IT Security

Klausur an der Hochschule Karlsruhe – University of Applied Sciences
Wintersemester 2023/24, Dienstag, 06.02.2024, 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

Es ist kalt in Deutschland, daher haben Sie entschieden, die Gunst der Stunde zu nutzen und bauen *Hola!,* eine Plattform für Cloud Computing auf Gran Canaria auf, mit Meerwasserkühlung, Mitarbeitern, die auch im Süden arbeiten wollen und günstigem Strom.

Für die häufig anzutreffenden digitalen Nomaden, die Ihnen bei der Realisierung helfen ist es nötig, die Begriffe aus dem Themenbereich IT Security zu erklären.

Zum Glück haben Sie die Vorlesung bei Fischi (und vielleicht bei Gio) besucht und können kurz und prägnant die folgenden Begriffe erklären/definieren:

Sniffing, statische Redundanz, Wurm, Pentest, ARP-Spoofing, Heartbeat, OWASP, Proxy, Asymmetrische Verschlüsselung, Anomalieerkennung

Aufgabe 2: Safety

A)__/6 B)__/7 C)__/7 D)__/8 E)__/4 F)__/5 __/37 Punkte

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

B) *Hola!* Hat zwei Rechenzentren, eines auf Gran Canaria und eines auf Teneriffa, jedes davon hat eine Verfügbarkeit von 80%. Jede Insel ist mit jeweils zwei redundanten Seekabeln (Verfügbarkeit jeweils 50%) ans Internet angeschlossen. *Hola!* funktioniert nur, wenn beide RZs laufen und erreichbar sind. Wie hoch ist die Verfügbarkeit von *Hola!*?

C) Wie würde sich die Gesamtverfügbarkeit verändern wenn Sie ein weiteres für den Betrieb notwendiges RZ auf der dritten Insel Fuerteventura hinzu nehmen? Es hat ebenfalls eine Verfügbarkeit von 80% und ist auch mit 2 Seekabeln (Verfügbarkeit jeweils 50%) ans Internet angeschlossen.

D) Angenommen, *Hola!* würde auch funktionieren, wenn nur mindestens ein RZ auf einer der Inseln funktionieren und erreichbar sein würde – wie wäre dann die Verfügbarkeit von *Hola!*?

E) Die Verfügbarkeit von Software lässt sich eindeutig verbessern durch (bitte ankreuzen):

[ ] Optimierung der Bootzeiten [ ] Einsatz von Watchdogs
[ ] Herunterfahren der Server [ ] Vermeidung von Passwörtern
[ ] Nutzung sicherer Betriebssysteme [ ] 16bit CPUs
[ ] geeignete Entwicklungsmethoden [ ] Vermeidung von Bugfixes

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)__/5 F)__/9 __/53 Punkte

A) Eine Insel ist natürlich die bevorzugte topologische Abwehrmaßnahme Ihres Cloud-Computing Unternehmens. Welche Vor- und Nachteile hat dieses Pattern?

B) Bei *Hola!* Im Web-Interface wurde eine XSS-Lücke entdeckt, die auch schon ausgenutzt wird. Erklären Sie anhand eines Schaubilds den Ablauf wie die XSS Lücke ausgenutzt werden kann. Was müssten die Angreifer tun, um daraus eine XSRF-Attacke zu machen?

C) Nicht nur XSS macht *Hola!* zu schaffen, auch DDoS Attacken von Botnetzen aus sind ein ständiger Threat.

- Welche Eigenschaften haben Bots (mindestens, auch gerade im Vergleich zu anderen Malware-Arten)?
- Welche Bot-Eigenschaften sind nur manchmal ausgeprägt?
- Was ist der Unterschied zwischen DoS und DDoS?
- Nennen Sie mindestens 3 Maßnahmen, mit denen Sie versuchen können sich vor den DDoS Angriffen durch Bots zu schützen

D) Sie haben die Vorschläge aus Aufgabe C) 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 bei der Konkurrenz) dazu verwenden können, um DDoS Attacken zu simulieren.

E) Ordnen Sie die folgenden SSDLC-Aktivitäten der richtigen Phase zu:

`Anforderungsphase`	`Fuzzing Tests`
`Entwurfsphase`	`Bedrohungsmodellierung`
`Entwicklungsphase`	`Reaktionsplan`
`Überprüfungsphase`	`Risikobewertung`
`Deploymentphase`	`Statische Code Analyse`

F) 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?
- Welche Maßnahmen die zum Schutz gegen Bufferoverflows existieren werden durch ROP ausgehebelt?