Netzwerke, Kapitel 3.8

Kontrollfragen 1

1. Nennen Sie einige Bedrohungen der Sicherheit.
   - *Denial of Service (DoS)*
   - *Men-in-the-Middle Attacke (MITM)*
   - *Replay Attacken*
   - *Manipulation, Abhören, Sniffer, …*
   - *Viren, Würmer, SPAM, …*
   - *Phishing, Brute-Force, …*

2. Was ist DoS?
   Denial of Service (DoS)
   Angriff auf einen Host (Server) mit dem Ziel, einen oder mehrere seiner Dienste arbeitsunfähig zu machen.
   - *Ping of Death (erzeugt Buffer Overflow)*
   - *Smurf-Attacke, SYN-Flood, Teardrop-Attacke, Land-Attacke, WinNuke, Botnet, …*

3. Nennen Sie einige Authentifizierungsverfahren.
   - *SecurID RSA (Zufallszahlengenerator, OneTimeToken)*
   - *RADIUS (Remote Authentication Dial-In User Service)*
   - *Kerberos*

4. Nenn Sie 3 Verschlüsselungsprotokolle.
   - *IPSec (IP Security)*
   - *SSL (Secure Sockets Layer)*
   - *SSH (Secure Shell)*

5. Was ist der Vorteil eines VPN?
   Virtuelles Privates Netz, von aussen geschlossenes Netzwerk. Ist für den Benutzer transparent.

6. Nennen Sie einen prinzipiellen Nachteil der symmetrischen Verschlüsselung?
   Der geheime Schlüssel muss zuerst sicher ausgetauscht werden.
   Eignet sich nicht für eine „Open User Group“.

7. Was ist der Vorteil der asymmetrischen Verschlüsselung?
   Benutzerfreundliche, für Open-User-Group tauglich.
   Es muss keinen geheimen Schlüssel im Voraus ausgetauscht werden.

8. Welche Anforderungen erfüllt eine digitale Signatur?
   Die Identität des Senders ist überprüfbar. (Elektronische Unterschrift)

9. Was ist ein Hash?
   Berechnet aus beliebigem Quelltext eine Bitfolge fester Länge = Hash-Funktion

10. Welche Informationen benutzt eine Firewall für ihre Entscheidungen?
    Regel-Listen
    Richtung, Quelle, Ziel, Port, Protokoll, Aktion