[root@netsec]>

IT Security

Klausur an der Hochschule Karlsruhe - Technik und Wirtschaft
Sommersemester 2018, Mittwoch, 18.07.2018

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 die Suche nach den größten und gefährlichsten Schätzen der Menschheit ist der Heldin Cara Loft aus unserer Story „Comb Raider“ nichts zu aufwändig. Sie investiert heftig in IT-Sicherheit für ihre Schatzsuchinfrastrukturen!

Erklären Sie ihr dazu kurz folgende 10 Begriffe aus der IT Security Vorlesung: XSRF, ARP-Spoofing, Zurechenbarkeit, ISO 27001, Hybridredundanz, Keystroke Logging, Firewall, SQL Injection, ASLR, Forensik

Aufgabe 2: Safety

A)__/8 B)__/12 C)__/8 D)__/6 E) __/6 __/40 Punkte

A) Das RZ von Cara Loft liegt auf einer Einsamen Insel. Mögliche Zugänge sind: die gut geschützte Vordertür (hält laut Hersteller 80 von hundert Einbruchsversuchen stand) und ein Unterwasserversorgungstunnel der von mutigen Angreifern ertaucht werden kann. Die Erfolgswahrscheinlichkeit diesen Weg unbeschadet zu überstehen wird mit 10 von hundert Versuchen eingeschätzt. Wie hoch ist die Wahrscheinlichkeit, dass ein Eindringling sich Zugang zum RZ verschafft?

B) Wenn ein Angreifer in das RZ von Cara eindringen möchte, hat er natürlich die Möglichkeiten, physisch Zugang zu suchen wie in Aufgabenteil A). Daneben gibt es natürlich auch die theoretische Möglichkeit, über das Netz einzubrechen. Die Einbruchswahrscheinlichkeit über XSS liegt bei 10%, über Buffer Overflow bei 10%, über Social Engineering bei 10%. Der Schaden bei einem erfolgreichen Einbruch über das Netz oder über physischen Zugang läge bei 10.000.000€, berechnen Sie das Risiko (nach der einfachen ISO-Definition)!

C) Das RZ benötigt natürlich viel Energie, welche (leider) noch durch ein Atomkraftwerk (welches Cara günstig über E-Bay erstanden hat) erzeugt wird. Da es sich um ein älteres Modell handelt, schlägt der Sicherheitschef vor, weitere Sicherheitsmaßnahmen umzusetzen. Sollten diese eher auf die Verfügbarkeit oder Zuverlässigkeit einzahlen – Begründen Sie Ihre Antwort.

D) Über den schwierigen Zugang zum Insel-RZ von Cara Loft haben wir nun schon gehört – die Maßnahmen zur Verfügbarkeit der Systeme im RZ sollen nun erhöht werden – entscheiden Sie zwischen symmetrischer und asymmetrischer Redundanz und begründen Sie Ihre Wahl!

E) Welche Vorteile und Nachteile bietet so ein RZ auf einer einsamen Insel in Bezug auf *Safety* im Vergleich zu einem klassischen RZ in einer beliebigen Großstadt?

Aufgabe 3: Security

A)__/10 B)__/5 C)__/5 D)__/6 E)__/10 F)__/8 G)__/6 __/50 Punkte

A) Schreiben Sie in Pseudocode einen einfachen Paketfilter, der am Internet-Anschluss von Cara‘s 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 Cara benachrichtigt werden.

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

C) 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 Skilift bzgl. Wochen-Skipässen
[ ] Zugangskontrolle am Hafen von Cara‘s RZ-Insel bzgl. obiger Policy

D) Cara‘s RZ-Insel 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			

E) Wie schon in 2B) zu erkennen kommt es gelegentlich zu XSS Attacken auf Cara‘s Infrastruktur. Zeichnen Sie ein Client Side XSS Szenario und erklären Sie die Reihenfolge der Vorgänge, bei dem Szenario sollen mindestens zwei Browser-Clients, ein Frontend-Webserver und ein DB-Server vorkommen.

F) Wie könnte so eine XSS aus Aufgabe E) für die Infrastruktur des ganzen RZs gefährlich werden? Beschreiben Sie ein Angriffsszenario.

G) Neben XSS sind Buffer Overflows immer wieder mal ein Problem für Cara - Welche Eigenschaften sollte Shellcode, der bei der Ausnutzung der Buffer Overflows herangezogen wird haben, damit er wirkungsvoll ist?