Christian Schindelhauer
Sneha Mohanty

Freiburg, den 8. Dezember 2021
Abgabeschluss 14. Dezember 2021, 23:59 Uhr UTC+1

Übungen zur Vorlesung
Rechnernetze
Winter 2021/2022
Blatt 8

Bitte laden Sie eine PDF-Datei in ILIAS hoch, andere Abgaben werden ignoriert. Schreiben Sie alle Namen und Matrikelnummern der Gruppenteilnehmer auf die Abgabe.

Aufgabe 1: Zertifikate (3 Punkte)

Rufen Sie die Kurswebseite *https://cone.informatik.uni-freiburg.de/lehre/aktuell/rechnernetze-ws21/* auf und untersuchen Sie das Zertifikat des Servers. *(Hinweis: Das Zertifikat einer Webseite kann bei gängigen Browsern mit Click auf das Schlüsselsymbol in der Adresszeile angesehen werden.)*

a) Identizifieren Sie den Aussteller des Zertifikats. (1 Punkte)

b) Geben Sie zwei Domain-Namen an, für die dieses Zertifikat noch gilt. (1 Punkte)

c) Angenommen, Ihr Browser bestätigt die Vertrauenswürdigkeit einer Webseite aufgrund des Zertifikats. Welche Bedrohungsszenarien sind dann noch denkbar? Beschreiben Sie hierzu zwei mögliche Angriffswege oder Sicherheitsrisiken. (1 Punkte)

d) Der Impfstatus einer Person wird durch das Vorzeigen und Verifizieren eines digitalen Impfzertifikats (z.B. durch QR-Code) überprüft. Beschreiben Sie, welche Technologien und Infrastruktur die Authentizität dieses Nachweises sicherstellen. Diskutieren Sie, ob die CovPass-Check-App Zertifikate auch offline verifizeren kann. (3 Bonuspunkte)

Aufgabe 2: Firewall (4 Punkte)

Ein Werkzeug zur Konfiguration von Firewalls in Unix-basierten Systemen ist *iptables*. Ihre Aufgabe ist es, Firewallregeln nach bestimmten Kriterien zu erstellen und gegebene Konfigurationen zu interpretieren. Geben Sie Ihre Firewallregeln entweder als Kommandozeilenbefehl oder als Eintrag in der Konfigurationsdatei */etc/iptables/iptables.rules* an. Es ist zur Beantwortung der Frage nicht nötig, eine Firewall konkret zu konfigurieren. (Wer empfehlen, solche Tests in einer virtualisierten Testumgebung vorzunehmen.)

Eine ausführliche Dokumentation zur Verwendung von iptables finden Sie unter:

- *https://wiki.archlinux.org/title/iptables*
- *https://wiki.archlinux.org/title/Simple_stateful_firewall*

Geben Sie nun die Konfiguration für die folgenden Anforderungen an.

a) Ihr System soll per SSH erreichbar sein, um Fernwartung zu gewährleisten. SSH benutzt das Protokoll TCP und Port 22. (1 Punkt)

b) Sie haben zu Testzwecken einen Webserver auf Port 1234 gestart. Jedoch möchten Sie verhindern, dass dieser Dienst von außerhalb erreichbar ist. Blockieren Sie nur diesen Dienst. Über das Loopback-Interface soll die Erreichbarkeit gegeben sein. (Zwei Kommandos notwendig) (1 Punkt)

c) Was bewirkt folgende Konfigurationseinstellung? Warum könnte sich ein Administrator für die Implementierung dieser Regel entscheiden? (1 Punkt)

```
iptables -A INPUT -p icmp -j DROP
```

d) Bewerten Sie die Aussage: „Standardmäßig werden alle eingehenden Verbindungen blockiert“. Beschreiben Sie, warum Sie diese Regel in den meisten Firewallkonfigurationen finden werden. Nachfolgend ist die Umsetzung dieser Regel in iptables. (1 Punkt)

```
iptables -P INPUT DROP
```

Aufgabe 3: Bitstopfen (3 Punkte)

Betrachten Sie (abweichend von der Vorlesung) die Flagbitsequenz `1001`. Geben Sie im Folgenden alle Berechnungsschritte vollständig an.

a) Wandeln Sie die in der Vorlesung vorgestellte Methode so ab, dass sie mit dieser Flagbitsequenz funktioniert. Beschreiben Sie, wie eine Nachricht mit Flagbitsequenzen und durch Ihr Bitstopfen zum Senden vorbereitet wird. (1 Punkt)

b) Angenommen, Sie empfangen die Bitsequenz:
`1001 0101 0101 0111 1011 0111 0101 0101 0110 1101 1100 1`
Entstopfen Sie die Nachricht mit Ihren Verfahren. Ist es möglich? Und falls ja, welche Bitsequenz wurde übermittelt? (1 Punkt)

c) Sie wollen die folgende Nachricht versenden:
`0010 0100 1010 1000 0110 0010 0110`
Nutzen Sie die oben angegebene Flagbitsequenz und die von Ihnen beschriebene Methode, um die Nachricht zum Senden vorzubereiten. (1 Punkt)