HOCHSCHULE AUGSBURG – FAKULTÄT FÜR INFORMATIK

IT-SICHERHEIT - TESTKLAUSUR

Testsemester XXXX – XX.XX.XXXX – XX:XX

Prüfer:	Prof. Dr. Dominik Merli, Prof. Dr. Lothar Braun
Prüfungsdauer:	90 Minuten
Erlaubte Hilfsmittel:	keine

Hinweise:

- Tragen Sie auf allen Seiten Ihren Name und Ihre Matrikel-Nr. ein.
- Überprüfen Sie, ob Ihnen alle Seiten vorliegen.
- Bearbeiten Sie die Aufgaben auf den Aufgabenblättern.
  Benutzen Sie ggf. auch die Rückseiten der Aufgabenblätter.
- Verwenden Sie zum Schreiben keinen Bleistift und keine rote Farbe.
- Falls eine Aufgabe Ihrer Meinung nach unvollständig oder mehrdeutig ist,
  treffen Sie eine geeignete Annahme und dokumentieren Sie diese.

AUFGABE 1: NETZWERKSICHERHEIT

a) Nennen Sie die ausgeschriebene Version von IDS und IPS und erklären diese Begriffe. (4 Punkte)

b) Erklären Sie was passiert, wenn Sie den Befehl `nmap -p 22 203.0.113.254` auf einer Linux Konsole ausführen. (2 Punkte)

c) Erklären Sie, was ein Paketfilter und eine Layer 7 Firewall sind und wodurch sie sich unterscheiden. (6 Punkte)

d) Erklären Sie wie ein Ping Flooding Angriff abläuft, welche Auswirkung er hat und welches Protokoll dabei genutzt wird. Nennen Sie eine Schutzmaßnahme, die Pings aber nicht komplett blockiert. (4 Punkte)

e) Nennen Sie zwei Maßnahmen zur virtuellen Segmentierung eines Netzwerks und zwei weitere zum Schutz des Netzwerkzugangs auf Layer 1. (4 Punkte)

AUFGABE 2: BEDROHUNGS- UND RISIKOANALYSE

a) Nennen Sie das jeweilige Schutzziel, das in den folgenden Beispielen betroffen ist und erklären Sie seine Bedeutung. (8 Punkte)

Beispiel 1: Bei einem Man-in-the-Middle Angriff verändert der Angreifer die Netzwerkpakete in einer Kommunikation.

Beispiel 2: Durch Brute-Forcing konnte das Passwort einer passwort-geschützten Datei ermittelt und deren Inhalt gelesen werden.

Beispiel 3: Nach einem Denial-of-Service Angriff ist ein Web-Server nicht mehr erreichbar.

Beispiel 4: Ein Mitarbeiter in der Buchhaltung wird per E-Mail vom Geschäftsführer aufgefordert eine bestimmte Rechnung auf das in der E-Mail angegebene Konto zu überweisen. Später stellt sich heraus, dass die E-Mail nicht vom Geschäftsführer sondern von einem Angreifer stammte.

b) Stellen Sie sich vor, Sie sind Experte für industrielle Sicherheit und müssen eine Bedrohungs- und Risikoanalyse für ein neues Industrie-Gerät, das Ihr Unternehmen herstellt. Das Gerät erfasst den pH-Wert einer Säure in einer Prozessanlage. Der Wert wird per Netzwerk an andere Maschinen im selben Prozessnetzwerk und an einen Datenbank-Server geschickt. Die Korrektheit des pH-Werts ist kritisch für die Produktqualität und Safety-Maßnahmen in der Anlage. Der Zugang zum Web-Interface ist durch das im Handbuch abgedruckte Passwort `xHww8!n6JK#23` geschützt. Dort können Kalibrierungswerte für den Sensor eingestellt werden. Es ist davon auszugehen, dass im späteren Einsatz verschiedene Drittfirmen Zutritt zu den Industrieanlagen haben, in denen das Gerät eingesetzt werden soll. Bisher sind außer dem Passwortschutz keinerlei Sicherheitsmaßnahmen geplant. Füllen Sie die folgenden Teilbereiche einer Bedrohungs- und Risikoanalyse aus.

Nennen Sie vier Personen(gruppen), die als Angreifer in Frage kommen, und deren Motivationfür einen Angriff (4 Punkte):

Nennen Sie zwei Assets und die dazugehörigen Schutzziele (4 Punkte):

Beschreiben Sie zwei mögliche Bedrohungsszenarien (4 Punkte):

AUFGABE 3: KRYPTOGRAPHIE

a) Nennen Sie den jeweiligen Netzwerk-Typ, der als Basis für die Algorithmen DES und AES verwendet wird. (2 Punkte)

b) Erklären Sie, warum Triple DES entwickelt wurde und seine grobe Funktionsweise im Vergleich zu DES. Nennen Sie zusätzlich die verwendete Schlüssellänge und die aktuelle Einschätzung des dadurch erreichbaren Sicherheitsniveaus. (6 Punkte)

c) Erklären Sie zwei wichtige Unterschiede zwischen dem Cipher Block Chaining Modus (CBC) und dem Counter Modus (CTR). (4 Punkte)

d) Beurteilen Sie die folgenden Aussagen mit RICHTIG oder FALSCH und begründen Sie kurz Ihre Antwort. Antworten ohne Begründung werden nicht berücksichtigt. (8 Punkte)

Aussage 1: Digitale Signaturen auf Basis von RSA schützen die Integrität und Vertraulichkeit einer Nachricht.

Aussage 2: Das Sicherheitsniveau von RSA-Signaturen mit 4096-bit Schlüsseln ist höher als das Sicherheitsniveau von ECDSA-Signaturen mit 224-bit Schlüssel.

Aussage 3: Die Signatur-Verifikation mit RSA ist schneller als die Verifikation mit ECDSA.

Aussage 4: Die Sicherheit von RSA kann mit einem großen universellen Quantencomputer gebrochen werden. ECDSA ist hingegen eine zukunftssichere Alternative auch wenn Quantencomputer verfügbar sind.

AUFGABE 4: TYPISCHE ANGRIFFE

a) Erklären Sie den Begriff *Ransomware*. (3 Punkte)

b) Erklären Sie kurz wie Seitenkanalangriffe funktionieren und nennen Sie drei physikalische Eigenschaften, die als Basis für einen solchen Angriff dienen können. (5 Punkte)

c) Erklären Sie anhand eines Beispiels, wie ein Phishing-Angriff funktioniert und welches Ziel die Angreifer dabei verfolgen. (4 Punkte)

d) Beurteilen Sie die folgenden Aussagen über Angriffe auf IT-Systeme mit RICHTIG oder FALSCH und begründen Sie kurz Ihre Antwort. Antworten ohne Begründung werden nicht berücksichtigt. (8 Punkte)

Aussage 1: Reverse Engineering von Produkten ist oft zeitaufwändige Handarbeit.

Aussage 2: Industrie-Geräte müssen nicht gegen Angriffe durch Skript-Kiddies geschützt werden, da Kinder diese Geräte nicht erwerben können.

Aussage 3: Man-in-the-Middle Angriffe gehen immer mit einer Manipulation der belauschten Daten einher.

Aussage 4: Beim Passwort-Brute-Forcing wird versucht ein Passwort durch geschicktes und automatisiertes Ausprobieren zu erraten.

AUFGABE 5: SCHLÜSSELVERWALTUNG

a) Ein Key Distribution Center (KDC) ermöglicht Schlüsselverwaltung ohne asymmetrische Kryptographie. Erklären Sie was ein KDC ist und wie Bob und Alice es nutzen können, um sicher miteinander kommunizieren zu können. (7 Punkte)

b) Nennen Sie drei Nachteile der Schlüsselverwaltung mit Hilfe eines KDC. (3 Punkte)

c) Nennen Sie die drei Mindest-Bestandteile eines Zertifikats und die beiden Schutzziele, die dadurch erreicht werden. (5 Punkte)

d) Nennen Sie drei Fälle, in denen ein Zertifikat revoziert werden muss. Erklären Sie zusätzlich was CRL in diesem Kontext bedeutet. (5 Punkte)