TestOut®

Security Pro - English 5.1.x

LESSON PLAN

Powered by LABSIM

Table of Contents

1.1: Security Overview

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

Lecture Focus Questions:

- What challenges does a security professional face?
- What is the difference between *integrity* and *non-repudiation*?
- What process provides confidentiality by converting data into a form that it is unlikely to be usable by an unintended recipient?
- What are the three main goals of the CIA of Security?
- Which security expression refers to verifying that someone is who they say they are?
- What are key components of risk management?
- What are three types of threat agents?

Video/Demo	Time
1.1.1 Security Challenges	8:22
1.1.2 Security Roles and Concepts	5:37
1.1.3 Threat Agent Types	8:20
1.1.5 General Attack Strategy	8:51
1.1.6 General Defense Strategy	18:25
Total Video Time	**49:35**

Fact Sheets

- 1.1.4 Security Introduction
- 1.1.7 Attack and Defense Strategy Overview

Number of Exam Questions

12 questions

Total Time

About 72 minutes

1.2: Using the Simulator

Summary

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

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

Video/Demo		Time
1.2.1 Using the Simulator		13:19
	Total Video Time	**13:19**

Lab/Activity

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

Total Time

About 24 minutes

2.1: Access Control Models

Lecture Focus Questions:

- What is access control and why is it important?
- How does the Discretionary Access Control (DAC) provide access control?
- What type of entries does the Discretionary Access Control List (DACL) contain?
- What is the function of each of the two types of labels used by the Mandatory Access Control (MAC) access model?
- What is the difference between *role-based* access control and *rule-based* access control?
- How are Rule-Based Access Control and Mandatory Access Control (MAC) similar?
- In security terms, what does AAA refer to?

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

- Implement DAC by configuring a discretionary access control list (DACL).

This section covers the following Security Pro exam objective:

- 5.1 Harden Network Devices (using a Cisco Small Business Switch).
  - Implement access lists, deny everything else

Video/Demo	**Time**
2.1.1 Access Control Models	3:38
2.1.5 Implementing Discretionary Access Control	6:09
Total Video Time	**9:47**

Fact Sheets

- 2.1.2 Access Control Facts
- 2.1.3 Access Control Model Facts
- 2.1.4 Access Control Model Examples

Number of Exam Questions

15 questions

Total Time

About 40 minutes

2.2: Authentication

Lecture Focus Questions:

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

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

- Use a biometric scanner to enroll (record) fingerprints that can be used for authentication.
- Configure fingerprint settings to automate execution of an application.
- Use single sign-on to access all authorized resources on the network.

Video/Demo	Time
2.2.1 Authentication Part 1	11:26
2.2.2 Authentication Part 2	8:53
2.2.4 Using a Biometric Scanner	3:49
2.2.5 Using Single Sign-on	12:20
Total Video Time	**36:28**

Fact Sheets

- 2.2.3 Authentication Facts
- 2.2.6 Single Sign-on Facts

Number of Exam Questions

15 questions

Total Time

About 62 minutes

2.3: Authorization

Lecture Focus Questions:

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

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

- Create a group and add members to the group.
- Examine the elements of an access token using **whoami /all**.
- After changing user privileges, gain access to newly assigned resources by creating a new access token (logging on again).

Video/Demo	Time
2.3.1 Authorization	5:15
2.3.2 Cumulative Access	9:32
2.3.4 Examining the Access Token	9:08
Total Video Time	**23:55**

Fact Sheets

2.3.3 Authorization Facts

Number of Exam Questions

4 questions

Total Time

About 33 minutes

2.4: Access Control Best Practices

Lecture Focus Questions:

- What is the difference between *implicit deny* and *explicit allow*?
- What is the difference between *implicit* deny and *explicit* deny? Which is the strongest?
- How does implementing the principle of separation of duties increase the security in an organization?
- What aspects of security does job rotation provide?
- How do creeping privileges occur?

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

- Enable and disable User Account Control (UAC).
- Use alternate credentials to run programs that require elevated privileges.

This section covers the following Security Pro exam objective:

- 5.1 Harden Network Devices (using a Cisco Small Business Switch).
  - Implement access lists, deny everything else

Video/Demo	Time
2.4.1 Access Control Best Practices	3:12
2.4.2 Viewing Implicit Deny	10:13
Total Video Time	**13:25**

Fact Sheets

2.4.3 Best Practices Facts

Number of Exam Questions

12 questions

Total Time

About 31 minutes

2.5: Active Directory Overview

Lecture Focus Questions:

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

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

- Open and navigate the Active Directory Users and Computers dialog.
- Distinguish between Organizational Unit (OU) and folder resources.
- View and edit user and group account properties.

Video/Demo	Time
2.5.1 Active Directory Introduction	9:04
2.5.2 Active Directory Structure	9:25
2.5.3 Viewing Active Directory	8:05
Total Video Time	**26:34**

Fact Sheets

2.5.4 Active Directory Facts

Number of Exam Questions

3 questions

Total Time

About 35 minutes

2.6: Windows Domain Users and Groups

Lecture Focus Questions:

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

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

- Create domain user accounts.
- Modify user account properties, including changing logon and password settings in the user account.
- Rename a user account.
- Reset a user account password and unlock the account.
- Enable and disable an account.

This section covers the following Security Pro exam objectives:

- 1.1 Create, modify, and delete user profiles.
  - Manage Windows Domain Users and Groups
    - Create, rename, and delete users and groups
    - Lock and unlock user accounts
    - Assign users to appropriate groups
    - Change a user's password
- 1.2 Harden authentication.
  - Configure the Domain GPO to control local administrator group membership and Administrator password

Video/Demo	Time
2.6.1 Creating User Accounts	4:50
2.6.2 Managing User Account Properties	7:45
2.6.5 Managing Groups	5:05
Total Video Time	**17:40**

Lab/Activity

- 2.6.3 Create User Accounts
- 2.6.4 Manage User Accounts
- 2.6.6 Create a Group
- 2.6.7 Create Global Groups

Fact Sheets

- 2.6.8 User Account Management Facts

Number of Exam Questions
5 questions

Total Time
About 48 minutes

2.7: Linux Users

Lecture Focus Questions:

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

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

- Create, rename, lock, and unlock a user account.
- Change a user's password.
- Rename or remove a user account.

This section covers the following Security Pro exam objective:

- 1.1 Create, modify, and delete user profiles.
  - Manage Linux Users and Groups
    - Create, rename, and delete users and groups
    - Assign users to appropriate groups
    - Lock and unlock user accounts
    - Change a user's password

Video/Demo	Time
2.7.1 Linux User and Group Overview	19:14
2.7.2 Managing Linux Users	9:28
Total Video Time	**28:42**

Lab/Activity

- 2.7.4 Create a User Account
- 2.7.5 Rename a User Account
- 2.7.6 Delete a User
- 2.7.7 Change Your Password
- 2.7.8 Change a User's Password
- 2.7.9 Lock and Unlock User Accounts

Fact Sheets

- 2.7.3 Linux User Commands and Files

Number of Exam Questions

7 questions

Total Time

About 71 minutes

2.8: 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?

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

- Create groups and define the group ID.
- Change secondary group membership for specific user accounts.
- Enable a group password.

This section covers the following Security Pro exam objective:

- 1.1 Create, modify, and delete user profiles.
  - Manage Linux Users and Groups
    - Create, rename, and delete users and groups
    - Assign users to appropriate groups

Video/Demo	Time
2.8.1 Managing Linux Groups	3:15
Total Video Time	**3:15**

Lab/Activity

- 2.8.3 Rename and Create Groups
- 2.8.4 Add Users to a Group
- 2.8.5 Remove a User from a Group

Fact Sheets

- 2.8.2 Linux Group Commands

Number of Exam Questions

3 questions

Total Time

About 27 minutes

2.9: Linux User Security

Lecture Focus Questions:

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

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

- Configure password aging.
- Configure password login limits.
- Configure the maximum concurrent logins by a user.
- Use the **ulimit** command to restrict user resource usage.

This section covers the following Security Pro exam objective:

- 1.1 Create, modify, and delete user profiles.
  - Manage Linux Users and Groups
    - Configure password aging
  - Restrict use of common access accounts

Video/Demo	Time
2.9.1 Linux User Security and Restrictions	9:53
2.9.2 Configuring Linux User Security and Restrictions	6:40
Total Video Time	**16:33**

Fact Sheets

2.9.3 Linux User Security and Restriction Facts

Number of Exam Questions

5 questions

Total Time

About 27 minutes

2.10: Group Policy Overview

Lecture Focus Questions:

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

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

- View the setting defined in a GPO.
- Create a GPO.
- Link a GPO to OUs.
- Edit the settings of a GPO.
- Import GPO settings.

This section covers the following Security Pro exam objectives:

- 1.1 Create, modify, and delete user profiles.
  - Manage Windows Local Users and Groups
    - Restrict use of local user accounts
  - Restrict use of common access accounts
- 1.2 Harden authentication.
  - Configure the Domain GPO to enforce User Account Control

Video/Demo	Time
2.10.1 Group Policy Overview	8:41
2.10.2 Viewing Group Policy	14:31
Total Video Time	**23:12**

Lab/Activity

2.10.4 Create and Link a GPO

Fact Sheets

2.10.3 Group Policy Facts

Number of Exam Questions

3 questions

Total Time

About 37 minutes

2.11: Hardening Authentication 1

Lecture Focus Questions:

- What characteristics on a Microsoft system typically define a *complex* password?
- What is the *clipping level* and how does it affect an account login?
- 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?

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

- Control logical access by configuring user account and account lockout policies.
- Configure day/time restrictions, computer restrictions, and expiration dates for user accounts.
- Enable and disable user accounts.
- Configure the password policy for a domain.
- Using Group Policy Management, configure security settings such as password policy settings to define requirements for user passwords.
- Using Group Policy Management, configure user right assignments to identify actions users can perform on a system.

This section covers the following Security Pro exam objectives:

- 1.1 Create, modify, and delete user profiles.
  - Manage Windows Local Users and Groups
    - Restrict use of local user accounts
  - Restrict use of common access accounts
- 1.2 Harden authentication.
  - Configure Domain GPO Account Policy to enforce a robust password policy
  - Disable or rename default accounts such as Guest and Administrator
- 5.1 Harden Network Devices (using a Cisco Small Business Switch).
  - Use secure passwords

Video/Demo	Time	
2.11.1 Hardening Authentication	19:31	
2.11.2 Configuring User Account Restrictions	9:30	
2.11.4 Configuring Account Policies and UAC Settings		14:18
2.11.6 Hardening User Accounts	10:20	
Total Video Time	**53:39**	

Lab/Activity

- 2.11.3 Configure User Account Restrictions
- 2.11.5 Configure Account Policies
- 2.11.7 Restrict Local Accounts

- 2.11.8 Secure Default Accounts
- 2.11.9 Enforce User Account Control

Fact Sheets

- 2.11.10 Hardening Authentication Facts

Number of Exam Questions

11 questions

Total Time

About 95 minutes

2.12: Hardening Authentication 2

Lecture Focus Questions:

- What are the two different categories of smart cards and how they are read by the smart card reader?
- What are the advantages and disadvantages of using smart cards?
- When would you choose to use *fine-grained* password policies?

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

- Configure authentication for a smart card.
- Implement a fine-grained password policy to create a more restrictive policy set.

This section covers the following Security Pro exam objectives:

- 1.1 Create, modify, and delete user profiles.
  - Manage Windows Local Users and Groups
    - Restrict use of local user accounts
  - Restrict use of common access accounts
- 1.2 Harden authentication.
  - Configure a GPO for Smart Card authentication for sensitive resources

Video/Demo	Time
2.12.1 Configuring Smart Card Authentication	6:20
2.12.4 Using Fine-Grained Password Policies	7:00
Total Video Time	**13:20**

Lab/Activity

- 2.12.2 Configure Smart Card Authentication
- 2.12.6 Create a Fine-Grained Password Policy

Fact Sheets

- 2.12.3 Smart Card Authentication Facts
- 2.12.5 Fine-Grained Password Policy Facts

Number of Exam Questions

5 questions

Total Time

About 39 minutes

2.13: Remote Access

Lecture Focus Questions:

- How does EAP differ from CHAP or MS-CHAP?
- What is the difference between *authentication* and *authorization*?
- How does tunneling protect packets in transit through an unsecured network?
- What are examples of criteria used to restrict remote access?
- Which remote server solution performs better and is considered more secure?
- What types of attacks are remote access servers vulnerable to?

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

- Configure a remote access server to accept remote access connections.
- Control remote access authorization using network policies.
- Configure ports on a VPN server to allow VPN connections.
- Configure a VPN client connection.

This section covers the following Security Pro exam objective:

- 1.2 Harden authentication.
  - Configure secure Remote Access

Video/Demo	Time
2.13.1 Remote Access	8:44
2.13.3 RADIUS and TACACS+	6:52
Total Video Time	**15:36**

Fact Sheets

- 2.13.2 Remote Access Facts
- 2.13.4 RADIUS and TACACS+ Facts

Number of Exam Questions

15 questions

Total Time

About 41 minutes

2.14: Network Authentication

Lecture Focus Questions:

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

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

- Edit Kerberos Policy settings using Group Policy Management.
- Provide authentication backwards compatibility for pre-Windows 2000 clients using Group Policy.

This section covers the following Security Pro exam objectives:

- 1.2 Harden authentication.
  - Implement centralized authentication
- 1.3 Manage Certificates.
  - Configure Domain GPO Kerberos Settings

Video/Demo	Time
2.14.1 Network Authentication Protocols	14:09
2.14.2 Network Authentication via LDAP	10:31
2.14.4 Controlling the Authentication Method	6:39
2.14.6 Browsing a Directory Tree via LDAP	6:38
2.14.7 Trusts and Transitive Access	5:34
2.14.9 Credential Management	10:06
Total Video Time	**53:37**

Lab/Activity

- 2.14.5 Configure Kerberos Policy Settings

Fact Sheets

- 2.14.3 Network Authentication Facts
- 2.14.8 Trusts and Transitive Access Facts
- 2.14.10 Credential Management Facts

Number of Exam Questions

14 questions

Total Time
About 88 minutes

2.15: Identity Management

Lecture Focus Questions:

- What are the advantages of implementing IDM? Disadvantages?
- What is the significance of the *authoritative source* of an item?
- What does entitlement define?
- What is automated provisioning?

Video/Demo	Time
2.15.1 Identity Management	16:31
Total Video Time	**16:31**

Fact Sheets

2.15.2 Identity Management Facts

Number of Exam Questions

4 questions

Total Time

About 26 minutes

3.1: Cryptography

Lecture Focus Questions:

- What is a legitimate use for cryptanalysis?
- How is the strength of a cryptosystem related to the length of the key?
- Which of the following is typically kept secret, the encryption algorithm or the key (or both)?
- What is the difference between a transposition cipher and a substitution cipher?
- What is a legitimate use of steganography?
- What methods are used in a brute force attack?
- What is the difference between a Registration Authority and a Certificate Authority?

This section covers the following Security Pro exam objective:

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

Video/Demo	Time
3.1.1 Cryptography Concepts	4:30
3.1.3 Cryptographic Attacks	17:48
Total Video Time	**22:18**

Fact Sheets

- 3.1.2 Cryptography Facts
- 3.1.4 Cryptographic Attack Facts

Number of Exam Questions

15 questions

Total Time

About 48 minutes

3.2: Hashing

Lecture Focus Questions:

- What security goal or function is provided by hashes?
- Why doesn't a hash provide message encryption?
- When comparing MD5 and SHA-1, which method provides greater security? Why?
- What is a *collision* and why is this condition undesirable in a hashing algorithm?
- Why is *high amplification* an indicator of a good hashing algorithm?

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

- Generate a hash value for a file.
- Compare hash values to verify message integrity.

Video/Demo		Time
3.2.1 Hashing		11:31
3.2.3 Using Hashes		7:43
	Total Video Time	**19:14**

Fact Sheets

3.2.2 Hashing Facts

Number of Exam Questions

12 questions

Total Time

About 37 minutes

3.3: Symmetric Encryption

Lecture Focus Questions:

- A user needs to communicate securely with 5 other users using symmetric key encryption. How many keys are required?
- How are symmetric keys typically exchanged between communication partners?
- What is an advantage of increasing the number of bits in the key? What is a disadvantage?
- Why are symmetric key stream ciphers considered to be slower than symmetric key block ciphers?
- Considering symmetric key stream ciphers and block ciphers, which would you select to process large amounts of data? Why?
- How does 3DES differ from DES?

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

- Perform a brute force analysis of encrypted data to recover original data.

Video/Demo	Time
3.3.1 Symmetric Encryption	5:27
3.3.2 HMAC	6:14
3.3.4 Cracking a Symmetric Encryption Key	4:11
Total Video Time	**15:52**

Fact Sheets

3.3.3 Symmetric Encryption Facts

Number of Exam Questions

15 questions

Total Time

About 36 minutes

3.4: Asymmetric Encryption

Lecture Focus Questions:

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

Video/Demo	Time
3.4.1 Asymmetric Encryption	8:56
Total Video Time	**8:56**

Fact Sheets

3.4.2 Asymmetric Encryption Facts

Number of Exam Questions

12 questions

Total Time

About 26 minutes

3.5: Public Key Infrastructure (PKI)

Lecture Focus Questions:

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

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

- Manage certificates by requesting, approving, and installing certificates.
- Revoke a certificate and publish it to the CRL.
- Create and configure a subordinate CA.
- Manage certificate templates by deploying certificates for different purposes.
- Create and issue custom certificate templates.

This section covers the following Security Pro exam objective:

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

Video/Demo	Time
3.5.1 Certificates	11:02
3.5.2 Managing Certificates	14:45
3.5.5 CA Implementation	5:17
3.5.6 Configuring a Subordinate CA	14:13
Total Video Time	**45:17**

Lab/Activity

- 3.5.3 Manage Certificates

Fact Sheets

- 3.5.4 Certificate Lifecycle Facts
- 3.5.7 PKI Management Facts

Number of Exam Questions

15 questions

Total Time

About 76 minutes

3.6: Cryptography Implementations

Lecture Focus Questions:

- What are the advantages of asymmetric over symmetric encryption? What are the disadvantages?
- How are asymmetric encryption and hashing combined to create digital signatures?
- What is the difference between digital *signatures* and digital *envelopes*?
- How does the protection offered by BitLocker differ from EFS?
- How does S-HTTP differ from HTTPS? Which is more secure?
- Which types of traffic can SSL protect?

Video/Demo	Time
3.6.1 Combining Cryptographic Methods	10:30
3.6.2 Hardware Based Encryption Devices	7:13
Total Video Time	**17:43**

Fact Sheets

3.6.3 Cryptographic Implementation Facts

Number of Exam Questions

15 questions

Total Time

About 38 minutes

4.1: Security Policies

Lecture Focus Questions:

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

This section covers the following Security Pro exam objective:

- 2.1 Promote Information Security Awareness.
  - Exchanging content between Home and Work
  - Storing of Personal Information on the Internet
  - Using Social Networking Sites
  - Password Management
  - Information Security

Video/Demo	Time
4.1.1 Security Policies	7:23
4.1.2 Data Privacy Laws	9:43
4.1.6 Information Classification	5:40
4.1.8 Data Retention Policies	11:40
4.1.9 Wiping a Hard Drive	12:58
Total Video Time	**47:24**

Fact Sheets

- 4.1.3 Security Policy Facts
- 4.1.4 Security Documentation Facts
- 4.1.5 Security Management Facts
- 4.1.7 Information Classification Facts
- 4.1.10 Data Retention Facts

Number of Exam Questions

15 questions

Total Time

About 88 minutes

4.2: Manageable Network Plan

Lecture Focus Questions:

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

This section covers the following Security Pro exam objective:

- 2.3 Maintain Hardware and Software Inventory.

Video/Demo	Time
4.2.1 Manageable Network Plan	16:49
4.2.2 Manageable Network Plan 2	14:05
Total Video Time	**30:54**

Fact Sheets

4.2.3 Manageable Network Plan Facts

Number of Exam Questions

3 questions

Total Time

About 39 minutes

4.3: Business Continuity

Lecture Focus Questions:

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

This section covers the following Security Pro exam objective:

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

Video/Demo	Time
4.3.1 Business Continuity	2:39
4.3.2 Succession Planning	5:23
Total Video Time	**8:02**

Fact Sheets

4.3.3 Business Continuity Facts

Number of Exam Questions

7 questions

Total Time

About 21 minutes

4.4: Risk Management

Lecture Focus Questions:

- What kinds of components are *tangible* assets?
- How can an asset have both a tangible and intangible value?
- Why is determining the value of an asset important to an organization?
- How is *quantitative* analysis different than *qualitative* analysis?
- Which components are used to measure risk quantitatively?
- What method is typically deployed in risk *transference*?
- Why is risk *rejection* not a wise risk response?

Video/Demo	Time
4.4.1 Risk Management	4:04
4.4.2 Security Controls	3:21
4.4.3 Data Loss Prevention (DLP)	4:57
Total Video Time	**12:22**

Fact Sheets

4.4.4 Risk Management Facts

Number of Exam Questions

15 questions

Total Time

About 33 minutes

4.5: Incident Response

Lecture Focus Questions:

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

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

- Gather and authenticate forensic information from a system using a computer forensic tool.
- Analyze and record forensic evidence.
- View and build a case using the forensic evidence that has been gathered.

Video/Demo	Time
4.5.1 First Responder	7:17
4.5.2 Basic Forensic Procedures	18:31
4.5.3 Using Forensic Tools	6:17
4.5.4 Creating a Forensic Drive Image	10:00
Total Video Time	**42:05**

Fact Sheets

- 4.5.5 Incident Response Facts
- 4.5.6 Forensic Investigation Facts

Number of Exam Questions

15 questions

Total Time

About 68 minutes

4.6: Social Engineering

Lecture Focus Questions:

- How is *passive* social engineering different than *active* social engineering?
- What methods do attackers use to make an interaction appear legitimate?
- How is employee awareness training the most effective countermeasure for social engineering?
- What specific countermeasures should be implemented to mitigate social engineering?
- How is tailgating different than piggybacking?
- How does using bookmarks instead of e-mail links improve security?

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

- Identify and ignore e-mail hoaxes to protect system resources.
- Train users to identify phishing scams by mousing over links, verifying the URL, and verifying HTTPS.

Video/Demo	Time
4.6.1 Social Engineering	4:40
4.6.2 Phishing Variations	13:04
4.6.4 Investigating a Social Engineering Attack	9:45
Total Video Time	**27:29**

Lab/Activity

- 4.6.5 Respond to Social Engineering

Fact Sheets

- 4.6.3 Social Engineering Facts

Number of Exam Questions

15 questions

Total Time

About 53 minutes

4.7: Certification and Accreditation

Lecture Focus Questions:

- Which methods does a reference monitor use to determine levels of access?
- Where is the reference monitor in relation to the security perimeter?
- How does *layering* provide security to an operating system?
- In a layered system, where does the operating system function?
- How does commercial classification labeling differ from military?
- How does acceptance differ from certification and accreditation?

Video/Demo	Time
4.7.1 Trusted Computing	10:01
4.7.2 Certification and Accreditation	4:46
Total Video Time	**14:47**

Fact Sheets

4.7.3 Certification and Accreditation Facts

Number of Exam Questions

12 questions

Total Time

About 32 minutes

4.8: Development

Lecture Focus Questions:

- How does the *spiral* model combine the *waterfall* model and the *prototype* model?
- How should security be employed in the different stages of development?
- What does *functional design* entail?
- When is change control necessary?
- What are the responsibilities of developers after a product is released?

Video/Demo	Time
4.8.1 System Development Life Cycle	8:40
4.8.2 System Development Life Cycle 2	7:49
Total Video Time	**16:29**

Fact Sheets

- 4.8.3 SDLC Facts
- 4.8.4 Software Development Models

Number of Exam Questions

7 questions

Total Time

About 34 minutes

4.9: Employee Management

Lecture Focus Questions:

- How can pre-employment processing improve the security of an organization?
- What is the role of the policy handbook regarding security?
- What guidelines must be considered when monitoring employees?
- Why should employees be required to sign employment agreements?
- How are *separation of duties* and *two-man control* different?
- How can collusion be avoided?
- What is the importance of a clear job description?

Video/Demo	Time
4.9.1 Employment Practices	13:45
Total Video Time	**13:45**

Fact Sheets

- 4.9.2 Employee Management Facts
- 4.9.3 Employee Documents Facts
- 4.9.4 Ethics Facts

Number of Exam Questions

15 questions

Total Time

About 44 minutes

4.10: Third-Party Integration

Lecture Focus Questions:

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

Video/Demo	Time
4.10.1 Third-Party Integration Security Issues	11:24
Total Video Time	**11:24**

Fact Sheets

4.10.2 Third-Party Integration Security Facts

Number of Exam Questions

4 questions

Total Time

About 21 minutes

5.1: Physical Security

Lecture Focus Questions:

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

This section covers the following Security Pro exam objective:

- 3.1 Harden Data Center Physical Access.
  - Implement Access Rosters
  - Utilize Visitor Identification and control
  - Protect Doors and Windows
  - Implement Physical Intrusion Detection Systems

Video/Demo	Time
5.1.1 Physical Security	18:39
5.1.2 Tailgating and Piggybacking	3:28
Total Video Time	**22:07**

Lab/Activity

- 5.1.4 Implement Physical Security

Fact Sheets

- 5.1.3 Physical Security Facts

Number of Exam Questions

15 questions

Total Time

About 48 minutes

5.2: Hardware Security

Lecture Focus Questions:

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

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

- Protect the physical access of a workstation.

This section covers the following Security Pro exam objective:

- 3.1 Harden Data Center Physical Access.
  - Utilize Visitor Identification and control
  - Protect Doors and Windows
  - Implement Physical Intrusion Detection Systems

Video/Demo	Time
5.2.1 Hardware Security Guidelines	7:50
5.2.2 Breaking into a System	7:30
Total Video Time	**15:20**

Fact Sheets

5.2.3 Hardware Security Facts

Number of Exam Questions

4 questions

Total Time

About 25 minutes

5.3: Environmental Controls

Lecture Focus Questions:

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

Video/Demo	Time
5.3.1 Environmental Controls	6:00
5.3.2 Environmental Monitoring	11:33
5.3.3 Hot and Cold Aisles	5:17
Total Video Time	**22:50**

Fact Sheets

- 5.3.4 Environmental Control Facts
- 5.3.5 Fire Protection Facts

Number of Exam Questions

11 questions

Total Time

About 44 minutes

5.4: Mobile Devices

Lecture Focus Questions:

- What types of electronic devices are considered part of the mobile devices group?
- How do you unlock a mobile device after it has gone into *lockout*?
- Under what conditions would you consider using *remote wipe* on a mobile device?
- What mobile device feature can display its current location if lost or stolen?
- What security technique ensures data confidentiality if a mobile device is lost or stolen?

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

- Secure a mobile device.

This section covers the following Security Pro exam objectives:

- 2.1 Promote Information Security Awareness.
  - Traveling with Personal Mobile Devices
  - Exchanging content between Home and Work
  - Password Management
  - Photo/GPS Integration
  - Information Security
  - Auto-lock and Passcode Lock
- 3.2 Harden mobile devices (Laptop).
  - Set a BIOS Password
  - Set a Login Password
  - Implement full disk encryption
- 6.2 Implement Patch Management/System Updates.
  - Apply the latest Apple Software Updates

Video/Demo	Time
5.4.1 Mobile Device Security	7:34
5.4.3 BYOD Security Issues	9:33
5.4.5 Securing Mobile Devices	10:20
Total Video Time	**27:27**

Lab/Activity

- 5.4.6 Secure an iPad

Fact Sheets

- 5.4.2 Mobile Device Security Facts
- 5.4.4 BYOD Security Facts

Number of Exam Questions
8 questions

Total Time
About 51 minutes

5.5: Mobile Device Security Enforcement

Lecture Focus Questions:

- What is the role of a *mobile device management (MDM)* solution?
- What are the two different types of configurations that can be used when deploying Windows Intune?
- Which Intune management portal is used by end users to manage their own account and enroll devices?
- Windows Intune uses two types of groups to manage users and devices. Which group is used to deploy Intune agent settings?
- What two ways can you enroll standard computer systems in Windows Intune?

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

- Edit and enforce various mobile device policies.
- Create and configure a new user account.
- Enroll a mobile device and link it to a user account.
- Perform remote tasks on a mobile device, including a remote wipe.

Video/Demo	Time
5.5.1 Enforcing Security Policies on Mobile Devices	7:57
5.5.2 Enrolling Devices and Performing a Remote Wipe	8:49
5.5.4 Mobile Application Security	9:00
Total Video Time	**25:46**

Fact Sheets

- 5.5.3 Mobile Device Security Enforcement Facts
- 5.5.5 Mobile Application Security Facts

Number of Exam Questions

8 questions

Total Time

About 44 minutes

5.6: Telephony

Lecture Focus Questions:

- What methods can be used to send digital data through Plain Old Telephone System (POTS) lines?
- What are common threats to a PBX system? How do you secure the PBX?
- What types of security issues must be considered when using VoIP?
- What is the difference between *cramming* and *slamming*?
- What countermeasures protect against war dialing?
- What is the function of the SIP protocol?
- How can VLANs increase network security on systems with VoIP implemented?

Video/Demo	Time
5.6.1 Telephony	15:00
Total Video Time	**15:00**

Fact Sheets

5.6.2 Telephony Security Facts

Number of Exam Questions

4 questions

Total Time

About 24 minutes

6.1: Network Layer Protocol Review

Lecture Focus Questions:

- What is the OSI model and why is it important in understanding networking?
- What are the advantages of using a theoretical model to describe networking?
- What type of network would the 192.168.174.34 address represent?
- What are the two parts of an IPv6 address and what do they represent?
- Under what conditions would you choose to subnet a network?

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

- Configure IPv6.
- Configure subnetting.

Video/Demo	Time
6.1.1 OSI Model	4:08
6.1.3 IP Addressing	17:22
6.1.5 Configuring IPv6	5:28
6.1.6 IP Subnetting	12:35
6.1.7 Configuring Subnetting	8:07
Total Video Time	**47:40**

Fact Sheets

- 6.1.2 OSI Model Facts
- 6.1.4 IP Address Facts
- 6.1.8 Subnetting Facts

Number of Exam Questions

9 questions

Total Time

About 72 minutes

6.2: Transport Layer Protocol Review

Lecture Focus Questions:

- What are the major differences between TCP and UDP?
- How can ICMP messages be used to provide a valuable security tool?
- What is the best practice when deciding which protocol ports to allow through a network firewall?
- Why would an administrator find it important to run a port scanner on the system?

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

- Analyze a TCP three-way handshake.

Video/Demo	Time
6.2.1 Network Protocols	4:45
6.2.3 Analyzing a TCP Three-way Handshake	2:14
6.2.4 TCP and UDP Ports	9:02
Total Video Time	**16:01**

Fact Sheets

- 6.2.2 Network Protocol Facts
- 6.2.5 Common Ports

Number of Exam Questions

15 questions

Total Time

About 42 minutes

6.3: Perimeter Attacks 1

Lecture Focus Questions:

- What types of resources make organizational reconnaissance so readily available?
- How is *footprinting* used to determine the operating system of the recipient?
- How does a Distributed Reflective Denial of Service (DRDoS) increase the severity of a DoS attack?
- What countermeasures will help to mitigate DoS and DDoS attacks?

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

- View and analyze captured traffic using a network analyzer.
- Analyze captured traffic to determine the extent to which the bandwidth is being compromised.
- Perform a port scan on a system using **netstat** to determine connections and listening ports.
- Perform a port scan using **nmap** to find all the open ports on a remote system.
- Use a UDP flooder to test network bandwidth.
- Scan for MAC addresses and the corresponding IP addresses using a MAC address scanning tool.
- Perform an ARP poisoning attack on a host to identify vulnerabilities.
- Use a sniffer to detect an unusually high traffic pattern of ARP replies.

Video/Demo	Time
6.3.1 Reconnaissance	2:40
6.3.2 Performing Reconnaissance	9:01
6.3.4 Denial of Service (DoS)	7:49
6.3.5 Xmas Tree Attacks	3:23
6.3.7 Performing a UDP Flood Attack	3:54
Total Video Time	**26:47**

Fact Sheets

- 6.3.3 Reconnaissance Facts
- 6.3.6 DoS Attack Facts

Number of Exam Questions

15 questions

Total Time

About 52 minutes

6.4: Perimeter Attacks 2

Lecture Focus Questions:

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

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

- Perform queries on name server records using **nslookup**.
- Restrict zone transfers to specific servers.
- Map malicious Web sites to a loopback address (127.0.0.0) in the HOSTS file.
- Identify who has registered a domain name using **Whois.net** and **SamSpade.org**.
- Gather organizational information using Google, job boards, or other common Internet tools.

Video/Demo	Time
6.4.1 Session and Spoofing Attacks	6:41
6.4.3 Performing ARP Poisoning	4:24
6.4.5 DNS Attacks	4:30
6.4.7 Examining DNS Attacks	13:29
Total Video Time	**29:04**

Lab/Activity

- 6.4.8 Prevent Zone Transfers

Fact Sheets

- 6.4.2 Session Based Attack Facts
- 6.4.4 Spoofing Facts
- 6.4.6 DNS Attack Facts

Number of Exam Questions

15 questions

Total Time

About 65 minutes

6.5: Security Appliances

Lecture Focus Questions:

- To which security device might you choose to restrict access by user account?
- What types of restrictions can be configured for proxy servers?
- What types of entities commonly use Internet content filtering software?
- What functions does keyword filtering provide?
- How can Network Access Controls (NAC) help to improve the security of a network?

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

- Enable Parental Controls for a user and configure control settings for allowed Web sites, time limits, games, and specific programs.
- Enable *activity reporting* to view Web browsing activities of a user in which you have configured parental controls.
- Manage users on a security appliance.
- Restrict access to a security appliance based on IP address.
- Use a security appliance to set a user for LAN access only.

This section covers the following Security Pro exam objectives:

- 4.1 Harden the Network Perimeter (using a Cisco Network Security Appliance).
  - Change the Default Username and Password
- 7.1 Implement Application Defenses.
  - Configure Parental Controls to enforce Web content filtering

Video/Demo	Time
6.5.1 Security Solutions	4:02
6.5.2 Security Zones	5:32
6.5.4 All-In-One Security Appliances	4:30
6.5.6 Configuring Network Security Appliance Access	6:55
Total Video Time	**20:59**

Lab/Activity

- 6.5.7 Configure Network Security Appliance Access

Fact Sheets

- 6.5.3 Security Zone Facts
- 6.5.5 Security Solution Facts

Number of Exam Questions

4 questions

Total Time

About 40 minutes

6.6: Demilitarized Zones (DMZ)

Lecture Focus Questions:

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

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

- Add a server to a DMZ.
- Configure a DMZ port to act as a DHCP Server.

This section covers the following Security Pro exam objective:

- 4.1 Harden the Network Perimeter (using a Cisco Network Security Appliance).
  - Create a DMZ

Video/Demo		Time
6.6.1 Demilitarized Zones		9:49
6.6.2 Configuring a DMZ		5:42
	Total Video Time	**15:31**

Lab/Activity

6.6.3 Configure a DMZ

Fact Sheets

6.6.4 DMZ Facts

Number of Exam Questions

8 questions

Total Time

About 34 minutes

6.7: Firewalls

Lecture Focus Questions:

- What is the difference between a network-based firewall and a host-based firewall?
- When would you choose to implement a host-based firewall?
- What traffic characteristics can be specified in a filtering rule for a packet filtering firewall?
- How does a packet filtering firewall differ from a circuit-level gateway?
- Why is a packet filtering firewall a *stateless* device?
- What types of filter criteria can an application layer firewall use for filtering?

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

- Enable Windows Firewall and configure exceptions to control communications through the firewall.
- Configure inbound and outbound rules to control traffic.
- Create a custom rule to allow ICMP Echo Requests through a firewall.
- Import and export firewall rules to other machines to create firewalls with uniform settings.

This section covers the following Security Pro exam objective:

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

Video/Demo	Time
6.7.1 Firewalls	5:33
6.7.3 Configuring a Perimeter Firewall	9:47
Total Video Time	**15:20**

Lab/Activity

6.7.4 Configure a Perimeter Firewall

Fact Sheets

6.7.2 Firewall Facts

Number of Exam Questions

15 questions

Total Time

About 41 minutes

6.8: Network Address Translation (NAT)

Lecture Focus Questions:

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

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

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

This section covers the following Security Pro exam objective:

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

Video/Demo	Time
6.8.1 Network Address Translation	15:57
6.8.2 Configuring NAT	5:11
Total Video Time	**21:08**

Fact Sheets

6.8.3 NAT Facts

Number of Exam Questions

6 questions

Total Time

About 33 minutes

6.9: Virtual Private Networks (VPN)

Lecture Focus Questions:

- What are the three ways VPNs can be implemented?
- What is a VPN concentrator?
- What function do VPN endpoints provide?
- Which IPsec mode does not encrypt the header of a transmission? Why?
- What are the three types of protocols used by VPNs?
- Which IPsec protocol does not encrypt data?

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

- Configure a remote access VPN connection.

This section covers the following Security Pro exam objective:

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

Video/Demo	Time
6.9.1 Virtual Private Networks (VPNs)	10:16
6.9.2 Configuring a VPN	4:25
Total Video Time	**14:41**

Lab/Activity

- 6.9.3 Configure a Remote Access VPN
- 6.9.4 Configure a VPN Connection iPad

Fact Sheets

- 6.9.5 VPN Facts
- 6.9.6 VPN Protocol Facts

Number of Exam Questions

11 questions

Total Time

About 46 minutes

6.10: Web Threat Protection

Lecture Focus Questions:

- How have Web threats become more sophisticated?
- Which Web threat protections prevent a user from visiting restricted Web sites?
- How is Web threat filtering implemented?
- What types of filters can be used by spam blockers?

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

- Configure Web threat protection.

This section covers the following Security Pro exam objectives:

- 4.1 Harden the Network Perimeter (using a Cisco Network Security Appliance).
  - Implement Web Threat Protection
- 7.1 Implement Application Defenses.
  - Configure Parental Controls to enforce Web content filtering

Video/Demo	Time
6.10.1 Web Threat Protection	9:29
6.10.2 Configuring Web Threat Protection	4:26
Total Video Time	**13:55**

Lab/Activity

6.10.3 Configure Web Threat Protection

Fact Sheets

6.10.4 Web Threat Protection Facts

Number of Exam Questions

4 questions

Total Time

About 28 minutes

6.11: Network Access Control (NAC)

Lecture Focus Questions:

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

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

- Configure Network Access Protection to restrict network access to only clients that meet specified health criteria.
- Add the necessary role services to implement Network Access Protection (NAP).
- Enable NAP on an enforcement point.
- Create domain and server isolation rules.
- Configure system health validator and health policy settings.

Video/Demo	Time
6.11.1 Network Access Protection	19:58
6.11.2 Implementing NAP with DHCP Enforcement	15:56
Total Video Time	**35:54**

Fact Sheets

6.11.3 NAP Facts

Number of Exam Questions

4 questions

Total Time

About 45 minutes

6.12: Wireless Overview

Lecture Focus Questions:

- What is the role of a wireless access point (WAP)?
- What is the difference in functionality between an *omnidirectional* antenna and a *directional* antenna?
- What two methods are available for configuring a wireless network?
- What are the advantages of using the WiMAX protocol for long-range wireless networking?

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

- Manually connect to a wireless network.
- Manage wireless networks.
- Secure a wireless network from unauthorized connections.

Video/Demo	Time
6.12.1 Wireless Networking Overview	5:35
6.12.2 Wireless Antenna Types	8:03
6.12.4 Wireless Encryption	6:46
6.12.6 Configuring a Wireless Connection	12:22
Total Video Time	**32:46**

Lab/Activity

- 6.12.7 Secure a Wireless Network

Fact Sheets

- 6.12.3 Wireless Networking Facts
- 6.12.5 Wireless Encryption Facts

Number of Exam Questions

15 questions

Total Time

About 63 minutes

6.13: Wireless Attacks

Lecture Focus Questions:

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

Video/Demo	Time
6.13.1 Wireless Attacks	13:29
6.13.3 Using Wireless Attack Tools	9:06
6.13.4 Detecting Rogue Hosts	7:37
Total Video Time	**30:12**

Fact Sheets

- 6.13.2 Wireless Attack Facts

Number of Exam Questions

15 questions

Total Time

About 51 minutes

6.14: Wireless Defenses

Lecture Focus Questions:

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

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

- Configure a wireless access point by disabling the SSID broadcast and enabling security.
- Configure a wireless network profile to automatically connect even if the SSID broadcast is turned off.
- Scan a network to detect wireless access points and determine if the access points are secure.

This section covers the following Security Pro exam objective:

- 4.2 Secure Wireless Devices and Clients.
  - Change the Default Username, Password, and Administration limits
  - Implement WPA2
  - Configure Enhanced Security
    - MAC filtering
    - SSID cloaking
    - Power Control
  - Disable Network Discovery

Video/Demo	Time
6.14.1 Wireless Security Considerations	12:54
6.14.2 Wireless Authentication	4:40
6.14.4 Configuring a Wireless Access Point	19:54
6.14.7 Configuring a Captive Portal	12:02
Total Video Time	**49:30**

Lab/Activity

- 6.14.5 Obscure a Wireless Network
- 6.14.6 Configure a Wireless Profile

Fact Sheets

- 6.14.3 Wireless Authentication Facts
- 6.14.8 Wireless Security Facts

Number of Exam Questions

15 questions

Total Time

About 85 minutes

7.1: Network Devices

Lecture Focus Questions:

- What are the security advantages of using switches over hubs?
- What security problems could static routing pose on a large network?
- What security threat do broadcasts allow?
- What information does a router ACL use to allow or reject packets?

Video/Demo		Time
7.1.1 Network Devices		5:51
	Total Video Time	**5:51**

Fact Sheets

7.1.2 Network Device Facts

Number of Exam Questions

7 questions

Total Time

About 18 minutes

7.2: Network Device Vulnerabilities

Lecture Focus Questions:

- For security considerations, what is the first thing you should do when new hardware and software is turned on for the first time?
- What are the characteristics of a complex password?
- How is privilege escalation different than hacking into a system to gain access to resources?
- What measures should be completed to protect against backdoors?

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

- Search a database for default passwords for network devices.

This section covers the following Security Pro exam objective:

- 5.1 Harden Network Devices (using a Cisco Small Business Switch).
  - Change the Default Username and Password on network devices

Video/Demo	Time
7.2.1 Device Vulnerabilities	1:47
7.2.3 Searching Defaultpasswords.com	1:23
7.2.4 Securing a Switch	3:21
Total Video Time	**6:31**

Lab/Activity

- 7.2.5 Secure a Switch

Fact Sheets

- 7.2.2 Device Vulnerability Facts

Number of Exam Questions

4 questions

Total Time

About 21 minutes

7.3: Switch Attacks

Lecture Focus Questions:

- What types of attacks are commonly perpetrated against switches?
- How does MAC flooding make a switch function as a hub? What is this state called?
- How are switches indirectly involved in ARP poisoning?
- How does the attacker hide his identity when performing MAC spoofing?
- What is a more secure alternative to using the Dynamic Trunking Protocol (DTP)?

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

- Secure a switch.

This section covers the following Security Pro exam objective:

- 5.1 Harden Network Devices (using a Cisco Small Business Switch).
  - Implement Port Security

Video/Demo		Time
7.3.1 Switch Attacks		5:04
	Total Video Time	**5:04**

Fact Sheets

7.3.2 Switch Attack Facts

Number of Exam Questions

4 questions

Total Time

About 15 minutes

7.4: Router Security

Lecture Focus Questions:

- What hashing algorithm is used to encrypt the password on a Cisco device?
- What secure protocols should you use to remotely manage a router?
- What type of actions can be used to ensure the physical security of network devices?

This section covers the following Security Pro exam objectives:

- 5.1 Harden Network Devices (using a Cisco Small Business Switch).
  - Shut down unneeded services and ports
  - Implement Port Security
  - Remove unsecure protocols (FTP, telnet, rlogin, rsh)
  - Run latest iOS version
- 8.2 Protect Data Transmissions across open, public networks.
  - Encrypt Data Communications

Video/Demo		Time
7.4.1 Router Security		8:57
	Total Video Time	**8:57**

Fact Sheets

7.4.2 Router Security Facts

Number of Exam Questions

4 questions

Total Time

About 18 minutes

7.5: Switch Security

Lecture Focus Questions:

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

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

- Create VLANs and assign switch ports to VLANs.
- Configure a trunk port on a switch.
- Harden a switch.
- Secure access to a new switch.

This section covers the following Security Pro exam objective:

- 5.1 Harden Network Devices (using a Cisco Small Business Switch).
  - Implement Port Security
  - Remove unsecure protocols (FTP, telnet, rlogin, rsh)
  - Run latest iOS version
  - Segment Traffic using VLANs

Video/Demo	Time
7.5.1 Switch Security	13:01
7.5.2 Switch Loop Protection	10:47
7.5.4 Configuring VLANs from the CLI	4:32
7.5.6 Configuring VLANs	3:32
7.5.8 Hardening a Switch	14:10
Total Video Time	**46:02**

Lab/Activity

- 7.5.5 Explore VLANs from the CLI
- 7.5.7 Explore VLANs
- 7.5.9 Harden a Switch
- 7.5.10 Secure Access to a Switch
- 7.5.11 Secure Access to a Switch 2

Fact Sheets

- 7.5.3 Switch Security Facts

Number of Exam Questions

15 questions

Total Time

About 92 minutes

7.6: Intrusion Detection and Prevention

Lecture Focus Questions:

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

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

- Monitor network activity using intrusion detection software to capture and view network traffic.

Video/Demo	Time
7.6.1 Intrusion Detection	7:14
7.6.2 Detection vs. Prevention Controls	7:50
7.6.4 Implementing Intrusion Monitoring	3:33
7.6.5 Implementing Intrusion Prevention	7:51
Total Video Time	**26:28**

Lab/Activity

- 7.6.6 Implement Intrusion Prevention

Fact Sheets

- 7.6.3 IDS Facts

Number of Exam Questions

15 questions

Total Time

About 52 minutes

7.7: SAN Security

Lecture Focus Questions:

- How does LUN masking increase security?
- What are the three different ways that fabric zoning can be implemented?
- What is the role of VSANs?
- What device connection controls can be implemented to protect SANs from common network attacks?
- What types of authentication mechanisms are available for Fibre Channel SANs?

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

- Secure an iSCSI SAN using an access control list and mutual authentication.

Video/Demo	Time
7.7.1 SAN Security Issues	14:32
7.7.2 Configuring an iSCSI SAN	9:57
Total Video Time	**24:29**

Fact Sheets

7.7.3 SAN Security Facts

Number of Exam Questions

5 questions

Total Time

About 35 minutes

8.1: Malware

Lecture Focus Questions:

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

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

- Scan a system with anti-malware software to identify potential threats.
- Configure Windows Defender protections to secure a network from malware.
- Quarantine and remove malware.
- Analyze startup programs to detect possible malware.

This section covers the following Security Pro exam objectives:

- 6.1 Harden Computer Systems Against Attack.
  - Protect against spyware and unwanted software using Windows Defender

- 9.2 Review security logs and violation reports, implement remediation.

Video/Demo	Time
8.1.1 Malware	9:28
8.1.4 Implementing Malware Protections	23:43
8.1.5 Using Windows Defender	14:22
Total Video Time	**47:33**

Lab/Activity

- 8.1.6 Configure Windows Defender

Fact Sheets

- 8.1.2 Malware Facts
- 8.1.3 Malware Protection Facts

Number of Exam Questions

15 questions

Total Time

About 78 minutes

8.2: Password Attacks

Lecture Focus Questions:

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

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

- Analyze the strength of passwords by using a rainbow table to perform a cryptanalysis attack on the hashed values of passwords.
- Use SnadBoy's Revelation to reveal a password.
- Use a keylogger to capture a password.

Video/Demo	Time
8.2.1 Password Attacks	2:04
8.2.3 Using Rainbow Tables	4:48
8.2.4 Capturing Passwords	5:40
Total Video Time	**12:32**

Fact Sheets

8.2.2 Password Attack Facts

Number of Exam Questions

4 questions

Total Time

About 22 minutes

8.3: Windows System Hardening

Lecture Focus Questions:

- What is *hardening*? How does it benefit the security of an organization?
- How do you reduce the attack surface of a device?
- What is a *security baseline*?
- What is the difference between a *hotfix* and a *patch*? Why would you use one over the other?

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

- Harden a system by changing default account passwords and verifying user and group assignments.
- Lock down system security by installing only required software and roles and disabling unnecessary services.
- Use security templates to apply or audit security settings on your system.
- Use Group Policy to deploy multiple settings to multiple machines in an Active Directory domain.
- Use Windows Updates and WSUS to automate patch management of your Windows system.

This section covers the following Security Pro exam objectives:

- 6.1 Harden Computer Systems Against Attack.
  - Configure a GPO to enforce Workstation/Server security settings
  - Configure Domain GPO to enforce use of Windows Firewall
- 6.2 Implement Patch Management/System Updates.
  - Configure Windows Update

Video/Demo

	Time
8.3.1 Operating System Hardening	5:13
8.3.3 Hardening an Operating System	6:41
8.3.4 Managing Automatic Updates	18:31
8.3.6 Configuring Windows Firewall	10:11
8.3.8 Configuring Windows Firewall Advanced Features	16:59
8.3.9 Configuring Parental Controls	18:21
Total Video Time	**1:15:56**

Lab/Activity

- 8.3.5 Configure Automatic Updates
- 8.3.7 Configure Windows Firewall
- 8.3.10 Configure Parental Controls

Fact Sheets

- 8.3.2 Hardening Facts

Number of Exam Questions
10 questions

Total Time
About 106 minutes

8.4: Hardening Enforcement

Lecture Focus Questions:

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

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

- Configure a GPO.
- Implement controls using a security template.

This section covers the following Security Pro exam objective:

- 6.1 Harden Computer Systems Against Attack.
  - Configure a GPO to enforce Workstation/Server security settings
  - Configure Domain Servers GPO to remove unneeded services (such as File and Printer Sharing)

Video/Demo	Time
8.4.1 Hardening Enforcement with GPOs	1:50
8.4.2 Using Security Templates and Group Policy	6:53
8.4.3 Configuring GPOs to Enforce Security	15:24
Total Video Time	**24:07**

Lab/Activity

- 8.4.5 Manage Services with Group Policy

Fact Sheets

- 8.4.4 Hardening Enforcement Facts

Number of Exam Questions

4 questions

Total Time

About 39 minutes

8.5: File Server Security

Lecture Focus Questions:

- How can you identify if a permission has been inherited?
- How do Share and NTFS permissions differ?
- On what elements can NTFS permissions be set?
- How can you view the users that have permissions for a particular drive?
- How can permissions inheritance influence the effective permissions that a user has? How can you determine if a permission is inherited or specifically assigned?
- As the administrator, you have given Fred the write permission to the SalesReport file, but he cannot write to the file. What items would you check to determine why Fred can't write to the file?

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

- Configure the NTFS permissions by turning off the permissions inheritance.
- Assign NTFS permission for a folder to the appropriate group.

This section covers the following Security Pro exam objectives:

- 6.1 Harden Computer Systems Against Attack.
  - Configure NTFS Permissions for Secure file sharing
- 8.2 Protect Data Transmissions across open, public networks.
  - Implement secure protocols

Video/Demo	Time
8.5.1 File Server Security	7:58
8.5.2 Scanning for Open Ports	3:52
8.5.5 Configuring NTFS Permissions	14:05
Total Video Time	**25:55**

Lab/Activity

- 8.5.6 Configure NTFS Permissions
- 8.5.7 Disable Inheritance

Fact Sheets

- 8.5.3 File System Security Facts
- 8.5.4 File Permission Facts

Number of Exam Questions

8 questions

Total Time

About 54 minutes

8.6: Linux Host Security

Lecture Focus Questions:

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

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

- Scan for open ports on Linux.
- Identify open network connections on Linux.

Video/Demo	Time
8.6.1 Linux Host Security	7:10
8.6.2 Removing Unneeded Services and Scanning Ports	6:30
Total Video Time	**13:40**

Fact Sheets

8.6.3 Network Security Facts

Number of Exam Questions

4 questions

Total Time

About 23 minutes

8.7: Static Environment Security

Lecture Focus Questions:

- What type of common consumer devices have been used to conduct malicious activities?
- What are the reasons that smart devices are common targets for cipher criminals?

Video/Demo	Time
8.7.1 Security Risks in Static Environments	4:26
Total Video Time	**4:26**

Fact Sheets

8.7.2 Static Environment Security Facts

Number of Exam Questions

3 questions

Total Time

About 13 minutes

9.1: Web Application Attacks

Lecture Focus Questions:

- What are two ways that drive-by download attacks occur?
- What countermeasures can be used to eliminate buffer overflow attacks?
- How can cross-site scripting (XSS) be used to breach the security of a Web user?
- What is the best method to prevent SQL injection attacks?
- What mitigation practices will help to protect Internet-based activities from Web application attacks?

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

- Improve security by using a Firefox add-on, NoScript, to protect against XSS and drive-by-downloadings.
- Configure pop-up blockers to block or allow pop-ups.
- Implement phishing protection within the browser.
- Configure Internet Explorer Enhanced Security Configuration security settings to manage the security levels of security zones.

This section covers the following Security Pro exam objective:

- 7.1 Implement Application Defenses.
  - Configure Web Application Security

Video/Demo	Time
9.1.1 Web Application Attacks	2:49
9.1.2 Cross-site Request Forgery (XSRF) Attack	10:51
9.1.3 Injection Attacks	14:30
9.1.4 Header Manipulation	9:01
9.1.5 Zero Day Application Attacks	6:59
9.1.6 Client Side Attacks	6:22
9.1.8 Preventing Cross-site Scripting	4:05
Total Video Time	**54:37**

Fact Sheets

9.1.7 Web Application Attack Facts

Number of Exam Questions

15 questions

Total Time

About 75 minutes

9.2: Internet Browsers

Lecture Focus Questions:

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

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

- Customize security levels and security settings for security zones in Internet Explorer.
- Download and manage add-ons in Internet Explorer.
- Protect privacy by configuring cookie handling.
- Clear the browser cache.

This section covers the following Security Pro exam objective:

- 7.1 Implement Application Defenses.
  - Configure a GPO to enforce Internet Explorer settings
  - Configure Secure Browser Settings

Video/Demo	Time
9.2.1 Managing Security Zones and Add-ons	20:26
9.2.2 Configuring IE Enhanced Security	9:11
9.2.3 Managing Cookies	12:38
9.2.5 Clearing the Browser Cache	9:28
9.2.7 Implementing Popup Blockers	7:26
9.2.10 Enforcing IE Settings through GPO	12:47
Total Video Time	**1:11:56**

Lab/Activity

- 9.2.4 Configure Cookie Handling
- 9.2.6 Clear the Browser Cache
- 9.2.8 Configure IE Popup Blocker
- 9.2.11 Enforce IE Settings through GPO
- 9.2.12 Configure IE Preferences in a GPO

Fact Sheets

- 9.2.9 Internet Explorer Security Facts

Number of Exam Questions
8 questions

Total Time
About 110 minutes

9.3: E-mail

Lecture Focus Questions:

- What are the advantages of scanning for e-mail viruses at the server instead of at the client?
- How can spam cause denial of service?
- What is a best practice when configuring an SMTP relay to prevent spammers from using your mail server to send mail?
- How can you protect yourself against phishing attacks?
- What services do S/MIME and PGP provide for e-mail?
- How does S/MIME differ from PGP?

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

- Filter junk mail by selecting the level of junk e-mail protection you want.
- Control spam on the client by configuring safe sender, blocked senders, white lists, and black lists.
- Configure e-mail filtering to block e-mails from specified countries and languages.
- Configure relay restrictions to specify who can relay through the SMTP server.

This section covers the following Security Pro exam objectives:

- 2.1 Promote Information Security Awareness.
  - Utilizing E-mail best practices
- 7.1 Implement Application Defenses.
  - Configure Secure E-mail Settings

Video/Demo	Time
9.3.1 E-mail Security	4:43
9.3.3 Protecting a Client from Spam	10:29
9.3.4 Securing an E-mail Server	2:45
9.3.6 Securing E-mail on iPad	5:52
Total Video Time	**23:49**

Lab/Activity

- 9.3.5 Configure E-mail Filters
- 9.3.7 Secure E-mail on iPad

Fact Sheets

- 9.3.2 E-mail Security Facts

Number of Exam Questions

8 questions

Total Time

About 47 minutes

9.4: Network Applications

Lecture Focus Questions:

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

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

- Set up content filters for downloading or uploading copyrighted materials.
- Use P2P file sharing programs to search for and share free files.
- Block ports used by P2P software.
- Secure instant messaging by blocking invitations from unknown persons.

Video/Demo	Time
9.4.1 Network Application Security	2:19
9.4.2 Spim	3:43
9.4.3 Using Peer-to-peer Software	3:04
9.4.4 Securing Windows Messenger	2:48
9.4.5 Configuring Application Control Software	9:05
Total Video Time	**20:59**

Fact Sheets

9.4.6 Network Application Facts

Number of Exam Questions

5 questions

Total Time

About 31 minutes

9.5: Virtualization

Lecture Focus Questions:

- What is the relationship between the host and the guest operating systems?
- What is the function of the hypervisor?
- How can virtualization be used to increase the security on a system?
- What are the advantages of virtualization? Disadvantages?
- What is the purpose of load balancing?
- What type of load balancing distributes a workload?

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

- Create and configure a new virtual machine.
- Configure the virtual machine by allocating resources for memory and a virtual hard disk.
- Create a virtual network and configure it as an external, internal, or private virtual network.

Video/Demo	Time
9.5.1 Virtualization Introduction	4:01
9.5.2 Virtualization Benefits	3:08
9.5.3 Load Balancing with Virtualization	10:40
9.5.4 Creating Virtual Machines	4:22
9.5.5 Managing Virtual Machines	5:09
9.5.7 Adding Virtual Network Adapters	1:30
9.5.8 Creating Virtual Switches	3:26
Total Video Time	**32:16**

Lab/Activity

- 9.5.6 Create Virtual Machines
- 9.5.9 Create Virtual Switches

Fact Sheets

- 9.5.10 Virtualization Facts

Number of Exam Questions

8 questions

Total Time

About 56 minutes

9.6: Application Development

Lecture Focus Questions:

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

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

- Use AppArmor to harden a Linux system.
- Implement application whitelisting with AppLocker.

This section covers the following Security Pro exam objective:

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

Video/Demo	Time
9.6.1 Secure Coding Concepts	16:18
9.6.2 Application Hardening	11:02
9.6.4 Hardening Applications on Linux	4:26
9.6.5 Implementing Application Whitelisting with AppLocker	13:03
9.6.7 Implementing Data Execution Preventions (DEP)	4:01
9.6.10 NoSQL Security	5:18
Total Video Time	**54:08**

Lab/Activity

- 9.6.6 Implement Application Whitelisting with AppLocker
- 9.6.8 Implement Data Execution Preventions (DEP)

Fact Sheets

- 9.6.3 Application Development Security Facts
- 9.6.9 Hardening Applications Facts
- 9.6.11 NoSQL Security Facts

Number of Exam Questions

6 questions

Total Time

About 86 minutes

10.1: Redundancy

Lecture Focus Questions:

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

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

- Configure a mirrored or a RAID 5 volume for data redundancy.

This section covers the following Security Pro exam objective:

- 8.1 Protect and maintain the integrity of data files.
  - Implement redundancy and failover mechanisms

Video/Demo	Time
10.1.1 Redundancy	4:55
10.1.2 Redundancy Measurement Parameters	5:12
10.1.4 RAID	7:27
10.1.5 Implementing RAID	6:16
10.1.8 Clustering	9:06
Total Video Time	**32:56**

Lab/Activity

- 10.1.7 Configure Fault Tolerant Volumes

Fact Sheets

- 10.1.3 Redundancy Facts
- 10.1.6 RAID Facts
- 10.1.9 Clustering Facts

Number of Exam Questions

15 questions

Total Time

About 68 minutes

10.2: Backup and Restore

Lecture Focus Questions:

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

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

- Back up a Windows system.
- Schedule automatic backups for Windows computers.

This section covers the following Security Pro exam objectives:

- 6.3 Perform System Backups and Recovery.
- 8.1 Protect and maintain the integrity of data files.
  - Perform data backups and recovery

Video/Demo	Time
10.2.1 Backup and Restore	13:27
10.2.4 Backing Up Workstations	6:18
10.2.6 Restoring Workstation Data from Backup	2:19
10.2.7 Backing Up a Domain Controller	2:33
10.2.9 Restoring Server Data from Backup	2:12
Total Video Time	**26:49**

Lab/Activity

- 10.2.5 Back Up a Workstation
- 10.2.8 Back Up a Domain Controller

Fact Sheets

- 10.2.2 Backup and Restore Facts
- 10.2.3 Backup Management Facts

Number of Exam Questions

15 questions

Total Time

About 62 minutes

10.3: File Encryption

Lecture Focus Questions:

- On which computers should you implement EFS?
- What is the FEK? How is it used?
- Under what conditions can EFS encryption be compromised?
- What happens when an EFS encrypted file is copied over the network using the SMB protocol?
- Once a system encrypted with Bitlocker boots, who is able to access files?

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

- Encrypt a file to secure data using EFS.
- Authorize additional users who can access files encrypted with EFS.
- Encrypt a file using GPG.
- Protect hard drive contents with BitLocker.
- Configure settings to control BitLocker using Group Policy.

This section covers the following Security Pro exam objectives:

- 8.1 Protect and maintain the integrity of data files.
  - Implement encryption technologies
- 8.2 Protect Data Transmissions across open, public networks.
  - Encrypt Data Communications

Video/Demo	Time
10.3.1 Encrypting File System (EFS)	11:47
10.3.2 Securing Files using EFS	11:45
10.3.4 PGP and GPG	4:34
10.3.5 Encrypting Files with GPG	4:58
10.3.6 BitLocker and Database Encryption	13:02
10.3.7 Configuring BitLocker	6:17
Total Video Time	**52:23**

Lab/Activity

- 10.3.3 Encrypt Files with EFS
- 10.3.8 Configure BitLocker with a TPM

Fact Sheets

- 10.3.9 File Encryption Facts

Number of Exam Questions

8 questions

Total Time

About 76 minutes

10.4: Secure Protocols

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 referenced as being *stateful*?
- What is the difference between IPSec *tunnel* mode and *transport* mode?

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

- Add SSL bindings to a Web site to support secure connections.
- Modify Web site settings to require SSL.
- Use SSL from a browser to create a secure connection.
- Enforce the use of IPSec through Connection Security Rules.

This section covers the following Security Pro exam objectives:

- 2.1 Promote Information Security Awareness.
  - Using SSL Encryption
- 8.2 Protect Data Transmissions across open, public networks.
  - Implement secure protocols

Video/Demo	Time
10.4.1 Secure Protocols	8:44
10.4.2 Secure Protocols 2	15:26
10.4.4 Adding SSL to a Web Site	5:23
10.4.6 IPSec	5:14
10.4.8 Requiring IPSec for Communications	14:22
Total Video Time	**49:09**

Lab/Activity

- 10.4.5 Allow SSL Connections

Fact Sheets

- 10.4.3 Secure Protocols Facts
- 10.4.7 IPSec Facts

Number of Exam Questions

15 questions

Total Time

About 80 minutes

10.5: Cloud Computing

Lecture Focus Questions:

- What are the advantages of cloud computing?
- Which cloud computing service model delivers software applications to the client?
- What is the difference between *Infrastructure as a Service* and *Platform as a Service*?
- How does the cloud computing service reduce the risk of security breaches?

Video/Demo	Time
10.5.1 Cloud Computing Introduction	15:59
10.5.2 Cloud Computing Security Issues	6:32
Total Video Time	**22:31**

Fact Sheets

10.5.3 Cloud Computing Facts

Number of Exam Questions

5 questions

Total Time

About 33 minutes

11.1: Vulnerability Assessment

Lecture Focus Questions:

- Why should an administrator perform a vulnerability assessment on the system?
- What is the most important step to perform before running a vulnerability scan? Why?
- How does a *port scanner* identify devices with ports that are in a listening state?
- How do *network mappers* discover devices and identify open ports on those devices?
- What types of items does OVAL identify as a *definition*?

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

- Scan a network with a vulnerability scanner, such as Nessus or MBSA, to identify risk factors.
- Download the latest security update information before starting a vulnerability scan.
- View security scan reports and identify vulnerabilities.
- Perform a port scan using **nmap** on a single machine.
- Use a password cracker to analyze a network for password vulnerabilities.

This section covers the following Security Pro exam objective:

- 9.4 Review vulnerability reports, implement remediation.

Video/Demo	Time
11.1.1 Vulnerability Assessment	4:55
11.1.3 Scanning a Network with Nessus	18:26
11.1.4 Scanning a Network with Retina	12:12
11.1.5 Scanning for Vulnerabilities Using MBSA	6:02
11.1.9 Performing Port and Ping Scans	2:36
11.1.10 Checking for Weak Passwords	9:21
Total Video Time	**53:32**

Lab/Activity

- 11.1.6 Review a Vulnerability Scan 1
- 11.1.7 Review a Vulnerability Scan 2
- 11.1.8 Review a Vulnerability Scan 3

Fact Sheets

- 11.1.2 Vulnerability Assessment Facts

Number of Exam Questions

14 questions

Total Time

About 88 minutes

11.2: Penetration Testing

Lecture Focus Questions:

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

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

- Identify available penetration testing tools that can be used to analyze the security of a network.
- Utilize penetration testing tools to identify vulnerabilities in information systems.
- Verify the distribution of a security tool to ensure its integrity.

Video/Demo	Time
11.2.1 Penetration Testing	2:32
11.2.3 Exploring Penetration Testing Tools	11:22
Total Video Time	**13:54**

Fact Sheets

11.2.2 Penetration Testing Facts

Number of Exam Questions

12 questions

Total Time

About 31 minutes

11.3: Protocol Analyzers

Lecture Focus Questions:

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

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

- Capture and analyze packets to troubleshoot a network using Wireshark.

Video/Demo	Time
11.3.1 Protocol Analyzers	3:07
11.3.3 Analyzing Network Traffic	6:50
Total Video Time	**9:57**

Fact Sheets

11.3.2 Protocol Analyzer Facts

Number of Exam Questions

8 questions

Total Time

About 23 minutes

11.4: Log Management

Lecture Focus Questions:

- How does logging affect system resources?
- What factors should you take into consideration when archiving log files?
- What types of information are included in events recorded in logs?

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

- Use Event Viewer to troubleshoot a system by viewing details of a logged event.
- Manage logging by saving or clearing logs, configuring filtering of logs, or attaching a task to a log or event.
- Identify operating system activities, warnings, informational messages, and error messages using *system logs*.

This section covers the following Security Pro exam objectives:

- 9.1 Implement Logging and Auditing.
  - Configure Domain GPO for Event Logging
- 9.2 Review security logs and violation reports, implement remediation.
- 9.3 Review audit reports, implement remediation.
- 9.4 Review vulnerability reports, implement remediation.

Video/Demo	Time
11.4.1 Logs	3:25
11.4.3 Logging Events with Event Viewer	3:52
11.4.4 Windows Event Subscriptions	10:36
11.4.5 Configuring Source-initiated Subscriptions	4:50
11.4.6 Configuring Remote Logging on Linux	8:23
Total Video Time	**31:06**

Fact Sheets

- 11.4.2 Log Facts
- 11.4.7 Remote Logging Facts

Number of Exam Questions

15 questions

Total Time

About 57 minutes

11.5: Audits

Lecture Focus Questions:

- How can you protect audit log files from access and modification attacks?
- When would you choose an *external auditor* over an *internal auditor*?
- What is the difference between *privilege auditing* and *usage auditing*?
- How can *escalation auditing* help to secure the system?

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

- Configure the audit logon events policy to audit the failure of a logon attempt.
- View and evaluate the recorded logs under Security in Event Viewer.

This section covers the following Security Pro exam objectives:

- 5.1 Harden Network Devices (using a Cisco Small Business Switch).
  - Turn on logging with timestamps
- 9.1 Implement Logging and Auditing.
  - Configure Domain GPO Audit Policy
- 9.2 Review security logs and violation reports, implement remediation.
- 9.3 Review audit reports, implement remediation.
- 9.4 Review vulnerability reports, implement remediation.

Video/Demo	Time
11.5.1 Audits	3:13
11.5.3 Auditing the Windows Security Log	11:41
11.5.5 Auditing Device Logs	6:57
Total Video Time	**21:51**

Lab/Activity

- 11.5.4 Configure Advanced Audit Policy
- 11.5.6 Enable Device Logs

Fact Sheets

- 11.5.2 Audit Facts

Number of Exam Questions

7 questions

Total Time

About 44 minutes

Practice Exams

A.0: Security Pro Practice Exams

Security Pro Domain 1: Access Control and Identity Management (22 questions)
Security Pro Domain 2: Policies, Procedures, Awareness (1 questions)
Security Pro Domain 3: Physical Security (2 questions)
Security Pro Domain 4: Perimeter Defenses (10 questions)
Security Pro Domain 5: Network Defenses (7 questions)
Security Pro Domain 6: Host Defenses (7 questions)
Security Pro Domain 7: Application Defenses (10 questions)
Security Pro Domain 8: Data Defenses (6 questions)
Security Pro Domain 9: Audits and Assessments (5 questions)
Security Pro Certification Practice Exam (15 questions)

B.0: CompTIA Security+ Practice Exams

CompTIA Security+ Domain 1: Network Security, All Questions (171 questions)
CompTIA Security+ Domain 2: Compliance and Operational Security, All Questions (128 questions)
CompTIA Security+ Domain 3: Threats and Vulnerabilities, All Questions (178 questions)
CompTIA Security+ Domain 4: Application, Data and Host Security, All Questions (70 questions)
CompTIA Security+ Domain 5: Access Control and Identity Management, All Questions (98 questions)
CompTIA Security+ Domain 6: Cryptography, All Questions (92 questions)
CompTIA Security+ Certification Practice Exam (100 questions)

C.0: (ISC)2 SSCP Practice Exams (Prior to April 2015)

(ISC)2 SSCP Domain 1: Access Control, All Questions (60 questions)
(ISC)2 SSCP Domain 2: Security Operations and Administration, All Questions (64 questions)
(ISC)2 SSCP Domain 3: Monitoring and Analysis, All Questions (21 questions)
(ISC)2 SSCP Domain 4: Risk, Response, and Recovery, All Questions (38 questions)
(ISC)2 SSCP Domain 5: Cryptography, All Questions (90 questions)
(ISC)2 SSCP Domain 6: Networks and Communications, All Questions (68 questions)
(ISC)2 SSCP Domain 7: Malicious Code and Attacks, All Questions (85 questions)
(ISC)2 SSCP Certification Practice Exam (125 questions)

Appendix A: Exam Objectives

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

Objectives for CompTIA's Security+ exam, and the SSCP exam, are outlined within the **Security+ Practice Exams** section.

#	Domain	Module.Section
1.0	**Access Control and Identity Management**	

1.1	Create, modify, and delete user profiles.
	• Manage Windows Domain Users and Groups
	  ○ Create, rename, and delete users and groups
	  ○ Assign users to appropriate groups
	  ○ Lock and unlock user accounts
	  ○ Change a user's password
	• Manage Linux Users and Groups
	  ○ Create, rename, and delete users and groups
	  ○ Assign users to appropriate groups
	  ○ Lock and unlock user accounts
	  ○ Change a user's password
	  ○ Configure password aging
	• Manage Windows Local Users and Groups
	  ○ Restrict use of local user accounts
	• Restrict use of common access accounts
		2.6, 2.7, 2.8, 2.9, 2.10, 2.11, 2.12

1.2	Harden authentication. • Configure Domain GPO Account Policy to enforce a robust password policy • Configure the Domain GPO to control local administrator group membership and Administrator password • Disable or rename default accounts such as Guest and Administrator • Configure the Domain GPO to enforce User Account Control • Configure a GPO for Smart Card authentication for sensitive resources • Configure secure Remote Access • Implement centralized authentication	2.6, 2.10, 2.11, 2.12, 2.13, 2.14

	Manage Certificates.	
1.3	• Approve, deny, and revoke certificate requests • Configure Domain GPO Kerberos Settings	2.14 3.1, 3.5
2.0	**Policies, Procedures, and Awareness**	
	Promote Information Security Awareness.	
2.1	• Traveling with Personal Mobile Devices • Exchanging content between Home and Work • Storing of Personal Information on the Internet • Using Social Networking Sites • Using SSL Encryption • Utilizing E-mail best practices • Password Management • Photo/GPS Integration • Information Security • Auto-lock and Passcode Lock	4.1 5.4 9.3 10.4
	Evaluate Information Risk.	
2.2	• Perform Risk calculation • Risk avoidance, transference, acceptance, mitigation, and deterrence	4.3
2.3	Maintain Hardware and Software Inventory.	4.2
3.0	**Physical Security**	
	Harden Data Center Physical Access.	
3.1	• Implement Access Rosters • Utilize Visitor Identification and control • Protect Doors and Windows • Implement Physical Intrusion Detection Systems	5.1, 5.2
	Harden mobile devices (iPad).	
3.2	• Apply updates • Set Autolock • Enable passcodes • Configure network security settings	5.4, 5.5
	Harden mobile devices (Laptop).	
3.3	• Set a BIOS Password	5.4, 5.5

	• Set a Login Password • Implement full disk encryption	
4.0	**Perimeter Defenses**	
4.1	Harden the Network Perimeter (using a Cisco Network Security Appliance). • Change the Default Username and Password • Configure a Firewall • Create a DMZ • Configure NAT • Configure VPN • Implement Web Threat Protection	6.5, 6.6, 6.7, 6.8, 6.9, 6.10

4.2	Secure Wireless Devices and Clients.
	
	• Change the Default Username, Password, and Administration limits
	• Implement WPA2
	• Configure Enhanced Security
	  ○ MAC filtering
	  ○ SSID cloaking
	  ○ Power Control
	• Disable Network Discovery
		6.14

5.0	**Network Defenses**	
5.1	Harden Network Devices (using a Cisco Small Business Switch). • Change the Default Username and Password on network devices • Use secure passwords • Shut down unneeded services and ports • Implement Port Security • Remove unsecure protocols (FTP, telnet, rlogin, rsh) • Implement access lists, deny everything else • Run latest iOS version • Turn on logging with timestamps • Segment Traffic using VLANs	2.1, 2.4, 2.11 7.2, 7.3, 7.4, 7.5 11.5
5.2	Implement Intrusion Detection/Prevention (using a Cisco Network Security Appliance). • Enable IPS protection for a LAN and DMZ	7.6

	• Apply IPS Signature Updates • Configure IPS Policy	
6.0	**Host Defenses**	
	Harden Computer Systems Against Attack.	
6.1	• Configure a GPO to enforce Workstation/Server security settings • Configure Domain GPO to enforce use of Windows Firewall • Configure Domain Servers GPO to remove unneeded services (such as File and Printer Sharing) • Protect against spyware and unwanted software using Windows Defender • Configure NTFS Permissions for Secure file sharing	8.1, 8.3, 8.4, 8.5
	Implement Patch Management/System Updates.	
6.2	• Configure Windows Update • Apply the latest Apple Software Updates	5.4 8.3
6.3	Perform System Backups and Recovery.	10.2
7.0	**Application Defenses**	
	Implement Application Defenses.	
7.1	• Configure a GPO to enforce Internet Explorer settings • Configure a GPO for Application Whitelisting • Enable Data Execution Prevention (DEP) • Configure Web Application Security • Configure Parental Controls to enforce Web content filtering • Configure Secure Browser Settings • Configure Secure E-mail Settings • Configure virtual machines and switches	6.5, 6.10 9.1, 9.2, 9.3, 9.5, 9.6
	Implement Patch Management/Software Updates.	
7.2	• Configure Microsoft Update	8.3
8.0	**Data Defenses**	
8.1	Protect and maintain the integrity of data files.	10.1, 10.2, 10.3

	• Implement encryption technologies • Perform data backups and recovery • Implement redundancy and failover mechanisms	
	Protect Data Transmissions across open, public networks.	
8.2	• Encrypt Data Communications • Implement secure protocols • Remove unsecure protocols	7.4 8.5 5.4 10.3, 10.4
9.0	**Audits and Assessments**	
	Implement Logging and Auditing.	
9.1	• Configure Domain GPO Audit Policy • Configure Domain GPO for Event Logging	11.4, 11.5
9.2	Review security logs and violation reports, implement remediation.	8.1, 11.4 , 11.5
9.3	Review audit reports, implement remediation.	11.4, 11.5
9.4	Review vulnerability reports, implement remediation.	11.1. 11.4, 11.5

Appendix B: Approximate Time for the Course

The total time for the LabSim for Security Pro course is approximately **65 hours and 38 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 assinged per text lesson)
- Simulations (5 minutes assigned per simulation)
- Questions (1 minute per question)

Additionally, there are approximately another **34 hours and 9 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: Introduction					
1.1: Security Overview	72	50	0	10	12
1.2: Using the Simulator	24	14	10	0	0
Total	**1:36**	**1:04**	**0:10**	**0:10**	**0:12**
2.0: Access Control and Identity Management					
2.1: Access Control Models	40	10	0	15	15
2.2: Authentication	62	37	0	10	15
2.3: Authorization	33	24	0	5	4
2.4: Access Control Best Practices	31	14	0	5	12
2.5: Active Directory Overview	35	27	0	5	3
2.6: Windows Domain Users and Groups	48	18	20	5	5
2.7: Linux Users	71	29	30	5	7
2.8: Linux Groups	27	4	15	5	3
2.9: Linux User Security	27	17	0	5	5
2.10: Group Policy Overview	37	24	5	5	3
2.11: Hardening Authentication 1	95	54	25	5	11
2.12: Hardening Authentication 2	39	14	10	10	5
2.13: Remote Access	41	16	0	10	15
2.14: Network Authentication	88	54	5	15	14
2.15: Identity Management	26	17	0	5	4
Total	**11:40**	**5:59**	**1:50**	**1:50**	**2:01**
3.0: Cryptography					
3.1: Cryptography	48	23	0	10	15
3.2: Hashing	37	20	0	5	12
3.3: Symmetric Encryption	36	16	0	5	15
3.4: Asymmetric Encryption	26	9	0	5	12
3.5: Public Key Infrastructure (PKI)	76	46	5	10	15
3.6: Cryptography Implementations	38	18	0	5	15
Total	**4:21**	**2:12**	**0:05**	**0:40**	**1:24**

4.0: Policies, Procedures, and Awareness						
4.1: Security Policies		88	48	0	25	15
4.2: Manageable Network Plan		39	31	0	5	3
4.3: Business Continuity		21	9	0	5	7
4.4: Risk Management		33	13	0	5	15
4.5: Incident Response		68	43	0	10	15
4.6: Social Engineering		53	28	5	5	15
4.7: Certification and Accreditation		32	15	0	5	12
4.8: Development		34	17	0	10	7
4.9: Employee Management		44	14	0	15	15
4.10: Third-Party Integration		21	12	0	5	4
	Total	**7:13**	**3:50**	**0:05**	**1:30**	**1:48**
5.0: Physical Security						
5.1: Physical Security		48	23	5	5	15
5.2: Hardware Security		25	16	0	5	4
5.3: Environmental Controls		44	23	0	10	11
5.4: Mobile Devices		51	28	5	10	8
5.5: Mobile Device Security Enforcement		44	26	0	10	8
5.6: Telephony		24	15	0	5	4
	Total	**3:56**	**2:11**	**0:10**	**0:45**	**0:50**
6.0: Perimeter Defenses						
6.1: Network Layer Protocol Review		72	48	0	15	9
6.2: Transport Layer Protocol Review		42	17	0	10	15
6.3: Perimeter Attacks 1		52	27	0	10	15
6.4: Perimeter Attacks 2		65	30	5	15	15
6.5: Security Appliances		40	21	5	10	4
6.6: Demilitarized Zones (DMZ)		34	16	5	5	8
6.7: Firewalls		41	16	5	5	15
6.8: Network Address Translation (NAT)		33	22	0	5	6
6.9: Virtual Private Networks (VPN)		46	15	10	10	11
6.10: Web Threat Protection		28	14	5	5	4
6.11: Network Access Control (NAC)		45	36	0	5	4
6.12: Wireless Overview		63	33	5	10	15
6.13: Wireless Attacks		51	31	0	5	15
6.14: Wireless Defenses		85	50	10	10	15
	Total	**11:37**	**6:16**	**0:50**	**2:00**	**2:31**
7.0: Network Defenses						
7.1: Network Devices		18	6	0	5	7
7.2: Network Device Vulnerabilities		21	7	5	5	4
7.3: Switch Attacks		15	6	0	5	4
7.4: Router Security		18	9	0	5	4
7.5: Switch Security		92	47	25	5	15
7.6: Intrusion Detection and Prevention		52	27	5	5	15
7.7: SAN Security		35	25	0	5	5
	Total	**4:11**	**2:07**	**0:35**	**0:35**	**0:54**
8.0: Host Defenses						
8.1: Malware		78	48	5	10	15

8.2: Password Attacks		22	13	0	5	4
8.3: Windows System Hardening		106	76	15	5	10
8.4: Hardening Enforcement		39	25	5	5	4
8.5: File Server Security		54	26	10	10	8
8.6: Linux Host Security		23	14	0	5	4
8.7: Static Environment Security		13	5	0	5	3
	Total	**5:35**	**3:27**	**0:35**	**0:45**	**0:48**
9.0: Application Defenses						
9.1: Web Application Attacks		75	55	0	5	15
9.2: Internet Browsers		110	72	25	5	8
9.3: E-mail		47	24	10	5	8
9.4: Network Applications		31	21	0	5	5
9.5: Virtualization		56	33	10	5	8
9.6: Application Development		86	55	10	15	6
	Total	**6:45**	**4:20**	**0:55**	**0:40**	**0:50**
10.0: Data Defenses						
10.1: Redundancy		68	33	5	15	15
10.2: Backup and Restore		62	27	10	10	15
10.3: File Encryption		76	53	10	5	8
10.4: Secure Protocols		80	50	5	10	15
10.5: Cloud Computing		33	23	0	5	5
	Total	**5:19**	**3:06**	**0:30**	**0:45**	**0:58**
11.0: Assessments and Audits						
11.1: Vulnerability Assessment		88	54	15	5	14
11.2: Penetration Testing		31	14	0	5	12
11.3: Protocol Analyzers		23	10	0	5	8
11.4: Log Management		57	32	0	10	15
11.5: Audits		44	22	10	5	7
	Total	**4:03**	**2:12**	**0:25**	**0:30**	**0:56**

Total Course Time 65:38

Practice Exams

A.0: Security Pro Practice Exams	Number of Questions	Time
A.2: Security Pro Domain 1: Access Control and Identity Management	22	110
A.3: Security Pro Domain 2: Policies, Procedures, Awareness	1	5
A.4: Security Pro Domain 3: Physical Security	2	10
A.5: Security Pro Domain 4: Perimeter Defenses	10	50
A.6: Security Pro Domain 5: Network Defenses	7	35
A.7: Security Pro Domain 6: Host Defenses	7	35
A.8: Security Pro Domain 7: Application Defenses	10	50
A.9: Security Pro Domain 8: Data Defenses	6	30
A.10: Security Pro Domain 9: Audits and Assessments	5	25
A.11: Security Pro Certification Practice Exam	15	75
Total	**85**	**7:05**

B.0: CompTIA Security+ Practice Exams	Number of Questions	Time

B.2: CompTIA Security+ Domain 1: Network Security, All Questions	171	2:51
B.3: CompTIA Security+ Domain 2: Compliance and Operational Security, All Questions	128	2:08
B.4: CompTIA Security+ Domain 3: Threats and Vulnerabilities, All Questions	178	2:58
B.5: CompTIA Security+ Domain 4: Application, Data and Host Security, All Questions	70	1:10
B.6: CompTIA Security+ Domain 5: Access Control and Identity Management, All Questions	98	1:38
B.7: CompTIA Security+ Domain 6: Cryptography, All Questions	92	1:32
B.8: CompTIA Security+ Certification Practice Exam	100	1:40
Total	**837**	**13:57**
C.0: (ISC)2 SSCP Practice Exams (Prior to April 2015)	**Number of Questions**	**Time**
C.2: (ISC)2 SSCP Domain 1: Access Control, All Questions	60	1:00
C.3: (ISC)2 SSCP Domain 2: Security Operations and Administration, All Questions	64	1:04
C.4: (ISC)2 SSCP Domain 3: Monitoring and Analysis, All Questions	21	105
C.5: (ISC)2 SSCP Domain 4: Risk, Response, and Recovery, All Questions	38	190
C.6: (ISC)2 SSCP Domain 5: Cryptography, All Questions	90	1:30
C.7: (ISC)2 SSCP Domain 6: Networks and Communications, All Questions	68	1:08
C.8: (ISC)2 SSCP Domain 7: Malicious Code and Attacks, All Questions	85	1:25
C.9: (ISC)2 SSCP Certification Practice Exam	125	2:05
Total	**551**	**13:07**
Total Practice Exam Time 34:09		