Grundlagen der Rechnersicherheit - 21.07.2015 - Gedächtnisprotokoll

Insgesamt 81 Punkte

1.) Multiple Choice Fragen

Insgesamt 10 Punkte - 10 Fragen, falsche geben Minuspunkte

Zu Definitionen wie Security, Safety, Same-Origin-Policy usw.

2.) Inkrementelles und Differentielles Backup definieren und Vor- und Nachteile vergleichen (5 Punkte?)

3.) Bufferoverflow erklären (Skizze möglich, nicht notwendig) und 2 mögliche Fehler nennen (4 Punkte)

4.) Authentifizierung (10 Punkte?)

a) 4 Möglichkeiten, sich zu authentifizieren

b) Vor- und Nachteile von ACLs und Capabilities diskutieren

5.) (6 Punkte?)

a) Zwei Schwachstellen nennen, die durch Sprachgrenzen entstehen

b) DNS-Reflection erklären (evtl. mit Skizze)

6.) Verschlüsselung (21 Punkte)

a) Cipher Block Chaining, wenn 1 Bit fehlerhaft, welche Blöcke sind dann verändert? Erklären.

b) Ist f(x) = x mod 128 eine gut gewählte Hashfunktion? Warum nicht?

c) RSA-Schlüssel für p=3 und q=11 berechnen

d) Wie groß sollte die Schlüssel/Blocklänge gewählt werden?

e) Signieren sie die Zahl 3.

7.) Take-Grant-Modell (12 Punkte)

Vier verschiedene Graphen (2 de-jure, 2 de-facto), die mit den Regeln hergeleitet werden sollten oder erklären, warum die Rechte nicht übernommen werden können.

8.) HRU-Modell (6 Punkte)

Hier waren verschiedene Befehle gegeben und eine Tabelle mit Subjekten, Objekten und deren Rechten.

Es sollte ein sicherer und ein unsicherer Zustand erzeugt und erklärt werden.

9.) Entscheiden und erklären, ob Situation sich mit einer Paketfilter-Firewall lösen lässt (4 Punkte)

a) Verbindungen nur in eine Richtung durchlassen

b) Nachrichten über SMTP an beliebige Server schicken