CompTIA Network+ Domain 6-Network Security Study Guide

(Brought to you by RMRoberts.com)

Domain 6 Network Security

The CompTIA Network+ certification exam domain 6 comprises approximately 11 % of the total exam or approximately 11 questions. While the concepts being tested can be difficult you should have no problem as long as you understand the areas listed in this guide. A corresponding practice test is provided at www.RMRoberts.com at the following link (link here).

6.1 Explain the function of hardware and software security devices.

- Network based firewall
- Host based firewall
- IDS
- IPS
- VPN concentrator

6.2 Explain common features of a firewall

- Application layer vs. network layer
- Stateful vs. stateless
- Scanning services
- Content filtering

- Signature identification

- Zones

6.3 Explain the methods of network access security.
Filtering:
Compare ACL, Mac and IP filtering. Explain how each is configured.

ACL

MAC filtering

IP filtering

- Tunneling and encryption

SSL VPN

VPN

L2TP

PPTP

IPSEC

Remote access

Describe the two remote access protocols/methods below, RAS, and RDP

RAS

RDP

Describe the four protocols below and be sure to include any information concerning security.

PPPoE

PPP

VNC

ICA

6.4 Explain methods of user authentication .

- PKI

- Kerberos

- AAA

Compare the two remote access methods, RADIUS and TACACS+.

RADIUS

TACACS+

Network access control

Describe the method of security used for each of the four network access methods below.

802.1x

CHAP

MS-CHAP

EAP

6.5 Explain issues that affect device security .

Physical security

Restricting local and remote access

Secure methods vs. unsecure methods

Describe each of the protocols listed below as they relate to secure access methods.

SSH

HTTPS

SNMPv3

SFTP

SCP

TELNET

HTTP

FTP

RSH

RCP

SNMPv1/2

6.6 Identify common security threats and mitigation techniques.

Security threats

Describe each security threat listed below.

DoS

Viruses

Worms

Attackers

Man in the middle

Smurf

Rogue access points

Social engineering (phishing)

Mitigation techniques

Below are three items that directly relate to security. Describe how each can enhance network security.

Policies and procedures

User training

Patches and updates

You are free to distribute this study guide to your students when preparing for the CompTIA Network+ certification exam. Also check the www.RMRoberts.com website for more practice materials.