[root@netsec]>

IT Security

Klausur an der Hochschule Karlsruhe - Technik und Wirtschaft
Wintersemester 2016/17, Montag, 30.01.2017

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

Sie sind (endlich) Sicherheits-Beauftragter beim hippen Internet of Things Startup „Das Dolle Ding Online Sofort“ (DDDOS). Nachdem Ihre vollvernetzten Kaffeemaschinen, Kühlschränke und Klorollenhalter eine signifikante Beteiligung am letzten Angriff des berüchtigten IoT Botnetzes Sirei hatten, ist Ihr (in Sicherheitsfragen leider nicht so bewanderter) Entwicklungsleiter besorgt. Erklären Sie ihm kurz folgende 10 Begriffe aus der IT Security Vorlesung:
DDoS, Buffer Overflow, NAT, Zuverlässigkeit, asymmetrische Verschlüsselung, Spoofing, Schutzziele, Bastion, Bot, IT Grundschutz

Aufgabe 2: Safety

A)__/ 8 B)__/4 C)__/4 D)__/6 E)__/6 __/28 Punkte

A) Ihr Unternehmen bietet auch vernetzte Rauchmelder an, welche über WLAN und die Cloud einen Alarm auf Ihrer Handy App auslösen. Wie hoch ist die Verfügbarkeit der Alarmierung wenn in Ihrer Ein-Zimmer Studentenwohnung zwei Rauchmelder angebracht sind und alle beteiligten Elemente 80% Verfügbarkeit besitzen?

B) Welches Element der Kette würden Sie redundant ausführen, um die Verfügbarkeit zu erhöhen? Begründen Sie Ihre Antwort!

C) Seit dem Desaster mit dem Sirei Botnet haben ALLE (Anzahl: `n`) IoT Devices Ihres Unternehmens ein Selbstzerstörungsmechanismus welcher eine Verfügbarkeit von 90% hat. Mit welcher Wahrscheinlichkeit können Sie das Botnet über diesen Mechanismus während eines Angriffes komplett ausschalten?

D) Ihr Clouddienst der Ihre IoT Devices mit den Handy Apps verbindet soll auditiert werden. Welche Schutzziele halten Sie bei dem Dienst für beachtenswert? Begründen Sie Ihre Antwort kurz.

E) Nennen Sie mindestens 3 Szenarien welche bei einer Bedrohungsanalyse Ihres Clouddienstes gefunden wurden, mit den dazugehörenden Maßnahmen.

Aufgabe 3: Security

A)__/8 B)__/6 C)__/10 D)__/6 E)__/7 F)__/9 G)__/6 H)__/10 __/62 Punkte

A) Was sind (nach der in der Vorlesung gegebenen Definition) die Unterschiede zwischen einem Virus, einem Wurm, einem Trojaner und einem Bot?
Welche dieser Malware-Typen können negative Auswirkungen auf IoT Devices haben? Begründen Sie Ihre Antwort!

B) Welche Motivationen haben Botnetzbetreiber, gerade diese Art von Malware zu nutzen?

C) Ihr Boss hat Sie mit der Analyse eines Sirei Bots beauftragt. Schreiben Sie zum besseren Verständnis der Zusammenhänge für Ihren Boss in Pseudocode auf, wie der Bot prinzipiell funktioniert.

D) Sie sollen den Kunden Ihres DDDOS Startups helfen Ihre gekauften IoT Devices sicherer zu betreiben.
Schreiben Sie für die Kunden eine FAQ mit mindestens 3 Punkten und kurzer Erläuterung.

E) Der Sirei Bot hat Ihre vernetzten Klorollenhalter über eine Buffer-Overflow Lücke befallen.
Wie können Sie sich in der SW-Entwicklung besser vor dieser Art von Sicherheitslücke schützen?

F) Vor allem Aktionismus haben Sie vergessen, dass Ihr Chef noch gar nicht weiß wie ein Buffer-Overflow eigentlich funktioniert.
Erklären Sie Ihm (gerne anhand einer Skizze) den Ablauf.

G) Würden Sie als Strategie (Ihrem Chef) eher „Security by Design“ oder „Security by Obscurity“ empfehlen? Begründen Sie Ihre Wahl!

H) Wie könnten XSS/XSRF Lücken die Sicherheit Ihrer IoT Devices beeinträchtigen? Beschreiben Sie (idealerweise mit Hilfe von Skizzen) zwei mögliche Angriffsszenarien in Abhängigkeit davon wo sich die Lücke befindet.