220-802 Domain 2 – Security Study Guide

(Brought to you by RMRoberts.com)

The CompTIA A+ 220-802 Security Domain accounts for approximately 22 percent of the certification exam (20 questions). To better prepare you for this portion of the certification exam, we have prepared this study guide. You should list a brief amount of related information for each objective topic listed below, such as a description, or definition, or related facts.

Black text is taken directly from the CompTIA A+ certification examination objectives. Light gray text notes the author's comments to help clarify some of the more ambiguous objectives. Also, a list of helpful links have been provided below that can be used as sources in addition to the textbook and laboratory manual.

Please complete the study guide before attempting the practice test.

Below is a short list of basic security information/sources that you may find useful.
Microsoft security related information:
http://www.microsoft.com/security/default.aspx
http://www.microsoft.com/security/pc-security/default.aspx#Safety-products-and-scans
US Government Computer Security Resource Center.
http://csrc.nist.gov/csrc/government.html
Indiana University Security Information.
http://kb.iu.edu/data/akln.html
The SANS organization.
http://www.sans.org/
Web resource for UEFI.
http://www.uefi.org/learning_center/
FAQ BitLocker link at the Microsoft Website.
http://technet.microsoft.com/library/ee449438.aspx#BKMK_Vista

2.0 Security

2.1 Apply and use common prevention methods.

- Physical security

Lock doors

Describe each of the security methods below.

Tailgating

Securing physical documents/passwords/shredding

Biometrics

Badges

Key fobs

RFID badge

RSA token

Privacy filters

Retinal

- Digital security

The CompTIA is referring to digital security as the classification of software applications used in security in contrast to physical security, which was used to identify the objectives above.

Antivirus

Firewalls

Anti-spyware

User authentication/strong passwords

Directory permissions

Identify where directory permission can be configured.

- User education
- Principle of least privilege

2.2 Compare and contrast common security threats.

Define the following malware or security risk with sufficient description for accurate identification of each.

- Social engineering
- Malware
- Rootkits
- Phishing
- Shoulder surfing
- Spyware
- Viruses

- Worms

- Trojans

2.3 Implement security best practices to secure a workstation.

- Setting strong passwords
  Describe the characteristics of a strong password.

- Requiring passwords

- Restricting user permissions
  Where would you change user permissions?

  What is the difference between a permission and a user right?

- Changing default user names

- Disabling guest account
  Why would you disable the guest account?

- Screensaver required password
  Why would you enable the screen saver password?

  Where do you enable the screen saver password?

- Disable autorun

2.4 Given a scenario, use the appropriate data destruction/disposal method.

- Low level format vs. standard format

- Hard drive sanitation and sanitation methods

Overwrite

Drive wipe

- Physical destruction

Shredder

Drill

Electromagnetic

Degaussing tool

2.5 Given a scenario, secure a SOHO wireless network.

- Change default user-names and passwords
  How do you change the default administrator name and password?

- Changing SSID

- Setting encryption

- Disabling SSID broadcast

- Enable MAC filtering
  What is MAC filtering?

  Where do you configure MAC filtering?

- Antenna and access point placement

- Radio power levels

- Assign static IP addresses
  How do you assign a static IP address?

  What is the security advantage of assigning a static IP address as compared to configuring DHCP IP address assignment?

2.6 Given a scenario, secure a SOHO wired network.

- Change default usernames and passwords

- Enable MAC filtering

- Assign static IP addresses

- Disabling ports

- Physical security