[root@netsec]>

IT Security

Klausur an der Hochschule Karlsruhe - Technik und Wirtschaft
Wintersemester 2019/20, Mittwoch, 12.02.2019, 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

Begriffswelt

Bei Star Wars ist Imperator Palpatine von den Toten auferstanden und sorgt sich nun um die Sicherheit der Imperialen IT. Erklären Sie ihm bitte kurz schriftlich mindestens 10 der folgenden 11 Begriffe:

Rechtsverbindlichkeit, ISO 27001, Darth Vader, DDoS, Bot, Cross Site Request Forgery, NAT, TKG, VPN, OWASP, Open SAMM

Aufgabe 2: Safety

A)__/8 B)__/8 C)__/6 D)__/8 __/30 Punkte

A) Welche der folgenden Star Wars Technologien erfordert als Design-Ziel Zuverlässigkeit, und welche Verfügbarkeit? Kreuzen Sie an und begründen Sie jeweils kurz!

	Zuverlässigkeit	Verfügbarkeit
Medikit (Kombination aus Injektion + Defibrilator)	[ ]	[ ]
Supremacy (Raumschiff)-Antrieb)	[ ]	[ ]
Blaster (Waffe)	[ ]	[ ]
R2-D2 (Astromechdroide, Roboter)	[ ]	[ ]

B) Um auch wirklich sicher zu gehen, dass Planeten zerstört werden können, lässt Imperator Palpatine drei Todessterne bauen. Mindestens einer davon muss funktionieren, um einen Planeten zu zerstören. Jeder Todesstern hat eine Ausfallwahrscheinlichkeit von 50%. Außerdem darf kein Jedi kommen, wenn ein Jedi kommt, zerstört er alle drei – die Wahrscheinlichkeit dass ein Jedi auftaucht ist 80%.
Wie groß ist die Verfügbarkeit der Planetenzerstörungskräfte von Palpatine?

C) Mitarbeiter der Sturmtruppen machen häufig Fehler in der Wartung und Bedienung sicherheitsrelevanter Soft- und Hardware. Nennen Sie Maßnahmen aus dem Umfeld der IT-Security um die Wahrscheinlichkeit solcher Fehler zu verringern.

D) Welches bzw. welche Schutzziel(e) werden mit der Umsetzung der untenstehenden Maßnahmen jeweils verfolgt (Hinweis: lässt sich gut in einer Tabelle darstellen)?
Verschlüsselung, 4-Augen Prinzip, RAID, Ersatz-Todesstern, Paketfilter, Archivsystem, Zugangskontrolle zum RZ, Digitale Signatur

Aufgabe 3: Security

A)__/8 B)__/7 C)__/10 D)__/5 E)__/6 F)__/7 G)__/7 H)__/10 __/60 Punkte

A) Software, die für den Todesstern 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

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

- Stateful Inspection 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

C) Schreiben Sie in Pseudocode einen einfachen Paketfilter, der am Internet-Anschluss von Palpatines RZ für Sicherheit sorgen soll. Zugriffe per HTTPS (Port 443) müssen von überallher erlaubt sein, per SSH (Port 25) nur von IP 193.196.64.5, und wenn Zugriffe auf E-Mail (SMTP, Port 25) erfolgen, so soll Palpatine benachrichtigt werden.

D) Neben technischen Maßnahmen sind auch Regeln ein wichtiger Mechanismus, um Security zu stärken. Entwerfen Sie eine Policy (min. 5 Regeln) für Sturmtruppler, die zu Wartungsarbeiten ins RZ müssen.

E) Welche der folgenden Maßnahmen laden zu Spoofing ein? Bitte ankreuzen.

[ ] Abbildung von MAC Adressen auf IP Adressen
[ ] Filter nach IP-Quelladressen
[ ] Feststellung der Echtheit von Websites durch X.509 basierte Zertifikate
[ ] Zugangskontrolle am Todesstern bzgl. Sturmtruppenausweisen
[ ] Mails die einen Trojaner enthalten
[ ] Biometrische Zugangskontrolle zum Waffensystem des Todessterns

F) Der Todesstern wird immer wieder von DoS Attacken heimgesucht. Welche der folgenden Möglichkeiten sind typische Angriffsflächen für DoS und welche für DDoS Attacken? Bitte jeweils in den entsprechenden Spalten ankreuzen.

DoS	*DDoS*		*DoS*	*DDoS*	
[ ]	[ ]	Protokollschwächen	[ ]	[ ]	unterdimensionierte Serversysteme
[ ]	[ ]	ineffizienter Code	[ ]	[ ]	Lage des RZ auf einer Insel
[ ]	[ ]	Programmierfehler	[ ]	[ ]	Leitungslänge im RZ
[ ]	[ ]	Amplification durch Requestgrößen			
[ ]	[ ]	Amplification durch Requestzahlen			

G) Welche der folgenden Eigenschaften besitzt ein Wurm (nach der Definition aus der Vorlesung) auf jeden Fall? Streichen Sie unzutreffende aus der Liste. Extrapunkt: kennzeichnen Sie optionale Funktionen mit (o):

verbreitet sich über Datenträger
nutzt Buffer-Overflows
verbreitet sich selbständig über das Netz
lädt Funktionen nach
hat ein Trojaner
verschlüsselt Festplatten
sucht Opfer
versteckt sich
befällt Executables
macht Cryptomining

H) Durch einen Spion sind die Rebellen in den Besitz von geheimen Informationen gekommen, dass der Todesstern am Internet angeschlossen ist und durch den langen Bau auf einem veralteten Betriebssystem läuft.
Schreiben Sie für die Rebellen eine Schadsoftware, welche eine bekannte Bufferoverflow Lücke über das Netz ausnutzt und die Funktion „SchutzschildeDeaktivieren()“ ausführt.