

TestOut[®]

Security Pro - English 8.0.x

LESSON PLAN

Table of Contents

Table of Contents	2
1.0: Security Concepts	4
1.1: Security Introduction	4
1.2: Security Controls	7
1.3: Use the Simulator	9
2.0: Threats, Vulnerabilities, and Mitigations	10
2.1: Understanding Attacks	10
2.2: Social Engineering	14
2.3: Malware	17
3.0: Cryptographic Solutions	20
3.1: Cryptography	20
3.2: Cryptography Implementations	24
3.3: Hashing	26
3.4: Encryption	28
3.5: Public Key Infrastructure	31
4.0: Identity and Access Management	34
4.1: Access Control Models	34
4.2: Authentication	39
4.3: Authorization	44
4.4: Active Directory Overview	47
4.5: Hardening Authentication	50
4.6: Linux Users	53
4.7: Linux Groups	56
4.8: Remote Access	58
4.9: Network Authentication	60
5.0: Network Architecture	62
5.1: Enterprise Network Architecture	62
5.2: Security Appliances	65
5.3: Screened Subnets	68
5.4: Firewalls	70
5.5: Virtual Private Networks	72
5.6: Network Access Control	74
5.7: Network Device Vulnerabilities	75

5.8: Network Applications	77
5.9: Switch Security and Attacks	79
5.10: Router Security	82
6.0: Resiliency and Site Security	85
6.1: Physical Threats	85
6.2: Monitoring and Reconnaissance	88
6.3: Intrusion Detection	91
6.4: Protocol Analyzers	94
6.5: Analyzing Network Attacks	96
6.6: Analyzing Password Attacks	99
7.0: Vulnerability Management	102
7.1: Vulnerability Management	102
7.2: Vulnerability Scanning	105
7.3: Alerting and Monitoring	108
7.4: Penetration Testing	113
8.0: Network and Endpoint Security.....	116
8.1: Operating System Hardening	116
8.2: File Server Security	120
8.3: Linux Host Security	123
8.4: Wireless Overview	125
8.5: Wireless Attacks	127
8.6: Wireless Defenses	129
8.7: Data Transmission Security	132
8.8: Web Application Security	135
8.9: Application Development and Security	139
9.0: Incident Response.....	144
9.1: Incident Response and Mitigation	144
9.2: Log Management	147
9.3: Digital Forensics	150
9.4: Redundancy	152
9.5: Backup and Restore	155
10.0: Protocol, App, and Cloud Security	157
10.1: Host Virtualization	157
10.2: Virtual Networking	160
10.3: Software-Defined Networking	162

10.4: Cloud Services	163
10.5: Mobile Devices	166
10.6: Mobile Device Management	169
10.7: BYOD Security	172
10.8: Embedded and Specialized Systems	175
10.9: Email	178
11.0: Security Governance Concepts	181
11.1: Policies, Standards, and Procedures	181
11.2: Change Management	184
11.3: Automation and Orchestration	186
12.0: Risk Management Processes	188
12.1: Risk Management Processes and Concepts	188
12.2: Vendor Management	194
12.3: Audits and Assessments	197
13.0: Data Protection and Compliance	200
13.1: Data Classification and Compliance	200
13.2: Personnel Policies	204
Practice Exams	208
Appendix A: Approximate Time for the Course	209

1.0: Security Concepts

1.1: Security Introduction

Lecture Focus Questions:

- What is information security?
- What challenges does a security professional face?
- What aspects create a proactive approach to security?
- 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 the three types of threat agents?

The key terms for this section include:

Term	Definition
------	------------

Copyright © 2023 TestOut Corporation. Copyright © The Computing Technology Industry Association, Inc. (CompTIA). All Rights Reserved. Reference to any specific product, service, process, or method by trade name, trademark, manufacturer or otherwise on this website is for educational purposes only and does not constitute an implied or expressed recommendation or endorsement by said third party. Neither TestOut nor CompTIA have any affiliation with any of these companies, and the products and services advertised herein are not endorsed by them.

Security operations center (SOC)	The location where security professionals monitor and protect critical information assets in an organization.
Development and operations (DevOps)	A combination of software development and systems operations and refers to the practice of integrating one discipline with the other.
DevSecOps	A combination of software development, security operations, and systems operations and refers to the practice of integrating each discipline with the others.
Computer incident response team (CIRT)/computer security incident response team (CSIRT)/computer emergency response team (CERT)	Team with responsibility for incident response. The CSIRT must have expertise across a number of business domains (IT, HR, legal, and marketing, for instance).

This section helps you prepare for the following certification exam objectives:

Exam	Objective
CompTIA Security+ SY0-701	1.1 Compare and contrast various types of security controls.
	<ul style="list-style-type: none"> • Categories <ul style="list-style-type: none"> ○ Technical ○ Managerial ○ Operational ○ Physical
	1.2 Summarize fundamental security concepts.
	<ul style="list-style-type: none"> • Confidentiality, Integrity, and Availability (CIA)
CompTIA Security+ SY0-701	2.1 Compare and contrast common threat actors and motivations.
	<ul style="list-style-type: none"> • Threat actors <ul style="list-style-type: none"> ○ Nation-state ○ Organized crime

Video/Demo

 1.1.1 The Security Landscape

Time

3:47

Copyright © 2023 TestOut Corporation. Copyright © The Computing Technology Industry Association, Inc. (CompTIA). All Rights Reserved. Reference to any specific product, service, process, or method by trade name, trademark, manufacturer or otherwise on this website is for educational purposes only and does not constitute an implied or expressed recommendation or endorsement by said third party. Neither TestOut nor CompTIA have any affiliation with any of these companies, and the products and services advertised herein are not endorsed by them.

▶▶ 1.1.2 Security Concepts	4:12
▶▶ 1.1.4 Security Job Roles	<u>5:00</u>
Total Video Time	12:59

Fact Sheets

- ▶▶ 1.1.3 Security Introduction Facts

Number of Exam Questions

10 questions

Total Time

About 28 minutes

1.2: Security Controls

Lecture Focus Questions:

- What are the three types of control categories?
- What are preventative controls?
- What is the difference between corrective and compensating controls?

The key terms for this section include:

Term	Definition
Security control	A technology or procedure put in place to mitigate vulnerabilities and risk and to ensure the confidentiality, integrity, and availability (CIA) of information.
Managerial	A category of security control that provides oversight of information systems.
Operational	A category of security control that is implemented by people.
Technical	A category of security control that is implemented as a system.
Physical	A category of security control that is implemented by hardware used to deter or detect, such as as alarms, gateways, locks, lighting, and security cameras.
Preventive	A type of security control that acts before an incident to eliminate or reduce the likelihood that an attack can succeed.
Access control lists (ACLs)	The collection of access control entries (ACEs) that determines which subjects (user accounts, host IP addresses, and so on) are allowed or denied access to the object and the privileges given (read-only, read/write, and so on).
Detective	A type of security control that acts during an incident to identify or record that it is happening.
Corrective	A type of security control that acts after an incident to eliminate or minimize its impact.
Directive	A type of control that enforces a rule of behavior through a policy or contract.
Deterrent	A type of security control that discourages intrusion attempts.
Compensating	A security measure that takes on risk mitigation when a primary control fails or cannot completely meet expectations.
Chief Information Officer (CIO)	A company officer with the primary responsibility of managing information technology assets and procedures.
Chief Technology Officer (CTO)	A company officer with the primary role of making effective use of new and emerging computing platforms and innovations.
Chief Security Officer (CSO)	Typically, the job title of the person with overall responsibility for information assurance and systems security.

Information Systems
Security Officer
(ISSO)

Organizational role with technical responsibilities for implementation of security policies, frameworks, and controls.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
CompTIA Security+ SY0-701	<p>1.1 Compare and contrast various types of security controls.</p> <ul style="list-style-type: none">• Categories<ul style="list-style-type: none">○ Technical○ Managerial○ Operational○ Physical• Control types<ul style="list-style-type: none">○ Preventive○ Deterrent○ Detective○ Corrective○ Compensating○ Directive

Video/Demo

 1.2.1 Control Categories and Types

Time

4:18

Total Video Time

4:18

Fact Sheets

 1.2.2 Control Categories and Types Facts

Number of Exam Questions

11 questions

Total Time

About 26 minutes

1.3: Use the Simulator

Lecture Focus Questions:

- How do I complete simulation labs in this course?
- What features have been simulated in this environment?
- How will getting acquainted with the simulation environment help me acquire the necessary skills?

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
- Use the simulation interface to identify where simulated cables connect to the computer
- Attach simulated cables
- Configure a security appliance
- Install a security appliance

Key terms for this section include the following:

Term	Definition
Lab simulator	The lab simulator is a LabSim learning tool that presents a virtual environment that you can manipulate like an actual environment.
Lab tasks	The tasks necessary to complete the lab.
Navigation bar	A lab simulation feature used to change to a new location, such as a building, floor, or office.
Shelf	An area that contains hardware components that may be used in the simulation.
Exhibits	Additional information about the simulation environment that may be useful in completing the lab.

Video/Demo

- 📺 1.3.1 Use the Simulator
- 📺 1.3.2 Labsim Features

Total Video Time

Time

12:08

10:14

22:22

Total Time

About 23 minutes

2.0: Threats, Vulnerabilities, and Mitigations

2.1: Understanding Attacks

Lecture Focus Questions:

- What motivates threat actors to attack?
- What protections can you implement against inside threat actors?
- Which three types of threat actors are most likely to have high levels of funding?
- Why are nation-state threat actors especially dangerous?
- What attack surfaces are inherent within a supply chain?

Key terms for this section include the following:

Term	Definition
Threat actor	A person or entity responsible for an event that has been identified as a security incident or as a risk.
Internal/external	The degree of access that a threat actor possesses before initiating an attack. An external threat actor has no standing privileges, while an internal actor has been granted some access permissions.
Level of sophistication/capability	A formal classification of the resources and expertise available to a threat actor.
Resources/funding	The ability of threat actors to draw upon funding to acquire personnel, tools, and development of novel attack types.
Service disruption	A type of attack that compromises the availability of an asset or business process.
Data exfiltration	The process by which an attacker copies data from a private network to an external network.
Disinformation	A type of attack that falsifies an information resource that is normally trusted by others.
Blackmail	Demanding payment to prevent the release of information.
Extortion	Demanding payment to prevent or halt some type of attack.
Fraud	Falsifying records, such as an internal fraud that involves tampering with accounts.

Hacker	Often used to refer to someone who breaks into computer systems or spreads viruses. Ethical hackers prefer to think of themselves as experts on and explorers of computer security systems.
Unauthorized hacker	A hacker operating with malicious intent.
Authorized hacker	A hacker engaged in authorized penetration testing or other security consultancy.
Unskilled attacker	An inexperienced attacker that typically uses tools or scripts created by others.
Hacktivist	A threat actor that is motivated by a social issue or political cause.
Advanced persistent threat (APT)	An attacker's ability to obtain, maintain, and diversify access to network systems using exploits and malware.
Nation-state actors	A type of threat actor that is supported by the resources of its host country's military and security services.
Organized crime	A type of threat actor that uses hacking and computer fraud for commercial gain.
Internal threat	A type of threat actor who is assigned privileges on the system that cause an intentional or unintentional incident.
Unintentional or inadvertent insider threat	A threat actor that causes a vulnerability or exposes an attack vector without malicious intent.
Shadow IT	Computer hardware, software, or services used on a private network without authorization from the system owner.
Vulnerable software	Weakness that could be triggered accidentally or exploited intentionally to cause a security breach.
Unsupported systems	Product life cycle phase where mainstream vendor support is no longer available.
Unsecure network	Configuration that exposes a large attack surface, such as through unnecessary open service ports, weak or no authentication, use of default credentials, or lack of secure communications/encryption.
Lure	An attack type that will entice a victim into using or opening a removable device, document, image, or program that conceals malware.
Supply chain	The end-to-end process of supplying, manufacturing, distributing, and finally releasing goods and services to a customer.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
------	-----------

2.1 Compare and contrast common threat actors and motivations.

- Threat actors
 - Nation-state
 - Unskilled attacker
 - Hactivist
 - Insider threat
 - Organized crime
 - Shadow IT
- Attributes of actors
 - Internal/external
 - Resources/funding
 - Level of sophistication/capability
- Motivations
 - Data exfiltration
 - Espionage
 - Service disruption
 - Blackmail
 - Financial gain
 - Philosophical/political beliefs
 - Ethical
 - Revenge
 - Disruption/chaos
 - War

2.2 Explain common threat vectors and attack surfaces.

- Message-based
 - Email
 - Short Message Service (SMS)
 - Instant messaging (IM)
- Image-based
 - File-based
 - Removable device
 - Vulnerable software
 - Client-based vs. agentless
 - Unsupported systems and applications
 - Unsecure networks
 - Wireless
 - Wired
 - Bluetooth
 - Open service ports
 - Default credentials
 - Supply chain

- Managed service providers (MSPs)
- Vendors
- Suppliers

2.3 Explain various types of vulnerabilities.

- Supply chain
 - Service provider
 - Hardware provider
 - Software provider






2.4 Given a scenario, analyze indicators of malicious activity.

- Application attacks
 - Privilege escalation

2.5 Explain the purpose of mitigation techniques used to secure the enterprise.

- Least privilege

Video/Demo

	Time
 2.1.1 Threat Actor Types	6:58
 2.1.2 Threat Actor Types Facts	6:20
 2.1.3 General Attack Strategy	6:03
 2.1.4 General Defense Strategy	7:47
 2.1.6 Attack Surfaces	<u>8:18</u>

Total Video Time

35:26

Fact Sheets

-  2.1.2 Threat Actor Types Facts
-  2.1.5 Attack and Defense Strategy Overview
-  2.1.7 Attack Surfaces Facts

Number of Exam Questions

10 questions

Total Time

About 61 minutes

2.2: Social Engineering

Summary

As you study this section, answer the following questions:

- What is social engineering?
- What are the phases of a social engineering attack?
- What is pretexting and how is it used in social engineering?
- What are some of the most common social engineering techniques?
- How are motivation techniques effective in convincing targets to comply with a hacker's desires?
- What are common variations of phishing?
- How does a watering hole attack work?

In this section, you will learn to:

- Use the Social Engineer Toolkit.
- Investigate a social engineering attack.
- Identify social engineering.

Key terms for this section include the following:





Term	Definition
Social engineering	An activity where the goal is to use deception and trickery to convince unsuspecting users to provide sensitive data or to violate security guidelines.
Impersonation	A social engineering attack where an attacker pretends to be someone they are not.
Pretexting	A social engineering tactic where a team communicates, whether directly or indirectly, a lie or half-truth in order to get someone to believe a falsehood.
Phishing	An email-based social engineering attack in which the attacker sends email from a supposedly reputable source, such as a bank, to try to elicit private information from the victim.
Vishing	A human-based attack where the attacker extracts information while speaking over the phone or leveraging IP-based voice messaging services (VoIP).
Smishing	A form of phishing that uses SMS text messages to trick a victim into revealing information.
Pharming	A type of attack that redirects users from a legitimate website to a malicious one.

Typosquatting	An attack in which an attacker registers a domain name with a common misspelling of an existing domain, so that a user who misspells a URL in a browser is taken to the attacker's website.
Business email compromise	An impersonation attack in which the attacker gains control of an employee's account and uses it to convince other employees to perform fraudulent actions.
Watering hole attack	An attack in which an attacker targets specific groups or organizations, discovers which websites they frequent, and injects malicious code into those sites.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
CompTIA Security+ SY0-701	2.1 Compare and contrast common threat actors and motivations. <ul style="list-style-type: none"> • Threat actors <ul style="list-style-type: none"> ○ Unskilled attacker ○ Insider threat • Motivations
	2.2 Explain common threat vectors and attack surfaces. <ul style="list-style-type: none"> • Human vectors/social engineering <ul style="list-style-type: none"> ○ Phishing ○ Smishing ○ Vishing ○ Misinformation/disinformation ○ Impersonation ○ Business email compromise (BEC) ○ Pretexting ○ Watering hole ○ Brand impersonation ○ Typosquatting
	5.6 Given a scenario, implement security awareness practices. <ul style="list-style-type: none"> • User guidance and training <ul style="list-style-type: none"> ○ Social engineering • Development
TestOut Security Pro	5.0 Audit and Security Assessment 5.2 Assessment Techniques



5.2.2 Identify Social Engineering

Video/Demo	Time
 2.2.1 Social Engineering Overview	4:20
 2.2.3 Social Engineering Techniques	5:43
 2.2.5 Use the Social Engineer Toolkit	4:21
 2.2.6 Investigating a Social Engineering Attack	<u>6:26</u>
Total Video Time	20:50

Lab/Activity

-  2.2.7 Identify Social Engineering

Fact Sheets

-  2.2.2 Social Engineering Overview Facts
-  2.2.4 Social Engineering Techniques Facts

Number of Exam Questions

11 questions

Total Time

About 59 minutes

2.3: Malware

Lecture Focus Questions:

- What is the difference between a virus and a worm?
- Which types of malware typically use email to spread?
- What does it mean for software to be quarantined?
- Why is it a good practice to show file extensions?
- What must you do to ensure that you are protected from the latest virus variations?

In this section, you will learn to:

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

Key terms for this section include the following:

Term	Definition
Malware	Software that serves a malicious purpose, typically installed without the user's consent (or knowledge).
Trojan	A malicious software program hidden within an innocuous-seeming piece of software. Usually, the Trojan is used to try to compromise the security of the target computer.
Potentially unwanted programs (PUPs)/potentially unwanted applications (PUAs)	Software that cannot definitively be classed as malicious, but may not have been chosen or wanted by the user.
Virus	Malicious code inserted into an executable file image. The malicious code is executed when the file is run and can deliver a payload, such as attempting to infect other files.
Malicious process	A process executed without proper authorization from the system owner for the purpose of damaging or compromising the system.
Worm	A type of malware that replicates between processes in system memory and can spread over client/server network connections.
Shellcode	A lightweight block of malicious code that exploits a software vulnerability to gain initial access to a victim system.

Advanced persistent threat (APT)	An attacker's ability to obtain, maintain, and diversify access to network systems using exploits and malware.
Adware	Software that records information about a PC and its user. Adware is used to describe software that the user has acknowledged can record information about their habits.
Spyware	Software that records information about a PC and its users, often installed without the user's consent.
Keylogger	Malicious software or hardware that can record user keystrokes.
Backdoor	A mechanism for gaining access to a computer that bypasses or subverts the normal method of authentication.
Remote access Trojan (RAT)	Malware that creates a backdoor remote administration channel to allow a threat actor to access and control the infected host.
Botnet	A group of hosts or devices that has been infected by a control program called a bot, which enables attackers to exploit the hosts to mount attacks.
Command and control (C2 or C&C)	Infrastructure of hosts and services with which attackers direct, distribute, and control malware over botnets.
Covert channel	A type of attack that subverts network security systems and policies to transfer data without authorization or detection.
Internet Relay Chat (IRC)	A group communications protocol that enables users to chat, send private messages, and share files.
Rootkit	Class of malware that modifies system files, often at the kernel level, to conceal its presence.
Ransomware	Malware that tries to extort money from the victim by blocking normal operation of a computer and/or encrypting the victim's files and demanding payment.
Crypto-mining	Malware that hijacks computer resources to create cryptocurrency.
Logic bomb	A malicious program or script that is set to run under particular circumstances or in response to a defined event.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
------	-----------

Copyright © 2023 TestOut Corporation. Copyright © The Computing Technology Industry Association, Inc. (CompTIA). All Rights Reserved. Reference to any specific product, service, process, or method by trade name, trademark, manufacturer or otherwise on this website is for educational purposes only and does not constitute an implied or expressed recommendation or endorsement by said third party. Neither TestOut nor CompTIA have any affiliation with any of these companies, and the products and services advertised herein are not endorsed by them.

2.4 Given a scenario, analyze indicators of malicious activity.

CompTIA Security+ SY0-701




- Malware attacks
 - Ransomware
 - Trojan
 - Worm
 - Spyware
 - Bloatware
 - Virus
 - Keylogger
 - Logic bomb
 - Rootkit

3.1 Harden computer systems

TestOut Security Pro

3.1.2 Configure anti-virus protection

Video/Demo

-  2.3.1 Malware
-  2.3.4 Implementing Malware Protections
-  2.3.5 Use Windows Security

Time

6:02

6:27

4:03



Total Video Time

16:32

Lab/Activity

-  2.3.6 Configure Microsoft Defender

Fact Sheets

-  2.3.2 Malware Facts
-  2.3.3 Malware Protection Facts

Number of Exam Questions

11 questions

Total Time

About 55 minutes

3.0: Cryptographic Solutions

3.1: Cryptography

Lecture Focus Questions:

- What is the difference between symmetric and asymmetric encryption?
- Which part of a simple cryptographic system must be kept secret—the cipher, the ciphertext, or the key?
- Which algorithms can be used to generate a hash?
- What is the process of digitally signing a message?
- What is a legitimate use for steganography?
- What are uses of blockchain in addition to cryptocurrency?
- What are the properties of a public/private key pair?

In this section, you will learn to:

- Use steganography to hide a file.
- Hide files with OpenStego.

Key terms for this section include the following:

Term	Definition
Cryptography	The science and practice of altering data to make it unintelligible to unauthorized parties.
Plaintext	Unencrypted data that is meant to be encrypted before it is transmitted, or the result of the decryption of encrypted data.
Ciphertext	Data that has been enciphered and cannot be read without the cipher key.
Algorithm	Operations that transform a plaintext into a ciphertext with cryptographic properties; also called a cipher.
Cryptanalysis	The science, art, and practice of breaking codes and ciphers.
Encryption	Scrambling the characters used in a message so that the message can be seen but not understood or modified unless it can be deciphered. Encryption provides for a secure means of transmitting data and authenticating users. It is also used to store data securely. Encryption uses different types of cipher and one or more keys. The size of the key is one factor in determining the strength of the encryption product.
Key	In cryptography, a specific piece of information that is used in conjunction with an algorithm to perform encryption and decryption.

Symmetric encryption	Two-way encryption scheme in which encryption and decryption are both performed by the same key. Also known as shared-key encryption.
Key length	Size of a cryptographic key in bits. Longer keys generally offer better security, but key lengths for different ciphers are not directly comparable.
Asymmetric algorithm	Cipher that uses public and private keys. The keys are mathematically linked, using either Rivest, Shamir, Adleman (RSA) or elliptic curve cryptography (ECC) algorithms, but the private key is not derivable from the public one. An asymmetric key cannot reverse the operation it performs, so the public key cannot decrypt what it has encrypted, for example.
Public key	During asymmetric encryption, this key is freely distributed and can be used to perform the reverse encryption or decryption operation of the linked private key in the pair.
Private key	In asymmetric encryption, the private key is known only to the holder and is linked to, but not derivable from, a public key distributed to those with whom the holder wants to communicate securely. A private key can be used to encrypt data that can be decrypted by the linked public key or vice versa.
Blockchain	A concept in which an expanding list of transactional records listed in a public ledger is secured using cryptography.
Open public ledger	Distributed public record of transactions that underpins the integrity of blockchains.
Steganography	The practice of concealing a file, message, image, or video within another file, message, image, or video.








This section helps you prepare for the following certification exam objectives:

Exam	Objective
CompTIA Security+ SY0-701	<p>4.2 Implement Encryption Technologies</p> <p>4.2.1 Encrypt data communications</p> <p>1.4 Explain the importance of using appropriate cryptographic solutions</p>
TestOut Security Pro	<ul style="list-style-type: none"> • Public key infrastructure (PKI) <ul style="list-style-type: none"> ○ Public key ○ Private key ○ Key escrow • Encryption <ul style="list-style-type: none"> ○ Asymmetric ○ Symmetric

- Algorithms
- Key length
- Obfuscation
 - Steganography
- Hashing
- Salting
- Digital signatures
- Blockchain

2.4 Given a scenario, analyze indicators of malicious activity






- Cryptographic attacks
 - Downgrade
 - Collision
 - Birthday

Video/Demo	Time
 3.1.1 Cryptography Concepts	7:00
 3.1.3 Symmetric vs Asymmetric Encryption	9:40
 3.1.4 Symmetric and Asymmetric Encryption Facts	5:53
 3.1.5 Cryptography Algorithm	9:18
 3.1.8 Blockchain	3:32
 3.1.10 Use Steganography to Hide a File	3:17
 3.1.12 Cryptographic Attacks	<u>4:20</u>
Total Video Time	43:00

Lab/Activity

-  3.1.11 Hide Files with OpenStego

Fact Sheets

-  3.1.2 Cryptography Facts
-  3.1.4 Symmetric and Asymmetric Encryption Facts
-  3.1.6 Cryptography Algorithms Facts
-  3.1.9 Blockchain Facts
-  3.1.13 Cryptographic Attack Facts

Number of Exam Questions

11 questions

Total Time

Copyright © 2023 TestOut Corporation. Copyright © The Computing Technology Industry Association, Inc. (CompTIA). All Rights Reserved. Reference to any specific product, service, process, or method by trade name, trademark, manufacturer or otherwise on this website is for educational purposes only and does not constitute an implied or expressed recommendation or endorsement by said third party. Neither TestOut nor CompTIA have any affiliation with any of these companies, and the products and services advertised herein are not endorsed by them.

About 96 minutes

3.2: Cryptography Implementations

Lecture Focus Questions:

- How can cryptography support the goals of information security?
- What cryptographic information is stored in a digital certificate?
- Why is reusing encryption keys considered a weakness?
- What are the potential consequences if a company loses control of a private key?
- What mechanism informs clients about suspended or revoked keys?
- What functionality does a Trusted Platform Module (TPM) chip provide?

In this section, you will learn to:

- Verify a device for TPM.

The key terms for this section include:

Term	Definition
Obfuscation	A technique that essentially hides or camouflages code or other information so that it is harder to read by unauthorized users.
Steganography	A technique for obscuring the presence of a message, often by embedding information within a file or other entity.
Data masking	A de-identification method where generic or placeholder labels are substituted for real data while preserving the structure or format of the original data.
Tokenization	A de-identification method where a unique token is substituted for real data.
Key management system	In public key infrastructure (PKI), procedures and tools that centralizes generation and storage of cryptographic keys.
Trusted Platform Module (TPM)	Specification for secure hardware-based storage of encryption keys, hashed passwords, and other user- and platform-identification information.
Application programming interface (API)	Methods exposed by a script or program that allow other scripts or programs to use it. For example, an API enables software developers to access functions of the TCP/IP network stack under a particular operating system.
Secure enclave	CPU extensions that protect data stored in system memory so that an untrusted process cannot read it.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
CompTIA Security+ SY0-701	1.4 Explain the importance of using appropriate cryptographic solutions.

- Encryption
 - Level
 - Full-disk
 - Asymmetric
 - Symmetric
 - Key exchange
- Tools
 - Trusted Platform Module (TPM)
 - Hardware security module (HSM)
 - Key management system
 - Secure enclave
- Obfuscation
 - Steganography
 - Hashing
- Digital signatures

4.0 Data Security

4.2 Implement Encryption Technologies




TestOut Security Pro

4.2.1 Encrypt data communications

4.2.2 Encrypt files

Video/Demo

Time

- | | |
|---|-------------|
|  3.2.1 Combining Cryptographic Methods | 4:40 |
|  3.2.2 Hardware-Based Encryption Devices | 3:13 |
|  3.2.3 Verify Device for TPM | <u>2:56</u> |

Total Video Time

10:49

Fact Sheets

-  3.2.4 Cryptographic Implementation Facts

Number of Exam Questions

10 questions

Total Time

About 26 minutes

3.3: Hashing

Lecture Focus Questions:

- What is the output of hashing called?
- What are the five characteristics of a hash function?
- What are some common uses for hashing?
- What type of attack takes advantage of hash collisions?
- What are the main hashing algorithms used?

In this section, you will learn to:

- Use hashes.
- Compare MD5 hashes.

The key terms for this section include:

Term	Definition
Hashing algorithm	A function that converts an arbitrary-length string input to a fixed-length string output. A cryptographic hash function does this in a way that reduces the chance of collisions, where two different inputs produce the same output.
Cryptographic primitive	A single hash function, symmetric cipher, or asymmetric cipher.
Digital signature	A message digest encrypted using the sender's private key that is appended to a message to authenticate the sender and prove message integrity.
Salt	A security countermeasure that mitigates the impact of precomputed hash table attacks by adding a random value to ("salting") each plaintext input.
Key stretching	A technique that strengthens potentially weak input for cryptographic key generation, such as passwords or passphrases created by people, against brute force attacks.
Secure Hash Algorithm (SHA)	A cryptographic hashing algorithm created to address possible weaknesses in multi-domain authentication (MDA). The current version is SHA-2.
Message-Digest Algorithm 5 (MD5)	A cryptographic hash function producing a 128-bit output.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
CompTIA Security+ SY0-701	1.4 Explain the importance of using appropriate cryptographic solutions.

- Encryption
 - Algorithms
- Hashing
- Salting
- Digital signatures

4.0 Data Security
4.2 Implement Encryption Technologies

TestOut Security Pro


- 4.2.1 Encrypt data communications
- 4.2.2 Encrypt files

Video/Demo	Time
 3.3.1 Hashing	5:31
 3.3.2 Hashing Algorithms	3:33
 3.3.4 Using Hashes	<u>4:50</u>
Total Video Time	13:54

Lab/Activity

-  3.3.5 Compare an MD5 Hash

Fact Sheets

-  3.3.3 Hashing Facts

Number of Exam Questions

10 questions

Total Time

About 41 minutes

3.4: Encryption

Lecture Focus Questions:

- Which editions of Windows include Encrypting File System (EFS)?
- Why would you create a Data Recovery Agent (DRA)?
- Which standard does Pretty Good Privacy (PGP) and GNU Privacy Guard (GPG) follow?
- What partition/volumes are created when implementing BitLocker?
- What are three methods of database encryption?

In this section, you will learn to:

- Encrypt files using EFS.
- Encrypt files using GPG.
- Configure BitLocker with a Trusted Platform Module (TPM).

The key terms for this section include:







Term	Definition
Data at rest	Information that is primarily stored on specific media, rather than moving from one medium to another.
Data in transit (or data in motion)	Information that is being transmitted between two hosts, such as over a private network or the internet.
Data in use (or data in processing)	Information that is present in the volatile memory of a host, such as system memory or cache.
Transport/communication encryption	Encryption scheme applied to data-in-motion, such as WPA, IPsec, or TLS.
Key exchange	Any method by which cryptographic keys are transferred among users, thus enabling the use of a cryptographic algorithm.
Hash-based Message Authentication Code (HMAC)	A method used to verify both the integrity and authenticity of a message by combining a cryptographic hash of the message with a secret key.
Full disk encryption (FDE)	Encryption of all data on a disk (including system files, temporary files, and the page file) that can be accomplished via a supported OS, third party software, or at the controller level by the disk device itself.
Self-encrypting drives (SED)	A disk drive where the controller can automatically encrypt data that is written to it.
Key Encryption Key (KEK)	In storage encryption, the private key that is used to encrypt the symmetric bulk media encryption key

Opal Storage Specification	(MEK). This means that a user must authenticate to decrypt the MEK and access the media. Standards for implementing device encryption on storage devices.
----------------------------	--

This section helps you prepare for the following certification exam objectives:

Exam	Objective
CompTIA Security+ SY0-701	<p>1.4 Explain the importance of using appropriate cryptographic solutions.</p> <ul style="list-style-type: none"> • Encryption <ul style="list-style-type: none"> ○ Full-disk ○ Database • Tools <ul style="list-style-type: none"> ○ Trusted Platform Module (TPM) <p>2.5 Explain the purpose of mitigation techniques used to secure the enterprise.</p> <ul style="list-style-type: none"> • Encryption <p>4.0 Data Security 4.2 Implement Encryption Technologies</p>
TestOut Security Pro	<p>4.2.1 Encrypt data communications 4.2.2 Encrypt files</p>



Video/Demo

	Time
 3.4.1 Encrypting File System	3:48
 3.4.2 Encrypt Files	7:53
 3.4.4 PGP and GPG	2:27
 3.4.5 Encrypting Files with GPG	3:24
 3.4.6 BitLocker and Database Encryption	5:29
 3.4.7 Configuring BitLocker	<u>4:53</u>


Total Video Time

27:54

Lab/Activity

-  3.4.3 Encrypt Files with EFS
-  3.4.8 Configure BitLocker with a TPM

Fact Sheets

 3.4.9 File Encryption Facts

Number of Exam Questions

10 questions

Total Time

About 67 minutes

3.5: Public Key Infrastructure

Lecture Focus Questions:

- What is the lifecycle of an encryption key?
- What is the role of a certificate authority (CA)?
- What are the types of certificates?
- Which standard defines the format of certificates?
- Which trust model would be used to connect the CAs of two organization's?

In this section, you will learn to:

- Manage certificates.





The key terms for this section include:

Term	Definition
Public key infrastructure (PKI)	A framework of certificate authorities, digital certificates, software, services, and other cryptographic components deployed for the purpose of validating subject identities.
Third party CAs	In PKI, a public CA that issues certificates for multiple domains and is widely trusted as a root trust by operating systems and browsers.
Digital certificate	Identification and authentication information presented in the X.509 format and issued by a certificate authority (CA) as a guarantee that a key pair (as identified by the public key embedded in the certificate) is valid for a particular subject (user or host).
Public Key Cryptography Standards (PKCS)	A series of standards defining the use of certificate authorities and digital certificates.
Certificate signing request (CSR)	A Base64 ASCII file that a subject sends to a CA to get a certificate.
Common name (CN)	An X500 attribute expressing a host or username, also used as the subject identifier for a digital certificate.
Subject alternative name (SAN)	A field in a digital certificate allowing a host to be identified by multiple host names/subdomains.
Wildcard	In PKI, a digital certificate that will match multiple subdomains of a parent domain.
Certificate revocation list (CRL)	A list of certificates that were revoked before their expiration date.

Online Certificate Status Protocol (OCSP)	Allows clients to request the status of a digital certificate, to check whether it is revoked.
Root certificate	In PKI, a certificate authority that issues certificates to intermediate certificate authorities in a hierarchical structure.
Certificate chaining/Chain of trust	A method of validating a certificate by tracing each CA that signs the certificate up through the hierarchy to the root CA.
Self-signed certificate	A digital certificate that has been signed by the entity that issued it, rather than by a certificate authority.
Escrow	In key management, the storage of a backup key with a third party.

This section helps you prepare for the following certification exam objectives:




Exam	Objective
CompTIA Security+ SY0-701	<p>1.4 Explain the importance of using appropriate cryptographic solutions.</p> <ul style="list-style-type: none"> • Public key infrastructure (PKI) <ul style="list-style-type: none"> ○ Public key ○ Private key ○ Key escrow • Digital signatures • Certificates <ul style="list-style-type: none"> ○ Certificate authorities ○ Certificate revocation lists (CRLs) ○ Online Certificate Status Protocol (OCSP) ○ Self-signed ○ Third-party ○ Root of trust ○ Certificate signing request (CSR) generation ○ Wildcard
	<p>4.1 Given a scenario, apply common security techniques to computing resources.</p> <ul style="list-style-type: none"> • Application security <ul style="list-style-type: none"> ○ Input validation ○ Secure cookies ○ Static code analysis ○ Code signing

Video/Demo	Time
 3.5.1 Public Key Infrastructure	5:12
 3.5.3 Certificate Types	4:06
 3.5.5 Manage Certificates	11:23
 3.5.7 Certificate Concepts	<u>7:36</u>
Total Video Time	28:17

Lab/Activity

-  3.5.6 Manage Certificates

Fact Sheets

-  3.5.2 Public Key Infrastructure Facts
-  3.5.4 Certificate Types Facts
-  3.5.8 Certificate Concepts Facts

Number of Exam Questions

11 questions

Total Time

About 72 minutes

4.0: Identity and Access Management

4.1: Access Control Models

Lecture Focus Questions:

- What is access control and why is it important?
- How are rule-based access control and mandatory access control (MAC) similar?
- How does role-based control differ from rule-based control?
- How do separation of duties and job rotation differ?
- Which authentication type requires you to prove your identity?

The key terms for this section include:

Term	Definition
CIA Triad	Three principles of security control and management - confidentiality, integrity, and accessibility. Also known as the information security triad.
Confidentiality	The fundamental security goal of keeping information and communications private and protecting them from unauthorized access.
Integrity	The fundamental security goal of keeping organizational information accurate, free of errors, and without unauthorized modifications.
Availability	The fundamental security goal of ensuring that computer systems operate continuously and that authorized persons can access data that they need.
Non-repudiation	The security goal of ensuring that the party that sent a transmission or created data remains associated with that data and cannot deny sending or creating that data.
National Institute of Standards and Technology (NIST)	Develops computer security standards used by US federal agencies and publishes cybersecurity best practice guides and research.
cybersecurity frameworks (CSF)	Standards, best practices, and guidelines for effective security risk management. Some frameworks are general in nature, while others are specific to industry or technology types.
security controls	A technology or procedure put in place to mitigate vulnerabilities and risk and to ensure the confidentiality, integrity, and availability (CIA) of information.

Gap analysis	An analysis that measures the difference between the current and desired states in order to help assess the scope of work included in a project.
identity and access management (IAM)	A security process that provides identification, authentication, and authorization mechanisms for users, computers, and other entities to work with organizational assets like networks, operating systems, and applications.
Identification	The process by which a user account (and its credentials) is issued to the correct person. Sometimes referred to as enrollment.
Authentication	A method of validating a particular entity's or individual's unique credentials.
Authorization	The process of determining what rights and privileges a particular entity has.
Accounting	Tracking authorized usage of a resource or use of rights by a subject and alerting when unauthorized use is detected or attempted.
authentication, authorization, and accounting (AAA)	A security concept where a centralized platform verifies subject identification, ensures the subject is assigned relevant permissions, and then logs these actions to create an audit trail.
control plane	In zero trust architecture, functions that define policy and determine access decisions.
permissions	Security settings that control access to objects including file system items and network resources.
Discretionary access control (DAC)	An access control model where each resource is protected by an access control list (ACL) managed by the resource's owner (or owners).
Mandatory access control (MAC)	An access control model where resources are protected by inflexible, system-defined rules. Resources (objects) and users (subjects) are allocated a clearance level (or label).
Role-based access control (RBAC)	An access control model where resources are protected by ACLs that are managed by administrators and that provide user permissions based on job functions.
group account	A group account is a collection of user accounts that is useful when establishing file permissions and user rights because when many individuals need the same level of access, a group could be established containing all the relevant users.
Attribute-based access control (ABAC)	An access control technique that evaluates a set of attributes that each subject possesses to determine if access should be granted.

Rule-based access control	A nondiscretionary access control technique that is based on a set of operational rules or restrictions to enforce a least privileges permissions policy.
Least privilege	A basic principle of security stating that something should be allocated the minimum necessary rights, privileges, or information to perform its role.
Provisioning	The process of deploying an account, host, or application to a target production environment. This involves proving the identity or integrity of the resource, and issuing it with credentials and access permissions.
Deprovisioning	The process of removing an account, host, or application from the production environment. This requires revoking any privileged access that had been assigned to the object.
security identifier (SID)	The value assigned to an account by Windows and that is used by the operating system to identify that account.
group policy objects (GPOs)	On a Windows domain, a way to deploy per-user and per-computer settings such as password policy, account restrictions, firewall status, and so on.
geolocation	The identification or estimation of the physical location of an object, such as a radar source, mobile phone, or Internet-connected computing device.
time-of-day restrictions policy	Policies or configuration settings that limit a user's access to resources.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
CompTIA Security+ SYO-701	<p>1.2 Summarize fundamental security concepts.</p> <ul style="list-style-type: none"> • Confidentiality, Integrity, and Availability (CIA) • Non-repudiation • Authentication, Authorization, and Accounting (AAA) <ul style="list-style-type: none"> ○ Authenticating people ○ Authenticating systems ○ Authorization models • Gap analysis • Zero trust <ul style="list-style-type: none"> ○ Control plane <ul style="list-style-type: none"> ▪ Adaptive identity ▪ Threat scope reduction ▪ Policy-driven access control ▪ Policy Administrator ▪ Policy Engine ○ Data plane

Copyright © 2023 TestOut Corporation. Copyright © The Computing Technology Industry Association, Inc. (CompTIA). All Rights Reserved. Reference to any specific product, service, process, or method by trade name, trademark, manufacturer or otherwise on this website is for educational purposes only and does not constitute an implied or expressed recommendation or endorsement by said third party. Neither TestOut nor CompTIA have any affiliation with any of these companies, and the products and services advertised herein are not endorsed by them.

- Implicit trust zones
- Subject/System
- Policy enforcement point

2.5 Explain the purpose of mitigation techniques used to secure the enterprise.

- Access control
- Least privilege

4.6 Given a scenario, implement and maintain identity and access management.

- Provisioning/de-provisioning user accounts
- Permission assignments and implications
- Identity proofing
- Access controls
 - Mandatory
 - Discretionary
 - Role-based
 - Rule-based
 - Attribute-based
 - Time-of-day restrictions
 - Least privilege
- Multifactor authentication
 - Implementations
 - Hard/soft authentication tokens
 - Factors
 - Something you know
 - Something you have
 - Something you are
 - Somewhere you are

5.1 Summarize elements of effective security governance.

- Policies
 - Information security policies

Video/Demo

 4.1.1 Fundamental Security Concepts

Time

4:40

▶ 4.1.3 Access Control Best Practices

4:16

▶ 4.1.4 Access Control Models

5:06

Total Video Time

14:02

Fact Sheets

📄 4.1.2 Access Control Facts

📄 4.1.3 Access Control Best Practices

📄 4.1.5 Access Control Model Facts

Number of Exam Questions

10 questions

Total Time

About 40 minutes

4.2: Authentication

Lecture Focus Questions:

- What is the difference between authentication factors and attributes?
- What is an example of the "something you are" authentication type?
- What is an example of the "something you have" authentication type?
- What is multi-factor authentication?
- Which physical attributes can be used to identify an individual?

In this section, you will learn to:

- Use a biometric scanner
- Use single sign-on

The key terms for this section include:

Term	Definition
Multi-factor authentication (MFA)	An authentication scheme that requires the user to present at least two different factors as credentials; for example, something you know, something you have, something you are, something you do, and somewhere you are. Specifying two factors is known as 2FA.
Factors	In authentication design, different technologies for implementing authentication, such as knowledge, ownership/token, and biometric/inherence. These are characterized as something you know/have/are.
Personal identification number (PIN)	A number used in conjunction with authentication devices such as smart cards; as the PIN should be known only to the user, loss of the smart card should not represent a security risk.
Hard authentication token	Authentication token generated by a cryptoprocessor on a dedicated hardware device. As the token is never transmitted directly, this implements an ownership factor within a multi-factor authentication scheme.
Smart cards	A security device similar to a credit card that can store authentication information, such as a user's private key, on an embedded cryptoprocessor.
One-time password (OTP)	A password that is generated for use in one specific session and becomes invalid after the session ends.
Security key	Portable HSM with a computer interface, such as USB or NFC, used for multi-factor authentication.

Term	Definition
Soft authentication token	OTP sent to a registered number or email account or generated by an authenticator app as a means of two-step verification when authenticating account access.
Passwordless	Multi-factor authentication scheme that uses ownership and biometric factors, but not knowledge factors.
Attestation	Capability of an authenticator or other cryptographic module to prove that it is a root of trust and can provide reliable reporting to prove that a device or computer is a trustworthy platform.
NT LAN Manager (NTLM) authentication	A challenge-response authentication protocol created by Microsoft for use in its products.
Pluggable authentication module (PAM)	A framework for implementing authentication providers in Linux.
Directory service	A network service that stores identity information about all the objects in a particular network, including users, groups, servers, client computers, and printers.
Lightweight Directory Access Protocol (LDAP)	Protocol used to access network directory databases, which store information about authorized users and their privileges, as well as other organizational information.
Distinguished name (DN)	A collection of attributes that define a unique identifier for any given resource within an X.500-like directory.
Single sign-on (SSO)	Authentication technology that enables a user to authenticate once and receive authorizations for multiple services.
Kerberos	A single sign-on authentication and authorization service that is based on a time-sensitive, ticket-granting system.
Key distribution center (KDC)	A component of Kerberos that authenticates users and issues tickets (tokens).
Ticket Granting Ticket (TGT)	In Kerberos, a token issued to an authenticated account to allow access to authorized application servers.
Federation	A process that provides a shared login capability across multiple systems and enterprises. It essentially connects the identity management services of multiple systems.
Identity provider (IdP)	In a federated network, the service that holds the user account and performs authentication.
Security Assertion Markup Language (SAML)	An XML-based data format used to exchange authentication information between a client and a service.

Term	Definition
Simple Object Access Protocol (SOAP)	An XML-based web services protocol that is used to exchange messages.
Representational State Transfer (REST)	A standardized, stateless architectural style used by web applications for communication and integration.
Open Authorization (OAuth)	A standard for federated identity management, allowing resource servers or consumer sites to work with user accounts created and managed on a separate identity provider.
JavaScript Object Notation (JSON)	A file format that uses attribute-value pairs to define configurations in a structure that is easy for both humans and machines to read and consume.
Biometric authentication	An authentication mechanism that allows a user to perform a biometric scan to operate an entry or access system. Physical characteristics stored as a digital data template can be used to authenticate a user. Typical features used include facial pattern, iris, retina, fingerprint pattern, and signature recognition.
False Rejection Rate (FRR)	A biometric assessment metric that measures the number of valid subjects who are denied access.
False Acceptance Rate (FAR)	A biometric assessment metric that measures the number of unauthorized users who are mistakenly allowed access.
Crossover Error Rate (CER)	A biometric evaluation factor expressing the point at which FAR and FRR meet, with a low value indicating better performance.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
CompTIA Security+ SY0-701	<p>1.2 Summarize fundamental security concepts.</p> <ul style="list-style-type: none"> • Confidentiality, Integrity, and Availability (CIA) • Non-repudiation • Authentication, Authorization, and Accounting (AAA) <ul style="list-style-type: none"> ○ Authenticating people ○ Authenticating systems ○ Authorization models • Gap analysis • Zero trust <ul style="list-style-type: none"> ○ Control plane <ul style="list-style-type: none"> ▪ Adaptive identity ▪ Threat scope reduction

Exam	Objective
	<ul style="list-style-type: none"> ▪ Policy-driven access control ▪ Policy Administrator ▪ Policy Engine ○ Data plane <ul style="list-style-type: none"> ▪ Implicit trust zones ▪ Subject/System ▪ Policy enforcement point <p>2.5 Explain the purpose of mitigation techniques used to secure the enterprise.</p> <ul style="list-style-type: none"> • Access control • Least privilege <p>4.6 Given a scenario, implement and maintain identity and access management.</p> <ul style="list-style-type: none"> • Provisioning/de-provisioning user accounts • Permission assignments and implications • Identity proofing • Access controls <ul style="list-style-type: none"> ○ Mandatory ○ Discretionary ○ Role-based ○ Rule-based ○ Attribute-based ○ Time-of-day restrictions ○ Least privilege • Multi-factor authentication <ul style="list-style-type: none"> ○ Implementations <ul style="list-style-type: none"> ▪ Hard/soft authentication tokens ○ Factors <ul style="list-style-type: none"> ▪ Something you know ▪ Something you have ▪ Something you are ▪ Somewhere you are <p>5.1 Summarize elements of effective security governance.</p>

Exam	Objective
	<ul style="list-style-type: none"> • Policies <ul style="list-style-type: none"> ○ Information security policies

Video/Demo	Time
📺 4.2.1 Authentication	5:28
📺 4.2.3 Authentication Methods	5:03
📺 4.2.4 Authentication Methods Facts	4:52
📺 4.2.5 Biometrics and Authentication Technologies	4:17
📺 4.2.6 Use a Biometric Scanner	2:09
📺 4.2.7 Use Single Sign-on	<u>4:35</u>
Total Video Time	26:24

Fact Sheets

- 📄 4.2.2 Authentication Factors Facts
- 📄 4.2.4 Authentication Methods Facts
- 📄 4.2.8 Biometrics and Authentication Technologies Facts

Number of Exam Questions

10 questions

Total Time

About 52 minutes

4.3: Authorization

Summary

As you study this section, answer the following questions:

- How is authorization different from authentication?
- How does an access control list (ACL) help to increase network security?
- 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 access token

The key terms for this section include:




Term	Definition
Authorization	Granting a user on the computer system the right to use a resource.
Access control list (ACL)	A collection of access control entries that determines which users are allowed or denied access to an object and the privileges given to that user.
Effective permissions	Access rights are cumulative, giving the user combined permissions from multiple groups.
Deny permissions	Always override Allow permissions.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
CompTIA Security+ SY0-701	1.2 Summarize fundamental security concepts. <ul style="list-style-type: none">• Authentication, Authorization, and Accounting (AAA)<ul style="list-style-type: none">◦ Authorization models
	1.4 Explain the importance of using appropriate cryptographic solutions. <ul style="list-style-type: none">• Obfuscation<ul style="list-style-type: none">◦ Tokenization

Exam	Objective
TestOut Security Pro	2.5 Explain the purpose of mitigation techniques used to secure the enterprise.
	<ul style="list-style-type: none"> • Access control <ul style="list-style-type: none"> ○ Access control list (ACL) ○ Permissions
	4.6 Given a scenario, implement and maintain identity and access management.
	<ul style="list-style-type: none"> • Permission assignments and implications • Single sign-on (SSO) • Access controls <ul style="list-style-type: none"> ○ Discretionary
	2.5.2 Access control
	<ul style="list-style-type: none"> • 2.5.2.1 Access control list (ACL) • 2.5.2.2 Permissions
	4.6.8 Access control
	<ul style="list-style-type: none"> • 4.6.8.3 Role-based

Video/Demo

-  4.3.1 Authorization
-  4.3.2 Cumulative Access
-  4.3.4 Examining the Access Token

Time

3:18
2:59
7:47
14:04

Total Video Time

Fact Sheets

-  4.3.3 Authorization Facts

Number of Exam Questions

11 questions

Total Time

Copyright © 2023 TestOut Corporation. Copyright © The Computing Technology Industry Association, Inc. (CompTIA). All Rights Reserved. Reference to any specific product, service, process, or method by trade name, trademark, manufacturer or otherwise on this website is for educational purposes only and does not constitute an implied or expressed recommendation or endorsement by said third party. Neither TestOut nor CompTIA have any affiliation with any of these companies, and the products and services advertised herein are not endorsed by them.

About 36 minutes

4.4: Active Directory Overview

Summary

As you study this section, answer the following questions:

- What is the purpose of a domain?
- How do organizational units (OUs) simplify security administration?
- How do computer policies differ from user policies?
- What is the order in which Group Policy objects (GPOs) are applied?

In this section, you will learn to:

- Join a domain
- Manage Active Directory objects
- Create OUs
- Delete OUs
- Use Group Policy
- Create and link a GPO
- Create user accounts
- Manage user accounts
- Create a group
- Create Global Groups

The key terms for this section include:






Term	Definition
Domain	A domain is an administratively defined collection of network resources that share a common directory database and security policies. The domain is the basic administrative unit of an Active Directory structure.
Tree	A tree is a group of related domains that share the same contiguous DNS namespace.
Forest	A forest is a collection of related domain trees. The forest establishes the relationship between trees that have different DNS namespaces.
Organizational unit (OU)	An organizational unit is similar to a folder. It subdivides and organizes network resources within a domain.
Object	Each resource within Active Directory is identified as an object.
Domain controller	A domain controller is a server that holds a copy of the Active Directory database. It is also the copy of the Active Directory database on a domain controller that can be written to.
Replication	Replication is the process of copying changes to Active Directory on the domain controllers.

Term	Definition
Member servers	Member servers are servers in the domain that do not have the Active Directory database.
Policy	A policy is a set of configuration settings applied to users or computers.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
	1.2 Summarize fundamental security concepts. <ul style="list-style-type: none"> • Authentication, Authorization, and Accounting (AAA)
CompTIA Security+ SY0-701	4.5 Given a scenario, modify enterprise capabilities to enhance security. <ul style="list-style-type: none"> • Operating system security <ul style="list-style-type: none"> ◦ Group Policy
	1.1 Manage identity
TestOut Security Pro	1.1.1 Manage Windows local and domain users and groups 1.1.3 Manage Active Directory OUs

Video/Demo

	Time
 4.4.1 Active Directory Introduction	8:17
 4.4.2 Joining a Domain	8:38
 4.4.3 Managing Active Directory Objects	9:18
 4.4.7 Group Policy	8:47
 4.4.8 Use Group Policy	<u>6:04</u>

Total Video Time

41:04

Lab/Activity

- 🔗 4.4.5 Create OUs
- 🔗 4.4.6 Delete OUs
- 🔗 4.4.10 Create and Link a GPO
- 🔗 4.4.11 Create User Accounts
- 🔗 4.4.12 Manage User Accounts
- 🔗 4.4.13 Create a Group
- 🔗 4.4.14 Create Global Groups

Fact Sheets

-  4.4.4 Active Directory Facts
-  4.4.9 Group Policy Facts

Number of Exam Questions

10 questions

Total Time

About 146 minutes

4.5: Hardening Authentication

Lecture Focus Questions:

- 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 and UAC settings
- Use password managers
- Configure account password policies
- Hardening user accounts
- Restrict local accounts
- Secure default accounts
- Enforce user account control
- Configure smart card authentication

The key terms for this section include:

Term	Definition
Multifactor authentication	Using more than one method to authenticate users.
Smart cards	Similar in appearance to credit cards, smart cards have an embedded memory chip that contains encrypted authentication information. These cards are used for authentication.
Microprobing	The process of accessing a smart card's chip surface directly to observe, manipulate, and interfere with the circuit.
Radio frequency identification (RFID)	The wireless, non-contact use of radio frequency waves to transfer data.




This section helps you prepare for the following certification exam objectives:

Exam	Objective
CompTIA Security+ SY0-701	1.2 Summarize fundamental security concepts. <ul style="list-style-type: none">• Authentication, Authorization, and Accounting (AAA)<ul style="list-style-type: none">◦ Authenticating people
	2.4 Given a scenario, analyze indicators of malicious activity. <ul style="list-style-type: none">• Indicators

Exam	Objective
	<ul style="list-style-type: none"> ○ Account lockout ○ Concurrent session usage ○ Blocked content ○ Impossible travel ○ Resource inaccessibility <p>4.5 Given a scenario, modify enterprise capabilities to enhance security.</p> <ul style="list-style-type: none"> • Operating system security <ul style="list-style-type: none"> ○ Group Policy <p>4.6 Given a scenario, implement and maintain identity and access management.</p> <ul style="list-style-type: none"> • Provisioning/de-provisioning user accounts • Permission assignments and implications • Multifactor authentication <ul style="list-style-type: none"> ○ Implementations <ul style="list-style-type: none"> ▪ Security keys ○ Factors <ul style="list-style-type: none"> ▪ Something you have • Password concepts <ul style="list-style-type: none"> ○ Password best practices <ul style="list-style-type: none"> ▪ Length ▪ Complexity ▪ Reuse ▪ Expiration ▪ Age ○ Password managers ○ Passwordless • Privileged access management tools <ul style="list-style-type: none"> ○ Just-in-time permissions ○ Password vaulting ○ Temporal accounts

Video/Demo

Time

 4.5.1 Hardening Authentication	7:55
 4.5.2 Configure User Account Restrictions	4:22
 4.5.3 Configure Account Policies and UAC Settings	6:58

🖥️ 4.5.4 Use Password Managers	4:42
🖥️ 4.5.6 Hardening User Accounts	5:43
🖥️ 4.5.11 Configure Smart Card Authentication	<u>5:38</u>

Total Video Time **35:18**

Lab/Activity

- 🔑 4.5.5 Configure Account Password Policies
- 🔑 4.5.7 Restrict Local Accounts
- 🔑 4.5.8 Secure Default Accounts
- 🔑 4.5.9 Enforce User Account Control
- 🔑 4.5.12 Configure Smart Card Authentication

Fact Sheets

- 📄 4.5.10 Hardening Authentication Facts
- 📄 4.5.13 Smart Card Authentication Facts

Number of Exam Questions

10 questions

Total Time

About 116 minutes

4.6: Linux Users

Lecture Focus Questions:

- How do you create a user in Linux?
- Why shouldn't passwords expire too frequently?
- Which directory contains configuration file templates copied into a new user's home directory?
- Which command deletes a user and the user's home directory simultaneously?

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
- Configure Linux User Security and Restrictions
- Configure SELinux

This section helps you prepare for the following certification exam objectives:

Exam	Objective
CompTIA Security+ SY0-701	2.5 Explain the purpose of mitigation techniques used to secure the enterprise. <ul style="list-style-type: none">• Hardening techniques<ul style="list-style-type: none">◦ Default password changes
	4.1 Given a scenario, apply common security techniques to computing resources. <ul style="list-style-type: none">• Application security
	4.5 Given a scenario, modify enterprise capabilities to enhance security. <ul style="list-style-type: none">• Operating system security• SELinux

Exam	Objective
TestOut Security Pro	4.6 Given a scenario, implement and maintain identity and access management. <ul style="list-style-type: none"> • Provisioning/de-provisioning user accounts • Password concepts <ul style="list-style-type: none"> ○ Reuse ○ Expiration
	1.1 Manage identity
	1.1.2 Manage Linux users and groups
	1.2 Harden authentication
	1.2.2 Manage account password

Video/Demo

 4.6.1 Linux User and Group Overview	11:10
 4.6.2 Managing Linux Users	7:57
 4.6.10 Linux User Security and Restrictions	7:11
 4.6.11 Configuring Linux User Security and Restrictions	7:16
 4.6.12 Configure SELinux	<u>4:55</u>

Total Video Time

38:29

Lab/Activity

- 🔑 4.6.4 Create a User Account
- 🔑 4.6.5 Rename a User Account
- 🔑 4.6.6 Delete a User
- 🔑 4.6.7 Change Your Password
- 🔑 4.6.8 Change a User's Password
- 🔑 4.6.9 Lock and Unlock User Accounts

Fact Sheets

-  4.6.3 Linux User Commands and Files
-  4.6.13 Linux User Security and Restriction Facts

Number of Exam Questions

10 questions

Total Time

Copyright © 2023 TestOut Corporation. Copyright © The Computing Technology Industry Association, Inc. (CompTIA). All Rights Reserved. Reference to any specific product, service, process, or method by trade name, trademark, manufacturer or otherwise on this website is for educational purposes only and does not constitute an implied or expressed recommendation or endorsement by said third party. Neither TestOut nor CompTIA have any affiliation with any of these companies, and the products and services advertised herein are not endorsed by them.

About 131 minutes

4.7: 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:

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

This section helps you prepare for the following certification exam objectives:

Exam	Objective
CompTIA Security+ SY0-701	4.6 Given a scenario, implement and maintain identity and access management. <ul style="list-style-type: none">• Provisioning/de-provisioning user accounts
TestOut Security Pro	1.1 Manage identity 1.1.2 Manage Linux users and groups

Video/Demo

- 📺 4.7.1 Managing Linux Groups

Total Video Time

Time

6:11

6:11

Lab/Activity

- 🔧 4.7.3 Rename and Create Groups
- 🔧 4.7.4 Add Users to a Group
- 🔧 4.7.5 Remove a User from a Group

Fact Sheets

- 📄 4.7.2 Linux Group Commands

Number of Exam Questions

10 questions

Total Time

About 58 minutes

4.8: Remote Access

Lecture Focus Questions:

- How does EAP differ from CHAP?
- How can remote access and tunneling be secured?
- What is the difference between RADIUS and TACACS+?



In this section, you will learn to:

- Configure a RADIUS solution

This section helps you prepare for the following certification exam objectives:

Exam	Objective
CompTIA Security+ SY0-701	3.2 Given a scenario, apply security principles to secure enterprise infrastructure. <ul style="list-style-type: none">• Secure communication/access<ul style="list-style-type: none">○ Virtual private network (VPN)○ Remote access○ Tunneling<ul style="list-style-type: none">▪ Internet Protocol Security (IPSec)
	4.1 Given a scenario, apply common security techniques to computing resources. <ul style="list-style-type: none">• Wireless security settings<ul style="list-style-type: none">○ AAA/Remote Authentication Dial-In User Service (RADIUS)
TestOut Security Pro	2.2 Harden network devices
	<ul style="list-style-type: none">• 2.2.3 Configure and access a virtual private network (VPN)

Video/Demo

-  4.8.1 Remote Access
-  4.8.3 Configuring a RADIUS Solution

Total Video Time



Time

3:16

3:04

6:20

Fact Sheets

-  4.8.2 Remote Access Facts
-  4.8.4 RADIUS and TACACS+ Facts

Number of Exam Questions

10 questions

Total Time

About 27 minutes

4.9: Network Authentication

Lecture Focus Questions:

- In the challenge/response process, what information is exchanged over the network during logon?
- What is included in a digital certificate?
- What is PKI?
- Which tool can manage authentication credentials on Windows hosts?

The key terms for this section include:

Term	Definition
Authentication	Authentication is the process of validating user credentials that prove user identity.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
CompTIA Security+ SY0-701	<p>3.8 Given a scenario, implement authentication and authorization solutions.</p> <ul style="list-style-type: none">• Authentication<ul style="list-style-type: none">○ EAP○ 802.1X○ Single sign-on (SSO)○ Security Assertions Markup Language (SAML)○ OAuth○ OpenID○ Kerberos
TestOut Security Pro	<p>1.0 Identity Management and Authentication</p> <p>1.2 Harden Authentication</p>

Video/Demo

- 📺 4.9.1 Network Authentication Protocols
- 📺 4.9.3 LDAP Authentication

Time

7:49

2:55

Total Video Time

10:44

Fact Sheets

- 📄 4.9.2 Network Authentication Facts
- 📄 4.9.4 LDAP Authentication Facts

Number of Exam Questions

10 questions

Copyright © 2023 TestOut Corporation. Copyright © The Computing Technology Industry Association, Inc. (CompTIA). All Rights Reserved. Reference to any specific product, service, process, or method by trade name, trademark, manufacturer or otherwise on this website is for educational purposes only and does not constitute an implied or expressed recommendation or endorsement by said third party. Neither TestOut nor CompTIA have any affiliation with any of these companies, and the products and services advertised herein are not endorsed by them.

Total Time
About 31 minutes

5.0: Network Architecture

5.1: Enterprise Network Architecture

Lecture Focus Questions:

- What is network architecture?
- What is Internet Protocol?
- What needs should be considered when setting up security zones?
- What security protocols help reduce the attack surface?

The key terms for this section include:

Term	Definition
Network architecture	The selection and placement of media, devices, protocols/services, and data assets.
Network infrastructure	The media, appliances, and addressing/forwarding protocols that support basic connectivity.
Internet Protocol (IP)	Provides the addressing mechanism for logical networks and subnets.
Attack surface	All the points at which a threat actor could gain access to hosts and services.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
CompTIA Security+ SY0-701	<p>3.1 Compare and contrast security implications of different architecture models.</p> <ul style="list-style-type: none">• Architecture and infrastructure concepts<ul style="list-style-type: none">○ Cloud<ul style="list-style-type: none">▪ Responsibility matrix▪ Hybrid considerations▪ Third-party vendors○ Infrastructure as code (IaC)○ Serverless○ Microservices○ Network infrastructure<ul style="list-style-type: none">▪ Physical isolation<ul style="list-style-type: none">▪ Air-gapped▪ Logical segmentation▪ Software-defined networking (SDN)▪ On-premises

- Centralized/decentralized
- Considerations
 - Availability
 - Resilience
 - Cost
 - Responsiveness
 - Scalability
 - Ease of deployment
 - Risk transference
 - Ease of recovery
 - Patch availability
 - Inability to patch
 - Power
 - Compute

3.2 Given a scenario, apply security principles to secure enterprise infrastructure.

- Infrastructure considerations
 - Device placement
 - Security zones
 - Attack surface
 - Connectivity
 - Failure modes
 - Fail-open
 - Fail-closed
 - Device attribute
 - Active vs. passive
 - Inline vs. tap/monitor
 - Load balancer
- Selection of effective controls

Video/Demo

 5.1.1 Enterprise Network Architecture

Total Video Time

Time

6:15

6:15

Fact Sheets

 5.1.2 Enterprise Network Architecture Facts

Number of Exam Questions

10 questions

Total Time
About 22 minutes

5.2: Security Appliances

Lecture Focus Questions:

- What are the benefits and risks of using proxy servers?
- What is the purpose of a content filtering server?
- What are the uses of a screened subnet?
- Why is a honeynet useful?
- What are the features of an all-in-one security appliance?
- What size organization should employ a all-in-one security appliance?

In this section, you will learn to:

- Configure a security appliance.
- Configure network security appliance access.

The key terms for this section include:

Term	Definition
Security zone	Portions of the network or system that have specific security concerns or requirements.
Wireless network	A network that does not require a physical connection.
Guest network	A network that grants internet access only to guest users. A guest network has a firewall to regulate guest user access.
Honeynet	A host (honeypot), network (honeynet), file (honeyfile), or credential/token (honeytoken) set up with the purpose of luring attackers away from assets of actual value and/or discovering attack strategies and weaknesses in the security configuration.
Ad hoc	A decentralized network that allows connections without a traditional base station or router. It allows users to connect two or more devices directly to each other for a specific purpose.
DNS sinkhole	A temporary DNS record that redirects malicious traffic to a controlled IP address.
Jump server	A hardened server that provides access to other hosts.
Agent-based filtering	Agent-based web filtering involves installing a software agent on desktop computers, laptops, and mobile devices. The agents enforce compliance with the organization's web filtering policies.
Screened subnet	A network that contains publicly accessible resources and is located between the private network and an untrusted network, such as the internet. It is protected by a firewall.
Proxy server	A type of firewall that stands as an intermediary between clients requesting resources from other servers.

Internet content filter	Software used to monitor and restrict content delivered across the web to an end user.
Fake telemetry	Deception strategy that returns spoofed data in response to network probes.
All-in-one security appliance	An appliance that combines many security functions into a single device.
Application-aware devices	A device that has the ability to analyze and manage network traffic based on the application-layer protocol.

This section helps you prepare for the following certification exam objectives:








Exam	Objective
CompTIA Security+ SY0-701	1.2 Summarize fundamental security concepts. <ul style="list-style-type: none"> • Deception and disruption technology <ul style="list-style-type: none"> ○ Honeypot ○ Honeynet ○ Honeyfile ○ Honeytoken
	3.2 Given a scenario, apply security principles to secure enterprise infrastructure. <ul style="list-style-type: none"> • Infrastructure considerations <ul style="list-style-type: none"> ○ Security zones • Failure modes <ul style="list-style-type: none"> ○ Fail-open ○ Fail-closed • Network appliances <ul style="list-style-type: none"> ○ Jump server ○ Proxy server ○ Load balancer ○ Sensors
	4.5 Given a scenario, modify enterprise capabilities to enhance security. <ul style="list-style-type: none"> • Web filter <ul style="list-style-type: none"> ○ Agent-based ○ Centralized proxy ○ Universal Resource Locator (URL) scanning ○ Content categorization

- Block rules
- Reputation

2.1 Harden Physical Access

TestOut Security Pro


2.1.2 Install and Configure a Security Appliance
2.1.4 Create and Configure a screened subnet

Video/Demo	Time
 5.2.1 Security Appliances	8:33
 5.2.2 Security Solutions	5:39
 5.2.3 Security Solution Facts	3:18
 5.2.4 Security Zones	4:48
 5.2.6 Configure Network Security Appliance Access	7:45
 5.2.9 Deceptive and Disruption Technology	8:28
 5.2.11 Detect Malicious Network Traffic with a Honeypot	3:20
 5.2.12 Configure Load Balancer	<u>5:33</u>
Total Video Time	47:24

Lab/Activity

-  5.2.7 Configure a Security Appliance
-  5.2.8 Configure Network Security Appliance Access

Fact Sheets

-  5.2.3 Security Solution Facts
-  5.2.5 Security Zone Facts
-  5.2.10 Deceptive and Disruption Technology Facts

Number of Exam Questions

10 questions

Total Time

About 97 minutes

5.3: Screened Subnets

Lecture Focus Questions:

- How is a honeypot used to increase network security?
- What is the typical configuration for a screened subnet?
- What is the function of each firewall in a two-firewall screened subnet?
- What type of computer might exist inside a screened subnet?
- What makes bastion hosts vulnerable to attack? How can you harden bastion hosts?

In this section, you will learn to:

- Configure a screened subnet.

The key terms for this section include:

Term	Definition
Screened subnet	A buffer network (or subnet) that is located between a private network and an untrusted network, such as the internet.
Bastion or sacrificial host	Any host that is exposed to attack and has been hardened or fortified against attack.
Screening router	The router that is most external to the network and closest to the internet.
Dual-homed gateway	A firewall device that typically has three network interfaces. One interface connects to the internet, one interface connects to the public subnet, and one interface connects to the private network.
Screened host gateway	A device residing within the screened subnet that requires users to authenticate in order to access resources within the screened subnet or the intranet.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
CompTIA Security+ SY0-701	4.5 Given a scenario, modify enterprise capabilities to enhance security. <ul style="list-style-type: none">• Firewall<ul style="list-style-type: none">○ Screened subnets
TestOut Security Pro	2.1 Harden Physical Access <ul style="list-style-type: none">2.1.4 Create and configure a screened subnet

Video/Demo

- 5.3.1 Screened Subnets
- 5.3.2 Configuring a Screened Subnet

Total Video Time

Time

6:17

3:17

9:34

Lab/Activity

- 5.3.3 Configure a Screened Subnet

Fact Sheets

- 5.3.4 Screened Subnet Facts

Number of Exam Questions

10 questions

Total Time

About 37 minutes

5.4: 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?
- How are firewall rules used and what are they based on?
- What network security devices can be used for intrusion detection?
- Where should a network-based firewall be placed?

In this section, you will learn to:

- Configure firewall rules.
- Configure firewall schedules.
- Configure a perimeter firewall.

The key terms for this section include:

Term	Definition
Firewall	A device, or software running on a device, that inspects network traffic and allows or blocks traffic based on a set of rules.
Web application firewall (WAF)	A firewall designed specifically to protect software running on web servers and their back-end databases from code injection and DoS attacks.
Network firewall	A firewall that is used to regulate traffic in and out of an entire network.
Stateless firewall	A firewall that allows or denies traffic by examining information in IP packet headers.
Stateful firewall	A firewall that allows or denies traffic based on virtual circuits of sessions. A stateful firewall is also known as a circuit-level proxy or circuit-level gateway.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
CompTIA Security+ SY0-701	<p>2.5 Explain the purpose of mitigation techniques used to secure the enterprise</p> <ul style="list-style-type: none">• Hardening techniques<ul style="list-style-type: none">○ Host-based firewall <p>3.2 Given a scenario, apply security principles to secure enterprise infrastructure.</p>

- Firewall types
 - Web application firewall (WAF)
 - Unified threat management (UTM)
 - Next-generation firewall (NGFW)
 - Layer 4/Layer 7

4.5 Given a scenario, modify enterprise capabilities to enhance security.




- Firewall
 - Rules
 - Access lists
 - Ports/protocols

2.0 Physical and Network Security

TestOut Security Pro

- Harden physical access
 - Install and configure a firewall

Video/Demo

-  5.4.1 Firewalls
-  5.4.3 Configuring Firewall Rules
-  5.4.4 Configure Firewall Schedules

Time

7:29

6:34

6:05

Total Video Time

20:08

Lab/Activity

-  5.4.5 Configure a Perimeter Firewall

Fact Sheets

-  5.4.2 Firewall Facts

Number of Exam Questions

10 questions

Total Time

About 48 minutes

5.5: Virtual Private Networks

Lecture Focus Questions:

- What are three ways a Virtual Private Network (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?
- How does a transport layer security (TLS) VPN work?

In this section, you will learn to:

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





The key terms for this section include:

Term	Definition
Virtual Private Network	A remote access connection that uses encryption to securely send data over an untrusted network.
Tunneling	The practice of encapsulating data from one protocol for safe transfer over another network such as the Internet.
Point-to-Point Tunneling Protocol (PPTP)	A early tunneling protocol developed by Cisco and Microsoft to support VPNs over PPP and TCP/IP. PPTP is highly vulnerable to password cracking attacks and considered obsolete.
Layer 2 Forwarding (L2F)	A tunneling protocol developed by Cisco to establish virtual private network connections over the internet.
Internet Protocol Security (IPsec)	Network protocol suite used to secure data through authentication and encryption as the data travels across the network or the Internet.
Secure Sockets Layer (SSL)	A well-established protocol to secure IP protocols, such as HTTP and FTP. And can also be used to secure other application protocols and as a virtual private networking (VPN) solution.
Transport Layer Security (TLS)	Security protocol that uses certificates for authentication and encryption to protect web communications and other application protocols.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
------	-----------

	2.2 Harden Network Devices
TestOut Security Pro	2.2.3 Configure and Access a Virtual Private Network (VPN)
	3.2 Given a scenario, apply security principles to secure enterprise infrastructure.
CompTIA Security+ SY0-701	<ul style="list-style-type: none"> • Secure communication/access <ul style="list-style-type: none"> ○ Virtual private network (VPN)

Video/Demo	Time
 5.5.1 Virtual Private Networks	7:00
 5.5.2 Configuring a VPN	9:07
 5.5.3 Configuring a VPN Client	2:35
 5.5.6 Configure Remote Access, non VPN	<u>3:34</u>
Total Video Time	22:16

Lab/Activity

-  5.5.4 Configure a Remote Access VPN
-  5.5.5 Configure a VPN Connection iPad

Fact Sheets

-  5.5.7 Virtual Private Network Facts
-  5.5.8 VPN Protocol Facts

Number of Exam Questions

11 questions

Total Time

About 73 minutes

5.6: Network Access Control

Lecture Focus Questions:

- How do remediation servers and auto-remediation help clients become compliant?
- What are the security standards NAC uses for evaluation?
- What is an NAC agent? What types of NAC agents are available?
- What are the four steps of the NAC process?

The key terms for this section include:

Term	Definition
Network access control (NAC)	A general term for the collected protocols, policies, and hardware that authenticate and authorize access to a network at the device level.
Bring your own device (BYOD)	Security framework and tools to facilitate use of personally owned devices to access corporate networks and data.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
CompTIA Security+ SY0-701	4.5 Given a scenario, modify enterprise capabilities to enhance security. <ul style="list-style-type: none">• Network access control (NAC)

Video/Demo

- 📺 5.6.1 Network Access Control

Total Video Time

Time

6:29

6:29

Fact Sheets

- 📄 5.6.2 Network Access Control Facts

Number of Exam Questions

10 questions

Total Time

About 22 minutes

5.7: Network Device Vulnerabilities

Lecture Focus Questions:

- For security, 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?
- What are major risks of hard-coded passwords on devices throughout the enterprise?
- What are the resources you can use to keep track of existing technology vulnerabilities in an organization?

In this section, you will learn to:

- Search for default passwords.
- Establish an unauthorized SSH connection.
- Secure a switch.

The key terms for this section include:

Term	Definition
Privilege escalation	A software bug or design flaw in an application that allows an attacker to gain access to system resources or additional privileges that aren't typically available.
Backdoor	An unprotected and usually lesser known access method or pathway that may allow attackers access to system resources.
Zero-day vulnerability	A software vulnerability that is unknown to the vendor that can be exploited by attackers.
Common Vulnerabilities and Exposures (CVEs)	A repository of vulnerabilities hosted by MITRE Corporation.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
	2.3 Explain various types of vulnerabilities.
CompTIA Security+ SY0-701	<ul style="list-style-type: none">• Misconfiguration• Zero-day
	2.4 Given a scenario, analyze indicators of malicious activity.

- Privilege escalation





4.6 Given a scenario, implement and maintain identity and access management.

- Password concepts
 - Password best practices
 - Length
 - Complexity

2.2 Harden Network Devices

TestOut Security Pro

2.2.1 Configure and Access a Switch

Video/Demo	Time
 5.7.1 Device Vulnerabilities	6:52
 5.7.3 Searching for Default Passwords	2:53
 5.7.4 Unauthorized SSH Connection	4:17
 5.7.5 Securing a Switch	<u>2:55</u>
Total Video Time	16:57

Lab/Activity

- 🔧 5.7.6 Secure a Switch

Fact Sheets

-  5.7.2 Device Vulnerability Facts

Number of Exam Questions

10 questions

Total Time

About 44 minutes

5.8: Network Applications

Lecture Focus Questions:

- How does application vulnerability scanning differ from general vulnerability scanning?
- What is package monitoring used for?
- What security measures should you incorporate to control the use of networking software?
- What is static analysis?
- What is dynamic analysis?

In this section, you will learn to:

- Configure application control software.

The key terms for this section include:

Term	Definition
Peer-to-peer (P2P) software	Software that allows users to share content without centralized servers or centralized access control.
Instant messaging	Real-time text messaging communication that supports picture, music, and document exchange.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
	4.3 Explain various activities associated with vulnerability management.
CompTIA Security+ SY0-701	<ul style="list-style-type: none">• Identification methods<ul style="list-style-type: none">◦ Application security<ul style="list-style-type: none">▪ Static analysis▪ Dynamic analysis▪ Package monitoring
	3.2 Implement Application Defenses
TestOut Security Pro	3.2.1 Implement Application Whitelisting 3.2.3 Configure web application security

Video/Demo

 5.8.1 Network Application Security

Time

3:42

 5.8.2 Configure Application Control Software

7:43

Total Video Time

11:25

Copyright © 2023 TestOut Corporation. Copyright © The Computing Technology Industry Association, Inc. (CompTIA). All Rights Reserved. Reference to any specific product, service, process, or method by trade name, trademark, manufacturer or otherwise on this website is for educational purposes only and does not constitute an implied or expressed recommendation or endorsement by said third party. Neither TestOut nor CompTIA have any affiliation with any of these companies, and the products and services advertised herein are not endorsed by them.

Fact Sheets

 5.8.3 Network Application Facts

Number of Exam Questions

10 questions

Total Time

About 27 minutes

5.9: Switch Security and Attacks

Lecture Focus Questions:

- How are switches indirectly involved in Address Resolution Protocol (ARP) poisoning?
- How does the attacker hide his identity when performing media access control (MAC) address spoofing?
- What is the function of a trunk port?
- How is port security different from port filtering?
- What are some important considerations when deciding which secure protocols to implement?

In this section, you will learn to:

- Harden a switch.
- Secure access to a switch.
- Use best practices to ensure switch security.

The key terms for this section include:





Term	Definition
Virtual LAN (VLAN)	A logical grouping of computers based on switch port.
MAC filtering/port security	A switch feature that restricts connection to a given port based on the MAC address.
Port authentication	A switch feature that follows the 802.1x protocol to allow only authenticated devices to connect.
Content-addressable memory (CAM) table	A table maintained by a switch that contains MAC addresses and their corresponding port locations.
Dynamic Host Configuration protocol (DHCP) snooping	A security feature on some switches that filters out untrusted DHCP messages.
Dynamic ARP Inspection (DAI)	A security feature on some switches that verifies each ARP request has a valid IP to MAC binding.
MAC flooding	An attack that overloads a switch's MAC forwarding table to make the switch function like a hub.
ARP spoofing	An attack in which the attacker's MAC address is associated with the IP address of a target's device.
VLAN hopping	An attack in which the source MAC address is changed on frames sent by the attacker.
Double tagging	An attack in which the attacking host adds two VLAN tags instead of one to the header of the frames that it transmits.

MAC spoofing	An attack in which the source MAC address is changed in the header of a frame.
Dynamic Trunking Protocol (DTP)	An unsecure protocol that could allow unauthorized devices to modify a switch's configuration.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
CompTIA Security+ SY0-701	4.1 Given a scenario, apply common security techniques to computing resources. <ul style="list-style-type: none"> Hardening targets <ul style="list-style-type: none"> Switches
	4.5 Given a scenario, modify enterprise capabilities to enhance security. <ul style="list-style-type: none"> Implementation of secure protocols <ul style="list-style-type: none"> Protocol selection Port selection Transport method
TestOut Security Pro	2.2 Harden Network Devices 2.2.1 Configure and access a switch




Video/Demo

 5.9.1 Switch Features	9:28
 5.9.2 Securing Network Switches	7:34
 5.9.4 Switch Attacks	11:09
 5.9.6 Hardening a Switch	<u>10:35</u>

Total Video Time

38:46

Lab/Activity

-  5.9.7 Harden a Switch
-  5.9.8 Secure Access to a Switch
-  5.9.9 Secure Access to a Switch 2

Fact Sheets

-  5.9.3 Switch Security Facts
-  5.9.5 Switch Attack Facts

Number of Exam Questions

10 questions

Copyright © 2023 TestOut Corporation. Copyright © The Computing Technology Industry Association, Inc. (CompTIA). All Rights Reserved. Reference to any specific product, service, process, or method by trade name, trademark, manufacturer or otherwise on this website is for educational purposes only and does not constitute an implied or expressed recommendation or endorsement by said third party. Neither TestOut nor CompTIA have any affiliation with any of these companies, and the products and services advertised herein are not endorsed by them.

Total Time
About 95 minutes

5.10: Router Security

Lecture Focus Questions:

- Why should you change the default settings on new routers?
- Which secure protocols should you use to remotely manage a router?
- What actions can you take 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:

- Configure ACLs.
- Restrict Telnet and SSH access.
- Permit traffic.
- Block source hosts.

The key terms for this section include:

Term	Definition
Router	A network device that transmits data from one network to another.
Access control list (ACL)	A list of permissions associated with a network object, such as a router or a switch, that controls traffic at a network interface level.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
CompTIA Security+ SY0-701	2.3 Explain various types of vulnerabilities. <ul style="list-style-type: none">• Hardware<ul style="list-style-type: none">◦ Firmware
	2.5 Explain the purpose of mitigation techniques used to secure the enterprise. <ul style="list-style-type: none">• Access control<ul style="list-style-type: none">◦ Access control list (ACL)◦ Permissions• Hardening techniques<ul style="list-style-type: none">◦ Disabling ports/protocols◦ Default password changes

3.2 Given a scenario, apply security principles to secure enterprise infrastructure.

- Secure communication/access
 - Remote access

4.1 Given a scenario, apply common security techniques to computing resources.

- Hardening targets
 - Routers

4.5 Given a scenario, modify enterprise capabilities to enhance security.

- Implementation of secure protocols
 - Protocol selection





5.1 Summarize elements of effective security governance.

- Standards
 - Access control


2.2 Harden Network Devices

2.2.5 Configure Router Security

TestOut Security Pro

Video/Demo	Time
 5.10.1 Router Security	7:00
 5.10.2 Router ACLs	2:45
 5.10.3 Router Security Facts	3:31
 5.10.4 Configuring ACLs	<u>7:09</u>
Total Video Time	20:25

Lab/Activity

-  5.10.5 Restrict Telnet and SSH Access
-  5.10.6 Permit Traffic
-  5.10.7 Block Source Hosts

Fact Sheets

-  5.10.3 Router Security Facts

Copyright © 2023 TestOut Corporation. Copyright © The Computing Technology Industry Association, Inc. (CompTIA). All Rights Reserved. Reference to any specific product, service, process, or method by trade name, trademark, manufacturer or otherwise on this website is for educational purposes only and does not constitute an implied or expressed recommendation or endorsement by said third party. Neither TestOut nor CompTIA have any affiliation with any of these companies, and the products and services advertised herein are not endorsed by them.

Number of Exam Questions

10 questions

Total Time

About 72 minutes

6.0: Resiliency and Site Security

6.1: Physical Threats

Lecture Focus Questions:

- What types of physical controls can be implemented to protect the perimeter of a building?
- How does an access control vestibule work?
- How are physical access controls similar to technical system security?
- How can environmental design enhance physical security?
- What are four types of sensors and how do they work?

In this section, you will learn to:

- Implement physical security.

The key terms for this section include:

Term	Definition
Physical security	Physical security is the protection of corporate assets from threats such as unauthorized entry, theft or damage.
Access list	A list of personnel who are authorized to enter a secure facility.
Access control vestibule	A specialized entrance with two locking doors that create a security buffer zone between two areas.
Bollard	Bollards are short, sturdy posts used to prevent a vehicle from crashing into a secure area.
Smart card	Access cards that have encrypted access information. Smart cards can be contactless or require contact.
Proximity card	Proximity cards, also known as radio frequency identification (RFID) cards, are a subset of smart cards that use the 125 kHz frequency to communicate with proximity readers.
Biometric Locks	Biometric locks increase security by using fingerprints or iris scans. They reduce the threat from lost keys or cards.
Sensor	A component in an alarm system that identifies unauthorized entry via infrared-, ultrasonic-, microwave-, or pressure-based detection of thermal changes or movement.
Radio frequency ID (RFID)	A means of encoding information into passive tags which can be energized and read by radio waves from a reader device.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
CompTIA Security+ SY0-701	<p>1.2 Summarize fundamental security concepts.</p> <ul style="list-style-type: none"> • Physical security <ul style="list-style-type: none"> ○ Bollards/barricades ○ Access control vestibule ○ Fencing ○ Video surveillance ○ Security guard ○ Access badge ○ Lighting ○ Sensors <ul style="list-style-type: none"> ▪ Infrared ▪ Pressure ▪ Microwave ▪ Ultrasound <p>2.4 Given a scenario, analyze indicators of malicious activity.</p> <ul style="list-style-type: none"> • Physical attacks <ul style="list-style-type: none"> ○ Brute force ○ Radio frequency identification (RFID) cloning ○ Environmental <p>3.4 Explain the importance of resilience and recovery in security architecture.</p> <ul style="list-style-type: none"> • Power <p>4.6 Given a scenario, implement and maintain identity and access management.</p> <ul style="list-style-type: none"> • Multifactor authentication <ul style="list-style-type: none"> ○ Biometrics
TestOut Security Pro	<p>2.1 Harden Physical Access</p> <p>2.1.1 Implement physical security</p>

Video/Demo

 6.1.1 Physical Security

Time

5:03

Total Video Time

5:03

Lab/Activity

- 🔑 6.1.3 Implement Physical Security

Fact Sheets

- 📄 6.1.2 Physical Security Facts

Number of Exam Questions

10 questions

Total Time

About 33 minutes

6.2: Monitoring and Reconnaissance

Lecture Focus Questions:

- What is the goal of network monitoring?
- What is the difference between passive and active reconnaissance?
- What tool is a search engine for internet-connected devices?
- What are common techniques used in active reconnaissance?

In this section, you will learn to:

- Perform port and ping scans.
- Perform reconnaissance with Nmap.

The key terms for this section include:

Term	Definition
IP scanners	Special tools that allow a network administrator to scan the entire network to find all connected devices and their IP addresses.
Reconnaissance	Also known as <i>footprinting</i> . This is the process of gathering information about a target before beginning any penetration test or security audit.
Active reconnaissance	The process of gathering information by interacting with the target in some manner.
Passive reconnaissance	The process of gathering information about a target with no direct interaction with the target.
Packet sniffing	The act of capturing data packets transmitted across the network and analyzing them for important information.
War driving	The act of driving around with a wireless device looking for open vulnerable wireless networks.
War flying	The act of using drones or unmanned aerial vehicles to find open wireless networks.
Eavesdropping	The act of covertly listening in on a communication between other people.
Open-Source Intelligence (OSINT)	Any data that is collected from publicly available sources such as social media, search engines, company websites, media sources, or public government sources.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
CompTIA Security+ SY0-701	2.2 Explain common threat vectors and attack surfaces.

- Unsecure networks
- Open service ports

2.5 Explain the purpose of mitigation techniques used to secure the enterprise.

- Monitoring

4.1 Given a scenario, apply common security techniques to computing resources.

- Monitoring

4.3 Explain various activities associated with vulnerability management.

- Identification methods
 - Open-source intelligence (OSINT)

4.4 Explain security alerting and monitoring concepts and tools.

- Monitoring computing resources
 - Systems
 - Infrastructure
 - Infrastructure
- Tools
 - Vulnerability scanners

4.5 Given a scenario, modify enterprise capabilities to enhance security.

- Firewall
 - Ports/protocols

4.9 Given a scenario, use data sources to support an investigation.

- Data sources
 - Packet captures

5.4 Summarize elements of effective security compliance.

- Compliance monitoring





5.5 Explain types and purposes of audits and assessments.

- Internal
 - Compliance
- Penetration testing
 - Reconnaissance
 - Passive
 - Active

2.2 Harden network devices

TestOut Security Pro

2.2.4 Harden a wireless network

Video/Demo	Time
 6.2.1 Network Monitoring	5:52
 6.2.3 Performing Port and Ping Scans	4:42
 6.2.4 Reconnaissance	6:27
 6.2.5 Perform Reconnaissance with Nmap	<u>4:10</u>
Total Video Time	21:11

Fact Sheets

-  6.2.2 Network Monitoring Facts
-  6.2.6 Reconnaissance Facts

Number of Exam Questions

10 questions

Total Time

About 42 minutes

6.3: Intrusion Detection

Lecture Focus Questions:

- What is the difference between an IDS and IPS?
- Which component gathers data from source devices?
- Why is a false negative the worst possible action by an IDS?
- Which detection method causes more false negatives?
- What is the difference between a host-based and network-based IDS/IPS implementation method?

In this section, you will learn to:

- Implement intrusion detection and prevention.

The key terms for this section include:

Term	Definition
Intrusion detection system (IDS)	Device or software that monitors, logs, and detects security breaches, but takes no action to stop or prevent the attack.
Intrusion prevention system (IPS)	Device that monitors, logs, detects, and can also react to stop or prevent security breaches.
Sensor	IDS component that passes data from the source to the analyzer.
Engine	IDS component that analyzes sensor data and events, generates alerts, and logs all activity.
Signature-based detection	Also referred to as pattern matching, dictionary recognition, or misuse-detection (MD-IDS). This detection method looks for patterns in network traffic and compares them to known attack patterns called signatures.
Heuristic-based detection	Also referred to as behavior, anomaly, or statistical-based detection. This detection method first defines a baseline of normal network traffic and then monitors traffic looking for anything that falls outside that baseline.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
CompTIA Security+ SY0-701	2.5 Explain the purpose of mitigation techniques used to secure the enterprise. <ul style="list-style-type: none">• Hardening techniques

- Host-based intrusion prevention system (HIPS)

3.2 Given a scenario, apply security principles to secure enterprise infrastructure.

- Infrastructure considerations
 - Device attribute
 - Inline vs. tap/monitor
 - Network appliances
 - Intrusion prevention system (IPS)/intrusion detection system (IDS)
 - Sensors

4.3 Explain various activities associated with vulnerability management.

- Analysis
 - False positive
 - False negative

4.5 Given a scenario, modify enterprise capabilities to enhance security.

- IDS/IPS
 - Trends
 - Signatures
- User behavior analytics

5.6 Given a scenario, implement security awareness practices.

- Anomalous behavior recognition
 - Unexpected

TestOut Security
Pro

5.2 Assessment techniques
5.2.1 Implement intrusion detection

Video/Demo

- 📺 6.3.1 Intrusion Detection
- 📺 6.3.3 Implement Intrusion Detection and Prevention

Time

4:53

6:13

Total Video Time

11:06

Lab/Activity

 6.3.4 Implement Intrusion Prevention

Fact Sheets

 6.3.2 IDS Facts

Number of Exam Questions

10 questions

Total Time

About 39 minutes

6.4: Protocol Analyzers

Lecture Focus Questions:

- What mode must a NIC be in to perform packet sniffing?
- What needs to be configured on a switch so all packets are sent to the sniffing device?
- Why would a network administrator need to use a protocol analyzer?

In this section, you will learn to:

- Analyze network traffic.

The key terms for this section include:

Term	Definition
Protocol analyzer	Hardware or software used for monitoring and analyzing digital traffic over a network. Protocol analyzers go by other names, such as packet sniffers, packet analyzers, network analyzers, network sniffers, or network scanners.
Promiscuous mode	A mode in which the NIC processes every frame it sees, not just those addressed to it.
Port mirroring	A switch mode in which all frames sent to all other switch ports will be forwarded on the mirrored port.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
	2.4 Given a scenario, analyze indicators of malicious activity. <ul style="list-style-type: none">• Network attacks<ul style="list-style-type: none">○ On-path○ Credential replay
CompTIA Security+ SY0-701	2.5 Explain the purpose of mitigation techniques used to secure the enterprise. <ul style="list-style-type: none">• Hardening techniques<ul style="list-style-type: none">○ Disabling ports/protocols
	4.1 Given a scenario, apply common security techniques to computing resources.

- Monitoring

4.5 Given a scenario, modify enterprise capabilities to enhance security.




- Firewall
 - Ports/protocols
- Implementation of secure protocols

4.9 Given a scenario, use data sources to support an investigation.

- Data sources
 - Packet captures

Video/Demo

Time

-  6.4.1 Protocol Analyzers
-  6.4.2 Protocol Analyzer Facts
-  6.4.3 Analyzing Network Traffic

3:39

5:41

6:46

Total Video Time

16:06

Fact Sheets

-  6.4.2 Protocol Analyzer Facts

Number of Exam Questions

10 questions

Total Time

About 32 minutes

6.5: Analyzing Network Attacks

Lecture Focus Questions:

- In which type of attack does the hacker place themselves between two devices to intercept communications?
- What are common indicators of a DDoS attack?
- What is the usual result of a distributed denial-of-service attack?
- What is a reflected DDoS attack?
- What are some indicators of a DNS attack?

In this section, you will learn to:

- Analyze ARP poisoning.
- Poison ARP and analyze with Wireshark.
- Analyze DNS poisoning.
- Poison DNS.
- Analyze SYN flood.
- Perform and analyze a SYN flood.
- Examine DNS attacks.







The key terms for this section include:

Term	Definition
On-path attack	An attack where the threat actor makes an independent connection between two victims and is able to read and possibly modify traffic.
Credential replay	An attack that uses a captured authentication token to start an unauthorized session without having to discover the plaintext password for an account.
Distributed reflected DoS (DRDoS)	A malicious request to a legitimate server is created and sent as a link to the victim, so that a server-side flaw causes the malicious component to run on the target's browser.
Amplification attack	A type of reflected attack that targets weaknesses in specific application protocols to make the attack more effective at consuming target bandwidth. Amplification attacks exploit protocols that allow the attacker to manipulate the request in such a way that the target is forced to respond with a large amount of data.
DNS poisoning	An attack where a threat actor injects false resource records into a client or server cache to redirect a domain name to an IP address of the attacker's choosing.
Distributed denial-of-service (DDoS)	An attack that involves the use of infected Internet-connected computers and devices to disrupt the normal flow of traffic of a server or service by overwhelming the target with traffic.




This section helps you prepare for the following certification exam objectives:

Copyright © 2023 TestOut Corporation. Copyright © The Computing Technology Industry Association, Inc. (CompTIA). All Rights Reserved. Reference to any specific product, service, process, or method by trade name, trademark, manufacturer or otherwise on this website is for educational purposes only and does not constitute an implied or expressed recommendation or endorsement by said third party. Neither TestOut nor CompTIA have any affiliation with any of these companies, and the products and services advertised herein are not endorsed by them.

Exam	Objective
<p>CompTIA Security+ SY0-701</p> <p>TestOut Security Pro</p>	<p>2.1 Compare and contrast common threat actors and motivations. 2.1.3 - Motivations 2.1.3.1 - Data exfiltration</p> <p>2.4 Given a scenario, analyze indicators of malicious activity.</p> <ul style="list-style-type: none"> • Network attacks <ul style="list-style-type: none"> ○ Distributed denial-of-service (DDoS) <ul style="list-style-type: none"> ▪ Amplified ▪ Reflected ○ Domain Name System (DNS) attacks ○ Wireless ○ On-path ○ Credential replay ○ Malicious code • Application attacks <ul style="list-style-type: none"> ○ Privilege escalation <p>4.7 Explain the importance of automation and orchestration related to secure operations.</p> <ul style="list-style-type: none"> • Use cases of automation and scripting <p>4.9 Given a scenario, use data sources to support an investigation.</p> <ul style="list-style-type: none"> • Data sources <ul style="list-style-type: none"> ○ Packet captures <p>5.5 Explain types and purposes of audits and assessments.</p> <ul style="list-style-type: none"> • Penetration testing <ul style="list-style-type: none"> ○ Reconnaissance <p>5.2 Assessment Techniques</p> <ul style="list-style-type: none"> • Analyze Network Attacks

Video/Demo	Time
 6.5.1 Analyzing Network Attacks	6:01
 6.5.3 Analyzing ARP Poisoning	5:05
 6.5.5 Analyzing DNS Poisoning	6:14
 6.5.7 Analyzing a SYN Flood	6:14
 6.5.9 Examining DNS Attacks	11:55
 6.5.10 Malicious Code	<u>7:02</u>
Total Video Time	42:31

Lab/Activity

-  6.5.4 Poison ARP and Analyze with Wireshark
-  6.5.6 Poison DNS
-  6.5.8 Analyze a SYN Flood Attack

Fact Sheets

-  6.5.2 Analyzing Network Attacks Facts
-  6.5.11 Malicious Code Facts

Number of Exam Questions

10 questions

Total Time

About 99 minutes

6.6: Analyzing Password Attacks

Lecture Focus Questions:

- Where would an attacker gather information to guess a user's password?
- What social engineering technique involves looking through trash?
- What does password spraying help the attacker avoid?
- What is the best defense against password-cracking attempts?
- What is the difference between an online and an offline password attack?

In this section, you will learn to:

- Crack a password using rainbow tables
- Crack a password with John the Ripper






The key terms for this section include:

Term	Definition
Online password attack	An attack where the threat actor interacts with the authentication service directly—a web login form or VPN gateway, for instance.
Offline attack	An attack where once the attacker has obtained a password database, the cracker does not interact with the authentication system.
Social engineering	An activity where the goal is to use deception and trickery to convince unsuspecting users to provide sensitive data or to violate security guidelines.
Shoulder surfing	An eavesdropping technique where the listener obtains passwords or other confidential information by looking over the shoulder of the target.
Brute force attack	A type of password attack where an attacker uses an application to exhaustively try every possible alphanumeric combination to crack encrypted passwords.
Password spraying	A brute force attack in which multiple user accounts are tested with a dictionary of common passwords.
Dictionary attack	A type of password attack that compares encrypted passwords against a predetermined list of possible password values.
Rainbow attack	Similar to dictionary attacks, however, a rainbow attack uses special tables called rainbow tables that have common passwords and the generated hash of each password.



This section helps you prepare for the following certification exam objectives:

Exam	Objective
------	-----------

CompTIA Security+ SY0-701	1.4 Explain the importance of using appropriate cryptographic solutions.
	<ul style="list-style-type: none"> • Hashing • Salting
	2.2 Explain common threat vectors and attack surfaces.
	<ul style="list-style-type: none"> • Default credentials • Human vectors/social engineering
	2.4 Given a scenario, analyze potential indicators of malicious activity. Password attacks
TestOut Security Pro	<ul style="list-style-type: none"> • Spraying • Dictionary • Brute force
	5.6 Given a scenario, implement security awareness practices.
	<ul style="list-style-type: none"> • User guidance and training <ul style="list-style-type: none"> ◦ Password management
	5.2 Assessment Techniques Analyze password attacks

Video/Demo	Time
 6.6.1 Password Attacks	7:23
 6.6.2 Password Attack Facts	8:07
 6.6.3 Using Rainbow Tables	3:28
 6.6.5 Crack Passwords	7:59
 6.6.6 Crack Password Protected Files	<u>3:18</u>
Total Video Time	30:15

Lab/Activity

-  6.6.4 Crack Password with Rainbow Tables
-  6.6.7 Crack a Password with John the Ripper

Fact Sheets

-  6.6.2 Password Attack Facts

Number of Exam Questions

10 questions

Total Time

About 70 minutes

7.0: Vulnerability Management

7.1: Vulnerability Management

Lecture Focus Questions:

- Why is vulnerability management critical to cybersecurity strategy?
- In what ways do legacy and end-of-life systems increase the risk of vulnerabilities?
- What factors should be considered when conducting a vulnerability analysis?
- Why is reporting crucial for vulnerability management?
- How do threat feeds help with vulnerability management?

In this section, you will learn to:

- Explore end-of-life software/hardware

The key terms for this section include:

Term	Definition
Vulnerability management	Identifying and managing the risks to a network, including the operating system, applications, and other components of an organization's IT operations.
Vulnerability scan	Utilizes automated scanning processes to identify and evaluate potential issues.
Threat feed	Real-time, continuously updated sources of information about potential threats and vulnerabilities.
Penetration testing	We pay you to hack into systems to make sure people can't hack into systems (a very off quote from Sneakers).

This section helps you prepare for the following certification exam objectives:

Exam	Objective
CompTIA Security+ SY0-701	1.1 Compare and contrast various types of security controls. <ul style="list-style-type: none">• Control types<ul style="list-style-type: none">◦ Compensating
	2.3 Explain various types of vulnerabilities. <ul style="list-style-type: none">• Operating system (OS)-based• Hardware

- Firmware
- End-of-life
- Legacy





4.3 Explain various activities associated with vulnerability management.

- Identification methods
 - Vulnerability scan
 - Threat feed
 - Open-source intelligence (OSINT)
 - Proprietary/third-party
 - Information-sharing organization
 - Dark web
 - Penetration testing
 - Responsible disclosure program
 - Bug bounty program
 - System/process audit
- Analysis
 - Confirmation
 - Prioritize
 - Common Vulnerability Scoring System (CVSS)
 - Common Vulnerability Enumeration (CVE)
 - Vulnerability classification
 - Exposure factor
 - Environmental variables
 - Industry/organizational impact
 - Risk tolerance
- Vulnerability response and remediation
 - Patching
 - Insurance
 - Segmentation
 - Compensating controls
 - Exceptions and exemptions
- Validation of remediation
 - Rescanning
 - Audit
 - Verification




4.4 Explain security alerting and monitoring concepts and tools.

- Tools

	<ul style="list-style-type: none"> ○ Vulnerability scanners
	4.8 Explain appropriate incident response activities.
	<ul style="list-style-type: none"> • Threat hunting
	4.9 Given a scenario, use data sources to support an investigation.
	<ul style="list-style-type: none"> • Data sources <ul style="list-style-type: none"> ○ Vulnerability scans
	3.1 Harden computer systems
	3.1.4 Configure Windows Update
TestOut Security Pro	5.2 Assessment techniques
	5.2.3 Scan for vulnerabilities

Video/Demo	Time
 7.1.1 Vulnerability Management	5:53
 7.1.3 Vulnerability Identification Methods Facts	5:55
 7.1.4 Vulnerability Analysis and Remediation	4:50
 7.1.6 Explore End of Life Software / Hardware	<u>2:59</u>
Total Video Time	19:37

Fact Sheets

-  7.1.2 Vulnerability Type Facts
-  7.1.3 Vulnerability Identification Methods Facts
-  7.1.5 Vulnerability Analysis and Remediation Facts

Number of Exam Questions

11 questions

Total Time

About 51 minutes

7.2: Vulnerability Scanning

Lecture Focus Questions:

- What is the purpose of vulnerability scanning?
- What information is critical in vulnerability scanning?
- What software is available to complete a vulnerability scan on a network?

In this section, you will learn to:

- Conduct vulnerability scans.
- Scan a network with Nessus.
- Scan a network with OpenVAS.
- Scan for cleartext vulnerabilities.
- Scan for FTP vulnerabilities.
- Scan for TLS vulnerabilities.
- Scan for Windows vulnerabilities.
- Scan for Linux vulnerabilities.
- Scan for domain controller vulnerabilities.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
CompTIA Security+ SY0-701	2.2 Explain common threat vectors and attack surfaces. <ul style="list-style-type: none">• Vulnerable software
	4.3 Explain various activities associated with vulnerability management. <ul style="list-style-type: none">• Identification methods<ul style="list-style-type: none">○ Vulnerability scan○ Application security<ul style="list-style-type: none">▪ Static analysis▪ Dynamic analysis▪ Package monitoring• Analysis<ul style="list-style-type: none">○ Common Vulnerability Enumeration (CVE)○ Vulnerability classification
	4.4 Explain security alerting and monitoring concepts and tools.

- Monitoring computing resources
 - Systems
 - Applications
 - Infrastructure
- Activities
 - Scanning
 - Reporting
- Tools
 - Vulnerability scanners

4.9 Given a scenario, use data sources to support an investigation.





- Data sources
 - Dashboards

5.2 Assessment techniques

TestOut Security Pro

5.2.3 Scan for vulnerabilities



Video/Demo

	Time
 7.2.1 Vulnerability Scanning	4:20
 7.2.2 Conduct Vulnerability Scans	3:58
 7.2.3 Scanning a Network with Nessus	3:14
 7.2.4 Scanning a Network with OpenVAS	<u>4:28</u>

Total Video Time

16:00

Lab/Activity

-  7.2.6 Scan for Cleartext Vulnerabilities
-  7.2.7 Scan for FTP Vulnerabilities
-  7.2.8 Scan for TLS Vulnerabilities
-  7.2.9 Scan for Windows Vulnerabilities
-  7.2.10 Scan for Linux Vulnerabilities
-  7.2.11 Scan for Domain Controller Vulnerabilities

Fact Sheets

-  7.2.5 Vulnerability Scanning Facts

Number of Exam Questions

10 questions

Total Time

About 103 minutes

7.3: Alerting and Monitoring

Lecture Focus Questions:

- What is the importance of monitoring a network?
- What tools are available to monitor a network for vulnerabilities?
- What role does SIEM play in network security?
- What is the risk of false positive alerts and alarms?

In this section, you will learn to:

- Analyze network traffic with Netflow.

The key terms for this section include:

Term	Definition
Network monitors	Collects data about network infrastructure appliances, such as switches, access points, routers, firewalls. This is used to monitor load status for CPU/memory, state tables, disk capacity, fan speeds/temperature, network link utilization/error statistics, and so on.
Netflow	A Cisco-developed means of reporting network flow information to a structured database.
System monitors	A system monitor implements the same functionality as a network monitor for a computer host. Like switches and routers, server hosts can report health status using SNMP traps.
System logs	Logs function both as an audit trail of actions and (if monitored regularly) provide a warning of intrusion attempts. Log review is a critical part of security assurance.
Vulnerability scanners	A vulnerability scanner will report the total number of unmitigated vulnerabilities for each host. Consolidating these results can show the status of hosts across the whole network and highlight issues with a particular patch or configuration issue.
Antivirus	Antivirus software detects malware by signature regardless of type, though detection rates can vary quite widely from product to product.
Data loss prevention	Data loss prevention (DLP) mediates the copying of tagged data to restrict it to authorized media and services.
Security information and event management (SIEM)	Software designed to manage security data inputs and provide reporting and alerting. The core function of a SIEM tool is to collect and correlate data from network sensors and appliance/host/application logs.

Reporting	A managerial control that provides insight into the security system's status.
Alert tuning	Correlation rules that reduce the incidence of false positive alerts and alarms.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
CompTIA Security+ SY0-701	<p>1.4 Explain the importance of using appropriate cryptographic solutions.</p> <ul style="list-style-type: none"> • Obfuscation <ul style="list-style-type: none"> ○ Tokenization ○ Data masking <p>2.5 Explain the purpose of mitigation techniques used to secure the enterprise.</p> <ul style="list-style-type: none"> • Monitoring <p>3.2 Given a scenario, apply security principles to secure enterprise infrastructure.</p> <ul style="list-style-type: none"> • Infrastructure considerations <ul style="list-style-type: none"> ○ Sensors <p>3.3 Compare and contrast concepts and strategies to protect data.</p> <ul style="list-style-type: none"> • General data considerations <ul style="list-style-type: none"> ○ Data at rest ○ Data in transit ○ Data in use • Methods to secure data • Encryption <ul style="list-style-type: none"> ○ Masking ○ Tokenization ○ Permission restrictions

4.1 Given a scenario, apply common security techniques to computing resources.

- Monitoring

4.3 Explain various activities associated with vulnerability management.

- Identification methods
 - Vulnerability scan

4.4 Explain security alerting and monitoring concepts and tools.

- Monitoring computing resources
 - Systems
 - Infrastructure
- Activities
 - Log aggregation
 - Alerting
 - Reporting
 - Archiving
 - Alert response and remediation/validation
 - Alert tuning
- Tools
 - Security Content Automation Protocol (SCAP)
 - Benchmarks
 - Agents/agentless
 - Security information and event management (SIEM)
 - Antivirus
 - Data loss prevention (DLP)
 - Simple Network Management Protocol (SNMP) traps
 - NetFlow
 - Vulnerability scanners

4.9 Given a scenario, use data sources to support an investigation.

- Log data
 - Firewall logs

- Endpoint logs
- OS-specific security logs
- IPS/IDS logs
- Network logs
- Data sources
 - Dashboards

5.1 Summarize elements of effective security governance.

- Procedures
 - Playbooks

5.6 Given a scenario, implement security awareness practices.

- Reporting and monitoring

3.1 Harden computer systems

3.1.2 Configure anti-virus protection

4.2 Implement Encryption Technologies






TestOut Security Pro

4.2.1 Encrypt data communications




4.2.2 Encrypt files

5.1 Implement logging and auditing

5.1.2 Enable device logs

Video/Demo	Time
 7.3.1 Alerting and Monitoring	4:23
 7.3.2 Alerting and Monitoring Facts	5:59
 7.3.3 SIEM and SOAR	4:30
 7.3.5 Analyze Network Traffic with Netflow	3:19
 7.3.6 Data Loss Prevention	<u>6:48</u>
Total Video Time	24:59

Fact Sheets

-  7.3.2 Alerting and Monitoring Facts
-  7.3.4 SIEM and SOAR Facts
-  7.3.7 DLP Facts

Number of Exam Questions

10 questions

Total Time

About 50 minutes

7.4: Penetration Testing

Lecture Focus Questions:

- What is the purpose of a penetration test?
- What are the different types of penetration tests?
- What is the role of the purple team?
- Which document defines what is included in the penetration test?
- What is the final phase in the penetration testing life cycle?

In this section, you will learn to:

- Explain the types of penetration testing tools.

The key terms for this section include:

Term	Definition
White box test	Penetration test in which the ethical hacker is given full knowledge of the target or network. This test allows for a comprehensive and thorough test, but is not very realistic.
Black box test	Penetration test in which the ethical hacker has no information regarding the target or network. This type of test best simulates an outside attack and ignores the insider threats.
Gray box test	Penetration test in which the ethical hacker is given partial information of the target or network, such as IP configurations, email lists, etc. This test simulates the insider threat.
Bug bounty	These unique tests are setup by organizations such as Google, Facebook, and others. Ethical hackers can receive compensation by reporting bugs and vulnerabilities they discover.
Scope of work	A very detailed document that defines exactly what is going to be included in the penetration test. This document is also referred to as the statement of work.
Rules of engagement	A document that defines exactly how the penetration test will be carried out.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
CompTIA Security+ SY0-701	2.2 Explain common threat vectors and attack surfaces. <ul style="list-style-type: none">• Human vectors/social engineering

4.3 Explain various activities associated with vulnerability management.

- Identification methods
 - Open-source intelligence (OSINT)
- Penetration testing
 - Bug bounty program

4.4 Explain security alerting and monitoring concepts and tools.

- Tools
 - Vulnerability scanners

5.3 Explain the processes associated with third-party risk assessment and management.

- Agreement types
 - Work order (WO)/statement of work (SOW)
- Rules of engagement

5.5 Explain types and purposes of audits and assessments.

- Penetration testing
 - Physical
 - Offensive
 - Defensive
 - Integrated
 - Known environment
 - Partially known environment
 - Unknown environment
 - Reconnaissance
 - Passive
 - Active

TestOut Security
Pro

5.2 Assessment techniques

5.2.3 Scan for vulnerabilities

Video/Demo

 7.4.1 Penetration Testing

Time

4:11

Copyright © 2023 TestOut Corporation. Copyright © The Computing Technology Industry Association, Inc. (CompTIA). All Rights Reserved. Reference to any specific product, service, process, or method by trade name, trademark, manufacturer or otherwise on this website is for educational purposes only and does not constitute an implied or expressed recommendation or endorsement by said third party. Neither TestOut nor CompTIA have any affiliation with any of these companies, and the products and services advertised herein are not endorsed by them.

🖥️ 7.4.4 Exploring Penetration Testing Tools
Total Video Time

11:29
15:40

Fact Sheets

- 📄 7.4.2 Penetration Testing Facts
- 📄 7.4.3 Penetration Testing Methods

Number of Exam Questions

10 questions

Total Time

About 36 minutes

8.0: Network and Endpoint Security

8.1: Operating 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 install only software that you need?
- What is a security baseline?
- What is the difference between a hotfix and a patch? Why would you use one instead of the other?

In this section, you will learn to:

- Harden an operating system.
- Manage automatic updates.
- Configure automatic updates.
- Configure Microsoft Defender Firewall.

The key terms for this section include:

Term	Definition
Patches	A small unit of supplemental code meant to address either a security problem or a functionality flaw in a software package or operating system.
Patch management	Identifying, testing, and deploying OS and application updates. Patches are often classified as critical, security-critical, recommended, and optional.
Allow list	A security configuration where access is denied to any entity (software process, IP/domain, and so on) unless the entity appears on an allow list, also known as a whitelist.
Block list	A security configuration where access is generally permitted to a software process, IP/domain, or other subject unless it is listed as explicitly prohibited.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
CompTIA Security+ SY0-701	1.4 Explain the importance of using appropriate cryptographic solutions <ul style="list-style-type: none">• Encryption

- Level
- Full-disk

2.2 Explain common threat vectors and attack surfaces

- Removable device

2.5 Explain the purpose of mitigation techniques used to secure the enterprise.

- Access control
- Application allow list
- Patching
- Encryption
- Monitoring
- Least privilege
- Configuration enforcement
- Decommissioning
- Hardening techniques
 - Installation of endpoint protection
 - Host-based firewall
 - Disabling ports/protocols
 - Default password changes
 - Removal of unnecessary software

4.1 Given a scenario, apply common security techniques to computing resources.

- Secure baselines
 - Establish
 - Deploy
 - Maintain
- Hardening targets
 - Workstations

4.3 Explain various activities associated with vulnerability management.

- Vulnerability response and remediation
 - Patching

4.5 Given a scenario, modify enterprise capabilities to enhance security.

- Operating system security
 - Group Policy

4.6 Given a scenario, implement and maintain identity and access management.

- Provisioning/de-provisioning user accounts
- Access controls
 - Least privilege
- Multifactor authentication

4.7 Explain the importance of automation and orchestration related to secure operations.

- Use cases of automation and scripting
 - Security groups

1.1 Manage identity

1.1.1 Manage Windows local and domain users and groups

1.2 Harden authentication

1.2.5 Configure and link Group Policy Objects (GPO)

2.1 Harden physical access

2.1.3 Install and configure a firewall

3.1 Harden computer systems





3.1.2 Configure anti-virus protection

3.1.4 Configure Windows Update



3.2 Implement application defenses

3.2.1 Implement an application allow list

TestOut Security Pro

Video/Demo	Time
 8.1.1 Operating System Hardening	7:54
 8.1.3 Hardening an Operating System	6:45
 8.1.4 Managing Automatic Updates	4:39
 8.1.6 Configure Microsoft Defender Firewall	<u>4:40</u>
Total Video Time	23:58

Lab/Activity

-  8.1.5 Configure Automatic Updates
-  8.1.7 Configure Microsoft Defender Firewall

Fact Sheets

-  8.1.2 Hardening Facts

Number of Exam Questions

10 questions

Total Time

About 63 minutes

8.2: File Server Security

Lecture Focus Questions:

- How can you identify inherited permissions?
- How do Share and NTFS permissions differ?
- On which elements can NTFS permissions be set?
- How can you view the users who have permissions for a particular drive?

In this section, you will learn to:

- Configure NTFS permissions.
- Disable inheritance.

Key terms for this section include the following:

Term	Definition
Shared folder	A folder whose contents are available over the network.
Network-attached storage (NAS)	A standalone storage device or appliance that acts as a file server.
Storage area network (SAN)	A special network composed of high-speed storage that is shared by multiple servers.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
CompTIA Security+ SY0-701	1.2 Summarize fundamental security concepts. <ul style="list-style-type: none">• Physical security
	1.4 Explain the importance of using appropriate cryptographic solutions. <ul style="list-style-type: none">• Encryption<ul style="list-style-type: none">◦ Level<ul style="list-style-type: none">▪ Full-disk▪ File
	2.2 Explain common threat vectors and attack surfaces. <ul style="list-style-type: none">• File-based

2.5 Explain the purpose of mitigation techniques used to secure the enterprise.

- Access control
 - Access control list (ACL)
 - Permissions
- Least privilege
- Hardening techniques
 - Removal of unnecessary software

3.2 Given a scenario, apply security principles to secure enterprise infrastructure.

- Secure communication/access
 - Virtual private network (VPN)
 - Tunneling
 - Internet protocol security (IPSec)

4.1 Given a scenario, apply common security techniques to computing resources.

- Hardening targets
- Servers

4.2 Explain the security implications of proper hardware, software, and data asset management.

- Acquisition/procurement process

4.3 Explain various activities associated with vulnerability management.



- Identification methods
 - System/process audit

4.5 Given a scenario, modify enterprise capabilities to enhance security.


- Implementation of secure protocols

	<ul style="list-style-type: none"> • File integrity monitoring
	4.6 Given a scenario, implement and maintain identity and access management.
	<ul style="list-style-type: none"> • Provisioning/de-provisioning user accounts • Access controls <ul style="list-style-type: none"> ◦ Least privilege
	3.1 Harden computer systems
TestOut Security Pro	3.1.1 Configure file system inheritance
	3.1.3 Configure NTFS permissions
	4.2 Implement Encryption Technologies
	4.2.2 Encrypt files



Video/Demo

 8.2.1 File Server Security	Time 6:35
 8.2.4 Configuring NTFS Permissions	<u>11:11</u>
Total Video Time	17:46

Lab/Activity

-  8.2.5 Configure NTFS Permissions
-  8.2.6 Disable Inheritance

Fact Sheets

-  8.2.2 File System Security Facts
-  8.2.3 File Permission Facts

Number of Exam Questions

10 questions

Total Time

About 62 minutes

8.3: Linux Host Security

Lecture Focus Questions:

- How do you check for unnecessary network services on a Linux system?
- Why is it important to identify open ports? What utility can identify open ports?
- Which utility can identify network statistics on a system?
- Which commands should you use to disable unneeded daemons?
- What are iptables?

In this section, you will learn to:

- Remove unnecessary services.
- Install and update iptables.

Key terms for this section include the following:

Term	Definition
iptables	iptables is a firewall command line utility for Linux operation systems that uses three policy chains to allow or block network traffic.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
CompTIA Security+ SY0-701	2.2 Explain common threat vectors and attack surfaces. <ul style="list-style-type: none">• Removable device
	2.5 Explain the purpose of mitigation techniques used to secure the enterprise. <ul style="list-style-type: none">• Patching• Hardening techniques<ul style="list-style-type: none">○ Host-based firewall○ Host-based intrusion prevention system (HIPS)○ Disabling ports/protocols○ Removal of unnecessary software
TestOut Security Pro	2.1 Harden physical access
	2.1.3 Install and configure a firewall

Video/Demo

Time

📺 8.3.1 Linux Host Security	14:08
📺 8.3.2 Removing Unnecessary Services	3:59
📺 8.3.4 Configure iptables	<u>3:59</u>

Total Video Time

22:06

Fact Sheets

- 📄 8.3.3 Linux Host Security Facts
- 📄 8.3.5 Configure iptables Facts

Number of Exam Questions

10 questions

Total Time

About 43 minutes

8.4: Wireless Overview

Lecture Focus Questions:

- Which device broadcasts information and data over radio waves?
- What are the two modes of wireless network configuration?
- Where is a Wireless LAN Controller (WLC) installed?

In this section, you will learn to:

- Configure a wireless connection.

The key terms for this section include:

Term	Definition
Service set identifier (SSID)	A unique name that identifies a wireless network.
Wireless access point (WAP)	A wireless access point broadcasts information and data over radio waves.
Wireless interface	The interface in a device, such as a laptop or smart phone, that connects to the wireless access point.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
CompTIA Security+ SY0-701	<p>4.1 Given a scenario, apply common security techniques to computing resources.</p> <ul style="list-style-type: none">• Wireless devices<ul style="list-style-type: none">○ Installation considerations<ul style="list-style-type: none">▪ Site surveys○ Heat maps• Wireless security settings<ul style="list-style-type: none">○ Wi-Fi Protected Access 3 (WPA3)○ AAA/Remote Authentication Dial-In User Service (RADIUS)
TestOut Security Pro	<p>2.2 Harden Network Devices</p> <p>2.2.2 Configure and Access a Wireless Network</p> <p>2.2.4 Harden a Wireless Network</p>

Video/Demo

Time

Copyright © 2023 TestOut Corporation. Copyright © The Computing Technology Industry Association, Inc. (CompTIA). All Rights Reserved. Reference to any specific product, service, process, or method by trade name, trademark, manufacturer or otherwise on this website is for educational purposes only and does not constitute an implied or expressed recommendation or endorsement by said third party. Neither TestOut nor CompTIA have any affiliation with any of these companies, and the products and services advertised herein are not endorsed by them.

8.4.1 Wireless Networking Overview	5:56
8.4.2 Wireless Installation	3:22
8.4.4 Configuring a Wireless Connection	<u>5:24</u>

Total Video Time

14:42

Lab/Activity

- 8.4.5 Configure a Wireless Network

Fact Sheets

- 8.4.3 Wireless Networking Facts

Number of Exam Questions

10 questions

Total Time

About 42 minutes

8.5: Wireless Attacks

Lecture Focus Questions:

- What is the difference between bluejacking and bluesnarfing?
- What is an initialization vector used for?
- How can you discover rogue access points?
- What is the difference between passive and active radio frequency identification (RFID) tags?

In this section, you will learn to:

- Detect rogue hosts.
- Configure rogue host protection.

The key terms for this section include:

Term	Definition
Rogue access points	Any unauthorized access point added to a network.
Initialization vector (IV)	A seed value used in encryption. The seed value and the key are used in an encryption algorithm to generate additional keys or encrypt data.
Radio frequency identification (RFID)	RFID uses radio waves to transmit data from small circuit boards called RFID tags to special scanners.
Near Field Communication (NFC)	NFC allows two-way communication between two devices. The devices must be within a few centimeters of each other. NFC is a newer technology built on RFID.
Interference	A signal that corrupts or destroys a wireless signal. Interference can affect communication of access points and other wireless devices.
Evil twin	A wireless access point that deceives users into believing that it is a legitimate network access point.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
CompTIA Security+ SY0-701	2.2 Explain common threat vectors and attack surfaces. <ul style="list-style-type: none">• Unsecure networks<ul style="list-style-type: none">○ Wireless○ Bluetooth
	2.4 Given a scenario, analyze indicators of malicious activity.

- Physical attacks
 - Radio frequency identification (RFID) cloning
- Network attacks
- Wireless
 - Credential replay

4.1 Given a scenario, apply common security techniques to computing resources

- Wireless devices
 - Installation considerations
- Wireless security settings
 - Wi-Fi Protected Access 3 (WPA3)
 - Authentication protocols



2.2 Harden network devices

TestOut Security Pro

2.2.2 Configure and access a wireless network

2.2.4 Harden a wireless network

Video/Demo

-  8.5.1 Wireless Attacks
-  8.5.3 Detecting Rogue Hosts

Total Video Time

Time

7:35

3:42

11:17

Lab/Activity

-  8.5.4 Configure Rogue Host Protection

Fact Sheets

-  8.5.2 Wireless Attack Facts

Number of Exam Questions

10 questions

Total Time

About 39 minutes

8.6: Wireless Defenses

Lecture Focus Questions:

- Which settings in a wireless access point can you configure to improve security?
- Which cryptographic protocol uses a Remote Authentication Dial-In User Service (RADIUS) server?
- Which access method forces a user to view and interact with it before accessing a network?
- What are the three components in an 802.1x setup?
- Which EAP standard is considered to be one of the most secure?

In this section, you will learn to:

- Harden a wireless network.
- Configure a wireless intrusion prevention system.

The key terms for this section include:

Term	Definition
Wi-Fi Protected Access (WPA)	The most commonly used cryptographic protocol in use for wireless networks. WPA2 and WPA3 are the two versions in use.
Pre-shared key (PSK)	Wireless access method that utilizes a passphrase for users to connect.
Wi-Fi Protected Setup (WPS)	Wireless access method that allows a device to securely connect to a wireless network without typing the PSK.
Open network	Wireless access method that has no authentication.
Captive portal	Wireless access method that forces a user to view and interact with it before accessing a network.
802.1x	Standard for local area networks that is used to authenticate users to a wireless network. It was created by The Institute of Electrical and Electronics Engineers Standards Association (IEEE-SA).
Remote Authentication Dial-In User Service (RADIUS)	A protocol used to authenticate users in a enterprise environment to a wireless network.
Extensible Authentication Protocol (EAP)	An authentication framework that uses a set of interface standards. EAP allows various authentication methods to be used.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
------	-----------

2.2 Explain common threat vectors and attack surfaces.

- Unsecure networks
 - Wireless
- Default credentials

2.3 Explain various types of vulnerabilities.

- Hardware
 - Firmware

2.5 Explain the purpose of mitigation techniques used to secure the enterprise.

- Hardening techniques
 - Default password changes

CompTIA Security+
SY0-701




3.2 Given a scenario, apply security principles to secure enterprise infrastructure.

- Infrastructure considerations
 - Network appliances
 - Intrusion prevention system (IPS)/intrusion detection system (IDS)
 - Port security
 - 802.1X
 - Extensible Authentication Protocol (EAP)
- Secure communication/access
 - Tunneling
 - Transport Layer Security (TLS)



4.1 Given a scenario, apply common security techniques to computing resources.

- Wireless devices
 - Installation considerations
- Wireless security settings
 - Wi-Fi Protected Access 3 (WPA3)
 - Cryptographic protocols

TestOut Security Pro	<ul style="list-style-type: none"> ○ AAA/Remote Authentication Dial-In User Service (RADIUS) ○ Authentication protocols
	2.2 Harden Network Devices
	2.2.2 Configure and Access a Wireless Network
	2.2.4 Harden a Wireless Network

Video/Demo	Time
 8.6.1 Wireless Security	6:19
 8.6.3 Wireless Authentication and Access Methods	7:32
 8.6.5 Hardening a Wireless Access Point	<u>7:46</u>
Total Video Time	21:37

Lab/Activity

-  8.6.6 Harden a Wireless Network
-  8.6.7 Configure WIPS

Fact Sheets

-  8.6.2 Wireless Security Facts
-  8.6.4 Wireless Authentication and Access Methods Facts

Number of Exam Questions

11 questions

Total Time

About 72 minutes

8.7: 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 TLS to a website
- Allow SSL connections
- Require IPsec for communications

The key terms for this section include:

Term	Definition
Secure Sockets Layer (SSL)	A protocol that secures messages being transmitted on the internet.
Transport Layer Security (TLS)	A protocol that secures messages being transmitted on the internet. It is the successor to SSL 3.0.
Secure Shell (SSH)	A protocol that allows for secure interactive control of remote systems.
Hyper Text Transfer Protocol Secure (HTTPS)	A secure form of HTTP that uses either SSL or TLS to encrypt sensitive data before it is transmitted.
Secure Hypertext Transfer Protocol (S-HTTP)	An alternate protocol that is not widely used because it is not as secure as HTTPS.
Internet Protocol Security (IPsec)	A set of protocols that provides secure data transmission over unprotected TCP/IP networks.
Authentication Header (AH)	A protocol within IPsec that provides authenticity, non-repudiation, and integrity.
Encapsulating Security Payload (ESP)	A protocol within IPsec that provides all the security of AH plus confidentiality.
Security Association (SA)	The establishment of shared security information between two network entities to support secure communications.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
------	-----------

1.4 Explain the importance of using appropriate cryptographic solutions.

- Encryption
 - Transport/communication
 - Asymmetric
 - Key exchange
- Certificates
 - Certificate authorities

2.4 Given a scenario, analyze indicators of malicious activity.

CompTIA Security+
SY0-701

- Network attacks
 - Domain Name System (DNS) attacks

3.2 Given a scenario, apply security principles to secure enterprise infrastructure.

- Secure communication/access
 - Virtual private network (VPN)
 - Remote access
 - Tunneling
 - Transport Layer Security (TLS)
 - Internet Protocol Security (IPSec)

3.2 Implement application defenses




3.2.3 Configure web application security

TestOut Security Pro

4.2 Implement Encryption Technologies

4.2.1 Encrypt data communications

Video/Demo

	Time
 8.7.1 Secure Protocols	7:42
 8.7.3 Add TLS to a Website	7:22
 8.7.5 IPsec	6:04
 8.7.7 Requiring IPsec for Communications	<u>10:55</u>

Total Video Time

32:03

Lab/Activity

- 🔒 8.7.4 Allow SSL Connections

Fact Sheets

- 📄 8.7.2 Secure Protocol Facts
- 📄 8.7.6 IPsec Facts

Number of Exam Questions

11 questions

Total Time

About 71 minutes

8.8: Web Application Security

Lecture Focus Questions:

- What are the common forms of web application attacks?
- How do you mitigate replay attacks?
- What are some methods to prevent driver manipulation?
- How does SSL stripping work?

In this section, you will learn to:

- Clear the browser cache.
- Prevent cross-site scripting.
- Exploit SQL on a webpage.
- Perform an SQL injection attack.

The key terms for this section include:

Term	Definition
Privilege escalation	The exploitation of a misconfiguration, a bug, or design flaw to gain unauthorized access to resources.
Pointer/object dereferencing	An attack that retrieves a value stored in memory that can be exploited through a NULL pointer dereference.
Buffer overflow	An attack that exploits an operating system or an application that does not properly enforce boundaries for inputting data such as the amount of data or the type of data.
Resource exhaustion	An attack that focuses on depleting the resources of a network to create a denial-of-service to legitimate users.
Memory leak	A leak that happens when dynamic memory is allocated in a program, but no pointers are connected to it causing it to never be returned when requested.
Race conditions	A sequence of events with dependencies that a system is programmed to run in a certain order which can lead to a time-of-check to time-of-use bug vulnerability.
Error handling	The procedures in a program that respond to irregular input or conditions.
Improper input handling	The lack of validation, sanitization, filtering, decoding, or encoding of input data.
Replay attack	An attack that happens when network traffic is intercepted by an unauthorized person who then delays or replays the communication to its original receiver, acting as the original sender. The original sender is unaware of this occurrence.

Pass the hash	An attack in which an attacker obtains a hashed password and uses it to gain unauthorized access.
API attacks	A malicious use of an API (application programming interface).
SSL stripping	An attack that focuses on stripping the security from HTTPS-enabled websites.
Driver manipulation	An attack that focuses on device drivers. The attack uses refactoring or shimming.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
CompTIA Security+ SY0-701	<p>2.3 Explain various types of vulnerabilities.</p> <ul style="list-style-type: none"> • Application <ul style="list-style-type: none"> ○ Memory injection ○ Buffer overflow ○ Race conditions <ul style="list-style-type: none"> ▪ Time-of-check (TOC) ▪ Time-of-use (TOU) ○ Malicious update • Web-based <ul style="list-style-type: none"> ○ Structured Query Language injection (SQLi) ○ Cross-site scripting (XSS) • Hardware • Zero-day
	<p>2.4 Given a scenario, analyze indicators of malicious activity.</p> <ul style="list-style-type: none"> • Application attacks • Injection • Buffer overflow • Replay • Privilege escalation • Directory traversal <p>2.5 Explain the purpose of mitigation techniques used to secure the enterprise.</p> <ul style="list-style-type: none"> • Patching

3.2 Given a scenario, apply security principles to secure enterprise infrastructure.

- Infrastructure considerations
 - Intrusion prevention system (IPS)/intrusion detection system (IDS)

4.1 Given a scenario, apply common security techniques to computing resources.

- Application security
 - Secure cookies








4.6 Given a scenario, implement and maintain identity and access management.

- Single sign-on (SSO)
 - Lightweight Directory Access Protocol (LDAP)

3.2 Implement application defenses

TestOut Security Pro

3.2.3 Configure web application security
3.2.5 Configure browser settings

Video/Demo	Time
 8.8.1 Web Application Attacks	3:50
 8.8.2 XSS and CSRF Attacks	9:37
 8.8.3 Injection Attacks	3:57
 8.8.4 Zero Day Application Attacks	3:15
 8.8.7 Preventing Cross-Site Scripting	2:41
 8.8.8 SQL Injections	5:49
 8.8.9 Exploit SQL on a Web Page	<u>3:54</u>
Total Video Time	33:03

Lab/Activity

- 🔗 8.8.6 Clear the Browser Cache
- 🔗 8.8.11 Perform an SQL Injection Attack

Fact Sheets

Copyright © 2023 TestOut Corporation. Copyright © The Computing Technology Industry Association, Inc. (CompTIA). All Rights Reserved. Reference to any specific product, service, process, or method by trade name, trademark, manufacturer or otherwise on this website is for educational purposes only and does not constitute an implied or expressed recommendation or endorsement by said third party. Neither TestOut nor CompTIA have any affiliation with any of these companies, and the products and services advertised herein are not endorsed by them.

- ☰ 8.8.5 Web Browser Security Facts
- ☰ 8.8.10 Web Application Attack Facts

Number of Exam Questions

10 questions

Total Time

About 78 minutes

8.9: Application Development and Security

Lecture Focus Questions:

- What are two common standardized software development models?
- How should security be implemented in the different stages of development?
- What are the responsibilities of developers after a product is released?
- What are some important application hardening techniques?

In this section, you will learn to:

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

The key terms for this section include:

Term	Definition
Normalization	Data reorganized in a relational database to eliminate redundancy by having all data stored in one place and storing all related items together.
Stored procedures	One or more database statements stored as a group in a database's data dictionary, which when called, executes all the statements in the collection.
Code obfuscation	The deliberate act of creating source or machine code that is difficult for humans to understand. In other words, the code is camouflaged.
Code reuse	Using the same code multiple times.
Dead code	Code that is non-executable at run-time, or source code in a program that is executed but is not used in any other computation.
Memory management	A resource management process applied to computer memory. It allows your computer system to assign portions of memory, called blocks, to various running programs to optimize overall system performance.
Third-party libraries	A library where the code is not maintained in-house.
Software Development Kits (SDKs)	A set of software development tools that can be installed as one unit.
Data exposure	Unintended exposure of personal and confidential data.
Fuzz testing	A software testing technique that exposes security problems by providing invalid, unexpected, or random data to the inputs of an application.

Code signing	The process of digitally signing (encrypting) executables and scripts to confirm the software author and guarantee that the code has not been altered or corrupted since it was signed.
--------------	---

This section helps you prepare for the following certification exam objectives:

Exam	Objective
CompTIA Security+ SY0-701	1.3 Explain the importance of change management processes and the impact to security. <ul style="list-style-type: none"> • Version control
	2.2 Explain common threat vectors and attack surfaces. <ul style="list-style-type: none"> • Unsupported systems and applications
	2.5 Explain the purpose of mitigation techniques used to secure the enterprise. <ul style="list-style-type: none"> • Application allow list • Patching • Monitoring • Hardening techniques <ul style="list-style-type: none"> ○ Installation of endpoint protection ○ Host-based firewall ○ Removal of unnecessary software
	3.3 Compare and contrast concepts and strategies to protect data. <ul style="list-style-type: none"> • Methods to secure data <ul style="list-style-type: none"> ○ Obfuscation
	4.1 Given a scenario, apply common security techniques to computing resources. <ul style="list-style-type: none"> • Secure baselines <ul style="list-style-type: none"> ○ Establish • Application security <ul style="list-style-type: none"> ○ Input validation ○ Secure cookies

- Static code analysis
- Code signing
- Sandboxing

4.3 Explain various activities associated with vulnerability management.

- Identification methods
 - Application security
 - Static analysis
 - Dynamic analysis

4.5 Given a scenario, modify enterprise capabilities to enhance security.

- Operating system security
 - SELinux

4.6 Given a scenario, implement and maintain identity and access management.

- Provisioning/de-provisioning user accounts
- Access controls
 - Least privilege

4.7 Explain the importance of automation and orchestration related to secure operations.

- Use cases of automation and scripting
 - User provisioning
 - Resource provisioning
 - Security groups
 - Ticket creation
 - Enabling/disabling services and access
 - Integrations and Application programming interfaces (APIs)
- Benefits
 - Efficiency/time saving
 - Enforcing baselines
 - Staff retention
- Other considerations

- Complexity
- Cost
- Single point of failure
- Technical debt
- Ongoing supportability

5.1 Summarize elements of effective security governance.

- Policies
 - Software development lifecycle (SDLC)

5.2 Explain elements of the risk management process.







- Risk analysis
 - Exposure factor

3.2 Implement application defenses

3.2.1 Implement an application allow list

TestOut Security
Pro



Video/Demo

	Time
 8.9.1 Development Life Cycle	6:30
 8.9.2 Automation and Scripting	4:58
 8.9.4 Version Control Management	3:03
 8.9.6 Hardening Applications on Linux	4:28
 8.9.7 Implementing Application Whitelisting with AppLocker	8:10
 8.9.9 Implementing Data Execution Preventions	<u>2:35</u>




Total Video Time

29:44

Lab/Activity

-  8.9.8 Implement Application Whitelisting with AppLocker
-  8.9.10 Implement Data Execution Preventions

Fact Sheets

-  8.9.3 SDLC and Development Facts
-  8.9.5 Application Development Security Facts
-  8.9.11 Hardening Applications Facts

Number of Exam Questions

Copyright © 2023 TestOut Corporation. Copyright © The Computing Technology Industry Association, Inc. (CompTIA). All Rights Reserved. Reference to any specific product, service, process, or method by trade name, trademark, manufacturer or otherwise on this website is for educational purposes only and does not constitute an implied or expressed recommendation or endorsement by said third party. Neither TestOut nor CompTIA have any affiliation with any of these companies, and the products and services advertised herein are not endorsed by them.

10 questions

Total Time

About 79 minutes

9.0: Incident Response

9.1: Incident Response and Mitigation

Lecture Focus Questions:

- Why is the chain of custody so important in a forensic investigation?
- How do you ensure the integrity of collected digital evidence?
- When conducting a forensic investigation, what methods can you use to save the contents of memory?
- What would a computer forensic investigator analyze when conducting a live analysis compared to a dead analysis?
- What actions should you take when an incident occurs?

Key terms for this section include the following:

Term	Definition
Security incident	An event, or series of events, resulting from a security policy violation. A security incident has adverse effects on a company's ability to proceed with normal business.
Incident response	The action taken to deal with an incident, both during and after the incident.
First responder	The first person on the scene after a security incident has occurred.
Damage assessment	A preliminary onsite evaluation of damage or loss caused by a security incident.
Live analysis	An incident investigation that examines an active (running) computer system to analyze the live network connection, memory contents, and running programs.
Dead analysis	An incident investigation that examines data at rest, such as analyzing hard drive contents.
Big data analysis	An incident investigation that examines all types of data used in the organization, including text, audio, video, and log files. The investigation identifies anomalies that led up to the security incident.
Corroborative evidence	Evidence or information that supports another fact or detail.
Hearsay evidence	Evidence that is obtained from a source who doesn't have personal, firsthand knowledge.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
------	-----------

2.5 Explain the purpose of mitigation techniques used to secure the enterprise.

- Segmentation
- Isolation

4.8 Explain appropriate incident response activities.

CompTIA Security+
SY0-701

- Process
 - Preparation
 - Detection
 - Analysis
 - Containment
 - Eradication
 - Recovery
 - Lessons learned

5.1 Summarize elements of effective security governance.

- Procedures
 - Playbooks

5.2 Assessment techniques

TestOut Security Pro

5.2.4 Analyze network attacks
5.2.5 Analyze password attacks

Video/Demo

- 📺 9.1.1 Incident Response Process
- 📺 9.1.3 Isolate and Contain

Total Video Time

Time

3:39

2:58

6:37

Fact Sheets

- 📄 9.1.2 Incident Response Process Facts
- 📄 9.1.4 Isolate and Contain Facts

Number of Exam Questions

11 questions

Total Time
About 33 minutes

9.2: Log Management

Lecture Focus Questions:

- What does a security information and event management (SIEM) system do?
- Why are trends important for network management?
- What part does event correlation play in a SIEM?
- How do IT security teams use alerts?

In this section, you will learn to:

- Save captured files with Wireshark.
- Use Elasticsearch, Logstash, Kibana.
- Use NetworkMiner
- Configure remote logging on Linux
- Log events on pfSense.

Key terms for this section include the following:

Term	Definition
SIEM	A software tool used to compile and examine multiple data points gathered from across a network.
Sensor	A device that gathers data from a device or system. It provides the collected data to a monitoring system.
Trend	Patterns of activity discovered and reported to the SIEM.
Sensitivity	Customized threshold for sensor data that is sent to the SIEM.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
	2.5 Explain the purpose of mitigation techniques used to secure the enterprise. <ul style="list-style-type: none">• Monitoring
CompTIA Security+ SY0-701	3.2 Given a scenario, apply security principles to secure enterprise infrastructure. <ul style="list-style-type: none">• Infrastructure considerations<ul style="list-style-type: none">○ Intrusion prevention system (IPS)/intrusion detection system (IDS)○ Sensors

4.1 Given a scenario, apply common security techniques to computing resources.

- Secure baselines
 - Establish

4.3 Explain various activities associated with vulnerability management.

- Identification methods
 - Vulnerability scan
- Analysis
 - Common Vulnerability Enumeration (CVE)


4.4 Explain security alerting and monitoring concepts and tools.

- Activities
 - Log aggregation
 - Alerting
- Tools
 - Security information and event management (SIEM)
 - NetFlow
 - Vulnerability scanners

4.9 Given a scenario, use data sources to support an investigation.

- Log data
 - Firewall logs
 - Application logs
 - Endpoint logs
 - OS-specific security logs
 - IPS/IDS logs
 - Network logs
 - Metadata
- Data sources
 - Dashboards
 - Packet captures

	5.1 Implement Logging and Auditing
	5.1.2 Enable Device Logs
TestOut Security Pro	5.2 Assessment techniques
	5.2.1 Implement intrusion detection
	5.2.3 Scan for vulnerabilities

Video/Demo	Time
 9.2.1 Security Information and Event Management	3:31
 9.2.2 Log Management	6:46
 9.2.4 Monitoring Data and Metadata	6:05
 9.2.5 Saving Captured Files with Wireshark	3:49
 9.2.6 Use Elasticsearch Logstash Kibana	4:40
 9.2.7 Use NetworkMiner	3:35
 9.2.8 Configuring Remote Logging on Linux	6:27
 9.2.9 Logging Events on pfSense	<u>5:57</u>
Total Video Time	40:50

Fact Sheets

-  9.2.3 SIEM and Log Management Facts
-  9.2.10 Monitoring Data and Metadata Facts

Number of Exam Questions

10 questions

Total Time

About 61 minutes

9.3: Digital Forensics

Lecture Focus Questions:

- Why is a chain of custody important in an investigation?
- What importance does a provable timeline of events play in admissibility of digital forensic evidence?
- Why is it important to take a bit-by-bit copy of the logs?
- How does the order of volatility help you decide what to secure and preserve first?
- What is a digital forensic artifact?
- How does provenance play a vital role in digital forensics?

In this section, you will learn to:

- Create a forensic drive image with FTK, Guymager, and DC3DD.
- Examine a forensic drive image with Autopsy.

The key terms for this section include:

Term	Definition
Legal hold	A process designed to preserve all relevant information when litigation is reasonably expected to occur. A formal notice sent out to all employees of a company when litigation is eminent. The notice instructs all employees to retain electronically stored information (ESI).
Chain of custody	A record of the handling of gathered evidence. This gives all parties involved confidence that no evidence tampering has occurred.
Hashing	A function that converts an arbitrary-length string input to a fixed-length string output.
Provenance	Provenance demonstrates that the digital evidence gathered came from the documented source of evidence and that it has not been tampered with.










This section helps you prepare for the following certification exam objectives:

Exam	Objective
	4.8 Explain appropriate incident response activities.
CompTIA Security+ SY0-701	<ul style="list-style-type: none">• Digital forensics<ul style="list-style-type: none">○ Legal hold○ Chain of custody○ Acquisition○ Reporting○ Preservation

- E-discovery

4.9 Given a scenario, use data sources to support an investigation.

- Data sources
 - Vulnerability scans
 - Dashboards
 - Packet captures

Video/Demo	Time
 9.3.1 Forensic Documentation and Evidence	3:27
 9.3.2 Forensic Acquisition of Data	5:39
 9.3.3 Forensic Tools	2:22
 9.3.4 Create a Forensic Drive Image with FTK	7:23
 9.3.5 Create a Forensic Drive Image with Guymager	5:24
 9.3.6 Create a Forensic Drive Image with DC3DD	6:00
 9.3.7 Examine a Forensic Drive Image with Autopsy	6:10
 9.3.8 Forensic Data Integrity and Preservation	4:17
 9.3.9 Forensic Investigation Facts	<u>5:36</u>
Total Video Time	46:18

Fact Sheets

-  9.3.9 Forensic Investigation Facts

Number of Exam Questions

10 questions

Total Time

About 62 minutes

9.4: Redundancy

Lecture Focus Questions:

- Why is redundancy important to network security?
- Why would an organization use geographic dispersal?
- What are the levels of RAID and when would you use each level?
- Why would a system administrator want to use load balancers?
- What is an uninterruptible power supply used for?
- What is the difference between active/active and active/passive?
- What is the main advantage of RAID 0? Disadvantage?
- What is the difference between RAID 0+1 and RAID 1+0?

Key terms for this section include the following:

Term	Definition
Fault tolerance	The ability to respond to an unexpected hardware or software failure without loss of data or loss of operation.
Redundancy	A method for providing fault tolerance by using duplicate or multiple components that perform the same function.
Geographic dispersion	Using multiple locations to store data to mitigate downtime due to loss of availability at a location.
Multipath	A fault-tolerance technique that gives multiple physical paths between a CPU and a mass-storage appliance.
Load balancers	A process that distributes processing among multiple nodes.
Uninterruptible power supply (UPS)	A stand-alone power supply that allows servers to be gracefully shutdown during a power outage.
Virtual machine (VM)	A computer that uses software components, but acts like a physical machine. A virtual machine resides on a host machine.
Active/active	Two load balancers working in tandem to distribute network traffic.
Active/passive	Two load balancers with one actively working and the second in listening mode to take over if the active machine fails.
Virtual IP	An IP address that can be used by multiple endpoints. It is commonly used in failover systems and for load balancing.
Storage area network (SAN)	A dedicated, high speed network of storage devices. Usually used for file shares.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
------	-----------

3.1 Compare and contrast security implications of different architecture models.

- Architecture and infrastructure concepts
 - Cloud
 - Third-party vendors
 - Network infrastructure
 - High availability
- Considerations
 - Power

3.2 Given a scenario, apply security principles to secure enterprise infrastructure.

CompTIA Security+
SY0-701

- Infrastructure considerations
- Device attribute
 - Active vs. passive
- Load balancer

3.4 Explain the importance of resilience and recovery in security architecture.

- High availability
 - Load balancing vs. clustering
- Site considerations
 - Geographic dispersion
- Power
 - Generators
 - Uninterruptible power supply (UPS)

5.3 Explain the processes associated with third-party risk assessment and management.

- Vendor selection

4.1 Protect and Maintain Data files

TestOut Security Pro

4.1.2 Implement redundancy

Video/Demo

- ▶ 9.4.1 Redundancy
- ▶ 9.4.3 Hardware Clustering

Total Video Time

Time

5:37

7:48

13:25

Fact Sheets

- 📄 9.4.2 Redundancy Facts
- 📄 9.4.4 Clustering Facts

Number of Exam Questions

11 questions

Total Time

About 40 minutes

9.5: Backup and Restore

Lecture Focus Questions:

- Why are there different backup types?
- How often should you run a full backup?
- How do incremental and differential backups differ?
- How can you implement the 3-2-1 rule?
- What are the differences between network attached storage (NAS) and storage attached network (SAN)?

In this section, you will learn to:

- Configure network attached storage.
- Implement file backups.
- Back up files with file history.
- Recover a file from file history.
- Backup a domain controller.
- Restore server data from a backup.







Key terms for this section include the following:

Term	Definition
Full backup	A back up that captures all of the data on a machine. A full backup is always the first backup you should run.
Incremental backup	A backup that contains all changes since the last incremental backup.
Differential backup	A backup that contains all changes since the last full backup.
Snapshot	An instant copy of an individual computer. Snapshots are normally used on virtual machines (VMs) when changes may need to be reverted.
NAS	A network storage appliance often used to store backups or other files.
SAN	A network of fast storage appliances. A SAN stores file shares and other data that needs to be accessed quickly.
Offsite storage	A location where files are stored that is away from the physical office space where the data is created. Offsite storage is part of 3-2-1 rule.
Scalability	The ability to increase or decrease data storage space.
Restoration order	Pre-planned order in which servers will be restored following a disastrous event. The order is determined by the server's importance to the company's operation.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
CompTIA Security+ SY0-701	<p>3.4 Explain the importance of resilience and recovery in security architecture.</p> <ul style="list-style-type: none"> • Backups <ul style="list-style-type: none"> ○ Onsite/offsite ○ Frequency ○ Encryption ○ Snapshots ○ Recovery ○ Replication ○ Journaling
TestOut Security Pro	<p>4.0 Data Security</p> <p>4.1 Protect and Maintain Data files</p> <p>4.1.1 Perform data backups and recovery</p>




Video/Demo

	Time
 9.5.1 Backup Types	10:12
 9.5.2 Backup Storage Options	4:58
 9.5.4 Configure Network Attached Storage	5:11
 9.5.5 Implementing File Backups	2:44
 9.5.8 Backup a Domain Controller	2:39
 9.5.9 Restoring Server Data from Backup	<u>2:43</u>

Total Video Time

28:27

Lab/Activity

-  9.5.6 Back Up Files with File History
-  9.5.7 Recover a File from File History
-  9.5.10 Backup a Domain Controller

Fact Sheets

-  9.5.3 Backup Types and Storage Facts

Number of Exam Questions

10 questions

Total Time

About 80 minutes

10.0: Protocol, App, and Cloud Security

10.1: 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?
- How do you secure a container?

In this section, you will learn to:

- Use VMWare Player.
- Use Hyper-V.
- Create virtual machines.
- Use Windows Sandbox.
- Create containers.
- Secure containers.

Key terms for this section include the following:

Term	Definition
Physical machine	The physical computer with hardware, such as the hard disk drive(s), optical drive, RAM, and motherboard.
Virtual machine	A software implementation of a computer that executes programs like a physical machine.
Virtual hard disk (VHD)	A file that is created within the host operating system and simulates a hard disk for the virtual machine.
Hypervisor	A thin layer of software that resides between the guest operating system and the hardware. It creates and runs virtual machines.
Load balancing	A technique that disperses a workload between two or more computers or resources to achieve optimal resource utilization, throughput, or response time.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
	3.3 Implement virtualization
TestOut Security Pro	3.3.1 Create virtual machines 3.3.2 Create virtual switches

5.2 Assessment techniques

5.2.3 Scan for vulnerabilities

2.3 Explain various types of vulnerabilities.

- Virtualization
- Virtual machine (VM) escape
- Resource reuse

2.5 Explain the purpose of mitigation techniques used to secure the enterprise.

- Segmentation

3.1 Compare and contrast security implications of different architecture models.

- Architecture and infrastructure concepts
 - Network infrastructure
 - Logical segmentation
 - Containerization
 - Virtualization

3.2 Given a scenario, apply security principles to secure enterprise infrastructure.

- Infrastructure considerations
 - Load balancer

3.4 Explain the importance of resilience and recovery in security architecture.

- High availability
 - Load balancing vs. clustering








4.1 Given a scenario, apply common security techniques to computing resources.

CompTIA Security+
SY0-701

- Sandboxing

4.3 Explain various activities associated with vulnerability management.

- Identification methods
 - Vulnerability scan

Video/Demo	Time
 10.1.1 Host Virtualization Overview	10:07
 10.1.2 Load Balancing with Virtualization	6:08
 10.1.4 Use VMWare Player	4:38
 10.1.5 Use Hyper-V	5:37
 10.1.7 Use Windows Sandbox	3:32
 10.1.8 Create Containers	3:01
 10.1.9 Secure Containers	<u>5:09</u>
Total Video Time	38:12

Lab/Activity

-  10.1.6 Create Virtual Machines

Fact Sheets

-  10.1.3 Virtualization Facts

Number of Exam Questions

10 questions

Total Time

About 66 minutes

10.2: Virtual Networking

Lecture Focus Questions:

- How does a virtual network differ from a physical network?
- What is a Virtual Private Network (VPN)?
- What is a virtual machine?
- What terms are associated with virtualization and what do they mean?
- What is the Dynamic Host Configuration Protocol (DHCP)?
- How can physical devices become virtual ones?
- Who are some of the network virtualization service providers?

In this section, you will learn to:

- Configure virtual network devices.
- Create virtual switches.

Key terms for this section include the following:

Term	Definition
Virtual network	A computer network consisting of virtual and physical devices.
Virtual local area network (VLAN)	A virtual LAN running on top of a physical LAN.
Virtual private network (VPN)	A secure tunnel to another network that connects multiple remote end-points.
Virtual machine (VM)	A virtual computer that functions like a physical computer.
Virtual switch (vSwitch)	Software that facilitates the communication between virtual machines by checking data packets before moving them to a destination.
Virtual router (vRouter)	Software that replicates the functionality of a physical router.
Virtual firewall appliance (vFA)	Software that functions as a network firewall device. A virtual firewall appliance provides packet filtering and monitoring functions.
Virtual machine monitor (VMM)/hypervisor	Software, firmware, or hardware that creates and runs virtual machines.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
------	-----------

3.3 Implement virtualization

TestOut Security Pro

3.3.1 Create virtual machines

3.3.2 Create virtual switches

3.1 Compare and contrast security implications of different architecture models.




- Architecture and infrastructure concepts
 - Network infrastructure
 - Virtualization

CompTIA Security+
SY0-701

4.1 Given a scenario, apply common security techniques to computing resources.

- Sandboxing

Video/Demo

-  10.2.1 Virtual Networking Overview
-  10.2.2 Virtual Network Devices
-  10.2.3 Configuring Virtual Network Devices

Time

6:23

4:12

3:34


Total Video Time

14:09

Lab/Activity

-  10.2.6 Create Virtual Switches

Fact Sheets

-  10.2.4 Virtualization Implementation Facts
-  10.2.5 Virtual Networking Facts

Number of Exam Questions

10 questions

Total Time

About 47 minutes

10.3: Software-Defined Networking

Lecture Focus Questions:

- Which three layers exist in the software-defined networking (SDN) architecture?
- What is the function of the controller?
- What 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?

Key terms for this section include the following:

Term	Definition
Software-defined networking	An architecture that allows network and security professionals to manage, control, and make changes to a network.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
CompTIA Security+ SY0-701	3.1 Compare and contrast security implications of different architecture models. <ul style="list-style-type: none">• Architecture and infrastructure concepts<ul style="list-style-type: none">◦ Software-defined networking (SDN)

Video/Demo

- ▶ 10.3.1 Software-Defined Networking Basics
- ▶ 10.3.2 SDN Infrastructure and Architecture

Total Video Time

Time

3:30

2:34

6:04

Fact Sheets

- ▶ 10.3.3 SDN Facts

Number of Exam Questions

10 questions

Total Time

About 22 minutes

10.4: Cloud Services

Lecture Focus Questions:

- What is the difference between a hybrid cloud and a community cloud?
- What is the difference between infrastructure as a service (IaaS) and platform as a service (PaaS)?
- Which two implementations are available for software as a service (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?

Key terms for this section include the following:

Term	Definition
Cloud	A metaphor for the internet.
Cloud computing	Software, data access, computation, and storage services provided to clients through the internet.
Public cloud	A cloud that is deployed for shared use by multiple independent tenants.
Private cloud	A cloud that is deployed for use by a single entity.
Community cloud	Platforms, applications, storage, or other resources that are shared by several organizations.
Hybrid cloud	A cloud deployment that uses both private and public elements.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
	1.2 Summarize fundamental security concepts. <ul style="list-style-type: none">• Authentication, Authorization, and Accounting (AAA)<ul style="list-style-type: none">◦ Authenticating people
	2.2 Explain common threat vectors and attack surfaces.
CompTIA Security+ SY0-701	<ul style="list-style-type: none">• Supply chain<ul style="list-style-type: none">◦ Managed service providers (MSPs)◦ Vendors◦ Suppliers
	2.3 Explain various types of vulnerabilities. <ul style="list-style-type: none">• Cloud-specific• Supply chain

- Service provider

3.1 Compare and contrast security implications of different architecture models.

- Architecture and infrastructure concepts
 - Cloud
 - Hybrid considerations
 - Third-party vendors
 - Serverless
 - Virtualization
- Considerations




4.1 Given a scenario, apply common security techniques to computing resources.

- Hardening targets
 - Cloud infrastructure

5.3 Explain the processes associated with third-party risk assessment and management.

- Vendor assessment
 - Penetration testing
 - Right-to-audit clause
 - Independent assessments
- Vendor monitoring


Video/Demo

 10.4.1 Cloud Services Introduction	9:31
 10.4.2 Enhancing Cloud Performance	10:26
 10.4.3 Cloud Computing Security Issues	<u>5:40</u>

Total Video Time

25:37

Fact Sheets

-  10.4.4 Cloud Computing Facts
-  10.4.5 Cloud Storage Security Facts

Number of Exam Questions

11 questions

Copyright © 2023 TestOut Corporation. Copyright © The Computing Technology Industry Association, Inc. (CompTIA). All Rights Reserved. Reference to any specific product, service, process, or method by trade name, trademark, manufacturer or otherwise on this website is for educational purposes only and does not constitute an implied or expressed recommendation or endorsement by said third party. Neither TestOut nor CompTIA have any affiliation with any of these companies, and the products and services advertised herein are not endorsed by them.

Total Time
About 52 minutes

10.5: Mobile Devices

Lecture Focus Questions:

- Which process allows you to define specific apps that users can have on 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.
- Sideload an application.

The key terms for this section include:

Term	Definition
App whitelisting	The process of identifying apps that users are allowed to have on mobile devices.
Geotagging	The process of embedding GPS coordinates within mobile device files, such as image or video files created with the device's camera.
Data exfiltration	The unauthorized copy, transfer, or retrieval of data from a computer, server, or network.
Sandboxing	The isolation of an app so that it can't affect other areas of a computer or network.
Jailbreaking	The process of removing inherent protections placed by the device manufacturer.
Sideloading	Installing an app on a mobile device via a method other than the manufacturer's app repository.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Security Pro	2.2 Harden network devices
	2.2.6 Bring Your Own Device (BYOD) security
	2.3 Explain various types of vulnerabilities.
CompTIA Security+ SY0-701	<ul style="list-style-type: none">• Mobile device<ul style="list-style-type: none">○ Side loading○ Jailbreaking

2.5 Explain the purpose of mitigation techniques used to secure the enterprise.

- Application allow list
- Hardening techniques
 - Encryption

3.3 Compare and contrast concepts and strategies to protect data

- Methods to secure data
 - Encryption

4.1 Given a scenario, apply common security techniques to computing resources.

- Secure baselines
 - Establish
 - Deploy
- Hardening targets
 - Mobile devices
- Wireless devices
 - Installation considerations
- Mobile solutions
 - Mobile device management (MDM)
 - Deployment models
 - Bring your own device (BYOD)
 - Corporate-owned, personally enabled (COPE)
 - Choose your own device (CYOD)
 - Connection methods
 - Cellular
 - Wi-Fi
 - Bluetooth
 - Application security
 - Code signing
 - Sandboxing





4.5 Given a scenario, modify enterprise capabilities to enhance security.

- Operating system security

- Group Policy

4.6 Given a scenario, implement and maintain identity and access management.

- Password concepts
 - Password managers

Video/Demo	Time
 10.5.1 Mobile Device Connection Methods	4:51
 10.5.3 Enforcing Mobile Device Security	6:53
 10.5.5 Enforcing Security Policies on Mobile Devices	2:57
 10.5.6 Sideload an App	<u>6:41</u>
Total Video Time	21:22

Fact Sheets

-  10.5.2 Mobile Device Connection Facts
-  10.5.4 Enforcing Mobile Device Security Facts

Number of Exam Questions

11 questions

Total Time

About 48 minutes

10.6: Mobile Device Management

Lecture Focus Questions:

- What are four methods of mobile device management (MDM)?
- What are the benefits of implementing mobile application management (MAM)?
- What do Windows Information Protection (WIP) policies provide?
- How does Intune help you to secure data?

In this section, you will learn to:

- Enroll devices and perform a remote wipe.

The key terms for this section include:

Term	Definition
Windows Information Protection	A technology that helps protect against data leakage on company-owned and personal devices without disrupting the user experience.
Network fencing	Location compliance, known as network fencing, allows you to keep devices outside your corporate network from accessing network resources.
Mobile device management	The administration of mobile devices. MDM software generally allows for tracking devices; pushing apps and updates; managing security settings; and remotely wiping the device.
Mobile application management	The administration of applications on a mobile device. MAM software allows a system administrator to remotely install or remove organizational apps and to disable certain functions within the apps.
Enterprise mobility management (EMM)	A combination of MDM and MAM solutions in one package. EMM allows a system administrator to remotely manage hardware and applications on a mobile device.
Unified endpoint management (UEM)	An all-in-one device management solution. UEM allows a system administrator to manage local and mobile devices, including Internet of Things devices.
Bring your own device (BYOD)	The practice of having employees use their own personal mobile devices for business related tasks.




This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Security Pro	2.2 Harden network devices

CompTIA
Security+ SY0-701

- 2.2.6 Bring Your Own Device (BYOD) security
- 3.2 Implement application defenses
 - 3.2.1 Implement an application allow list
- 2.5 Explain the purpose of mitigation techniques used to secure the enterprise.
 - Application allow list
- 3.1 Compare and contrast security implications of different architecture models.
 - Considerations
 - Ease of deployment
- 4.1 Given a scenario, apply common security techniques to computing resources.
 - Mobile solutions
 - Mobile device management (MDM)
 - Deployment models
 - Bring your own device (BYOD)
- 4.2 Explain the security implications of proper hardware, software, and data asset management.
 - Disposal/decommissioning
 - Sanitization
 - Destruction
 - Data retention

Video/Demo

	Time
 10.6.1 Mobile Device Management	4:42
 10.6.3 Enroll Devices and Perform a Remote Wipe	3:22
 10.6.4 Mobile Application Management	<u>3:59</u>

Total Video Time

12:03

Fact Sheets

Copyright © 2023 TestOut Corporation. Copyright © The Computing Technology Industry Association, Inc. (CompTIA). All Rights Reserved. Reference to any specific product, service, process, or method by trade name, trademark, manufacturer or otherwise on this website is for educational purposes only and does not constitute an implied or expressed recommendation or endorsement by said third party. Neither TestOut nor CompTIA have any affiliation with any of these companies, and the products and services advertised herein are not endorsed by them.

- 10.6.2 Mobile Device Management Facts
- 10.6.5 Mobile Application Management Facts

Number of Exam Questions

10 questions

Total Time

About 33 minutes

10.7: BYOD Security

Lecture Focus Questions:

- How would you remediate a tablet or phone infected with malware?
- What is an acceptable use policy (AUP)? How does it benefit mobile security?
- How does virtual desktop infrastructure (VDI) provide enhanced security and better data protection?
- What is the difference between choose your own device (CYOD) and corporate owned, personally enabled (COPE)?
- How can you prevent malicious insider attacks?

In this section, you will learn to:

- Secure mobile devices.
- Secure an iPad.
- Create a guest network for BYOD.

The key terms for this section include:

Term	Definition
Bring your own device (BYOD)	A BYOD policy allows employees to use personal devices for work related tasks.
Acceptable use policy (AUP)	An AUP determines the rules for using corporate resources, such as internet access, computers, etc.
Virtual desktop infrastructure (VDI)	VDI is a technology that uses virtual machines and virtual desktops.
Choose your own device (CYOD)	In a CYOD system, the company provides a list of approved devices for an employee to choose from. The ownership and management of devices varies by organization.
Corporate owned, personally enabled (COPE)	In a COPE system, the company provides a list of approved devices for an employee to choose from. The company owns the device; the employee uses and manages the device.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Security Pro	2.2 Harden network devices
	2.2.6 Bring Your Own Device (BYOD) security
	3.2 Implement application defenses
	3.2.1 Implement an application allow list

2.5 Explain the purpose of mitigation techniques used to secure the enterprise.

- Application allow list
- Isolation

3.1 Compare and contrast security implications of different architecture models.

- Considerations
 - Ease of deployment

4.1 Given a scenario, apply common security techniques to computing resources.

- Hardening targets
 - Mobile devices
- Wireless devices
 - Installation considerations
- Mobile solutions
 - Mobile device management (MDM)
 - Deployment models
 - Bring your own device (BYOD)
 - Corporate-owned, personally enabled (COPE)
 - Choose your own device (CYOD)
 - Connection methods
 - Cellular
 - Wi-Fi
 - Bluetooth

4.2 Explain the security implications of proper hardware, software, and data asset management

- Disposal/decommissioning
 - Sanitization
 - Destruction
 - Data retention

4.5 Given a scenario, modify enterprise capabilities to enhance security.

- Network access control (NAC)




4.6 Given a scenario, implement and maintain identity and access management.

- Access controls

5.1 Summarize elements of effective security governance.

- Policies
 - Acceptable use policy (AUP)

Video/Demo

-  10.7.1 BYOD Security Issues
-  10.7.3 Securing Mobile Devices
-  10.7.5 Creating a Guest Network for BYOD

Time

10:17

5:40

7:25

Total Video Time

23:22

Lab/Activity

-  10.7.4 Secure an iPad
-  10.7.6 Create a Guest Network for BYOD

Fact Sheets

-  10.7.2 BYOD Security Facts

Number of Exam Questions

10 questions

Total Time

About 63 minutes

10.8: Embedded and Specialized Systems

Lecture Focus Questions:

- How can you minimize the damage of compromised embedded devices?
- What are common static environments within the Internet of Things (IoT)?

In this section, you will learn to:

- Configure smart home devices.

The key terms for this section include:

Term	Definition
Supervisory control and data acquisition (SCADA)	SCADA is an industrial computer system that monitors and controls a process.
Internet of Things (IoT)	The network of physical devices such as vehicles, home appliances, etc., that are embedded with electronics, software, sensors, actuators, and connectivity that enable them to connect, collect, and exchange data through the internet.
Arduino	Arduino is an open-source hardware and software platform for building electronic projects.
Raspberry Pi	Raspberry Pi is a low-cost device the size of a credit card that's powered by the Python programming language. It's manufactured into a single system on a chip (SoC).
Field Programmable Gate Array (FPGA)	FPGA (Field-Programmable Gate Array) is a reconfigurable integrated circuit that can be programmed to perform various tasks and functions.
Subscriber identity module (SIM) card	A SIM card encrypts data transmission and stores information.
Zigbee	Zigbee is a radio protocol that creates low-rate private area networks.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
CompTIA Security+ SY0-701	1.4 Explain the importance of using appropriate cryptographic solutions. <ul style="list-style-type: none">• Tools<ul style="list-style-type: none">○ Trusted Platform Module (TPM)

2.2 Explain common threat vectors and attack surfaces.

- Unsecure networks
 - Wireless
 - Wired
 - Bluetooth

3.1 Compare and contrast security implications of different architecture models.





- Architecture and infrastructure concepts
 - IoT
 - Industrial control systems (ICS)/supervisory control and data acquisition (SCADA)
 - Real-time operating system (RTOS)
 - Embedded systems

3.3 Compare and contrast concepts and strategies to protect data.

- Methods to secure data
 - Encryption

4.1 Given a scenario, apply common security techniques to computing resources.

- Hardening targets
 - Mobile devices
 - ICS/SCADA
 - Embedded systems
 - IoT devices
- Mobile solutions
 - Cellular
 - Wi-Fi
 - Bluetooth

Video/Demo	Time
 10.8.1 Embedded and Specialized Systems	8:16
 10.8.2 Smart Home	7:01
 10.8.3 Constraints and Security of Embedded Devices	4:45
 10.8.4 Communication of Embedded Systems	<u>6:30</u>
Total Video Time	26:32

Fact Sheets

-  10.8.5 Embedded and Specialized Systems Facts

Number of Exam Questions

10 questions

Total Time

About 42 minutes

10.9: 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 encrypt email coming only 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 accounts on an iPad.
- Secure email on an iPad.

The key terms for this section include:

Term	Definition
Spam	Unwanted and unsolicited email usually sent to many recipients.
SMTP relay	An email server that accepts mail and forwards it to other mail servers.
Phishing email	A fraudulent email claiming to be from a trusted organization. The email typically asks a user to verify personal information or send money.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
CompTIA Security+ SY0-701	2.4 Given a scenario, analyze indicators of malicious activity. <ul style="list-style-type: none">• Malware attacks<ul style="list-style-type: none">◦ Virus• Application attacks
	3.2 Given a scenario, apply security principles to secure enterprise infrastructure. <ul style="list-style-type: none">• Secure communication/access<ul style="list-style-type: none">◦ Tunneling

- Transport Layer Security (TLS)

4.1 Given a scenario, apply common security techniques to computing resources.

- Application security
 - Secure cookies

4.5 Given a scenario, modify enterprise capabilities to enhance security.

- Email security
 - Domain-based Message Authentication Reporting and Conformance (DMARC)
 - DomainKeys Identified Mail (DKIM)
 - Sender Policy Framework (SPF)
 - Gateway
- DLP

5.6 Given a scenario, implement security awareness practices.





- Phishing

3.2 Implement Application Defenses

TestOut Security
Pro

- 3.2.1 Implement an application allow list
- 3.2.4 Configure email filters and settings
- 3.2.5 Configure browser settings

Video/Demo

	Time
 10.9.1 Email Security	6:27
 10.9.3 Protecting a Client from Spam	3:56
 10.9.4 Securing an Email Server	2:54
 10.9.6 Securing Accounts on an iPad	<u>4:56</u>

Total Video Time

18:13

Lab/Activity

-  10.9.5 Configure Email Filters
-  10.9.7 Secure Email on iPad

Fact Sheets

 10.9.2 Email Security Facts

Number of Exam Questions

10 questions

Total Time

About 58 minutes

11.0: Security Governance Concepts

11.1: Policies, Standards, and Procedures

Lecture Focus Questions:

- What role do policies play in the framework of an organization?
- Why is compliance to policies important?
- How are standards different from policies?
- Describe four different types of standards an organization may establish internally.
- What problems does a playbook help an organization address?

The key terms for this section include:

Term	Definition
Policies	A strictly enforceable rule set that determines how a task should be completed.
Acceptable Use Policy (AUP)	A policy that governs employees' use of company equipment and Internet services. ISPs may also apply AUPs to their customers.
Information Security Policies	A document or series of documents that are backed by senior management and that detail requirements for protecting technology and information assets from threats and misuse.
Business Continuity & Continuity of Operations Plans (COOP)	A collection of processes that enable an organization to maintain normal business operations in the face of some adverse event.
Disaster Recovery	A documented and resourced plan showing actions and responsibilities to be used in response to critical incidents.
Software Development Life Cycle (SDLC)	The processes of planning, analysis, design, implementation, and maintenance that often govern software and systems development.
Guidelines	Best practice recommendations and advice for configuration items where detailed, strictly enforceable policies and standards are impractical.
Standards	Expected outcome or state of a task that has been performed in accordance with policies and procedures. Standards can be determined internally or measured against external frameworks.
Procedures	Detailed instructions for completing a task in a way that complies with policies and standards.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
CompTIA Security+ SY0-701	<p>4.6 Given a scenario, implement and maintain identity and access management.</p> <ul style="list-style-type: none">• Multifactor authentication• Password concepts<ul style="list-style-type: none">○ Length○ Complexity○ Reuse○ Expiration
	<p>5.1 Summarize elements of effective security governance.</p> <ul style="list-style-type: none">• Guidelines• Policies<ul style="list-style-type: none">○ Acceptable use policy (AUP)○ Information security policies○ Business continuity○ Disaster recovery○ Incident response○ Software development lifecycle (SDLC)○ Change management• Standards<ul style="list-style-type: none">○ Password○ Access control○ Physical security○ Encryption• Procedures<ul style="list-style-type: none">○ Playbooks• External considerations<ul style="list-style-type: none">○ Regulatory○ Legal○ Industry○ Local/regional○ National○ Global• Monitoring and revision

- Types of governance structures
 - Boards
 - Committees
 - Government entities
 - Centralized/decentralized

Video/Demo

Time

📺 11.1.1 Program Management and Oversight Overview

3:40

📺 11.1.2 Program Management and Oversight Facts

5:55

Total Video Time

9:35

Fact Sheets

📄 11.1.2 Program Management and Oversight Facts

📄 11.1.3 Policies, Standards, and Procedures

Number of Exam Questions

11 questions

Total Time

About 36 minutes

11.2: Change Management

Lecture Focus Questions:

- When is change management used, and what risks does it help mitigate?
- Who should be involved in change management?
- How do allow and deny lists help in change management?
- What is the purpose of version control in change management?

The key terms for this section include:

Term	Definition
Stakeholders	A person who has a business interest in the outcome of a project or is actively involved in its work.
Dependencies	Resources and other services that must be available and running for a service to start.
Version control	The practice of ensuring that the assets that make up a project are closely managed when it comes time to make changes.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
CompTIA Security+ SY0-701	<p>1.3 Explain the importance of change management processes and the impact to security.</p> <ul style="list-style-type: none">• Technical implications<ul style="list-style-type: none">○ Allow lists/deny lists○ Restricted activities○ Downtime○ Service restart○ Application restart○ Legacy applications○ Dependencies• Documentation<ul style="list-style-type: none">○ Updating diagrams○ Updating policies/procedures• Version control <p>5.1 Summarize elements of effective security governance.</p> <ul style="list-style-type: none">• Policies

- Change management
- Procedures
 - Change management
- Types of governance structures
 - Boards

5.2 Explain elements of the risk management process.

- Risk analysis

Video/Demo

- 📺 11.2.1 Change Management
- 📺 11.2.2 Change Management Facts

Time

4:15

6:40

Total Video Time

10:55

Fact Sheets

- 📄 11.2.2 Change Management Facts

Number of Exam Questions

10 questions

Total Time

About 26 minutes

11.3: Automation and Orchestration

Lecture Focus Questions:

- What roles do automation and scripting play in IT operations, specifically security management?
- How does an orchestrated system function if a threat is detected?
- How does automation help employees?
- What are five challenges that automation presents to maintaining security systems?

The key terms for this section include:

Term	Definition
Workforce multiplier	A tool or automation that increases employee productivity, enabling them to perform more tasks to the same standard per unit of time.
Reaction times	The elapsed time between an incident occurring and a response being implemented.
Single point of failure	A component or system that would cause a complete interruption of a service if it failed.
Technical debt	Costs accrued by keeping an ineffective system or product in place, rather than replacing it with a better-engineered one.
Standard configurations	In an IaC architecture, the property that an automation or orchestration action always produces the same result, regardless of the component's previous state.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
CompTIA Security+ SY0-701	<p>4.7 Explain the importance of automation and orchestration related to secure operations.</p> <ul style="list-style-type: none">• Use cases of automation and scripting<ul style="list-style-type: none">○ Ticket creation○ Enabling/disabling services and access○ Continuous integration and testing• Benefits<ul style="list-style-type: none">○ Efficiency/time saving○ Enforcing baselines○ Standard infrastructure configurations○ Staff retention○ Reaction time

- Workforce multiplier
- Other considerations
 - Complexity
 - Cost
 - Single point of failure
 - Technical debt
 - Ongoing supportability

Video/Demo

- 📺 11.3.1 Automation and Scripting
- 📺 11.3.2 Automation and Scripting Facts

Total Video Time

Time

5:25

6:09

11:34

Fact Sheets

- 📄 11.3.2 Automation and Scripting Facts

Number of Exam Questions

10 questions

Total Time

About 27 minutes

12.0: Risk Management Processes

12.1: Risk Management Processes and Concepts

Lecture Focus Questions:

- Why are disaster recovery policies important for an organization's security?
- What is the difference in acceptance and mitigation in risk management?
- What is the difference in qualitative and quantitative risk assessment?
- How is the annualized rate of occurrence (ARO) calculated?
- What are examples of external risk types?

The key terms for this section include:

Term	Definition
Risk management	The cyclical process of identifying, assessing, analyzing, and responding to risks.
Business impact analysis (BIA)	Systematic activity that identifies organizational risks and determines their effect on ongoing mission-critical operations.
Mission essential function (MEF)	Business or organizational activity that is too critical to be deferred for anything more than a few hours, if at all.
Maximum tolerable downtime (MTD)	The longest period that a process can be inoperable without causing irrevocable business failure.
Recovery time objective (RTO)	The maximum time allowed to restore a system after a failure event.
Work recovery time (WRT)	In disaster recovery, time additional to the RTO of individual systems to perform reintegration and testing of a restored or upgraded system following an event.
Recovery point objective (RPO)	The longest period that an organization can tolerate lost data being unrecoverable.
Mean time between failures (MTBF)	Metric for a device or component that predicts the expected time between failures.
Mean time to repair (MTTR)	Metric representing average time taken for a device or component to be repaired, replaced, or otherwise recover from a failure.
Risk identification	Within overall risk assessment, specific process of listing sources of risk due to threats and vulnerabilities.
Risk mitigation (or remediation)	The response of reducing risk to fit within an organization's willingness to accept risk.

Risk deterrence (or reduction)	In risk mitigation, the response of deploying security controls to reduce the likelihood and/or impact of a threat scenario.
Avoidance	In risk mitigation, the practice of ceasing activity that presents risk.
Risk acceptance	The response of determining that a risk is within the organization's appetite and no countermeasures other than ongoing monitoring is needed.
Risk exception	A category of risk management that uses alternate mitigating controls to control an accepted risk factor.
Risk exemption	A category of risk management that accepts an unmitigated risk factor.
Residual risk	Risk that remains even after controls are put into place.
Likelihood	In risk calculation, the chance of a threat being realized, expressed as a percentage.
Probability	The mathematical measure of the possibility of a risk occurring.
Impact	The severity of the risk if realized by factors such as the scope, value of the asset, or the financial impacts of the event.
Enterprise risk management (ERM)	The comprehensive process of evaluating, measuring, and mitigating the many risks that pervade an organization.
Risk assessment	The process of identifying risks, analyzing them, developing a response strategy for them, and mitigating their future impact.
Risk analysis	Process for qualifying or quantifying the likelihood and impact of a factor.
Quantitative risk analysis	A numerical method that is used to assess the probability and impact of risk and measure the impact.
Single loss expectancy (SLE)	The amount that would be lost in a single occurrence of a particular risk factor.
Annualized loss expectancy (ALE)	The total cost of a risk to an organization on an annual basis. This is determined by multiplying the SLE by the annual rate of occurrence (ARO).
Annualized rate of occurrence (ARO)	In risk calculation, an expression of the probability/likelihood of a risk as the number of times per year a particular loss is expected to occur.
Qualitative risk analysis	The process of determining the probability of occurrence and the impact of identified risks by using logical reasoning when numeric data is not readily available.
Inherent risk	Risk that an event will pose if no controls are put in place to mitigate it.
Risk register	A document highlighting the results of risk assessments in an easily comprehensible format (such as a 'traffic light' grid). Its

Heat map risk matrix	purpose is for department managers and technicians to understand risks associated with the workflows that they manage. A graphical table indicating the likelihood and impact of risk factors identified for a workflow, project, or department for reference by stakeholders.
Key Risk Indicators (KRIs)	The method by which emerging risks are identified and analyzed so that changes can be adopted to proactively avoid issues from occurring.
Risk owner	An individual who is accountable for developing and implementing a risk response strategy for a risk documented in a risk register.
Risk appetite	A strategic assessment of what level of residual risk is tolerable for an organization.
Risk tolerance	Determines the thresholds that separate different levels of risk.
Risk reporting	A periodic summary of relevant information about a project's current risks. It provides a summarized overview of known risks, realized risks, and their impact on the organization.
Continuity of operations (COOP)	Identifies how business processes should deal with both minor and disaster-level disruption by ensuring that there is processing redundancy supporting the workflow.
Capacity planning	A practice which involves estimating the personnel, storage, computer hardware, software, and connection infrastructure resources required over some future period of time.
Hot site	A fully configured alternate processing site that can be brought online either instantly or very quickly after a disaster.
Warm site	An alternate processing location that is dormant or performs noncritical functions under normal conditions, but which can be rapidly converted to a key operations site if needed.
Cold site	A predetermined alternate location where a network can be rebuilt after a disaster.
Geographic dispersion	A resiliency mechanism where processing and data storage resources are replicated between physically distant sites.
Platform diversity	Cybersecurity resilience strategy that increases attack costs by provisioning multiple types of controls, technologies, vendors, and crypto implementations.
Tabletop exercises	A discussion of simulated emergency situations and security incidents.
Simulations	A testing technique that replicates the conditions of a real-world disaster scenario or security incident.
Parallel processing tests	Running primary and backup systems simultaneously to validate the functionality and performance of backup systems without disrupting normal operations.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
CompTIA Security+ SY0-701	<p>3.4 Explain the importance of resilience and recovery in security architecture.</p> <ul style="list-style-type: none">• High availability• Site considerations<ul style="list-style-type: none">○ Hot○ Cold○ Warm○ Geographic dispersion• Platform diversity• Multi-cloud systems• Continuity of operations• Capacity planning<ul style="list-style-type: none">○ People○ Technology○ Infrastructure• Testing<ul style="list-style-type: none">○ Tabletop exercises○ Fail over○ Simulation○ Parallel processing• Backups
	<p>4.2 Explain the security implications of proper hardware, software, and data asset management.</p> <ul style="list-style-type: none">• Assignment/accounting
	<p>5.1 Summarize elements of effective security governance.</p> <ul style="list-style-type: none">• Policies<ul style="list-style-type: none">○ Business continuity○ Incident response
	<p>5.2 Explain elements of the risk management process.</p>

- Risk identification
- Risk assessment
 - Ad hoc
 - Recurring
 - One-time
 - Continuous
- Risk analysis
 - Qualitative
 - Quantitative
 - Single loss expectancy (SLE)
 - Annualized loss expectancy (ALE)
 - Annualized rate of occurrence (ARO)
 - Probability
 - Likelihood
 - Exposure factor
 - Impact
- Risk register
 - Key risk indicators
 - Risk owners
 - Risk threshold
- Risk tolerance
- Risk appetite
 - Expansionary
 - Conservative
 - Neutral
- Risk management strategies
 - Transfer
 - Accept
 - Exemption
 - Exception
 - Avoid
 - Mitigate
- Risk reporting
- Business impact analysis
 - Recovery time objective (RTO)
 - Recovery point objective (RPO)
 - Mean time to repair (MTTR)
 - Mean time between failures (MTBF)

Video/Demo	Time
▶ 12.1.1 Risk Types and Tolerance	4:47
▶ 12.1.3 Analyzing Risks	2:57
▶ 12.1.5 Business Continuity Planning	<u>5:02</u>
Total Video Time	12:46

Fact Sheets

- 📄 12.1.2 Risk Types and Tolerance Facts
- 📄 12.1.4 Analyzing Risks Facts
- 📄 12.1.6 Business Continuity Planning Facts

Number of Exam Questions

10 questions

Total Time

About 38 minutes

12.2: Vendor Management

Lecture Focus Questions:

- What are three types of third-party relationships?
- How does onboarding with a third-party create security risk?
- What security risks should be considered on a daily or ongoing basis?
- Why is it important to reevaluate security risks when offboarding?

The key terms for this section include:

Term	Definition
Due diligence	A legal principal that responsible parties have used best practice or reasonable care and have not been negligent in discharging their duties.
Conflict of interest	When an individual or organization has investments or obligations that could compromise their ability to act objectively, impartially, or in the best interest of another party.
Questionnaires	In vendor management, a structured means of obtaining consistent information, enabling more effective risk analysis and comparison.
Rules of Engagement (RoE)	A definition of how a pen test will be executed and what constraints will be in place. This provides the pen tester with guidelines to consult as they conduct their tests so that they don't have to constantly ask management for permission to do something.
Memorandum of Understanding (MOU)	Usually a preliminary or exploratory agreement to express an intent to work together that is not legally binding and does not involve the exchange of money.
Nondisclosure Agreement (NDA)	An agreement that stipulates that entities will not share confidential information, knowledge, or materials with unauthorized third parties.
Memorandum of Agreement (MOA)	Legal document forming the basis for two parties to cooperate without a formal contract (a cooperative agreement). MOAs are often used by public bodies.
Business Partnership Agreement (BPA)	Agreement by two companies to work together closely, such as the partner agreements that large IT companies set up with resellers and solution providers.
Master Service Agreement (MSA)	A contract that establishes precedence and guidelines for any business documents that are executed between two parties.
Service-level Agreement (SLA)	An agreement that sets the service requirements and expectations between a consumer and a provider.

Statement of Work (SOW)/Work Order (WO)

A document that defines the expectations for a specific business arrangement.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
CompTIA Security+ SY0-701	5.1 Summarize elements of effective security governance. <ul style="list-style-type: none">• Procedures<ul style="list-style-type: none">○ Onboarding/offboarding
	5.3 Explain the processes associated with third-party risk assessment and management. <ul style="list-style-type: none">• Vendor assessment<ul style="list-style-type: none">○ Penetration testing○ Right-to-audit clause○ Evidence of internal audits○ Independent assessments○ Supply chain analysis• Vendor selection<ul style="list-style-type: none">○ Due diligence○ Conflict of interest• Agreement types<ul style="list-style-type: none">○ Service-level agreement (SLA)○ Memorandum of agreement (MOA)○ Memorandum of understanding (MOU)○ Master service agreement (MSA)○ Work order (WO)/statement of work (SOW)○ Non-disclosure agreement (NDA)○ Business partners agreement (BPA)• Vendor monitoring• Questionnaires• Rules of engagement

Video/Demo

 12.2.1 Managing Third Parties

Total Video Time

Time

5:23

5:23

Fact Sheets

📄 12.2.2 Managing Third Parties Facts

Number of Exam Questions

10 questions

Total Time

About 21 minutes

12.3: Audits and Assessments

Lecture Focus Questions:

- What is an audit?
- What are the different types of audits?
- How do the types of audits differ from one another?

In this section, you will learn to:

- Audit the Windows security log.
- Configure advanced audit policies.
- Audit device logs on a switch.
- Enable device logs.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
CompTIA Security+ SY0-701	4.3 Explain various activities associated with vulnerability management. <ul style="list-style-type: none">• Identification methods<ul style="list-style-type: none">◦ System/process audit• Validation of remediation<ul style="list-style-type: none">◦ Audit
	4.4 Explain security alerting and monitoring concepts and tools. <ul style="list-style-type: none">• Activities<ul style="list-style-type: none">◦ Log aggregation
	4.5 Given a scenario, modify enterprise capabilities to enhance security. <ul style="list-style-type: none">• Operating system security<ul style="list-style-type: none">◦ Group Policy
	4.9 Given a scenario, use data sources to support an investigation.

- Log data
 - OS-specific security logs
 - Network logs

5.1 Summarize elements of effective security governance.

- Policies
 - Information security policies

5.5 Explain types and purposes of audits and assessments.

- Attestation
- Internal
 - Compliance
 - Audit committee
 - Self-assessments
- External
 - Regulatory
 - Examinations
 - Assessment
 - Independent third-party audit




1.2 Harden Authentication

1.2.5 Configure and Link Group Policy Objects (GPO)

TestOut Security Pro

5.1 Implement logging and auditing

5.1.1 Configure advanced audit policy

Video/Demo	Time
 12.3.1 Audits	5:12
 12.3.3 Auditing the Windows Security Log	5:23
 12.3.5 Auditing Device Logs on a Switch	<u>3:54</u>
Total Video Time	14:29

Lab/Activity

-  12.3.4 Configure Advanced Audit Policy

Copyright © 2023 TestOut Corporation. Copyright © The Computing Technology Industry Association, Inc. (CompTIA). All Rights Reserved. Reference to any specific product, service, process, or method by trade name, trademark, manufacturer or otherwise on this website is for educational purposes only and does not constitute an implied or expressed recommendation or endorsement by said third party. Neither TestOut nor CompTIA have any affiliation with any of these companies, and the products and services advertised herein are not endorsed by them.

🔒 12.3.6 Enable Device Logs

Fact Sheets

📄 12.3.2 Audit Facts

Number of Exam Questions

10 questions

Total Time

About 54 minutes

13.0: Data Protection and Compliance

13.1: Data Classification and Compliance

Lecture Focus Questions:

- What is the purpose of classifying data?
- What is the difference between PII and PHI?
- Why is it important to know data destruction types?
- How are privacy enhancing technologies used to protect PII?

Key terms for this section include the following:

Term	Definition
Data breach	When confidential or private data is read, copied, or changed without authorization. Data breach events may have notification and reporting requirements.
Escalated	In the context of support procedures, incident response, and breach-reporting, escalation is the process of involving expert and senior staff to assist in problem management.
Health Insurance Portability and Accountability Act (HIPAA)	US federal law that protects the storage, reading, modification, and transmission of personal healthcare data.
Regulated data	Information that has storage and handling compliance requirements defined by national and state legislation and/or industry regulations.
Trade secret	Intellectual property that gives a company a competitive advantage but hasn't been registered with a copyright, trademark, or patent.
Legal data	Documents and records that relate to matters of law, such as contracts, property, court cases, and regulatory filings.
Financial data	Data held about bank and investment accounts, plus information such as payroll and tax returns.
Human-readable data	Information stored in a file type that human beings can access and understand using basic viewer software, such as documents, images, video, and audio.
Non-human-readable data	Information stored in a file that human beings cannot read without a specialized processor to decode the binary or complex structure.

Data classification	The process of applying confidentiality and privacy labels to information.
Proprietary information or intellectual property (IP)	Information created by an organization, typically about the products or services that it makes or provides.
Data subjects	An individual that is identified by privacy data.
Data inventories	List of classified data or information stored or processed by a system.
Data retention	The process an organization uses to maintain the existence of and control over certain data in order to comply with business policies and/or applicable laws and regulations.
Disposal/decommissioning	In asset management, the policies and procedures that govern the removal of devices and software from production networks and their subsequent disposal through sale, donation, or as waste.
Sanitization	The process of thoroughly and completely removing data from a storage medium so that file remnants cannot be recovered.
Destruction	An asset disposal technique that ensures that data remnants are rendered physically inaccessible and irrevocable through degaussing, shredding, or incineration.
Certification	An asset disposal technique that relies on a third party to use sanitization or destruction methods for data remnant removal as well as providing documentary evidence that the process is complete and successful.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
CompTIA Security+ SY0-701	<p>3.3 Compare and contrast concepts and strategies to protect data.</p> <ul style="list-style-type: none"> • Data types <ul style="list-style-type: none"> ○ Regulated ○ Trade secret ○ Intellectual property ○ Legal information ○ Financial information ○ Human and non-human readable

- Data classifications
 - Sensitive
 - Confidential
 - Public
 - Restricted
 - Private
 - Critical

- General data considerations
 - Data sovereignty

4.2 Explain the security implications of proper hardware, software, and data asset management.

- Disposal/decommissioning
 - Sanitization
 - Destruction
 - Certification
 - Data retention

5.1 Summarize elements of effective security governance.





- Roles and responsibilities for systems and data
 - Controllers
 - Processors

5.4 Summarize elements of effective security compliance.





- Consequences of non-compliance
 - Fines
 - Sanctions
 - Reputational damage
 - Loss of license
 - Contractual impacts

- Privacy
 - Legal implications
 - Local/regional
 - National
 - Global

- Data subject
- Controller vs. processor
- Ownership
- Data inventory and retention
- Right to be forgotten

Video/Demo	Time
 13.1.1 Consequences of Breaches	4:35
 13.1.3 Information Classification	4:21
 13.1.5 Privacy and Responsibility of Data	8:11
 13.1.7 Data Destruction	<u>8:43</u>
Total Video Time	25:50

Fact Sheets

-  13.1.2 Consequences of Breaches Facts
-  13.1.4 Information Classification Facts
-  13.1.6 Privacy and Responsibility of Data
-  13.1.8 Data Destruction Facts

Number of Exam Questions

11 questions

Total Time

About 62 minutes

13.2: Personnel Policies

Lecture Focus Questions:

- How can an onboarding process improve the security of an organization?
- Why should employees be required to sign employment agreements?
- Why is it important to conduct an exit interview?
- What security issues must be identified and addressed during the onboarding phase of a third-party relationship?
- What is the role of the Service Level Agreement (SLA)?
- Why are policies important for organizational security?

The key terms for this section include:

Term	Definition
Onboarding	The process of bringing in a new employee, contractor, or supplier.
Offboarding	The process of ensuring that all HR and other requirements are covered when an employee leaves an organization.
Acceptable use policy (AUP)	A policy that governs employees' use of company equipment and Internet services. ISPs may also apply AUPs to their customers.
Code of conduct	Professional behavior depends on basic ethical standards, such as honesty and fairness. Some professions may have developed codes of ethics to cover difficult situations; some businesses may also have a code of ethics to communicate the values it expects its employees to practice.
Clean desk policy	An organizational policy that mandates employee work areas be free from potentially sensitive information; sensitive documents must not be left out where unauthorized personnel might see them.
Computer-based training (CBT)	Training and education programs delivered using computer devices and e-learning instructional models and design.
Anomalous behavior recognition	Systems that automatically detect users, hosts, and services that deviate from what is expected, or systems and training that encourage reporting of this by employees.
Database encryption	Applying encryption at the table, field, or record level via a database management system rather than via the file system.
Data sovereignty	In data protection, the principle that countries and states may impose individual requirements on data collected or stored within their jurisdiction.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
------	-----------

2.5 Explain the purpose of mitigation techniques used to secure the enterprise.

- Least privilege

3.3 Compare and contrast concepts and strategies to protect data.

- Data types
 - Regulated
 - Intellectual property
 - Legal information
 - Financial information
- Data classifications
- General data considerations
 - Data states
 - Data at rest
 - Data in transit
 - Data in use
 - Data sovereignty
 - Geolocation
- Methods to secure data
 - Encryption

CompTIA
Security+ SY0-701

4.1 Given a scenario, apply common security techniques to computing resources.

- Mobile solutions
 - Bring your own device (BYOD)

4.2 Explain the security implications of proper hardware, software, and data asset management.

- Disposal/decommissioning
 - Data retention
- Tools

- Data loss prevention (DLP)

4.6 Given a scenario, implement and maintain identity and access management.

- Access controls
 - Least privilege

4.8 Explain appropriate incident response activities.

- Training
- Digital forensics
 - Legal hold

5.1 Summarize elements of effective security governance.

- Policies
 - Acceptable use policy (AUP)
- Procedures
 - Onboarding/offboarding

5.4 Summarize elements of effective security compliance.

- Privacy
 - Legal implications
 - Data inventory and retention

5.6 Given a scenario, implement security awareness practices.

- Phishing
 - Recognizing a phishing attempt
- Anomalous behavior recognition
 - Risky
 - Unexpected
 - Unintentional
- User guidance and training
 - Policy/handbooks

- Situational awareness
- Removable media and cables
- Social engineering
- Reporting and monitoring
 - Initial
 - Recurring
- Development

TestOut Security Pro 5.0 Audit and Security Assessment
5.1 Implement Logging and Auditing

Video/Demo

- 📺 13.2.1 Personnel Policies
- 📺 13.2.3 Data Protection and Policies

Time

6:34

3:35

Total Video Time

10:09

Fact Sheets

- 📄 13.2.2 Personnel Policy Facts
- 📄 13.2.4 Data Protection and Policies Facts

Number of Exam Questions

10 questions

Total Time

About 31 minutes

Practice Exams

A.0: CompTIA Security+ SY0-701 - Practice Exams

CompTIA Security+ SY0-701 Certification Practice Exam (90 questions)

B.0: TestOut Security Pro - Practice Exams

TestOut Security Pro Certification Practice Exam (15 questions)

Appendix A: Approximate Time for the Course

The total time for the LabSim for Security Pro course is approximately **63 hours and 16 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 (12 minutes assigned per simulation)
- Questions (1 minute per question)

Additionally, there are approximately another **34 hours and 4 minutes** of Practice Test material at the end of the course.

The breakdown for this course is as follows:

Module	Sections	Time	Videos	Labs	Text	Exams
1.0: Security Concepts						
	1.1: Security Introduction	28	13	0	5	10
	1.2: Security Controls	26	5	0	5	16
	1.3: Use the Simulator	23	23	0	0	0
	Total	1:17	0:41	0:00	0:10	0:26
2.0: Threats, Vulnerabilities, and Mitigations						
	2.1: Understanding Attacks	61	36	0	15	10
	2.2: Social Engineering	59	21	12	10	16
	2.3: Malware	55	17	12	10	16
	Total	2:55	1:14	0:24	0:35	0:42
3.0: Cryptographic Solutions						
	3.1: Cryptography	96	43	12	25	16
	3.2: Cryptography Implementations	26	11	0	5	10
	3.3: Hashing	41	14	12	5	10
	3.4: Encryption	67	28	24	5	10
	3.5: Public Key Infrastructure	72	29	12	15	16
	Total	5:02	2:05	1:00	0:55	1:02
4.0: Identity and Access Management						
	4.1: Access Control Models	40	15	0	15	10
	4.2: Authentication	52	27	0	15	10
	4.3: Authorization	36	15	0	5	16
	4.4: Active Directory Overview	146	42	84	10	10
	4.5: Hardening Authentication	116	36	60	10	10
	4.6: Linux Users	131	39	72	10	10
	4.7: Linux Groups	58	7	36	5	10
	4.8: Remote Access	27	7	0	10	10

4.9: Network Authentication	31	11	0	10	10
Total	10:37	3:19	4:12	1:30	1:36
5.0: Network Architecture					
5.1: Enterprise Network Architecture	22	7	0	5	10
5.2: Security Appliances	97	48	24	15	10
5.3: Screened Subnets	37	10	12	5	10
5.4: Firewalls	48	21	12	5	10
5.5: Virtual Private Networks	73	23	24	10	16
5.6: Network Access Control	22	7	0	5	10
5.7: Network Device Vulnerabilities	44	17	12	5	10
5.8: Network Applications	27	12	0	5	10
5.9: Switch Security and Attacks	95	39	36	10	10
5.10: Router Security	72	21	36	5	10
Total	8:57	3:25	2:36	1:10	1:46
6.0: Resiliency and Site Security					
6.1: Physical Threats	33	6	12	5	10
6.2: Monitoring and Reconnaissance	42	22	0	10	10
6.3: Intrusion Detection	39	12	12	5	10
6.4: Protocol Analyzers	32	17	0	5	10
6.5: Analyzing Network Attacks	99	43	36	10	10
6.6: Analyzing Password Attacks	70	31	24	5	10
Total	5:15	2:11	1:24	0:40	1:00
7.0: Vulnerability Management					
7.1: Vulnerability Management	51	20	0	15	16
7.2: Vulnerability Scanning	103	16	72	5	10
7.3: Alerting and Monitoring	50	25	0	15	10
7.4: Penetration Testing	36	16	0	10	10
Total	4:00	1:17	1:12	0:45	0:46
8.0: Network and Endpoint Security					
8.1: Operating System Hardening	63	24	24	5	10
8.2: File Server Security	62	18	24	10	10
8.3: Linux Host Security	43	23	0	10	10
8.4: Wireless Overview	42	15	12	5	10
8.5: Wireless Attacks	39	12	12	5	10
8.6: Wireless Defenses	72	22	24	10	16
8.7: Data Transmission Security	71	33	12	10	16
8.8: Web Application Security	78	34	24	10	10
8.9: Application Development and Security	79	30	24	15	10
Total	9:09	3:31	2:36	1:20	1:42
9.0: Incident Response					
9.1: Incident Response and Mitigation	33	7	0	10	16
9.2: Log Management	61	41	0	10	10
9.3: Digital Forensics	62	47	0	5	10
9.4: Redundancy	40	14	0	10	16
9.5: Backup and Restore	80	29	36	5	10
Total	4:36	2:18	0:36	0:40	1:02

Copyright © 2023 TestOut Corporation. Copyright © The Computing Technology Industry Association, Inc. (CompTIA). All Rights Reserved. Reference to any specific product, service, process, or method by trade name, trademark, manufacturer or otherwise on this website is for educational purposes only and does not constitute an implied or expressed recommendation or endorsement by said third party. Neither TestOut nor CompTIA have any affiliation with any of these companies, and the products and services advertised herein are not endorsed by them.

10.0: Protocol, App, and Cloud Security						
10.1: Host Virtualization	66	39	12	5	10	
10.2: Virtual Networking	47	15	12	10	10	
10.3: Software-Defined Networking	22	7	0	5	10	
10.4: Cloud Services	52	26	0	10	16	
10.5: Mobile Devices	48	22	0	10	16	
10.6: Mobile Device Management	33	13	0	10	10	
10.7: BYOD Security	63	24	24	5	10	
10.8: Embedded and Specialized Systems	42	27	0	5	10	
10.9: Email	58	19	24	5	10	
Total	7:11	3:12	1:12	1:05	1:42	
11.0: Security Governance Concepts						
11.1: Policies, Standards, and Procedures	36	10	0	10	16	
11.2: Change Management	26	11	0	5	10	
11.3: Automation and Orchestration	27	12	0	5	10	
Total	1:29	0:33	0:00	0:20	0:36	
12.0: Risk Management Processes						
12.1: Risk Management Processes and Concepts	38	13	0	15	10	
12.2: Vendor Management	21	6	0	5	10	
12.3: Audits and Assessments	54	15	24	5	10	
Total	1:53	0:34	0:24	0:25	0:30	
13.0: Data Protection and Compliance						
13.1: Data Classification and Compliance	62	26	0	20	16	
13.2: Personnel Policies	31	11	0	10	10	
Total	1:33	0:37	0:00	0:30	0:26	
Total Course Time 63:16						

Practice Exams			
A.0: CompTIA Security+ SY0-701 - Practice Exams		Number of Questions	Time
A.2: CompTIA Security+ Domain Review (5 20 Question exams)	100		1:40
A.3 CompTIA Security+ Domain Review (5 exams with All Questions)	1359		22:39
A.4: CompTIA Security+ SY0-701 Certification Practice Exam	90		1:30
Total	1549		25:49
B.0: TestOut Security Pro - Practice Exams		Number of Questions	Time
B.2 TestOut Security Pro Domain review (5 exams)	84		7:00
B.3: TestOut Security Pro Certification Practice Exam	15		1:15
Total	15		8:15
Total Practice Exam Time 34:04			

Copyright © 2023 TestOut Corporation. Copyright © The Computing Technology Industry Association, Inc. (CompTIA). All Rights Reserved. Reference to any specific product, service, process, or method by trade name, trademark, manufacturer or otherwise on this website is for educational purposes only and does not constitute an implied or expressed recommendation or endorsement by said third party. Neither TestOut nor CompTIA have any affiliation with any of these companies, and the products and services advertised herein are not endorsed by them.