Informationssicherheit Klausurfragen

1. Es wurden vor kurzen viele Millionen Emailkonten gehackt. Welche Schutzziele sind durch diesen Emailhack bedroht (3 Stück)?

2. a) Nennen Sie zwei Regeln des Bella-Lapadula Modells?

   b) Welcher dieser Regeln steht im Widerspruch zu einem hirachischen rollenbasierten Modell?

3. Jemand ist auf die Adminstrationsoberfläche eines Routers eingeloggt und surft im gleichen Browser.
   a) Welches Risiko ergibt sich daraus?

   b) Erläutern Sie, anhand eines Beispiels, den Unterschied zwischen Reflected XSS und Stored XSS.

4. Fia-Feige-Schamir Verfahren: Es sind gegeben: N, s1, s2 und s3
   a) Welche Informationen müssen an den Lizenzierungsserver weitergeleitet werden.

   b) Welche weiteren Nummern werden benötigt um ein vollständiges Feige Fiat Schamir Verfahren durchzuführen?

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

   a) Address-Space-Layout-Randomization

   b) Canaries

   c) Non-Executable-Bit

6. SSL verwendet eine Kombination aus asymetrischen und symetrischen Verfahren.
   a) Warum wird dies so verwendet?

   b) Warum ist es wichtig einen guten Zufallsgenerator zu verwenden?

7. Snowden schreit durch das Telefon: p=19, g=5, A=4
   a) Welches Verfahren kommt hier zum Einsatz?

   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?

8. In den letzten Jahren vermehrten sich die Angriffe auf Root-Cas. Welche Gefahr entsteht hierbei für eine Trusted Computing Plattform wenn diese Angriffe erfolgreich sind?

9. IPSec: Zeichenen Sie eine Skizze in der der Unterschied zwischen Tunnel-Mode und Transport-Mode klar wird. Zeigen Sie jeweils einen Anwendungsfall. Wo wird der IPHeader geändert?

10. Fiat-Feige-Shamir: Der Lizenzserver besitzt folgende Informationen: N=77, s1=5, s2=15, s3=31
    a) Sie haben die Möglichkeit 8x128 bit, 4x 256 bit oder 1x 1024 bit Schüsselzahlen zu verwenden, Für welche Option entscheiden Sie sich und warum?

    b) Welche Informationen müssen Sie vor Beginn der Authentifizierung an den Lizenzserver übertragen?

11. Text gegeben: Cäsar Code
    a) Wie kann der Cäsar-Code geknackt werden?

    b) Berechnen Sie den Schlüssel

    c) Ersten Vier Worte

12. Die Client Firewall gilt als unsicher.
    a) Erklären Sie warum eine Client Firewall trotzdem von jedem Experten empfohlen wird

    b) Nennen Sie Vor- und Nachteile was gegen diese Aussage spricht.

13. Klassen zur Erhaltung der Schutzziele und Maßnahmen erklären.

14. Dynamische und Statische Rollenverteilung an Beispielen erklären.

15. SQL Injection skizzieren und erklären? (Was ist Best SQL Code)

16. Bufferoverflow erklären und beschreiben was rbp und rip machen?

17. Needham Schröder erlkären?

18. Access und Capability Listen an Beispiel von einem Betriebssystem erklären.

19. Zwei Klassen nennen die es bei Maßnahmen für die Erfüllung von Schutzzielen gibt und zu jeder genannten Klasse eine Maßnahme nennen.

20. Herr A will mit Herr B reden. Trifft Herr C der beide Schlüssel hat.
    a) Wie sicher ist der Austausch?

21. BufferOverflow Code gegeben.
    a) Welche Schwachstelle liegt vor?

    b) Wie konstruiert man so einen Angriff?

    c) Wie Ändern sich rdp und rip während des Angriffs?

22. Firewall:
    a) Was ist Synflooding?

    b) Was ist Stateful Filtering?

    c) Schützt Stateful Filtering vor einem Synflooding Angriff?