Rheinische Friedrich-Wilhelms-Universität Bonn

Bachelorstudiengänge Cyber-Security / Informatik

Prüfungsklausur

Semester: SoSe 2021	Versuch: 1. ☑ 2. □
Modulbezeichnung: ***Netzwerksicherheit***	
Modulnummer: *BA-INF 0147*	Prüfungsdatum: 05. *August 2021*
Prüfer: *Dr. Matthias Wübbeling*	

vom Prüfling auszufüllen:

Name:	Matrikel-Nr:
Vorname:	Semester:
Bachelor Informatik ☐ **Studiengang** Bachelor Cyber Security ☐	
Lehramt ☐ Informatik als Nebenfach ☐ FFF ☐	

vom Prüfer auszufüllen:

Bewertung:

*Noten und Notenwerte: **sehr gut (1,0; 1,3) – gut (1,7; 2,0; 2,3) – befriedigend (2,7; 3,0; 3,3) – ausreichend (3,7; 4,0) – nicht ausreichend (5,0)**

Datum: 05. *August 2021*

Unterschrift des Prüfers

Dr. Matthias Wübbeling Bonn, den 05. August 2021

Hinweise zur Modulprüfung zu „Netzwerksicherheit“ (BA-INF 0147)

Sommersemester 2021
10:15 Uhr – 11:45 Uhr

Hinweise (GENAU DURCHLESEN!) – Für Online-Klausuren gelten die vom Prüfungsausschuss im Vorfeld veröffentlichten Informationen

- Neben Papier und Schreibutensilien sind **keine weiteren Hilfsmittel** erlaubt. Verwenden Sie nur dokumentenechte Stifte (z.B. keine Bleistifte). Verwenden Sie keine roten Stifte.
- Vergessen Sie nicht, Ihren Namen und die Matrikelnummer auf *jedes* Blatt zu schreiben. Blätter ohne diese Angaben werden nicht gewertet.
- Schreiben Sie Ihre Lösungen auf die Aufgabenblätter möglichst in die dafür vorgesehenen Felder. Sie können auch die Rückseiten verwenden. Weiteres Schreibpapier kann von den Betreuern angefordert werden. Benutzen Sie kein mitgebrachtes Papier.
- Bitte schreiben Sie in Ihrem eigenen Interesse deutlich. Für nicht lesbare Lösungen können wir keine Punkte vergeben.
- Klausurblätter dürfen nicht voneinander getrennt werden.
- Werden mehrere unterschiedliche Lösungen für eine Aufgabe abgegeben, so wird die Aufgabe nicht gewertet.
- Im Fall von Täuschungsversuchen wird die Klausur sofort mit 0 Punkten bewertet. Eine Vorwarnung erfolgt nicht.
- In der Klausur können Sie 90 Punkte erhalten. Achten Sie darauf, dass Sie im Schnitt nicht viel mehr als 1 Minute pro Punkt zur Verfügung haben. Mit 50% dieser Gesamtpunktzahl haben Sie die Klausur sicher bestanden.

Viel Erfolg!

1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**Gesamt**
12	9	14	15	13	13	7	7	90

Aufgabe 1 : (Multiple-Choice, 12 Punkte [12x1, Bonus: 2 Punkte])

Bei den folgenden Multiple-Choice-Fragen wird für jedes richtig gesetzte Kreuz 1 Punkt vergeben. Bei falschen Antworten werden 0 Punkte vergeben. Zusätzlich zu den erreichbaren Punkten können Sie zwei Bonuspunkte erhalten. Diese sind nicht Teil der Gesamtpunktzahl, sondern echte Bonuspunkte und werden nur dann unter den folgenden Bedingungen angerechnet, wenn die Gesamtpunktzahl nicht bereits erreicht ist. Sie erhalten 1 Bonuspunkt, falls Sie mehr als 5 richtige Antworten geben. Sie erhalten 1 weiteren Bonuspunkt, wenn alle Antworten korrekt sind. Sie können für diese Aufgabe also bis zu 14 Punkte erreichen.

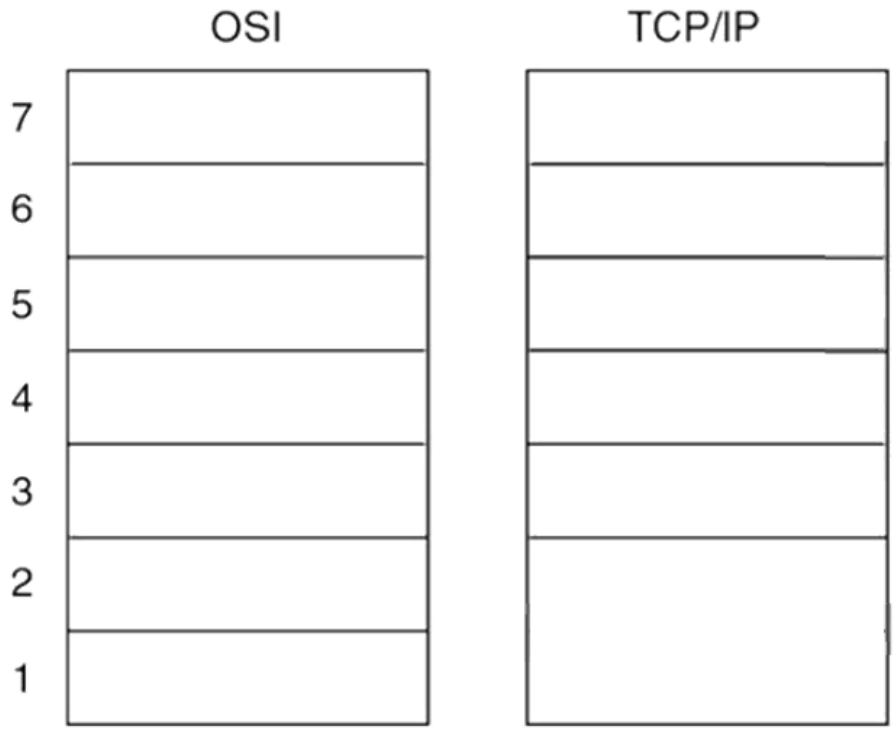
	Aussage	Richtig	Falsch
1	Die Vorlesung Netzwerksicherheit wurde über das Videoconferencing-Werkzeug ZOOM gehalten.	☐	☐
2	Bei einem Datenverbund geht es um den Austausch von Nachrichten.	☐	☐
3	Die Sitzungs-Schicht im TCP/IP-Schichtenmodell ist verantwortlich für die Zuordnung von Benutzer-Sitzungen für Webseiten.	☐	☐
4	Die Sitzungs-Schicht im TCP/IP-Schichtenmodell ist verantwortlich für die Verschlüsselung bei TLS.	☐	☐
5	IP ist ein verbindungsorientiertes Protokoll mit Drei-Wege-Handshake.	☐	☐
6	Die IP-Adresse bei IPv6 ist 1,5-mal so lang, wie bei IPv4.	☐	☐
7	Das Extensible-Authentication-Protokoll EAP erlaubt die Verwendung eines RADIUS-Servers für die Benutzerauthentifikation.	☐	☐
8	Spoofing bedeutet, dass ein Angreifer seine Rechte auf einem System ausweitet.	☐	☐
9	Bei TLS gibt es eine NULL-Verschlüsselung, um Klartext-Daten als TLS-Payload zu senden.	☐	☐
10	Asymmetrische Verschlüsselungsverfahren sind im Normalfall performanter als symmetrische Verschlüsselungsverfahren.	☐	☐
11	ASN1 ist eine abstrakte Syntaxnotation, die häufig in normativen Dokumenten zu finden ist.	☐	☐
12	Diffie-Hellman ist eine Key-Derivation-Function (KDF) nach PKCS#5.	☐	☐

Aufgabe 2: (Netzwerkstack, 9 Punkte [5x0,5 + 13x0,5])

a) Ordnen Sie die folgenden Netzwerkklassen basierend auf der geografischen Reichweite vom kleinsten Netzwerk bis zum Größten.

1. MAN
2. PAN
3. LAN
4. GAN
5. WAN

b) Ergänzen Sie die Namen der Schichten für die Modelle ISO/OSI (link) und TCP/IP (rechts).



Aufgabe 3: (Schutzziele der IT-Sicherheit, 14 Punkte [4+6+4])

a) Nennen Sie die vier übergeordneten Schutzziele der IT-Sicherheit und beschreiben Sie jedes Schutzziel in zwei Sätzen.

Lösung:

b) Das STRIDE-Modell ist ein Bedrohungsmodell. Nennen Sie für jeden der 6 Buchstaben die Bedrohung und das in der Vorlesung genannte vordergründig bedrohte Schutzziel.

Lösung:

c) In der Vorlesung wurde zwischen bewegten Daten, stationären Daten und lokalen Daten unterschieden. Nennen Sie für die Klasse der bewegten Daten jeweils eine Möglichkeit zur Sicherstellung der vier übergeordneten Schutzziele.

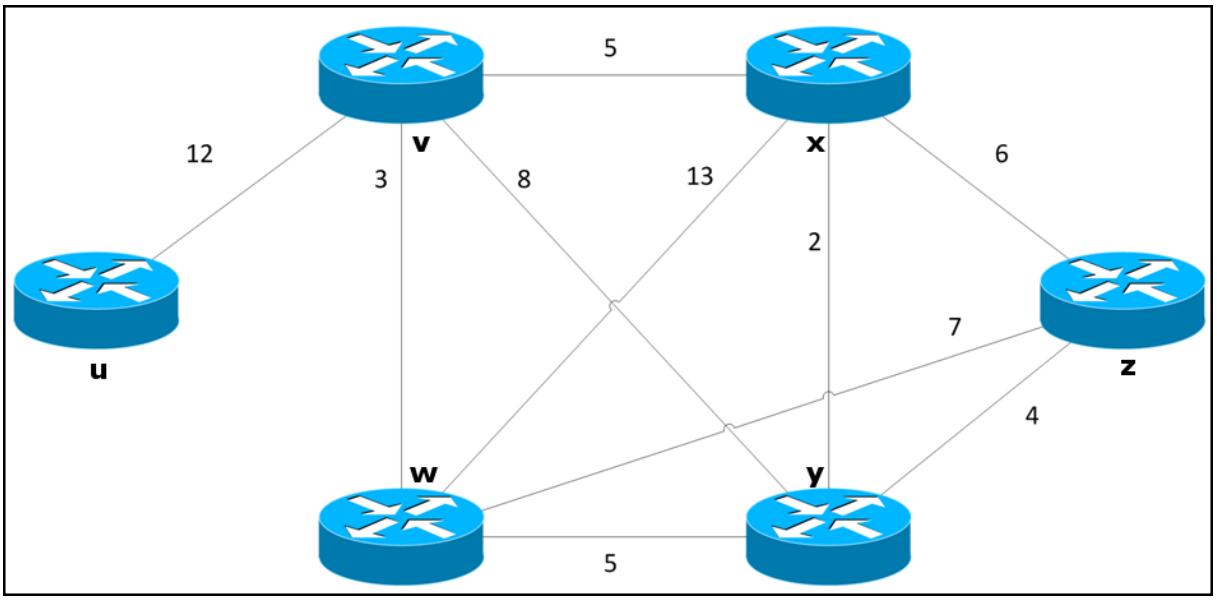
Lösung:

Aufgabe 4: (Intra-AS-Routing, 15 Punkte [6 + 9])

a) Vervollständigen Sie den Dijkstra-Algorithmus an den markierten Stellen.

```
01  N‘ = {u}
02  for all nodes v
03     if v adjacent to u
04        then D(v) = [          ]
05        else D(v) = [          ]
06  Loop:
07     find w not in N‘ such that [          ] is minimum
08     add w to N‘
09     update [          ] for all v adjacent to w and not in N‘:
10        [          ] = [                    ]
11  until all nodes in N‘
```

b) Führen Sie den Dijkstra-Algorithmus aus Sicht des **Knoten x** für das folgende Netzwerk aus, notieren Sie für jeden Schritt die Zwischenergebnisse wie in der Vorlesung gezeigt in einer Tabelle.



Lösung:

Aufgabe 5: (Inter-AS-Routing, 13 Punkte [4+3+6])

a) Geben Sie die in der Vorlesung besprochenen Schritte des Routen-Auswahl-Algorithmus von BGP an.

Lösung:

b) Geben Sie die vollständige Definition eines Prefix-Hijackings an (Stichwort: MOAS-Konflikt).

Lösung:

c) Geben Sie alle notwendigen Definitionen und die Berechnung an, um den Impact eines AS zu berechnen.

Lösung:

Aufgabe 6: (IPv6, 13 Punkte [4+2+7])

a) Generieren Sie aus der folgenden MAC-Adresse eine IPv6-Adresse, wie bei SLAAC.

52:54:00:12:35:02

Machen Sie dabei deutlich, welcher Teil der IPv6-Adresse Network-Präfix und welcher Teil Interface-Identifier ist.

Lösung:

b) Geben Sie den Scope der in a) generierten IPv6-Adresse an.

Lösung:

c) Was versteht man im Kontext von SLAAC unter DAD? Beschreiben sie den Ablauf von SLAAC, verorten Sie DAD und beschreiben den Mechanismus kurz und präzise (Max. 10 Sätze)

Lösung:

Aufgabe 7: (VPN, 7 Punkte [3+4])

a) Beschreiben Sie die beiden in der Vorlesung besprochenen Angriffe gegen Hashfunktionen und geben jeweils ein Beispiel.

b) Beschreiben Sie die IKE-Phasen I und II und erläutern Sie die Unterschiede.

Aufgabe 8: (Web-Authentifikation, 7 Punkte [2+5])

a) Beschreiben Sie den Unterschied zwischen Authentisierung und Authentifizierung.

b) Erläutern Sie (bildlich) den Ablauf von FIDO-2 für die Authentifikation einer Webseite. Gehen Sie hierbei von der Benutzung des Fingerabdrucksensors eines Mobiltelefons aus und benennen Sie explizit die verwendeten FIDO2-Protokolle.