IT Security

Klausur an der Hochschule Karlsruhe – University of Applied Sciences
Sommersemester 2023, Dienstag 18.07.2023, 11:00 Uhr

- Name:_____ Punkte:_____/100 (40 zum Bestehen) Note:____
- **Disclaimer:**
  - Der Lösungsweg muss bei allen Aufgaben ersichtlich sein
- - Keine Hilfsmittel

Aufgabe 1: Begriffswelt

__/10 __/10 Punkte

Sie finden dass Twitter, Threads, Mastodon und wie die Nachrichtenplattformen auch alle heißen mögen nicht gut genug performen und möchten Ihr eigenes Ding machen!

Quitter soll es heißen! Lauter Quitts und Quitten sollen die Nachrichtentypen der Zukunft sein!

Sicherheit soll eines der Alleinstellungsmerkmale Ihres neuen Dienstes sein! Deshalb klären Sie zunächst mit Ihrem Team zusammen die Begrifflichkeiten, zum Glück haben Sie die Vorlesung bei Fischi und Gio besucht und können kurz und prägnant die folgenden Begriffe definieren:

ISO27001, Injection, Schutzziele, DoS, Shell-Code, DMZ, Risiko, NAT, ARP-Spoofing, Policy

Aufgabe 2: Safety

A)__/6 B) __/6 C)__/6 D)__/11 E)__/3 F)__/5 __/37 Punkte

A) In der Vorlesung wird zwischen Safety und Security unterschieden. Bitte erklären Sie Ihrem Team bei Quitter kurz worin der Unterschied besteht. Finden Sie jeweils 3 Schadensszenarien als Beispiel.

B) Selbstverständlich ist neben der Sicherheit auch die Verfügbarkeit für Ihren Quitter Dienst von entscheidender Bedeutung. Ihre Quitter Registrierungsseite wird auf n Webservern mit einer Verfügbarkeit von jeweils 80% gehostet. Zeigen Sie wie die Verfügbarkeit im Zusammenhang mit n steht.

C) Leider hatte Ihr RZ Leiter einen schlechten Tag und alle Server hängen an der gleichen Stromversorgung, die nicht weiter abgesichert ist und eine Verfügbarkeit von 50% aufweist. Wie hoch ist damit die Verfügbarkeit wenn Sie 3 Webserver aus Aufgabe B) betreiben und keine weiteren Einflüsse beachten?

D) Der zugehörige Datenbankenserver ist als 1:1 Redundanz mit aktiven und passiven System Aufgebaut.

- Welche Art von Redundanz ist das? Wie ist die naheliegende Redundanzimplementierung der Komponenten?
- Was ist in diesem Zusammenhang ein Heartbeat?
- Welche Herausforderung gibt es bei der Umsetzung eines Heartbeats?
- Auf welchen Identitätsebenen können Sie die passiv=>aktiv Umschaltung implementieren? Welche Vor- Nachteile hat die jeweilige Umsetzung?
- Welcher problematische Zustand kann bei dem Übergang passiv=>aktiv eintreten? Was sind mögliche Ursachen dafür und wie können Sie einen solchen Zustand in Ihrer Umsetzung verhindern?

E) Sie befassen sich mit Möglichkeiten, die Sicherheitsmechanismen von Quitter zertifizieren zu lassen.
Welche der folgenden Möglichkeiten können hierzu sicherlich nicht herangezogen werden (bitte streichen):

- IT 32005
- Common Criteria
- ISO Common
- ISO 27001
- Facebook
- IT Mundschutz
- IT-Grundschutz

F) Viele Zertifizierungen basieren darauf, Schutzziele festzulegen und mit Maßnahmen zu versehen. Füllen Sie die untenstehende Tabelle aus um Ihren Mitarbeitern grob den Zusammenhang darzustellen:

	Redundanz	„Firewall“++	Kryptographie	Policies
Verfügbarkeit				
Integrität				
Vertraulichkeit				
Zurechenbarkeit				
Rechtsverbindlichkeit				

Aufgabe 3: Security

A)__/6 B) __/11 C)__/11 D)__/11 E)__/8 F)__/6 __/53 Punkte

A) Ihre Quitter Konkurrenz hatte in der Vergangenheit immer wieder mit (D)DoS Angriffen zu kämpfen. Erklären Sie kurz den Unterschied zwischen DoS und DDoS.
Nennen Sie jeweils 3 Maßnahmen mit denen Sie versuchen können sich davor zu schützen

B) Sie haben die Vorschläge aus Aufgabe A) endlich mit Ihrem Team umgesetzt. Da Sie die Vorlesung von Fischi und Gio besucht haben wissen Sie, dass man seine Sicherheitsmaßnahmen auch (regelmäßig) testen sollte.
Schreiben Sie in Pseudocode einen Bot den Sie (natürlich auf einer legal gemieteten Infrastruktur) dazu verwenden können, um DDoS Attacken zu simulieren.

C) Sicherheit sollte bei Ihrer Entwicklung von Quitter ja ein großes Thema sein. Deshalb achten Sie darauf von Anfang an einen SSDLC Prozess zu etablieren.
Welche Phasen beachtet Ihr Prozess (orientieren Sie sich an den in der Vorlesung vorgestellten Modellen)?
Welche sicherheitsrelevanten Tätigkeiten sind Bestandteil der jeweiligen Phase im Prozess?

D) Wenn Ihre Entwickler trotz der konsequenten Nutzung von SSDLC Fehler in der Eingabeverarbeitung machen, kann es zu Buffer Overflows kommen.

- Formulieren Sie für solch einen Fehler ein einfaches Beispiel in Pseudocode
- Welche Abhilfen kennen Sie, um Buffer Overflows vermeiden zu helfen?
- Eine modernere Variante nennt sich ROP – wie funktioniert diese grob?

E) Weitere Schwierigkeiten kann Ihnen bei der Umsetzung von Quitter die Eingabeverarbeitung der Quits im Web machen.
Welche Arten oder Varianten von Injection Attacken im Web kennen Sie?
Erstellen Sie in Form von einer Skizze und etwas Text jeweils Schulungsmaterial zum Ablauf für zwei davon um Ihre Entwickler bei der sicheren Programmierung zu unterstützen.

F) Sie sind ein großer Fan von Zero-Trust Prinzipien, klären Sie kurz Ihr Team auf:

- Was ist Zero Trust und weshalb ist es eine bessere Topologie für Ihre Quitter Infrastruktur als eine Onion/DMZ/Bastion?