[root@netsec]>

IT Security

Klausur an der Hochschule Karlsruhe - Technik und Wirtschaft
Wintersemester 2018/19, Mittwoch, 20.02.2019, 14:00 Uhr

Name:_____ Punkte:_____/100 (40 zum Bestehen) Note:____

Disclaimer:
- Zugelassene Hilfsmittel: keine ausser Stifte und Lineal
- Der Lösungsweg muss bei allen Aufgaben ersichtlich sein

Aufgabe 1: Begriffswelt

__/10 __/10 Punkte

Für das Live-Streaming der Handball-WM entsteht mit Ihrer Beratung ein großer IT-Setup. Sicherheit spielt dabei eine zentrale Rolle.

Erklären Sie zunächst kurz folgende 10 Begriffe aus der IT Security Vorlesung: XSRF, Zurechenbarkeit, ISO 27001, Hybridredundanz, Keystroke Logging, Firewall, ASLR, SSDLC, Risiko (nach ISO), Heartbeat

Aufgabe 2: Safety

A)__/6 B)__/8 C)__/8 D)__/6 E) __/7 __/35 Punkte

A) Nennen Sie 3 Beispiele für strafrechtlich relevante Vorgänge aus dem Bereich der IT-Sicherheit.

B) Die Eintrittswahrscheinlichkeit für einen gleichzeitigen Ausfall der beiden Cloud-Provider, die für die WM-Übertragung verwendet werden liegt bei 0,1%. Sollte dies passieren, so brechen Werbe-Einnahmen in der Höhe von 10000€/h weg. Die Einführung eines dritten Cloud-Providers würde 2400€/Tag kosten und der Ausfall wäre dann nur noch 0,05% wahrscheinlich. Lohnt es sich, den dritten Cloud-Provider zusätzlich zu nutzen?

C) Die Handballübertragung des Endspiels wird mit 4 schlechten Kameras aus unterschiedlichen Blickwinkeln aufgenommen, von denen jede eine Ausfallwahrscheinlichkeit von 70% hat. Die Rohdaten werden über einen nicht besonders stabilen gemeinsamen Uplink mit einer Verfügbarkeit von 80% zur Weiterverarbeitung geschickt.
Für die Übertragung sind mindestens zwei Blickwinkel erforderlich. Wie wahrscheinlich ist es, dass keine Übertragung vom Endspiel mehr erfolgt?

D) Was versteht man unter dem hierarchische und dem relationalen Modell in der Systemanalyse zur Verfügbarkeitsbestimmung?

D) Welches bzw. welche Schutzziel(e) werden mit der Umsetzung der untenstehenden Maßnahmen jeweils verfolgt?
Verschlüsselung, 4-Augen Prinzip, RAID, Ersatztorhüter, Paketfilter, Archivsystem, Zugangskontrolle zum RZ

Aufgabe 3: Security

A)__/6 B)__/6 C)__/18 D)__/5 E)__/10 F)__/6 G)__/6 __/57 Punkte

A) Zwei Standorte sollen so über das Internet verbunden werden, dass die Metadaten der Kommunikation von Nutzern der Standorte im öffentlichen Netz nicht erkannt werden sollen, was ist beim VPN Setup zu beachten?

B) Welche der folgenden Policies haben keine Relevanz für mehr Sicherheit bei der Softwareentwicklung von Streaming-Services, bitte streichen:
eingeschränkter Zugriff auf das Versionskontrollsystem
One-Way Verschlüsselung von Quelltext
Start von Anwendungen auf Systemen nur nach Passworteingabe
4-Augen Prinzip beim Bugfixing
Mindest-Testabdeckung von Unit-Tests
Entwicklung nur außerhalb von Gebäuden
Schulung der Entwickler
Code darf nur in Assembler entwickelt werden
SCRUM Entwicklungsprozess

C) Ein Angreifer hat Zugang zu der Netzwerkinfrastruktur der Handball-WM Live-Übertragung erlangt („geswitchtes“ Ethernet).

1. Welche Information kann der Angreifer in einer solchen Position erlangen und welche nicht (mit Begründung)?
2. Was müsste der Angreifer tun um „Man in the Middle“ Angriffe durchführen zu können? Beschreiben Sie die einzelnen Schritte wie er Vorgehen könnte.
3. Was müsste der Angreifer zusätzlich tun um verschlüsselte Verbindungen aufbrechen zu können?

D) Software, die für die Handball-WM notwendig ist, entsteht in einem Entwicklungsprozess den man in verschiede Phasen unterteilen kann. Ordnen sie die SSDLC Aktivitäten der richtigen Phase zu:

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

E) Live Events wie das Endspiel der Handball WM sind ein attraktives Ziel für (D)DOS Angriffe.
Was würden Sie als Sicherheitsverantwortlicher tun um sich gegen (D)DOS Angriffe zu schützen (min. 3 Maßnahmnen)
Schreiben Sie in Pseudocode einen Bot! der ein DDOS Angriff simuliert um Ihre Sicherheitsmaßnahmen auch überprüfen zu können und auch alle anderen in der Vorlesung besprochenen Eigenschaften eines Bots besitzt.

F) Welche der folgenden Aussagen sind falsch (bitte streichen):

- Stateful Insprection Filter funktionieren nur mit zustandsbehafteten Protokollen
- Statische Filter arbeiten mit Heuristiken
- Beim Erstellen von Filterregeln sollten nur ungewünschte Vorgänge gefiltert werden
- Intrusion Prevention Systeme finden alle Attacken
- Intrusion Prevention Systeme müssen nur einmalig konfiguriert werden
- Statische Filter schreibt man am besten selbst
- Dynamische Filter können per Rate Limit implementiert sein
- Statische Filter lassen sich durch Spoofing täuschen

G) Mit welcher Maßnahme können Sie sowohl Bufferoverflows als auch SQL Injections und XSS vermeiden?