[root@netsec]>

IT Security

Klausur an der Hochschule Karlsruhe - Technik und Wirtschaft
Sommersemester 2021, Mittwoch, 21.07.2021, 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

Die Britische Königsfamilie drängt ins digitale Zeitalter und lebt verteilt in der Welt! Das bedeutet natürlich dass sie mit IT-Security klar kommen müssen!

Lord Anthony Nerd und Lady Melissa Nerd sollen die moderne Begrifflichkeit des IT-Security-Umfeldes auch traditionsbewussten Verwandten nahebringen und haben sich dazu ein Rätsel ausgedacht, bei dem die korrekten Assoziationen der Begriffe in den Spalten A und B eingezeichnet werden sollen.

Lösen Sie es als seien Sie Teil der Familie!

Spalte A	Spalte B
Proxy	Eintrittswahrscheinlichkeit
ISO 27001	Sprungziel wahrscheinlich treffen
Shell Code	Security Organisation
Threat Model	Verteilter Angriff
OWASP	IT-Sicherheitsstandard
Insel	Angriff auf Datenbanken
DDoS	Client & Server
NOP-Rutsche	Angriffsflächen betrachten
Risiko	Topologische Abwehrmaßnahme
SQL Injection	Ohne 0-Bytes

Aufgabe 2: Safety

A)__/8 B)__/8 C)__/6 D)__/5 E)__/4 F)__/4 __/35 Punkte

A) Natürlich ist der Buckingham Palast vorzüglich gegen Einbruch abgesichert. Lord Nerd führt eine Sicherheitsüberprüfung durch und findet heraus: Die Wahrscheinlichkeit dass jemand bei einem der 3 Front-Fenster einbrechen kann ist jeweils 20%. Die Wahrscheinlichkeit dass der Einbrecher dann auch noch am zusätzlichen Kameraüberwachungssystem vorbeikommt liegt bei 80%.
Wie hoch ist die Wahrscheinlichkeit, dass ein Eindringling an der Kombination der Systeme Fenster und Kamera erfolgreich vorbeikommt?

B) Lady Melissa Nerd gibt zu bedenken, dass das Kameraüberwachungssystem nur eine Verfügbarkeit von 50% hat – was heißt das für die Wahrscheinlichkeit den Eindringling zu erkennen?

C) Die beiden schauen sich die Statistik der letzten Jahre an – wie viele Stunden im Jahr müsste das Kameraüberwachungssystem ungefähr statistisch nicht zur Verfügung gestanden haben?

D) Würden Sie den beiden empfehlen, auf ein auf Zuverlässigkeit optimiertes System umzusteigen? Bitte begründen Sie Ihre Empfehlung!

E) Die Zuordnung zu verschiedenen Maßnahmen-Klassen ist wohl auch noch nicht ausgefüllt worden. Bitte helfen Sie den Royals, indem Sie die Maßnahmen den Schutzzielen in der unten stehenden Tabelle zuordnen:

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

F) Lady Nerd befasst sich mit Möglichkeiten, die Sicherheitsmechanismen des Buckingham Palast zertifizieren zu lassen. Welche der folgenden Möglichkeiten spielen können hierzu sicherlich nicht herangezogen werden (bitte streichen. Die Tatsache dass die Story in England spielt ist vernachlässigbar):

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

Aufgabe 3: Security

A)__/7 B)__/8 C)__/5 D)__/5 E)__/6 F)__/5 G)__/8 H)__/0 I)__/6 J)__/5 __/55 Punkte

A) Lord Nerd hat auf der Royalen Website im Gästebuch(wichtige Funktion) eine XSS Lücke vom berühmten Bughunter Lord "R00b1n ^" gemeldet bekommen. Welche Konsequenzen kann die Lücke für die Besucher der Webseite haben? Was für eine Maßnahme soll Lord Nerd veranlassen um die Lücke zu schließen?

B) Können Sie im Auftrag von Lord Nerd seinem Neffen Lord Noob (am besten mit Hilfe einer Skizze) Erklären, wie so ein XSS Angriff abläuft?

C) Doppelgänger der Royal Family gibt es viele. Spoofing ist aber ein noch weiter verbreitetes Thema. Welche der folgenden Vorgänge haben nichts mit Spoofing zu tun? Bitte durchstreichen!
Fingerabdruckscan beim Zugang in das Schlafzimmer von Lady Nerd
Fest eingestellte MAC-Address Tabellen in den Switches des royalen Netzwerks
Prüfung der Lebensläufe bei der Einstellung neuer Palastwachen
DDoS Attacke auf den Provider von www.royals.uk
Vergrößerung der NOP-Rutsche vor dem Shell-Code beim Einbruch ins Netz

D) Um Spoofing zu vermeiden gibt es Identitätsüberprüfungen von Identitätsmerkmalen auf vielen Layern und an vielen Stellen.
Nennen Sie jeweils eine Möglichkeit, Spoofing zu erschweren für die entsprechenden Stellen an denen Identitätsmerkmale eine Rolle spielen:
Personalausweis, MAC-Adresse, Hostnamen im DNS, Hostnamen im Browser-URL, Haustürschlüssel, Absender E-Mail Adressen

E) Eine Insel ist natürlich die bevorzugte topologische Abwehrmaßnahme der Royals. Welche Vor- und Nachteile hat dieses Pattern?

F) Entwerfen Sie eine Policy mit mindestens 5 Regeln für den sicheren Zugang zum Rechenzentrum des Buckingham Palast.

G) Schreiben Sie bitte in Pseudocode einen einfachen Wurm für Lord Noob, an dem man erkennen kann, welche Eigenschaften so eine Malware haben muss, und um ihm zu helfen ins Netz vom Buckingham Palast einzudringen.

H) Wer ist aktuell Thronerbe in England?

I) Der Kühlschrank in der Palastküche zieht sich automatisch Softwareupdates aus dem Internet. Welche möglichen Schwachstellen ergeben sich daraus und wie könnten die Nerds dies verhindern?

J) Software, die für die Stammbaumverwaltung der königlichen Familie notwendig ist, entsteht in einem Entwicklungsprozess den man in verschiede Phasen unterteilen kann.
Ordnen Sie die SDLC Aktivitäten der richtigen Phase zu:

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