[root@netsec]>

IT Security

Klausur an der Hochschule Karlsruhe - Technik und Wirtschaft
Sommersemster 2017, Mittwoch, 19.07.2017, 11:00 Uhr

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

Disclaimer:
- Zugelassene Hilfsmittel: keine ausser Stifte und Lineal
- Der Lösungsweg muss bei allen Aufgaben ersichtlich sein
- Ähnlichkeiten mit realen Institutionen sind rein zufällig und nicht beabsichtigt

Aufgabe 1: Begriffswelt

__/10 __/10 Punkte

Das Land Molwanien will sein Wahlsystem digitalisieren und Wahlcomputer einsetzen. Nicht zuletzt wegen des Vermeidens von Wahlmanipulation bedarf es dazu einiges an Expertise. Zunächst ist eine klare Begrifflichkeit erforderlich. Erklären Sie dazu folgende Begriffe kurz:

NAT, Zuverlässigkeit, DDoS, Schutzziele, Bot, Stateful Inspection, dynamische Redundanz, Spoofing, Nadelöhr, Firewall

Aufgabe 2: Safety

A)__/6 B)__/4 C)__/10 D)__/10 E)__/4 __/34 Punkte

A) Der Chefentwickler der Wahlcomputer stellt Ungereimtheiten im Lastenheft fest. Safety und Security werden darin synonym verwendet. Erklären Sie weshalb das nicht korrekt ist. Nennen Sie jeweils 2 Beispiele für Security- sowie Safetymaßnahmen.

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

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

C) Die Wahllokale sollen mit Wahlcomputer ausgestattet werden. Ein Wahlcomputer hat laut Hersteller eine Verfügbarkeit von 50%. Die Internetanbindung im Wahllokal hat eine Verfügbarkeit von 90%, Strom kann mit 90% zur Verfügung gestellt werden. Wie viele Wahlcomputer benötigen Sie, um eine Verfügbarkeit von über 64% für das Wahllokal zu garantieren (bei möglichst minimalen Kosten!)?

D) Auch die Serverkomponenten müssen redundant ausgelegt werden. Es soll ein aktiv-passiv Setup aufgebaut werden.

1. Auf welchen Ebenen könnten Sie ein Takeover zwischen dem aktiven und dem passiven System durchführen?
2. In welchen Eigenschaften unterscheiden sich diese Ebenen zur Service-Übernahme? Stellen Sie strukturiert Vor- und Nachteile gegenüber!
3. Welche Rolle hat dabei der Heartbeat?
4. Welche Methoden, so einen Heartbeat zu implementieren fallen Ihnen ein?
5. Was versteht man unter einer „Split Brain“ Situation?

E) Welche Schutzziele sollten bei einem Wahlcomputer besondere Beachtung finden? Nennen Sie jeweils 2 konkrete Maßnahmen, welche die Schutzziele unterstützen.

Aufgabe 3: Security

A)__/6 B)__/15 C)__/5 D)__/10 E)__/10 __/46 Punkte

A) Die Wahlcomputer sollen automatisch mit Softwareupdates über das Netz versorgt werden können. Welche Schwachstellen ergeben sich daraus für einen potentiellen Angreifer? Wie könnten Sie das verhindern?

B) Bei einem Code Review der Wahlcomputer Software entdecken Sie folgenden Codeschnipsel:

```
void  FrageBenutzername () {
    char name [23];
    printf („Geben Sie Ihren Namen ein:\n“);

    gets(name);
    dbCon = OpenDbConnection();
    dbCon.execute(„INSERT INTO waehler (Name) VALUES (“+name+“);“);

    renderHTMLpage(„hallo “+name+“ danke für Ihre Stimme<br />“);
}
```

1) Welche potentielle Sicherheitsprobleme entstehen dadurch?
2) Verbessern Sie den Code so, dass er nicht mehr anfällig ist.
3) Welche weiteren Maßnahmen kennen Sie um die im Code entstandenen Sicherheitslücken zu vermeiden?

C) 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

D) Sie wollen die Sicherheit Ihrer Wahlcomputer überprüfen. Schreiben Sie in Pseudocode einen Port Scanner, welcher die gefundenen Informationen mit einer Vulnerability DB abgleicht und im Falle einer Sicherheitslücke einen Alarm triggert.

E) Die Wahlcomputer sollen entgegen Ihrer Empfehlung über das Internet mit der Zentrale verbunden werden. Zudem sollen noch die Wahlhelfer Laptops bekommen, mit denen Sie den Zustand der Wahlcomputer überwachen können. Selbstverständlich sollen diese auch im Internet surfen dürfen damit Ihnen nicht langweilig wird.
1) Skizzieren Sie den Aufbau des Netzes des Wahllokals – benutzen Sie die Sicherheitsbausteine aus der Vorlesung um einen optimalen Schutz zu gewährleisten.
2) Welche Richtlinien definieren Sie für die Laptops und deren Benutzung?