
Bitte hier unbedingt Matrikelnummer und Adresse eintragen, sonst keine Bearbeitung möglich.

Postanschrift: FernUniversität, D-58084 Hagen

Name, Vorname

Straße, Nr.

PLZ, Wohnort

FERNUNIVERSITÄT
in Hagen
EINGANG

INF

FERNUNIVERSITÄT
in Hagen
D-58084 Hagen

Fachbereich Informatik

Kurs: 1867 „Sicherheit im Internet II“

Hauptklausur am 19.02.2005

Hörerstatus:

- ☐ Vollzeitstudent
- ☐ Teilzeitstudent
- ☐ Zweithörer
- ☐ Gasthörer
- ☐ Bachelor
- ☐ Lehramt
- ☐ . . . . . .

Klausurort:

- ☐ Berlin
- ☐ Bochum
- ☐ Frankfurt
- ☐ Hamburg
- ☐ Karlsruhe
- ☐ Köln
- ☐ München
- ☐ Bregenz
- ☐ Wien
- ☐ . . . . . .

Zutreffendes unbedingt ankreuzen !

Aufgabe	1	2	3	4	5	6	Summe
erreichbare Punktzahl	20	10	20	8	20	22	100
bearbeitet							
erreichte Punktzahl							

Note: _____

Hagen, den _____ Betreuer: _____

Hinweise zur Hauptklausur des Kurses 01867 am 19.02.2005

- Die Klausurdauer beträgt: drei Stunden (10.00 bis 13.00 Uhr)
- **Es sind keine Hilfsmittel erlaubt.**
- Legen Sie Ihren Studenten- und Personalausweis zur Überprüfung durch die Aufsicht bereit.
- Füllen Sie vor Beginn der Klausur unbedingt das Deckblatt aus - und zwar in leserlicher Druckschrift.
- Füllen Sie bitte vor Inangriffnahme der Klausuraufgaben die Bescheinigung und den/das Leistungsnachweis/Zertifikat leserlich aus (natürlich bis auf die Note und Unterschrift). **Andernfalls wird kein Leistungsnachweis erstellt.**
- Die Bescheinigung für das Finanzamt ist nur mit Unterschrift und Stempel gültig. Nur vollständig ausgefüllte Bescheinigungen werden von uns abgestempelt, unterschrieben und Ihnen zugestellt.
- Überprüfen Sie die Vollständigkeit der Aufgabenstellungen! Die Klausur umfasst insgesamt 9 Seiten mit 6 Aufgaben.
- Schreiben Sie auf alle Lösungsbögen Ihren Namen und Ihre Matrikelnummer !
- Tragen Sie Ihre Lösungen in die dafür vorgegebenen Felder ein. Falls Sie damit nicht auskommen, benutzen Sie bitte die Rückseite der vorhergehenden Aufgabe. Verweisen Sie in diesem Fall darauf, dass diese Rückseite beschrieben ist.
- Bei Abgabe Ihrer Arbeit heften Sie bitte die ersten Seiten des übergebenen Klausurexemplares (Deckblatt, Bescheinigungen und Hinweise zur Klausur) vor Ihre Lösungsblätter. Kontrollieren Sie zum Schluss, dass Sie Ihre gesamte Arbeit geheftet abgeben. Nachträglich eingereichte Lösungen werden von uns nicht akzeptiert.
- Die zum Bestehen der Klausur erforderliche Punktzahl liegt noch nicht fest. Sie wird erst aus der tatsächlich erreichten Punkteverteilung ermittelt, liegt aber sicher nicht über 50% bzw. unter 30% der erreichbaren Punkte.
- Die Korrektur der Klausur wird voraussichtlich bis Mitte März 2005 erfolgt sein. Wir bitten, von vorzeitigen Nachfragen abzusehen.

Bei der Bearbeitung der Klausur wünschen wir Ihnen viel Erfolg!

Ihre Kursbetreuer

Aufgabe 1 (20 Punkte):

a) Beschreiben Sie den *Quadratic Sieve* Algorithmus. (10 Punkte)

b) Führen Sie die Faktorisierung der Zahl $n = 91$ mittels des Quadratic Sieve Algorithmus durch. (10 Punkte)

Aufgabe 2 (10 Punkte):

Beschreiben Sie die Schritte, die ein Kunde beim Kauf eines Artikels per Internet unter Nutzung des Paybox-Bezahlverfahrens ausführen muss.

Aufgabe 3 (20 Punkte):

a) Nennen Sie die Arten von Intrusion Detection Systemen (IDS), die im Kurs unterschieden werden? (5 Punkte)

b) Welche Art IDS erkennt in der Regel nicht einen Angriff an sich, sondern nur seine Auswirkungen? Erläutern Sie kurz Ihre Antwort. (3 Punkte)

c) Ein Network-based IDS hängt an einem Netzwerklink mit der Bandbreite 80 MBit/s (1 M = 10^6) und protokolliert von jedem IP-Paket die source address sowie die destination address (je 4 Byte). Alle IP-Pakete seien 80 Byte groß. Wieviele IP-Pakete pro Sekunde kann das IDS protokollieren, wenn die Bandbreite zur Protokoll-Festplatte 1 MByte/s beträgt? Wie hoch ist dann die prozentuale Auslastung des Netzwerklinks? Begründen Sie Ihre Antworten. (12 Punkte)

Aufgabe 4 (8 Punkte):

a) Nennen Sie die im System– bzw. Software-Entwurf üblichen Phasen. (5 Punkte)

b) In welcher Phase muss entschieden werden, ob ein System nur mit einer PIN zu Beginn der Sitzung oder mit PIN und TANs arbeitet, wobei bei jeder Transaktion eine TAN eingegeben werden muss. (3 Punkte)

Aufgabe 5 (20 Punkte):

a) Beschreiben Sie kurz die Technik des Tunneling. (6 Punkte)

b) Wird beim Einsatz von Encapsulation Security Payload (ESP) ein symmetrisches oder ein asymmetrisches Verschlüsselungsverfahren benutzt? Welche Möglichkeiten bestehen zum Schlüsseltausch? Bitte erläutern Sie die Durchführung bei den verschiedenen Möglichkeiten. (14 Punkte)

Aufgabe 6 (22 Punkte):

a) Was versteht man unter URL Hacking? Wozu wird URL Hacking außer zum Ausspähen von Passwörtern noch benutzt? (8 Punkte)

b) Wie kann man im folgenden Programm einen Buffer-Overflow Angriff ausführen? (14 Punkte)

```
#include <stdio.h>

int main(int argc,char *argv[])
{ char strng1[8] = "TestWd\0"; /* Gespeichertes Passwort */
  char strng2[8];

  printf("Passwort eingeben!\n");
  gets(strng2);

  if(strncmp(strng1,strng2,8)){
    printf("Falsches Passwort!\n"); exit(-1);
  }else application();

  return 0;
}
```