Sicherheit in Rechnernetzen - Klausur SoSe 2021

Aufgabe 1: DGEC Steckbrief (5 Punkte)

Erstellen Sie einen DGEC-Steckbrieb vom TCP-SYN-FLOOD-Angriff!
Zu welcher Fehlerklasse gehört die Schwachstelle?

Aufgabe 2: Spoofing (1 + 1 + 2 Punkte)

1. Was versteht man unter Spoofing?
2. Beschreiben Sie die Rolle des Spoofing bei Amplification Angriffen.
3. Hilfe IPsec gegen Spoofing? Begründen Sie Ihre Antwort.

Aufgabe 3: Man-in-the-Middle Angriffe (2 + 2 + 2 Punkte)

Ein MiM schneidet den Nachrichtenverkehr einer mit SSL verschlüsselten Client-Server-Verbindung mit und spielt Nachrichten wieder ein.

1. Ab welcher Nachricht im Hand-Shake wird eine Replay-Attacke verhindert?
2. TLS 1.3 bietet 1-RTT und 0-RTT.
   Was verhindert hier eine Replay-Atacke?
3. Wie werden Replay-Attacken im Keberos-Protokoll verhindert?

Aufgabe 4: Buffer-Overflow (2 + 2 + 3 + 2 Punkte)

1. Was versteht man unter einem Buffer-Overflow?
   Nennen Sie mindestens zwei Ziele, die ein Angreifer durch Ausnutzung von Buffer-Overflows anstreben kann.
2. Geben Sie eine Strategie und alle Schritte an, die notwendig sind, sodass ein Angreifer mittels Buffer-Overflow eigenen Code ausführen kann.
3. Gegeben Sei folgende C-Funktion:

   ```
   /* String-replace Funktion mit strcpy als verwundbare Funktion innerhalb einer if-Sektion */
   ```

   Beschreiben Sie kurz, unter welchen Umständen ein Buffer-Overflow auftreten kann.
   Begründen Sie Ihre Antwort.
4. Worin besteht die besondere Gefahr von Buffer-Overflow bei Programmen mit gesetztem setuid-Bit? Geben Sie zwei Gründe an wie Capabilities diese Gefahr reduzieren.

Aufgabe 5: Diffe-Hellman (1 + 2 + 1 +2 Punke)

Für die Durchführung des Diffe-Hellman-Verfahrens (DH) ist folgende Konfiguration mit p = 11 und g = 7 gegeben. Die von der Partei A gewählte zufällige Zahl $X_1 = 8$, Partei B wählt hingegen $X_2 = 7$.

1. Überprüfen Sie ob g eine primitive Wurzel von p ist.
2. Berechnen Sie den Wert von K_{12} Sowohl aus Sicht von A als auch von B.
3. Welches Problem soll DH lösen?
4. Gegen welchen Angriff ist DH anfällig?
   Beschreiben Sie einen solchen Angriff!
   Mit welcher Maßnahme kann diese Anfälligkeit behoben werden?