Study Guide for the Security - Domain 5 - CompTIA A+ Certification

This Study Guide for the CompTIA A+ Security sections of the 701 and 702 Certification Examination is presented by www.RMRoberts.com website.

Listed below are the test objectives for both, the 701 and 702 Certification Examinations. You must be familiar with all objectives listed.

The main problem we have encountered with the list of the security objectives is the fact that it does not accurately reflect the depth of knowledge that is actually required for each objective. Many objectives are ambiguous.

For example, in section 5.1 of the 701 certification the list simply states - Encryption Technologies. This is a very broad subject. There are entire books written on encryption technologies.

In general, when preparing for the A+ certification, a general knowledge of security principles will provide enough depth. If you were preparing for the CompTIA Security + Certification, a much more in-depth knowledge would be required.
You may find the following links helpful when preparing for the security domain of the A+ certification examination.

Microsoft File sharing
http://windows.microsoft.com/en-US/windows-vista/File-sharing-essentials

Microsoft Simple File Sharing
http://windows.microsoft.com/en-US/windows-vista/File-sharing-essentials

Microsoft Bitlocker and TPM is a must for the test!
http://technet.microsoft.com/en-us/library/cc732774.aspx

Microsoft EFS
http://technet.microsoft.com/en-us/library/cc721923(WS.10).aspx

Microsoft User Account Control UAC
http://technet.microsoft.com/en-us/library/cc731416(WS.10).aspx

The software Engineering Institute of Carnegie Mellon University
http://www.cert.org/homeusers/HomeComputerSecurity/
http://www.cert.org/tech_tips/home_networks.html

The US Department of Home Land Security
http://www.us-cert.gov/cas/tips/

The Microsoft Security Center
http://www.microsoft.com/security/default.aspx

Interesting TechNet article on basics of security
http://technet.microsoft.com/en-us/library/cc722487.aspx

The SANS organization
http://www.sans.org/
http://www.istl.org/02-fall/internet.html

How to Geek Share Permissions.
http://www.howtogeek.com/72718/how-to-understand-those-confusing-windows-7-fileshare-permissions/

Define each of the Domain 5 terms, as related to security. Notice the remarks in gray in the list of domain objectives. They are designed as an aid to better understand how the terms relate to each other, and how test items are created to match the term.

The 701 certification objectives.

5.0 Security

5.1 Explain the basic principles of security concepts and technologies

Encryption technologies

Define the difference between encryption and authentication technology. They are often confused but are actually two different technologies.

Data wiping / hard drive destruction / hard drive recycling

What is the best way to insure all data has been rendered inaccessible from a disk drive from a machine that is taken out of service?

Software firewall

What is the difference between a software firewall and a hardware firewall?

Port security

Exceptions

Exceptions, as related to port security and firewalls.

Authentication technologies

User name

Password

Biometrics

Smart cards

Basics of data sensitivity and data security

Compliance

Classifications

Social engineering

5.2 Summarize the following security features

Wireless encryption

WEPx and WPAx

Identify all common wireless technologies and rank them from least secure to most secure, or equal.

Client configuration (SSID)

Malicious software protection

Viruses

Trojans

Worms

Spam

Spyware

Adware

Grayware

BIOS Security

Drive lock

Passwords

Intrusion detection

TPM

Password management / password complexity

Locking workstation

How to secure a workstation by the following means:

Hardware

Operating system

Biometrics

Fingerprint scanner

The 702 certification objectives.

4.0 Security

Domain 4.0 Security for the 702 tests your ability to install and maintain antivirus software. In addition your ability to configure shares securely is also tested. I highly recommend that you download, install and configure two or three different trial versions of antivirus software. Explore the antivirus configuration options such as the quarantine feature and how to perform updates and schedule runs. Remove antivirus programs after you are familiar with each or at least disable them. You should only run one antivirus program on a computer. Two or more will cause problems with the computer performance!

4.1 **Given a scenario, prevent, troubleshoot and remove viruses and malware**

Use antivirus software

Identify malware symptoms

Quarantine infected systems

Research malware types, symptoms and solutions (virus encyclopedias)

Remediate infected systems

Update antivirus software

Signature and engine updates

Automatic vs. manual

Schedule scans

Repair boot blocks

Scan and removal techniques

Safe mode

Note: Some viruses can only be removed by the antivirus software when run in safe mode!

Boot environment

Educate end user

4.2 **Implement security and troubleshoot common issues**

Operating systems

Local users and groups: Administrator, Power Users, Guest, Users

Define and explain the security level of each of the four types of user accounts above.

Administrator

Power Users

Guest

Users

Vista/Windows 7 User Account Control (UAC)
Practice using the UAC and be able to compare/contrast by operating system (Windows 7, Vista, and XP).

NTFS vs. Share permissions
Memorize permissions for general sharing and NTFS sharing.

Allow vs. deny
Difference between moving and copying folders and files.
Recommend doing practical application of moving and copying files and observe the results.

File attributes
List the common file attributes and their file attribute symbol for example r+.

Shared files and folders
Which operating system first introduced simple file sharing?

How do you access the simple file sharing feature?

Administrative shares vs. local shares
How are administrative shares identified?

Permission propagation

Inheritance
Inheritance, as related to file and folder permissions

System files and folders
Inheritance, how do changing folder permissions affect file s inside that folder?

What happens to the permissions of a file when removed from one folder/directory and then placed inside a different folder/directory?

Encryption (Bitlocker, EFS)

User authentication
(User authentication as related to each of the following types of authentication, system, BIOS security, drives lock, passwords, intrusion detection, TPM.)

System

BIOS security

Drive lock

Passwords

Intrusion detection

TPM