



Prüfungssemester: SoSe 2023

Prüfungsdatum: 10.07.2023

Studiengang: INF-M / BE-M / CSE-M

Prüfungsfach: Sicherheit moderner Netzwerke

Dozent: Prof. Dr. Michael Jarschel

Matrikel-Nr.: _____

Semester: _____

Raum: NH, 13:00 Uhr

Platzziffer: _____

Hinweise:

- Legen Sie bitte ihren Personalausweis und Studierendenausweis bereit.
- Bitte verwenden Sie nur Kugelschreiber oder Füller, auf keinen Fall rote oder grüne Stifte.
- Es sind keine Hilfsmittel zugelassen!
- Bei Platzmangel benutzen Sie bitte die Rückseite des jeweiligen Angabenblattes.

Aufgabe	1	2	3	4	5	6	Summe
Punkte (max.)	(19)	(15)	(12)	(12)	(9)	(18)	(85)

Note:

Aufgabe 1: Netzsicherheit allgemein (19 Punkte):

- a) Geben Sie für die drei Kategorien der Netzsicherheit jeweils ein Beispiel für ein technisches System, dass in die entsprechende Kategorie fällt. (3 P.)

Prävention (Prevention)	
Erkennung (Detection)	
Analyse (Response)	

- b) Nennen Sie drei Ihnen bekannte Klassen von Firewalls und erklären Sie jeweils kurz die grundlegende Funktionsweise. (6 P.)

- c) Angreifer nutzen gerne Reflection-Angriffe, um den wahren Ursprung des Angriffs zu verschleiern. Dabei nutzen Sie Dienste, die öffentlich im Netz verfügbar sind aus. **Nennen Sie zwei mögliche Dienste**, die hierfür benutzt werden können **und erklären Sie warum manche Dienste für die Opfer gefährlicher sind als andere**. (4 P.)

- d) Warum Nennen und beschreiben Sie einen kurz einen Angriff, der die Integrität einer Datenübertragung gefährdet. (2 P.)

- e) Was versteht man unter DNS-Spoofing und welches Risiko besteht für ein Opfer davon? (4 P.)

- f) Können Firewalls erfolgreiche Phishing Angriffe verhindern? Begründen Sie Ihre Antwort! (2 P.)

Aufgabe 2: IPSec (15 Punkte):

- a) Die IT-Dienste in Ihrem Firmennetzwerk sind ausschließlich über HTTPS erreichbar. Dennoch soll der Zugriff nur durch authentifizierte Nutzer aus dem Firmennetz erfolgen. Für Mitarbeiter im Home-Office oder auf Dienstreise wird daher ein IPSec-VPN bereitgestellt. Würden Sie in diesem VPN auf AH oder ESP setzen? Begründen Sie Ihre Antwort! (2 P.)

- b) Welche Informationen sind in der Security Association Database (SAD) bei einem Teilnehmer gespeichert? (3 P.)

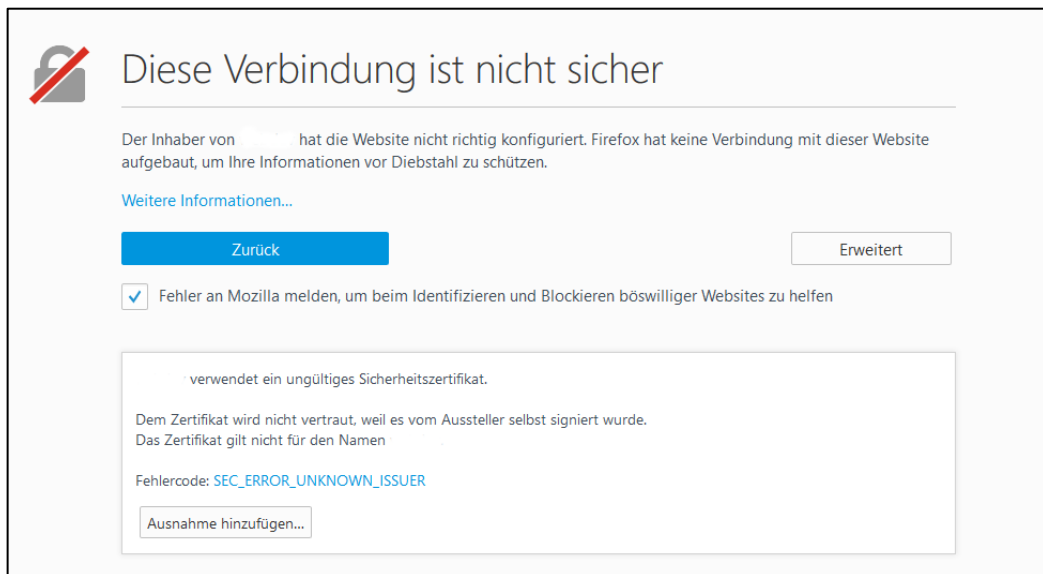
- c) Welches Problem bezüglich der maximalen Paketgröße (MTU) kann auftreten, wenn ein VPN-Tunnel auf einer Übertragungsstrecke liegt und wie könnte man dieses Problem umgehen? (3 P.)

- d) Ihr Unternehmen verfügt über eine DMZ (Demilitarized Zone) in Firmennetz. Würden Sie Ihren VPN-Endpunkt (VPN-Gateway) dort platzieren, so dass sich über das VPN einwählende Nutzer sich auch in der DMZ befinden? Begründen Sie Ihre Antwort! (3 P.)

- e) Ein Spieleentwickler setzt für die Konnektivität seines Multiplayer-Game auf ein IPSec VPN zur Verschlüsselung des Datenaustauschs. Für das Matchmaking baut der **Client** eine **direkte VPN-Verbindung** zu einem **öffentlichen Server** auf, wo er die Verbindungsinformationen zu anderen Spielern erhält. Der Austausch der Informationen während des Spiels findet im Peer-2-Peer Modus über eine **direkte VPN-Verbindung** zwischen den Spielern statt. Welchen IPSec Modus sollte der Entwickler für die jeweiligen Verbindungen nutzen? Warum ist IPSec hier vllt. nicht das Mittel der Wahl? (4 P.)

Aufgabe 3: Zertifikate (12 Punkte):

Die folgende Abbildung zeigt die Darstellung eines Browserzugriffs auf eine Webseite mit Firefox.



- a) Was kann Firefox hier nicht garantieren, so dass die Warnung aus der Abbildung notwendig wird? (2 P.)

- b) Tatsächlich kommt diese Fehlermeldung in der Praxis öfter vor – aber durchaus auch aus harmlosen Gründen. Können Sie sich einen solchen harmlosen Fall erklären? (2 P.)

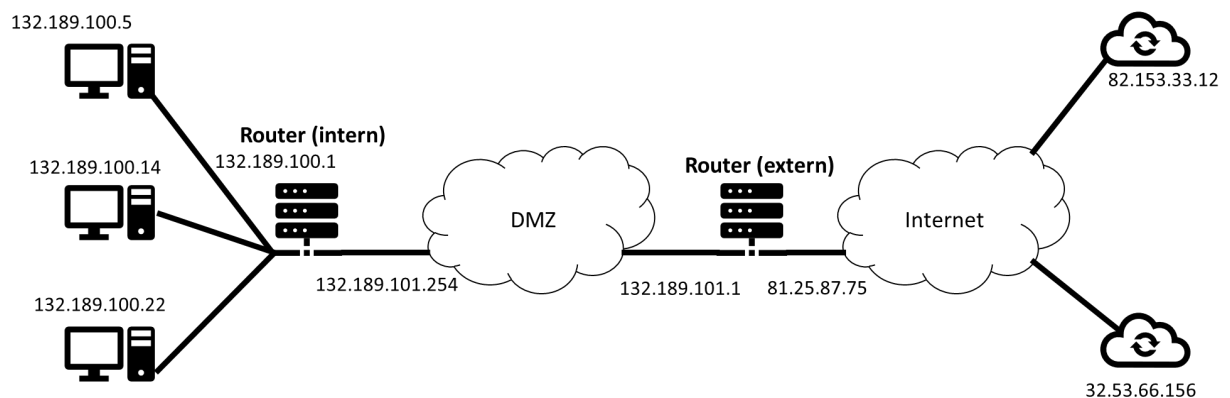
- c) Was müsste der Betreiber der Webseite tun, um die Fehlermeldung für alle ankommenden Anfragen von Browsern zu vermeiden? (2 P.)

- d) Nehmen Sie an, der Nutzer klickt im vorliegenden Fall auf „Ausnahme hinzufügen“ und akzeptiert somit das Zertifikat, damit die Fehlermeldung verschwindet. Ist dadurch die TLS-Verbindung automatisch theoretisch für jeden mitlesbar? Begründen Sie Ihre Entscheidung. (2 P.)

- e) Warum kommen bei TLS zum Schlüsselaustausch primär asymmetrische Verfahren zum Einsatz statt symmetrischer Verfahren? **Geben Sie mindestens zwei Gründe an!** (4 P.)

Aufgabe 4: Firewalls (15 Punkte):

Gegeben ist das abgebildete Szenario eines Firmennetzes. Das Netz besteht aus einem internen Bereich (132.189.100.0/24), der über einen Router mit einer zustandsbehafteten Firewall an die DMZ (Demilitarized Zone) angebunden ist. Im internen Netz hat der Router die IP-Adresse 132.189.100.1. In der DMZ liegt der Adressbereich 132.189.101.0/24 an. Beide Adressbereiche werden öffentlich geroutet. Der Router zum internen Netz besitzt hier die IP-Adresse 132.189.101.254. Die DMZ ist weiterhin ebenfalls über einen Router mit einer zustandslosen Paketfilter-Firewall an das Internet angebunden. Dieser hat zur DMZ hin die IP-Adresse 132.189.101.1 und die externe IP-Adresse 81.25.87.75.



Der Nutzer der Workstation mit der IP 132.189.100.5 im internen Netz möchte gerne auf den Cloud-Dienst im Internet mit der IP-Adresse 32.53.66.156 (TCP-Port 80) zugreifen. Die Nutzer der beiden anderen Workstation mit den IP-Adressen 132.189.100.14 und 132.189.100.22 wollen ebenfalls auf einen Cloud-Dienst mit der Adresse 82.153.33.12 (TCP-Port 80) zugreifen.

- a) Welchen Vorteil hat die zustandsbehaftete Firewall gegenüber dem zustandslosen Paketfilter? (2 P.)

- b) Die interne Firewall soll standardmäßig keinen Verkehr durchlassen. Erlaubte Zugriffe müssen explizit eingetragen werden (Whitelisting). Da die Firewall jedoch zustandsbehaftet ist, werden Regeln für die Rückrichtung dynamisch generiert und müssen nicht eingetragen werden. Spezifizieren die Filterregeln, die in der Firewall eingetragen sein müssen, damit nur HTTP(S) Verbindungen (TCP-Port 80 & 443) zwischen allen internen Hosts und beliebigen Hosts im Internet möglich sind. (5 P.)

c)

Nr.	Quell IP	Ziel IP	Protokoll	Quellport	Zielport	Aktion

- d) Die Firewall zwischen DMZ und Internet soll standardmäßig ebenfalls keinen Verkehr durchlassen. Erlaubte Zugriffe müssen explizit eingetragen werden (Whitelisting). Spezifizieren die Paketfilterregeln, die in der Firewall eingetragen sein müssen, damit nur die TCP-Verbindungen zwischen den drei spezifizierten internen Hosts und den beiden Cloud-Diensten zulässig sind! (6 P.)

Nr.	Quell IP	Ziel IP	Protokoll	Quellport	Zielport	Aktion

- e) Sind die oben gewählten Vorschriften für die Regeln der jeweiligen Firewalls sinnvoll? Begründen Sie Ihre Entscheidung! (2 P.)

Aufgabe 5: Wireless LAN (9 Punkte):

- a) Im Wireless LAN (WLAN) existiert das bekannte „Hidden Node/Terminal Problem“. Beschreiben Sie worum es sich dabei handelt mit Ihren eigenen Worten! (3 P.)

- b) Nennen Sie zwei mögliche Ursachen für das Hidden Node Problem! (2 P.)

- c) Da WLAN Clients typischerweise nicht gleichzeitig senden und empfangen können (half-duplex), können Kollisionen nicht verlässlich von den Clients im Netz detektiert werden. Daher wird im WLAN eine alternative „Random Access“-Methode verwendet. Wie heißt diese Methode? (1 P.)


- d) Was sind Beacon Frames im Kontext von IEEE 802.11 und was ist eine ihrer Aufgaben? (3 P.)

Aufgabe 6: Mobilfunknetze (18 Punkte):

- a) Nennen Sie drei Unterschiede zwischen Mobilfunk und WLAN. (3 P.)

- b) Welche Informationen (Daten, o.ä.) sind in der SIM-Karte permanent gespeichert? (4 P.)

- c) Skizzieren Sie den logischen Aufbau eines **LTE** Kernnetzes (Evolved Packet Core) mit seinen funktionalen Komponenten. (5 P.)



- d) Geben Sie für drei Komponenten des LTE-Kernnetzes (EPC) jeweils **stichpunktartig zwei Ihrer Aufgaben** an! (6 P.)

