1. Es wurden vor kurzem viele Millionen Emailkonten gehackt. Welche Schutzziele sind durch diesen Emailhack bedroht (3 Stück reichen)? Erklären Sie diese.

2.
   a) Nennen Sie zwei Regeln des Bella-Lapadula Modells.
      - No read up
      - No write down

   b) Welche dieser Regeln steht im Widerspruch zu einem hierarchischen rollenbasierten Modell?
      - No write down
      - Da in einem hierarchischen rollenbasierten Modell der obenstehende auch Zugriff auf alle unter ihm hat

3. Nennen Sie jeweils zwei Beispiele zu Stored- und Reflected XSS.
   - Stored XSS:
     - Wenn ein Schadcode auf dem Server liegt
     - Wird nun die Seite aufgerufen, wird der Schadcode ausgeführt ohne dass der User was davon weiß
     - TwitterPosts mit XSS drinnen
   - Reflected XSS:
     - Wenn ein Script in einer URL mit eingebunden ist
     - Wir der link angeklickt, so wird auch der Code auf der Seite ausgeführt
     - Email mit verdächtigem Link

4. Eine Person ist als Admin in der Routeroberfläche eingeloggt und surft im gleichen Browser. Welches Risiko kann dabei entstehen? Wie nennt man solche Arten von Angriffen?
   - CSRF – Cross Site Request Forgery
     - Klaut Cookies des Opfers und kann sich als er ausgeben, ohne dass er was weiß

   - Es kann sein, dass jemand anders Einstellungen am Router, als Admin, verändern kann

5. Fia-Feige-Schamir-Verfahren: Es sind gegeben: N, s1, s2 und s3.
   a) Welche Informationen müssen an den Lizenzierungsserver weitergeleitet werden?
      - N, Y, X, v1, v2, v3

   b) Welche weiteren Nummern werden benötigt um ein vollständiges Feige Fiat Schamir Verfahren durchzuführen?
      - r, s, a1, a2, a3

6. Es ist ein C-Programm gegeben. Darin enthalten war ein strcpy. Erläutern Sie, wie durch folgende Techniken der Angriff erschwert werden kann:

   Address-Space-Layer-Randomisation

   - Die Adressbereiche im Stack werden zufällig vergeben
   - So kann der Angreifer die Rücksprungadresse schwerer herausfinden, der zu seinem Shellcode führt

   Canaries

   - Zwischen den gespeicherten Adressen und den Variablen wird ein Zufallswert abgespeichert
   - Wenn dieser nun bei Funktionsende verändert wurde, bricht das Programm ab

   Non-Executable-Bit

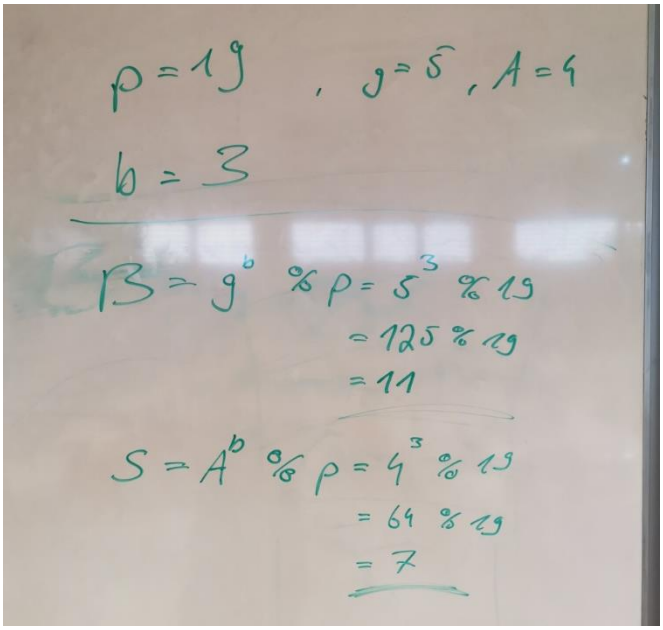
   - Ist dies gesetzt, können Daten im Stack nicht mehr ausgeführt werden
   - Somit ist das Einbringen eines Schadcodes hinfällig

7. SSL verwendet eine Kombination aus asymmetrischen und symmetrischen Verfahren.
   a) Warum wird dies so verwendet?
      - Damit die Vorteile von beiden genutzt werden
      - Das asymmetrische Verfahren wird zum Schlüsselaustausch genutzt
      - Das symmetrische Verfahren zum Versenden von Nachrichten

   b) Warum ist es wichtig einen guten Zufallsgenerator zu verwenden (SSL-Handshake)?
      - Damit Replay Attacken verhindert werden können
      - Das Herausfinder der Zufallszahl sollte sehr schwer bis unmöglich sein

8. Snowden schreit Ihnen durchs Telefon: p = 19, g = 5 und A = 4
   a) Welches Verfahren kommt hier zum Einsatz?
      - Diffie-Hellmann

b) Welche Antwort müssen Sie zurückschicken und auf welchen Key haben Sie sich geeinigt?

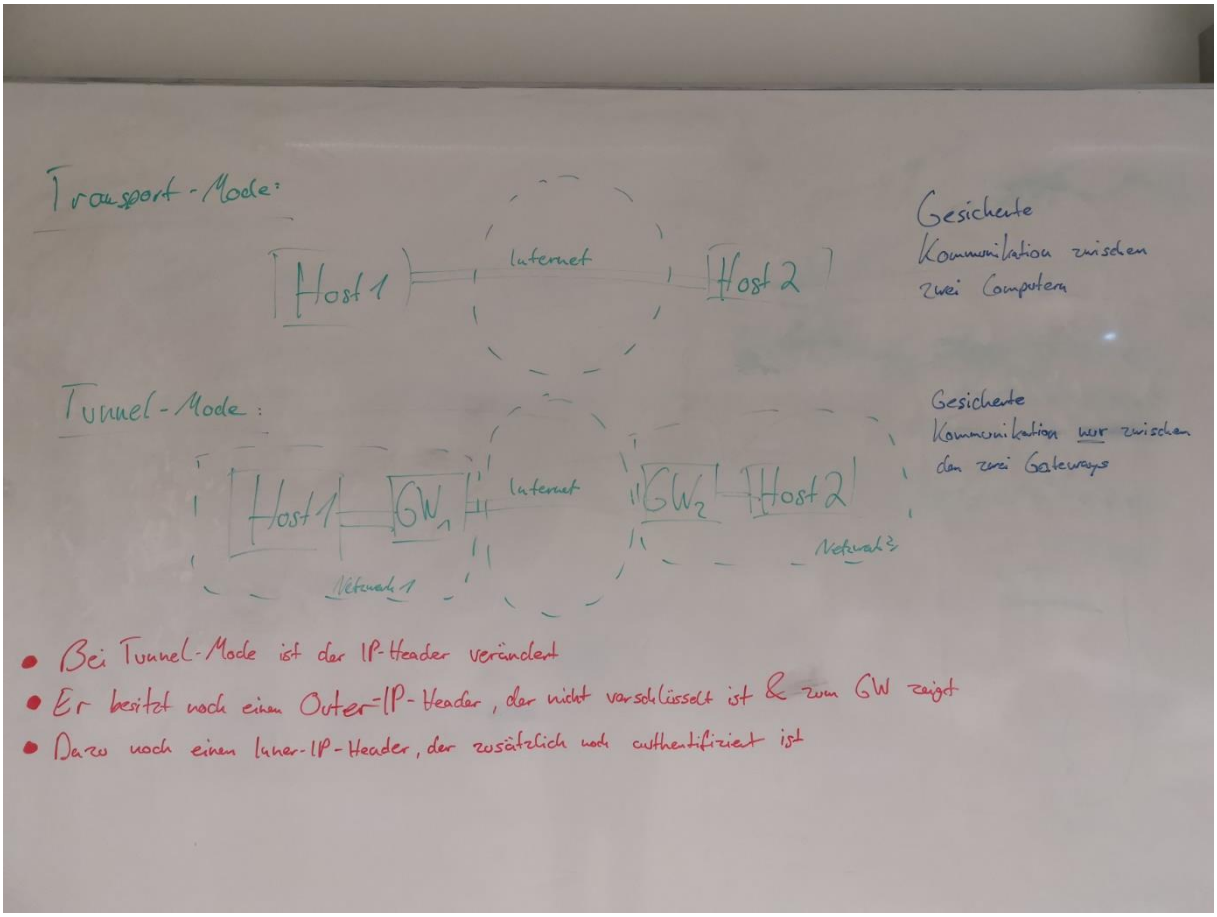


c) Warum ist es wichtig, dass Sie Snowden an seiner Stimme erkennen?
- Sonst gäbe es das Problem ‚Man in the Middle'
- Dieser würde für Snowden und mich einen eigenen Schlüssel berechnen und das Medium dazwischen sein
- Somit kann er alle Nachrichten verfolgen

d) Wie kann man Snowden erkennen, wenn nur über Datenaustausch kommuniziert werden kann (nicht mündlich)?
- Durch Zertifikate
- Er verschlüsselt seine Nachricht mit seinem PrivateKey und ich entschlüssele es mit seinem PublicKey
- So bin ich mir sicher, dass dies Snowden ist
- (FS4, S18)

9. In den letzten zwei Jahren vermehrten sich die Angriffe auf Root-CAs. Welche Gefahr entsteht hierbei für eine Trusted Computing Plattform, wenn diese Angriffe erfolgreich sind.
- Der Angreifer kann Zertifikate von der Plattform ausstellen
- Somit sind die Zertifikate nicht mehr vertrauenswürdig

10. IPSec: Zeichnen Sie eine Skizze, in der der Unterschied zwischen Tunnel-Mode und Transport-Mode klar werden. Zeigen Sie jeweils einen Anwendungsfall. Bei einem dieser Beiden Verfahren ist Der IP-Header verändert (aufgeteilt). Beschreiben Sie bei welchem. Warum ist dies so?



11. Fiat-Feige-Shamir: Der Lizenzserver besitzt folgende Informationen: N = 77, s1 = 5, s2 = 15, s3 = 31
    a) Sie haben die Möglichkeit 8x 128 bit, 4x 256 bit oder 1x 1024 bit Schlüsselzahlen zu verwenden. Für welche Option entscheiden Sie sich und warum?
        - 8 x 128bit, da man so das FFS öfter ausführt und die Wahrscheinlichkeit auf den Schlüssen zu kommen kleiner ist

    b) Welche Informationen müssen Sie vor Beginn der Authentifizierung an den Lizenzserver übertragen?
        - N
        - v1 = 5^2 % 77 = 25
        - v2 = 15^2 % 77 = 71
        - v3 = 31^2 % 77 = 37

12. An Ihrer Haustür hängt ein Text: NHMMFGJIJNSJKWFZLJKNHPY
    Sie erkennen sofort, dass es sich hier um den Cäsar-Code handeln muss, welcher leicht zu knacken ist.
    a) Wie kann der Cäsar-Code geknackt werden?
        - Durch die relative Häufigkeit des Deutschen Alphabetes
        - Dort ist der meiste Buchstabe das ‚e‘

b) Berechnen Sie den Schlüssel und wie lautet die wichtige Nachricht?
   - ‚IchHabeDeineFrauGefickt'

13. Die Client-Firewall gilt als unsicher.
    a) Erklären Sie warum eine Client-Firewall trotzdem von jedem Experten empfohlen wird.
       - Weil die Standartkonfiguration schon gut genug für den normalen Nutzer ist
       - Lieber eine schlechte Firewall haben, als garkeine

    b) Nennen Sie Vor- und Nachteile was gegen diese Aussage spricht.
       - Vorteile:
         - Skalierbar
         - Anwendungsnah
         - Ausbreitung von Viren kann an der Quelle bekämpft werden

       - Nachteil:
         - Kein 100%er Schutz
         - Unkenntnis der Nutzer
         - Ohne klar definierte Sicherheitskonzepte oft untauglich

14. Spoofing
    a) Erklären Sie was Spoofing ist?
       - Das klauen einer Identität
       - Ausgabe als diese Person, Gerät & Netzwerk

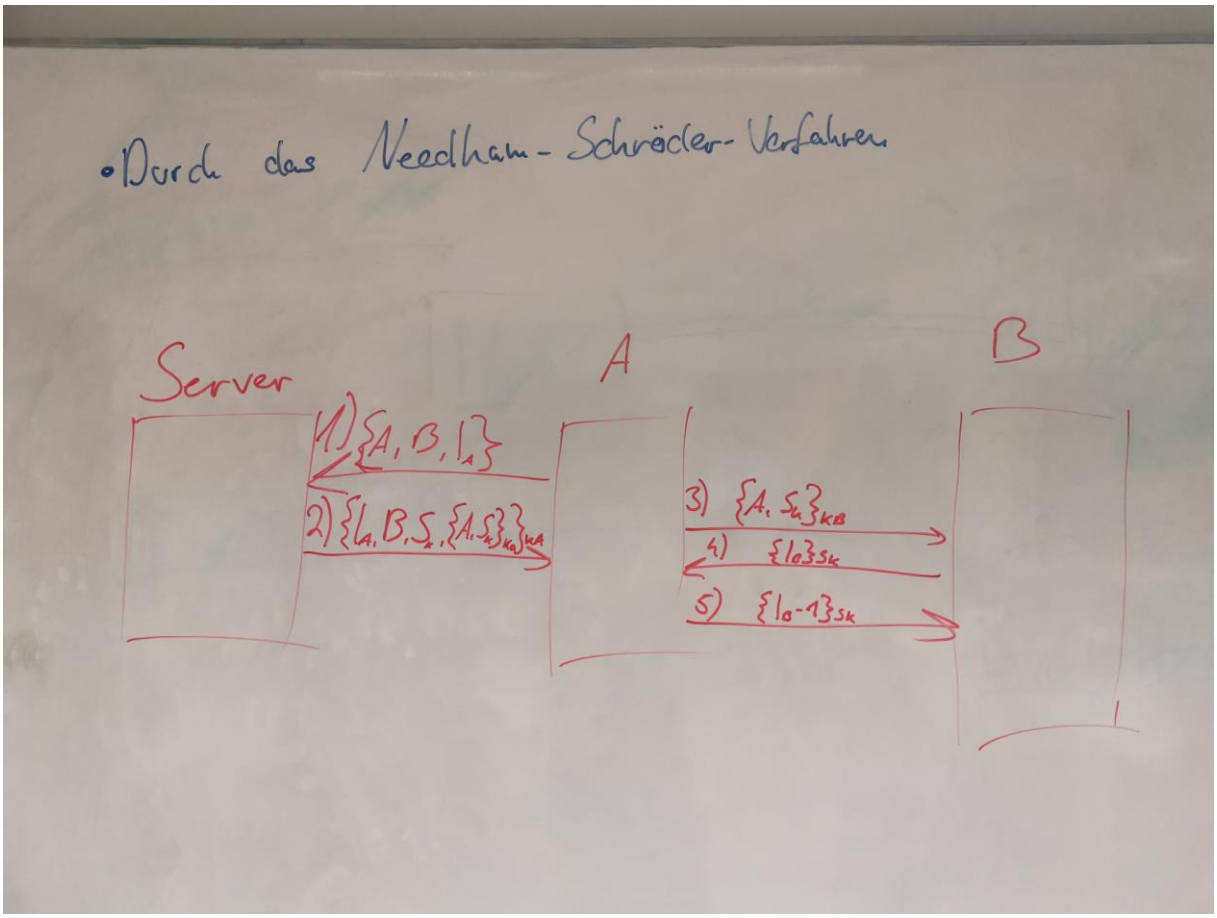
    b) Erklären Sie die Online Banking Spoofing Aufgabe, die Sie im Tutorium gemacht haben.
       - DNS-Spoofing
       - Wir haben die google.de Website geklont und mit dem Zugriff auf unseren DNS-Server wurde die geklonte Website aufgerufen

    c) Wie kann man sich gegen Spoofing schützen
       - Durch IPsec
       - Zertifikate
       - Nicht herunterladen von fremden Programmen
       - ARP Guards

15.
    a) Was versteht man unter einer Falltürfunktion
       - Eine Funktion die leicht in die eine Richtung geht, aber nur mit Zusatzinformation möglich ist, in die andere Richtung zu gehen
       - Ansonsten ist es sehr schwer, bis ganz unmöglich

    b) Warum sind diese bei der asymmetrischen Verschlüsselung so wichtig?
       - Damit man zB aus einem PublicKey nicht seinen PrivateKey errechnen kann

16. Sie treffen sich mit einem fremden Agenten, den Sie nicht kennen, wie stellen Sie sicher, dass ihr beide denselben Boss habt, der euch geschickt hat?



17. DNS – Spoofing
    a) Was ist DNS – Spoofing
        - Der DNS-Server leitet dich an eine andere abgeleitete Webseite weiter, die sich als diese Ausgibt, um zB dein Passwort zu bekommen

    b) Wie war DNS-Spoofing in der Übung
        - Wir haben die Google-Website geklont und durch den DNS-Server haben wir die Adresse von unserer geklonten Seite auf die von Google weitergeleitet

    c) Wie kann man sich gegen DNS-Spoofing wehren
        - Zertifikate
        - DNS over HTTPS

18. Internet vom Nachbarn ausgefallen, er hat nix gemacht. Welches Schutzziel wurde verletzt? Beschreiben sie wie dieses definiert ist. Wie schützt sich eine Firma in Bezug auf dieses Schutzziel?
    - Verfügbarkeit
    - Die Funktionalität wurde beeinträchtigt um ins Internet zu gehen
    - Die Dienste stehen nicht mehr zur Verfügung
    - Firmen schützen sich durch:

    - Backups
    - Firewalls um sich vor Angriffen zu schützen

19. MAC: Nennen Sie zwei Nachteile von MAC. Geben sie ein anderes Verfahren an und nennen sie die Vorteile gegenüber MAC
    - Skaliert schlecht
    - Access Level wird festgelegt und jedem User zugewiesen
    - Benötigt spezielle Dienste
    - RBAC
        - Skaliert gut
        - Einfacher Rechteentzug

20. Code mit strcpy und strcmp gegeben. Welches Risiko entsteht dadurch? Ist Non-Executable-Stack bei diesem konkreten Risiko sinnvoll? Wie kann das modifiziert werden?
    - BufferOverflow
    - Es werden die Länge der Eingaben nicht geprüft und somit kann das Programm abstürzen oder effektiv umgeleitet werden
21. Ja, da so kein Code im Stack ausgeführt werden kann und der Schadcode so hinfällig ist
22. Beschreiben Sie Syn-flood Angriffe. Ist eine Stateful-Inspection-Firewall bei solch einem Angriff hilfreich?
    - Wenn man einen Server mit Anfragen vollspamt, damit er Anfrage-Buffer voll wird und kein Anderer mehr darauf zugreifen kann (Dos-Angriff)
    - Ja ist sie, da wenn von einer IP zu viele offene Verbindungen stehen, sie keine neuen mehr von derselben IP annimmt

23. Beschreiben Sie den Unterschied von Viren und Trojaner. Beschreiben sie die Vorgehensweise eines Brückenkopftrojaners. Welche Merkmale hat der Trojaner aus der Übung mit „coolshell.exe“?
    - Trojaner verstecken sich als legitime Programme und laden den Schadcode nach einer bestimmten Zeit herunter
    - Viren sind der Schadcode und pflanzen sich in andere Programme ein
    - Sie verbreiten sich sehr schnell und nisten sich in Programme ein
    - Brückenkopftrojaner sind Trojaner ohne Schadcode, doch haben eine Backdoor wo sie ihren Schadcode im Nachhinein herunterladen
    - Wenn die Exe aufgerufen worden ist, wurde ein neues Bild in den Ordner „Pictures“ erstellt
    - Hat man den HexCode des Bildes in Base64 Decodiert, kam als Ergebnis „You got hacked dude“

24. Welche Möglichkeiten der Authentifizierung kennen Sie?
    - Needham-Schröder
    - Feige-Fiat-Schamir

25. Nennen Sie alle 6 Schutzziele der Informationssicherheit und erklären Sie deren Bedeutung.
    - Integrität
    - Vertraulichkeit
    - Verfügbarkeit

- Verbindlichkeit
- Authentizität
- Privatheit

26. Erläutern Sie die Unterschiede zwischen statischer und dynamischer Aufgabentrennung in einem rollenbasierten Sicherheitsmodell anhand der hypothetischen Rollen: Finanzbuchalter, Gehaltsempfänger und Unternehmensprüfer.
    - Statisch
        - Man darf nur eine Rolle maximal haben
    - Dynamisch
        - Man darf mehrere Rollen besitzen, aber sich nur maximal in einer aufhalten

27. Aktuelle C Compiler besitzen eine Option, welche im Stack abgelegte Daten nicht ausführbar macht. Welchen Sicherheitsgewinn verspricht man sich von dieser Maßnahme?
    - Non-Executable-Bit
    - Keine BufferOverflow wo Schadcode abgelegt werden kann, der ausgeführt wird
28. Weshalb ist es gefährlich Forenbeiträge von Benutzern nicht auf JavaScript Tags zu filtern? Erläutern Sie die Gefahr anhand eines hypothetischen Stored XSS Angriffs.
    - Sonst wird Schadcode ausgeführt, der zu schlimmen Problemen führen kann
    - Stored XSS wird auf einer Seite versteckt und dann ausgeführt, wenn die Seite geöffnet wird
    - So kann der User nicht wissen, dass was passiert und sich dagegen auch nicht wehren

29. Erläutern Sie die Begriffe Universalität und Beständigkeit für biometrische Merkmale sowie mögliche Probleme, falls diese nicht gegeben sind.
    - Universalität: Jeder Mensch besitzt es
    - Beständigkeit: Es ändert sich auf die Dauer nicht, bis nur kaum
    - Wenn dies nicht gegeben ist, ist es schwer zu erfassen ob es sich um diese Person handelt
    - Manche Menschen besitzt Sachen nicht, durch Behinderungen, Unfälle, usw.

30. Wo werden unter Windows 7 Security Descriptoren abgelegt und welche Informationen enthalten diese?
    - Es liegt direkt an der Datei

31. Obwohl zwei Rechner durch IPSEC miteinander sprechen, kann man beim mitsniffen der Verbindung erkennen, dass einer der beiden, Daten vom Webserver des anderen, abruft. Wie kann das sein und wieso ist dies nicht zwangsläufig ein Sicherheitsproblem?
    - Dies geschieht durch den Tunnel-Mode
    - Es ist kein Problem, da diese Information fürs Routing gebraucht wird

32. Was ist die Schwachstelle des PAP bzw CHAP? Warum ist das Needham-Schroeder-Protokoll besser?
    - Man in the Middle angriffe möglich

- Kein Authentifizierter dabei
- Needham-Schröder ist verschlüsselt und PAP/CHAP nicht

33. Was ist ein zero-Knowledge-Verfahren? Nennt eines.
    - FFS – Feige Fiat Schamir

34. Was ist eine Firewall?
    - Eine Sicherheitsmaßname die böse Nachrichten blockiert
    - Große Mauern, kleine Türen
    - Alles läuft durch den einen Eingang und wird kontrolliert

35. Welche Arten von Firewalls gibt es?
    - Client-Firewalls
    - Statefull Firewall
    - Application Level Firewalls
    - Hybride Firewalls
36. Was sind paketfilter?
    - Filterung von Datenpaketen nach:
        - Sender/Empfänger IP-Adresse
        - Ports
        - Protokollen
        - Physikalische Schnittstelle, auf der Pakete empfangen bzw. versendet werden
        - nach Paketgröße

37. Was ist Stateful Inspection?
    - Filterentscheidungen sind vom Zustand abhängig

38. Was ist Filtering Proxy?
    - Überprüft Zulässigkeit des Verbindungsaufbaus
    - Kann Verbindungen erstellen und abbrechen
    - Legt Zustandsinformationen an und verwaltet sie
    - Einfache Filterung (u.A. Logging)

39. Was ist Application Level gateway?
    - Anbieten von Anwendungs-spezifischen Proxy-Diensten
    - Proxis die auf spezielle Protokolle zugeschnitten sind

40. Was sind Personal Firewalls & Was sind die Vor- und Nachteile?
    - sind auf dem (eigenen) Computer installiert und sollen ihn gegen ungewollten Zugriff schützen
        - Einbruchsversuche
        - Viren
        - usw