heuristic/behavioral
  o Anomaly
  o Inline vs. passive
  o In-band vs. out-of-band
  o Rules
  o Analytics
    ▪ False positive
    ▪ False negative

• Router
  o ACLs
  o Antispoofing

• Switch
  o Port security
  o Layer 2 vs. Layer 3
  o Loop prevention
  o Flood guard

• Proxy
  o Forward and reverse proxy
  o Transparent
  o Application/multipurpose

• Load balancer
  o Scheduling
    ▪ Affinity
    ▪ Round-robin
  o Active-passive
  o Active-active
  o Virtual IPs

• Access point
  o SSID
<table>
<thead>
<tr>
<th>MAC filtering</th>
<th>Signal strength</th>
<th>Band selection/width</th>
<th>Antenna types and placement</th>
<th>Fat vs. thin</th>
<th>Controller-based vs. standalone</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIEM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Aggregation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Correlation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Automated alerting and triggers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Time synchronization</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Event deduplication</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Logs/WORM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DLP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>USB blocking</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cloud-based</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Email</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NAC</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dissolvable vs. permanent</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Host health checks</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Agent vs. agentless</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mail gateway</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Spam filter</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DLP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Encryption</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bridge</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSL/TLS accelerators</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSL decryptors</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Media gateway</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hardware security module</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 2.2 Given a scenario, use appropriate software tools to assess the security posture of an organization.

- Protocol analyzer
- Network scanners
  - Rogue system detection
  - Network mapping
- Wireless scanners/cracker
- Password cracker
- Vulnerability scanner
- Configuration compliance scanner
- Exploitation frameworks
- Data sanitization tools
- Steganography tools

| 2.5 | 6.9, 6.10 | 7.2 |
- Honeypot
- Backup utilities
- Banner grabbing
- Passive vs. active
- Command line tools
  - ping
  - netstat
  - tracert
  - nslookup/dig
  - arp
  - ipconfig/ip/ifconfig
  - tcpdump
  - nmap
  - netcat

<table>
<thead>
<tr>
<th>2.3</th>
<th>Given a scenario, troubleshoot common security issues.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Unencrypted credentials/cleartext</td>
</tr>
<tr>
<td></td>
<td>Logs and events anomalies</td>
</tr>
<tr>
<td></td>
<td>Permission issues</td>
</tr>
<tr>
<td></td>
<td>Access violations</td>
</tr>
<tr>
<td></td>
<td>Certificate issues</td>
</tr>
<tr>
<td></td>
<td>Data exfiltration</td>
</tr>
<tr>
<td></td>
<td>Misconfigured devices</td>
</tr>
<tr>
<td></td>
<td>Firewall</td>
</tr>
<tr>
<td></td>
<td>Content filter</td>
</tr>
<tr>
<td></td>
<td>Access points</td>
</tr>
<tr>
<td></td>
<td>Weak security configurations</td>
</tr>
<tr>
<td></td>
<td>Personnel issues</td>
</tr>
<tr>
<td></td>
<td>Policy violation</td>
</tr>
<tr>
<td></td>
<td>Insider threat</td>
</tr>
<tr>
<td></td>
<td>Social engineering</td>
</tr>
<tr>
<td></td>
<td>Social media</td>
</tr>
<tr>
<td></td>
<td>Personal email</td>
</tr>
<tr>
<td></td>
<td>Unauthorized software</td>
</tr>
<tr>
<td></td>
<td>Baseline deviation</td>
</tr>
<tr>
<td></td>
<td>License compliance violation (availability/integrity)</td>
</tr>
<tr>
<td></td>
<td>Asset management</td>
</tr>
<tr>
<td></td>
<td>Authentication issues</td>
</tr>
</tbody>
</table>

5.5, 5.8, 5.12
7.8
9.11
2.4 Given a scenario, analyze and interpret output from security technologies.

- HIDS/HIPS
- Antivirus
- File integrity check
- Host-based firewall
- Application whitelisting
- Removable media control
- Advanced malware tools
- Patch management tools
- UTM
- DLP
- Data execution prevention
- Web application firewall

2.5 Given a scenario, deploy mobile devices securely.

- Connection methods
  - Cellular
  - WiFi
  - SATCOM
  - Bluetooth
  - NFC
  - ANT
  - Infrared
  - USB
- Mobile device management concepts
  - Application management
  - Content management
  - Remote wipe
  - Geofencing
  - Geolocation
  - Screen locks
  - Push notification services
  - Passwords and pins
  - Biometrics
  - Context-aware authentication
  - Containerization
  - Storage segmentation
  - Full device encryption
- Enforcement and monitoring for:
  - Third-party app stores
  - Rooting/jailbreaking
  - Sideload
- Custom firmware
- Carrier unlocking
- Firmware OTA updates
- Camera use
- SMS/MMS
- External media
- USB OTG
- Recording microphone
- GPS tagging
- WiFi direct/ad hoc
- Tethering
- Payment methods

**Deployment models**
- BYOD
- COPE
- CYOD
- Corporate-owned
- VDI

### 2.6 Given a scenario, implement secure protocols.

**Protocols**
- DNSSEC
- SSH
- S/MIME
- SRTP
- LDAPS
- FTPS
- SFTP
- SNMPv3
- SSL/TLS
- HTTPS
- Secure POP/IMAP

**Use cases**
- Voice and video
- Time synchronization
- Email and web
- File transfer
- Directory services
- Remote access
- Domain name resolution
- Routing and switching
- Network address allocation
- Subscription services
2.7 Compare and contrast physical security and environmental controls.

- Environmental controls
  - HVAC
  - Fire suppression
  - EMI shielding
  - Hot and cold aisles
  - Environmental monitoring
  - Temperature and humidity controls
- Physical security
  - Hardware locks
  - Mantraps
  - Video
  - Surveillance
  - Fencing
  - Proximity readers
  - Access list
  - Proper lighting
  - Signs
  - Guards
  - Barricades
  - Biometrics
  - Protected distribution (cabling)
  - Alarms
  - Motion detection
- Control types
  - Deterrent
  - Preventive
  - Detective
  - Compensating
  - Technical
  - Administrative

3.0 Architecture and Design

3.1 Explain use cases and purpose for frameworks, best practices and secure configuration guides.

- Industry-standard frameworks and reference architectures
  - Regulatory
  - Non-regulatory
  - National vs. international
- Industry-specific frameworks
  - Benchmarks/secure configuration guides
    - Platform/vendor-specific guides
      - Web server
      - Operating system
      - Application server
      - Network infrastructure devices
    - General purpose guides
  - Defense-in-depth/layered security
    - Vendor diversity
    - Control diversity
      - Administrative
      - Technical
    - User training

### 3.2
Given a scenario, implement secure network architecture concepts.

- **Zones/topologies**
  - DMZ
  - Extranet
  - Intranet
  - Wireless
  - Guest
  - Honeynets
  - NAT
  - Ad hoc

- **Segregation/segmentation/isolation**
  - Physical
  - Logical (VLAN)
  - Virtualization
  - Air gaps

- **Tunneling/VPN**
  - Site-to-site
  - Remote access

- **Security device/technology placement**
  - Sensors
  - Collectors
  - Correlation engines
  - Filters
  - Proxies
  - Firewalls
  - VPN concentrators
  - SSL accelerators
  - Load balancers
<table>
<thead>
<tr>
<th>3.3</th>
<th>Given a scenario, implement secure systems design.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Hardware/firmware security</td>
</tr>
<tr>
<td></td>
<td>• FDE/SED</td>
</tr>
<tr>
<td></td>
<td>• TPM</td>
</tr>
<tr>
<td></td>
<td>• HSM</td>
</tr>
<tr>
<td></td>
<td>• UEFI/BIOS</td>
</tr>
<tr>
<td></td>
<td>• Secure boot and attestation</td>
</tr>
<tr>
<td></td>
<td>• Supply chain</td>
</tr>
<tr>
<td></td>
<td>• Hardware root of trust</td>
</tr>
<tr>
<td></td>
<td>• EMI/EMP</td>
</tr>
<tr>
<td></td>
<td>Operating systems</td>
</tr>
<tr>
<td></td>
<td>• Types</td>
</tr>
<tr>
<td></td>
<td>▪ Network</td>
</tr>
<tr>
<td></td>
<td>▪ Server</td>
</tr>
<tr>
<td></td>
<td>▪ Workstation</td>
</tr>
<tr>
<td></td>
<td>▪ Appliance</td>
</tr>
<tr>
<td></td>
<td>▪ Kiosk</td>
</tr>
<tr>
<td></td>
<td>▪ Mobile OS</td>
</tr>
<tr>
<td></td>
<td>• Patch management</td>
</tr>
<tr>
<td></td>
<td>• Disabling unnecessary ports and services</td>
</tr>
<tr>
<td></td>
<td>• Least functionality</td>
</tr>
<tr>
<td></td>
<td>• Secure configurations</td>
</tr>
<tr>
<td></td>
<td>• Trusted operating system</td>
</tr>
<tr>
<td></td>
<td>• Application whitelisting/blacklisting</td>
</tr>
<tr>
<td></td>
<td>• Disable default accounts/passwords</td>
</tr>
<tr>
<td></td>
<td>Peripherals</td>
</tr>
<tr>
<td></td>
<td>• Wireless keyboards</td>
</tr>
<tr>
<td></td>
<td>• Wireless mice</td>
</tr>
<tr>
<td></td>
<td>• Displays</td>
</tr>
<tr>
<td></td>
<td>• WiFi-enabled MicroSD cards</td>
</tr>
<tr>
<td></td>
<td>• Printers/MFDs</td>
</tr>
<tr>
<td></td>
<td>• External storage devices</td>
</tr>
<tr>
<td></td>
<td>• Digital cameras</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>3.4</th>
<th>Explain the importance of secure staging deployment concepts.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Sandboxing</td>
</tr>
</tbody>
</table>

Copyright © 2017 TestOut Corporation. CompTIA, A+, Network+, Security+, Linux+ and related trademarks and trade names are the trademarks of CompTIA. Microsoft, MCITP, MSTA, MCTS, Windows, and Office 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.
<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Environment</td>
</tr>
<tr>
<td></td>
<td>o Development</td>
</tr>
<tr>
<td></td>
<td>o Test</td>
</tr>
<tr>
<td></td>
<td>o Staging</td>
</tr>
<tr>
<td></td>
<td>o Production</td>
</tr>
<tr>
<td></td>
<td>Secure baseline</td>
</tr>
<tr>
<td></td>
<td>Integrity measurement</td>
</tr>
<tr>
<td>3.5</td>
<td>Explain the security implications of embedded systems.</td>
</tr>
<tr>
<td></td>
<td>SCADA/ICS</td>
</tr>
<tr>
<td></td>
<td>Smart devices/IoT</td>
</tr>
<tr>
<td></td>
<td>o Wearable technology</td>
</tr>
<tr>
<td></td>
<td>o Home automation</td>
</tr>
<tr>
<td></td>
<td>HVAC</td>
</tr>
<tr>
<td></td>
<td>SoC</td>
</tr>
<tr>
<td></td>
<td>RTOS</td>
</tr>
<tr>
<td></td>
<td>Printers/MFDs</td>
</tr>
<tr>
<td></td>
<td>Camera systems</td>
</tr>
<tr>
<td></td>
<td>Special purpose</td>
</tr>
<tr>
<td></td>
<td>o Medical devices</td>
</tr>
<tr>
<td></td>
<td>o Vehicles</td>
</tr>
<tr>
<td></td>
<td>o Aircraft/UAV</td>
</tr>
<tr>
<td>3.6</td>
<td>Summarize secure application development and deployment concepts.</td>
</tr>
<tr>
<td></td>
<td>Development life-cycle models</td>
</tr>
<tr>
<td></td>
<td>o Waterfall vs. Agile</td>
</tr>
<tr>
<td></td>
<td>Secure DevOps</td>
</tr>
<tr>
<td></td>
<td>o Security automation</td>
</tr>
<tr>
<td></td>
<td>o Continuous integration</td>
</tr>
<tr>
<td></td>
<td>o Baselining</td>
</tr>
<tr>
<td></td>
<td>o Immutable systems</td>
</tr>
<tr>
<td></td>
<td>o Infrastructure as code</td>
</tr>
<tr>
<td></td>
<td>Version control and change management</td>
</tr>
<tr>
<td></td>
<td>Provisioning and deprovisioning</td>
</tr>
<tr>
<td></td>
<td>Secure coding techniques</td>
</tr>
<tr>
<td></td>
<td>o Proper error handling</td>
</tr>
<tr>
<td></td>
<td>o Proper input validation</td>
</tr>
<tr>
<td></td>
<td>o Normalization</td>
</tr>
<tr>
<td></td>
<td>o Stored procedures</td>
</tr>
<tr>
<td></td>
<td>o Code signing</td>
</tr>
<tr>
<td></td>
<td>o Encryption</td>
</tr>
<tr>
<td></td>
<td>o Obfuscation/camouflage</td>
</tr>
</tbody>
</table>
• Code reuse/dead code
• Server-side vs. client-side execution and validation
• Memory management
• Use of third-party libraries and SDKs
• Data exposure
  • Code quality and testing
    o Static code analyzers
    o Dynamic analysis (e.g., fuzzing)
    o Stress testing
    o Sandboxing
    o Model verification
  • Compiled vs. runtime code

3.7 Summarize cloud and virtualization concepts.

  • Hypervisor
    o Type I
    o Type II
      o Application cells/containers
  • VM sprawl avoidance
  • VM escape protection
  • Cloud storage
  • Cloud deployment models
    o SaaS
    o PaaS
    o IaaS
    o Private
    o Public
    o Hybrid
    o Community
  • On-premise vs. hosted vs. cloud
  • VDI/VDE
  • Cloud access security broker
  • Security as a Service

3.8 Explain how resiliency and automation strategies reduce risk.

  • Automation/scripting
    o Automated courses of action
    o Continuous monitoring
    o Configuration validation
  • Templates
  • Master image

6.14, 6.16
7.13
9.14
9.12, 9.13
• Non-persistence
  o Snapshots
  o Revert to known state
  o Rollback to known configuration
  o Live boot media
• Elasticity
• Scalability
• Distributive allocation
• Redundancy
• Fault tolerance
• High availability
• RAID

3.9 Explain the importance of physical security controls.

  • Lighting
  • Signs
  • Fencing/gate/cage
  • Security guards
  • Alarms
  • Safe
  • Secure cabinets/enclosures
  • Protected distribution/Protected cabling
  • Airgap
  • Mantrap
  • Faraday cage
  • Lock types
  • Biometrics
  • Barricades/bollards
  • Tokens/cards
  • Environmental controls
    o HVAC
    o Hot and cold aisles
    o Fire suppression
  • Cable locks
  • Screen filters
  • Cameras
  • Motion detection
  • Logs
  • Infrared detection
  • Key management
# 4.0 Identity and Access Management

## 4.1 Compare and contrast identity and access management concepts.

- Identification, authentication, authorization and accounting (AAA)
- Multifactor authentication
  - Something you are
  - Something you have
  - Something you know
  - Somewhere you are
  - Something you do
- Federation
- Single sign-on
- Transitive trust

## 4.2 Given a scenario, install and configure identity and access services.

- LDAP
- Kerberos
- TACACS+
- CHAP
- PAP
- MSCHAP
- RADIUS
- SAML
- OpenID Connect
- OAuth
- Shibboleth
- Secure token
- NTLM

## 4.3 Given a scenario, implement identity and access management controls.

- Access control models
  - MAC
  - DAC
  - ABAC
  - Role-based access control
  - Rule-based access control
- Physical access control
### 4.4 Given a scenario, differentiate common account management practices.

**Account types**
- User account
- Shared and generic accounts/credentials
- Guest accounts
- Service accounts
- Privileged accounts

**General Concepts**
- Least privilege
- Onboarding/offboarding
- Permission auditing and review
- Usage auditing and review
- Time-of-day restrictions
- Recertification
- Standard naming convention
- Account maintenance
- Group-based access control
- Location-based policies

**Account policy enforcement**
- Credential management
- Group policy

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
|   |   | 3.9
|   |   | 6.2
|   |   | 7.2, 7.4,
|   |   | 7.5, 7.9
|   |   | 8.3, 8.8,
|   |   | 8.9, 8.11,
|   |   | 8.12, 8.13
5.0 **Risk Management**

5.1 Explain the importance of policies, plans and procedures related to organizational security.

- Standard operating procedure
- Agreement types
  - BPA
  - SLA
  - ISA
  - MOU/MOA
- Personnel management
  - Mandatory vacations
  - Job rotation
  - Separation of duties
  - Clean desk
  - Background checks
  - Exit interviews
  - Role-based awareness training
    - Data owner
    - System administrator
    - System owner
    - User
    - Privileged user
    - Executive user
  - NDA
  - Onboarding
  - Continuing education
  - Acceptable use policy/rules of behavior
  - Adverse actions
- General security policies
  - Social media networks/applications
  - Personal email

- Password complexity
- Expiration
- Recovery
- Disablement
- Lockout
- Password history
- Password reuse
- Password length

2.3
3.1, 3.7, 3.9
7.10
9.3
<table>
<thead>
<tr>
<th>5.2</th>
<th>Summarize business impact analysis concepts.</th>
<th>3.1, 9.12</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>RTO/RPO</td>
<td></td>
</tr>
<tr>
<td></td>
<td>MTBF</td>
<td></td>
</tr>
<tr>
<td></td>
<td>MTTR</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Mission-essential functions</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Identification of critical systems</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Single point of failure</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Impact</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Life</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Property</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Safety</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Finance</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Reputation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Privacy impact assessment</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Privacy threshold assessment</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>5.3</th>
<th>Explain risk management processes and concepts.</th>
<th>3.1, 3.2, 3.3, 6.1, 6.13</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Threat assessment</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Environmental</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Manmade</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Internal vs. external</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Risk assessment</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SLE</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ALE</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ARO</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Asset value</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Risk register</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Likelihood of occurrence</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Supply chain assessment</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Impact</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Quantitative</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Qualitative</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Testing</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Penetration testing authorization</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Vulnerability testing authorization</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Risk response techniques</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Accept</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Transfer</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Avoid</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Mitigate</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Change management</td>
<td></td>
</tr>
</tbody>
</table>
### 5.4 Given a scenario, follow incident response procedures.

- Incident response plan
  - Documented incident types/category definitions
  - Roles and responsibilities
  - Reporting requirements/escalation
  - Cyber-incident response teams
  - Exercise
- Incident response process
  - Preparation
  - Identification
  - Containment
  - Eradication
  - Recovery
  - Lessons learned

### 5.5 Summarize basic concepts of forensics.

- Order of volatility
- Chain of custody
- Legal hold
- Data acquisition
  - Capture system image
  - Network traffic and logs
  - Capture video
  - Record time offset
  - Take hashes
  - Screenshots
  - Witness interviews
- Preservation
- Recovery
- Strategic intelligence/counterintelligence gathering
  - Active logging
- Track man-hours

### 5.6 Explain disaster recovery and continuity of operation concepts.

- Recovery sites
  - Hot site
  - Warm site
  - Cold site
- Order of restoration
<table>
<thead>
<tr>
<th>5.7</th>
<th>Compare and contrast various types of controls.</th>
<th>4.1</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Deterrent</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Preventive</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Detective</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Corrective</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Compensating</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Technical</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Administrative</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Physical</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>5.8</th>
<th>Given a scenario, carry out data security and privacy practices.</th>
<th>3.1</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Data destruction and media sanitization</td>
<td>9.1</td>
</tr>
<tr>
<td></td>
<td>• Burning</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Shredding</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Pulping</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Pulverizing</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Degaussing</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Purging</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Wiping</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Data sensitivity labeling and handling</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Confidential</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Private</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Public</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Proprietary</td>
<td></td>
</tr>
</tbody>
</table>
### Data roles
- Owner
- Steward/custodian
- Privacy officer

### Data retention

### Legal and compliance

<table>
<thead>
<tr>
<th>6.0</th>
<th>Cryptography and PKI</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>Compare and contrast basic concepts of cryptography.</td>
</tr>
</tbody>
</table>

- Symmetric algorithms
- Modes of operation
- Asymmetric algorithms
- Hashing
- Salt, IV, nonce
- Elliptic curve
- Weak/deprecated algorithms
- Key exchange
- Digital signatures
- Diffusion
- Confusion
- Collision
- Steganography
- Obfuscation
- Stream vs. block
- Key strength
- Session keys
- Ephemeral key
- Secret algorithm
- Data-in-transit
- Data-at-rest
- Data-in-use
- Random/pseudo-random number generation
- Key stretching
- Implementation vs. algorithm selection
  - Crypt service provider
  - Crypt modules
- Perfect forward secrecy
- Security through obscurity
- Common use cases
  - Low power devices

---

2.4
9.2, 9.3, 9.5, 9.6, 9.9
6.2 Explain cryptography algorithms and their basic characteristics.

- Symmetric algorithms
  - AES
  - DES
  - 3DES
  - RC4
  - Blowfish/Twofish
- Cipher modes
  - CBC
  - GCM
  - ECB
  - CTM
  - Stream vs. block
- Asymmetric algorithms
  - RSA
  - DSA
  - Diffie-Hellman
    - Groups
    - DHE
    - ECDHE
  - Elliptic curve
  - PGP/GPG
- Hashing algorithms
  - MD5
  - SHA
  - HMAC
  - RIPEMD
- Key stretching algorithms
  - BCRYPT
  - PBKDF2
- Obfuscation
  - XOR
  - ROT13
  - Substitution ciphers
### 6.3 Given a scenario, install and configure wireless security settings.

- **Cryptographic protocols**
  - WPA
  - WPA2
  - CCMP
  - TKIP
- **Authentication protocols**
  - EAP
  - PEAP
  - EAP-FAST
  - EAP-TLS
  - EAP-TTLS
  - IEEE 802.1x
  - RADIUS Federation
- **Methods**
  - PSK vs. Enterprise vs. Open
  - WPS
  - Captive portals

### 6.4 Given a scenario, implement public key infrastructure.

- **Components**
  - CA
  - Intermediate CA
  - CRL
  - OCSP
  - CSR
  - Certificate
  - Public key
  - Private key
  - Object identifiers (OID)
- **Concepts**
  - Online vs. offline CA
  - Stapling
  - Pinning
  - Trust model
  - Key escrow
  - Certificate chaining
- **Types of certificates**
  - Wildcard
  - SAN
  - Code signing
  - Self-signed

---

Copyright © 2017 TestOut Corporation. CompTIA, A+, Network+, Security+, Linux+ and related trademarks and trade names are the trademarks of CompTIA. Microsoft, MCITP, MSCA, MCTS, Windows, and Office 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.
- Machine/computer
- Email
- User
- Root
- Domain validation
- Extended validation

**Certificate formats**
- DER
- PEM
- PFX
- CER
- P12
- P7B
Appendix C: Approximate Time for the Course

The total time for the LabSim for TestOut Security Pro course is approximately **57 hours and 43 minutes**. Time is calculated by adding the approximate time for each section which is calculated using the following elements:

- Video/demo times
- Text Lessons (5 minutes assigned per text lesson)
- Simulations (5 minutes assigned per simulation)
- Questions (1 minute per question)

Additionally, there are approximately another **24 hours and 12 minutes** of Practice Test material at the end of the course.

The breakdown for this course is as follows:

<table>
<thead>
<tr>
<th>Module</th>
<th>Sections</th>
<th>Time</th>
<th>Videos</th>
<th>Labs</th>
<th>Text</th>
<th>Exams</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1.0: Introduction</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.1: Security Overview</td>
<td>24</td>
<td>9</td>
<td>0</td>
<td>5</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>1.2: Using the Simulator</td>
<td>16</td>
<td>6</td>
<td>10</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td></td>
<td><strong>0:40</strong></td>
<td><strong>0:15</strong></td>
<td><strong>0:10</strong></td>
<td><strong>0:05</strong></td>
<td><strong>0:10</strong></td>
</tr>
<tr>
<td><strong>2.0: Security Basics</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.1: Understanding Attacks</td>
<td>41</td>
<td>25</td>
<td>0</td>
<td>10</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>2.2: Defense Planning</td>
<td>19</td>
<td>9</td>
<td>0</td>
<td>5</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>2.3: Access Control</td>
<td>28</td>
<td>11</td>
<td>0</td>
<td>5</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>2.4: Cryptography Basics</td>
<td>17</td>
<td>6</td>
<td>0</td>
<td>5</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>2.5: Network Monitoring</td>
<td>23</td>
<td>13</td>
<td>0</td>
<td>5</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>2.6: Incident Response</td>
<td>67</td>
<td>44</td>
<td>0</td>
<td>10</td>
<td>13</td>
<td></td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td></td>
<td><strong>3:15</strong></td>
<td><strong>1:48</strong></td>
<td><strong>0:00</strong></td>
<td><strong>0:40</strong></td>
<td><strong>0:47</strong></td>
</tr>
<tr>
<td><strong>3.0: Policies, Procedures, and Awareness</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.1: Security Policies</td>
<td>59</td>
<td>24</td>
<td>0</td>
<td>20</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>3.2: Risk Management</td>
<td>26</td>
<td>6</td>
<td>0</td>
<td>5</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>3.3: Business Continuity</td>
<td>14</td>
<td>3</td>
<td>0</td>
<td>5</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>3.4: Manageable Network Plan</td>
<td>26</td>
<td>16</td>
<td>0</td>
<td>5</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>3.5: Social Engineering</td>
<td>51</td>
<td>26</td>
<td>5</td>
<td>5</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>3.6: App Development and Deployment</td>
<td>27</td>
<td>10</td>
<td>0</td>
<td>10</td>
<td>7</td>
<td></td>
</tr>
<tr>
<td>3.7: Employee Management</td>
<td>39</td>
<td>9</td>
<td>0</td>
<td>15</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>3.8: Mobile Devices</td>
<td>22</td>
<td>11</td>
<td>0</td>
<td>5</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>3.9: Third-Party Integration</td>
<td>18</td>
<td>8</td>
<td>0</td>
<td>5</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td></td>
<td><strong>4:42</strong></td>
<td><strong>1:53</strong></td>
<td><strong>0:05</strong></td>
<td><strong>1:15</strong></td>
<td><strong>1:29</strong></td>
</tr>
<tr>
<td><strong>4.0: Physical</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.1: Physical Threats</td>
<td>40</td>
<td>15</td>
<td>5</td>
<td>5</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>4.2: Device Protection</td>
<td>19</td>
<td>9</td>
<td>0</td>
<td>5</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>4.3: Network Infrastructure Protection</td>
<td>15</td>
<td>5</td>
<td>0</td>
<td>5</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>4.4: Environmental Controls</td>
<td>30</td>
<td>10</td>
<td>0</td>
<td>10</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td></td>
<td><strong>1:44</strong></td>
<td><strong>0:39</strong></td>
<td><strong>0:05</strong></td>
<td><strong>0:25</strong></td>
<td><strong>0:35</strong></td>
</tr>
</tbody>
</table>
## 5.0: Perimeter

<table>
<thead>
<tr>
<th>5.1: Recon and Denial</th>
<th>50</th>
<th>25</th>
<th>0</th>
<th>10</th>
<th>15</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.2: Spoofing and Poisoning</td>
<td>68</td>
<td>33</td>
<td>5</td>
<td>15</td>
<td>15</td>
</tr>
<tr>
<td>5.3: Security Appliances</td>
<td>39</td>
<td>19</td>
<td>5</td>
<td>10</td>
<td>5</td>
</tr>
<tr>
<td>5.4: Demilitarized Zones (DMZ)</td>
<td>27</td>
<td>11</td>
<td>5</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>5.5: Firewalls</td>
<td>40</td>
<td>15</td>
<td>5</td>
<td>5</td>
<td>15</td>
</tr>
<tr>
<td>5.6: Network Address Translation (NAT)</td>
<td>33</td>
<td>22</td>
<td>0</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>5.7: Virtual Private Networks (VPN)</td>
<td>51</td>
<td>21</td>
<td>10</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>5.8: Web Threat Protection</td>
<td>27</td>
<td>12</td>
<td>5</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>5.9: Network Access Protection</td>
<td>31</td>
<td>21</td>
<td>0</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>5.10: Wireless Overview</td>
<td>54</td>
<td>24</td>
<td>5</td>
<td>10</td>
<td>15</td>
</tr>
<tr>
<td>5.11: Wireless Attacks</td>
<td>44</td>
<td>19</td>
<td>5</td>
<td>5</td>
<td>15</td>
</tr>
<tr>
<td>5.12: Wireless Defenses</td>
<td>60</td>
<td>25</td>
<td>10</td>
<td>10</td>
<td>15</td>
</tr>
</tbody>
</table>

**Total**: 8:44 4:07 0:55 1:35 2:07

## 6.0: Network

<table>
<thead>
<tr>
<th>6.1: Network Threats</th>
<th>19</th>
<th>9</th>
<th>0</th>
<th>5</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2: Network Device Vulnerabilities</td>
<td>28</td>
<td>13</td>
<td>5</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>6.3: Network Applications</td>
<td>23</td>
<td>13</td>
<td>0</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>6.4: Switch Attacks</td>
<td>16</td>
<td>6</td>
<td>0</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>6.5: Switch Security</td>
<td>60</td>
<td>25</td>
<td>15</td>
<td>5</td>
<td>15</td>
</tr>
<tr>
<td>6.6: Using VLANs</td>
<td>32</td>
<td>12</td>
<td>10</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>6.7: Router Security</td>
<td>43</td>
<td>18</td>
<td>15</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>6.8: Intrusion Detection and Prevention</td>
<td>53</td>
<td>28</td>
<td>5</td>
<td>5</td>
<td>15</td>
</tr>
<tr>
<td>6.9: Vulnerability Assessment</td>
<td>64</td>
<td>25</td>
<td>20</td>
<td>5</td>
<td>14</td>
</tr>
<tr>
<td>6.10: Protocol Analyzers</td>
<td>29</td>
<td>16</td>
<td>0</td>
<td>5</td>
<td>8</td>
</tr>
<tr>
<td>6.11: Remote Access</td>
<td>50</td>
<td>25</td>
<td>0</td>
<td>10</td>
<td>15</td>
</tr>
<tr>
<td>6.12: Network Authentication</td>
<td>62</td>
<td>32</td>
<td>5</td>
<td>10</td>
<td>15</td>
</tr>
<tr>
<td>6.13: Penetration Testing</td>
<td>32</td>
<td>15</td>
<td>0</td>
<td>5</td>
<td>12</td>
</tr>
<tr>
<td>6.14: Virtual Networking</td>
<td>34</td>
<td>14</td>
<td>5</td>
<td>10</td>
<td>5</td>
</tr>
<tr>
<td>6.15: Software-Defined Networking (SDN)</td>
<td>17</td>
<td>7</td>
<td>0</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>6.16: Cloud Services</td>
<td>26</td>
<td>16</td>
<td>0</td>
<td>5</td>
<td>5</td>
</tr>
</tbody>
</table>

**Total**: 9:48 4:34 1:20 1:35 2:19

## 7.0: Host

<table>
<thead>
<tr>
<th>7.1: Malware</th>
<th>55</th>
<th>25</th>
<th>5</th>
<th>10</th>
<th>15</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.2: Password Attacks</td>
<td>34</td>
<td>24</td>
<td>0</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>7.3: Windows System Hardening</td>
<td>60</td>
<td>35</td>
<td>10</td>
<td>5</td>
<td>10</td>
</tr>
<tr>
<td>7.4: Hardening Enforcement</td>
<td>37</td>
<td>22</td>
<td>5</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>7.5: File Server Security</td>
<td>52</td>
<td>19</td>
<td>10</td>
<td>10</td>
<td>13</td>
</tr>
<tr>
<td>7.6: Linux Host Security</td>
<td>36</td>
<td>26</td>
<td>0</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>7.7: Embedded Systems</td>
<td>21</td>
<td>11</td>
<td>0</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>7.8: Log Management</td>
<td>57</td>
<td>32</td>
<td>0</td>
<td>10</td>
<td>15</td>
</tr>
<tr>
<td>7.9: Audits</td>
<td>36</td>
<td>16</td>
<td>10</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>7.10: Email</td>
<td>46</td>
<td>21</td>
<td>10</td>
<td>5</td>
<td>10</td>
</tr>
<tr>
<td>7.11: BYOD Security</td>
<td>33</td>
<td>18</td>
<td>5</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>7.12: Mobile Device Management</td>
<td>55</td>
<td>32</td>
<td>5</td>
<td>10</td>
<td>8</td>
</tr>
<tr>
<td>7.13: Host Virtualization</td>
<td>50</td>
<td>34</td>
<td>5</td>
<td>5</td>
<td>6</td>
</tr>
</tbody>
</table>

**Total**: 9:32 5:15 1:05 1:25 1:47

Copyright © 2017 TestOut Corporation. CompTIA, A+, Network+, Security+, Linux+ and related trademarks and trade names are the trademarks of CompTIA. Microsoft, MCITP, MSCA, MCTS, Windows, and Office 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.
8.0: Application

<table>
<thead>
<tr>
<th>Topic</th>
<th>Time (min)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Control Models</td>
<td>55</td>
</tr>
<tr>
<td>Authentication</td>
<td>44</td>
</tr>
<tr>
<td>Authorization</td>
<td>30</td>
</tr>
<tr>
<td>Web Application Attacks</td>
<td>52</td>
</tr>
<tr>
<td>Internet Browsers</td>
<td>62</td>
</tr>
<tr>
<td>Application Development</td>
<td>68</td>
</tr>
<tr>
<td>Active Directory Overview</td>
<td>31</td>
</tr>
<tr>
<td>Windows Domain Users and Groups</td>
<td>49</td>
</tr>
<tr>
<td>Linux Users</td>
<td>62</td>
</tr>
<tr>
<td>Linux Groups</td>
<td>33</td>
</tr>
<tr>
<td>Linux User Security</td>
<td>26</td>
</tr>
<tr>
<td>Group Policy Overview</td>
<td>47</td>
</tr>
<tr>
<td>Hardening Authentication 1</td>
<td>71</td>
</tr>
<tr>
<td>Hardening Authentication 2</td>
<td>38</td>
</tr>
</tbody>
</table>

**Total: 11:08**

8.1: Access Control Models

8.2: Authentication

8.3: Authorization

8.4: Web Application Attacks

8.5: Internet Browsers

8.6: Application Development

8.7: Active Directory Overview

8.8: Windows Domain Users and Groups

8.9: Linux Users

8.10: Linux Groups

8.11: Linux User Security

8.12: Group Policy Overview

8.13: Hardening Authentication 1

8.14: Hardening Authentication 2

9.0: Data

<table>
<thead>
<tr>
<th>Topic</th>
<th>Time (min)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Management</td>
<td>38</td>
</tr>
<tr>
<td>Advanced Cryptography</td>
<td>28</td>
</tr>
<tr>
<td>Cryptography Implementations</td>
<td>24</td>
</tr>
<tr>
<td>Cryptographic Attacks</td>
<td>30</td>
</tr>
<tr>
<td>Symmetric Encryption</td>
<td>30</td>
</tr>
<tr>
<td>Asymmetric Encryption</td>
<td>23</td>
</tr>
<tr>
<td>File Encryption</td>
<td>59</td>
</tr>
<tr>
<td>Public Key Infrastructure (PKI)</td>
<td>64</td>
</tr>
<tr>
<td>Hashing</td>
<td>27</td>
</tr>
<tr>
<td>Data Transmission Security</td>
<td>67</td>
</tr>
<tr>
<td>Data Loss Prevention (DLP)</td>
<td>14</td>
</tr>
<tr>
<td>Redundancy</td>
<td>63</td>
</tr>
<tr>
<td>Backup and Restore</td>
<td>61</td>
</tr>
<tr>
<td>Cloud Storage</td>
<td>13</td>
</tr>
</tbody>
</table>

**Total: 9:01**

9.1: Data Management

9.2: Advanced Cryptography

9.3: Cryptography Implementations

9.4: Cryptographic Attacks

9.5: Symmetric Encryption

9.6: Asymmetric Encryption

9.7: File Encryption

9.8: Public Key Infrastructure (PKI)

9.9: Hashing

9.10: Data Transmission Security

9.11: Data Loss Prevention (DLP)

9.12: Redundancy

9.13: Backup and Restore

9.14: Cloud Storage

**Total Course Time 57:44**

Practice Exams

<table>
<thead>
<tr>
<th>Practice Exams</th>
<th>Number of Questions</th>
<th>Time (min)</th>
</tr>
</thead>
<tbody>
<tr>
<td>A.0: Security Pro Practice Exams</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A.2: Security Pro Domain 1: Access Control and Identity Management</td>
<td>24</td>
<td>120</td>
</tr>
<tr>
<td>A.4: Security Pro Domain 3: Physical Security</td>
<td>2</td>
<td>10</td>
</tr>
<tr>
<td>A.5: Security Pro Domain 4: Perimeter Defenses</td>
<td>9</td>
<td>45</td>
</tr>
<tr>
<td>A.6: Security Pro Domain 5: Network Defenses</td>
<td>7</td>
<td>35</td>
</tr>
<tr>
<td>A.7: Security Pro Domain 6: Host Defenses</td>
<td>7</td>
<td>35</td>
</tr>
<tr>
<td>A.8: Security Pro Domain 7: Application Defenses</td>
<td>10</td>
<td>50</td>
</tr>
<tr>
<td>A.9: Security Pro Domain 8: Data Defenses</td>
<td>6</td>
<td>30</td>
</tr>
<tr>
<td>A.10: Security Pro Domain 9: Audits and Assessments</td>
<td>2</td>
<td>10</td>
</tr>
<tr>
<td>A.11: Security Pro Certification Practice Exam</td>
<td>15</td>
<td>75</td>
</tr>
</tbody>
</table>

Copyright © 2017 TestOut Corporation. CompTIA, A+, Network+, Security+, Linux+ and related trademarks and trade names are the trademarks of CompTIA. Microsoft, MCITP, MSCA, MCTS, Windows, and Office 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.
<table>
<thead>
<tr>
<th>B.0: CompTIA Security+ Practice Exams</th>
<th>Number of Questions</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>B.2: CompTIA Security+ Domain 1: Threats, Attacks and Vulnerabilities, All Questions</strong></td>
<td>177</td>
<td>2:57</td>
</tr>
<tr>
<td><strong>B.3: CompTIA Security+ Domain 2: Technologies and Tools, All Questions</strong></td>
<td>147</td>
<td>2:27</td>
</tr>
<tr>
<td><strong>B.5: CompTIA Security+ Domain 4: Identity and Access Management, All Questions</strong></td>
<td>154</td>
<td>2:34</td>
</tr>
<tr>
<td><strong>B.6: CompTIA Security+ Domain 5: Risk Management, All Questions</strong></td>
<td>123</td>
<td>2:03</td>
</tr>
<tr>
<td><strong>B.7: CompTIA Security+ Domain 6: Cryptography and PKI, All Questions</strong></td>
<td>95</td>
<td>1:35</td>
</tr>
<tr>
<td><strong>B.8: CompTIA Security+ Certification Practice Exam</strong></td>
<td>100</td>
<td>1:40</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>1032</strong></td>
<td><strong>17:12</strong></td>
</tr>
</tbody>
</table>

**Total Practice Exam Time 24:12**