

Internet Security

Prüfung am 23.1.2003

Kennzahl

Matrikelnummer

Name

- Bitte füllen Sie die Angaben mit dokumentenechtem Schreibmaterial aus.
- Es sind keine Unterlagen erlaubt.
- Die Arbeitszeit beträgt 90 Minuten.

1. Geben Sie die grundlegenden Methoden an, um eine Attacke durchzuführen. Nennen sie für jede Methode ein Beispiel.

[5 Punkte]

1.

2.

3.

4.

5.

2. Stellen sie den TCP/IP Protokollstack dem OSI-Reference Modells graphisch gegenüber. Geben sie für die TCP/IP Layers auch die entsprechenden Protokolle an. Nennen Sie auch jene Schichten des OSI Reference Modells, die bei TCP/IP nicht implementiert sind.

[10 Punkte]

3. Nennen sie die drei Aufgaben des Transport Layers im OSI Reference Modell.
[3 Punkte]

1.

2.

3.

4. Wofür ist *IP Fragmentierung* notwendig? Wo wird es durchgeführt? Wo findet *Reassembling* statt? Welche Datenfelder des IP Protokolls werden dafür benötigt, und was ist die Aufgabe jedes Feldes?
[7 Punkte]

Datenfelder:

5. Nennen Sie zwei Attacken, welche IP Datagram Fragmentierung benutzen und erklären Sie sie kurz.
[2 Punkte]

6. Vergleichen sie die beiden Routingprotokolle RIP und OSPF.
[5 Punkte]

RIP

OSPF



7. Was ist OS Fingerprinting und warum kann es für einen Angreifer nützlich sein? Nennen sie typische Scans und deren Erkennungsmerkmale.
[5 Punkte]

8. Wie funktioniert TCP Hijacking? Beschreiben sie die Voraussetzungen und den Vorgang. Warum kommt es dabei zu ACK-Storms und wie können diese verhindert werden?
[8 Punkte]

9. Was ist DNS, wie ist der *namespace* organisiert und welche Protokolle werden dafür eingesetzt? Welche DNS-Servertypen gibt es?
[7 Punkte]

10. Warum ist NIS nicht sicher (worauf basiert es)? Nennen sie mindestens drei Gründe dafür.
[3 Punkte]
 - 1
 - 2
 - 3

11. Erklären den Vorgang der Unix-Passwort Authentifizierung im Detail – welche Rolle hat insbesondere das 12-bit *salt*?
[7 Punkte]
12. Was sind Stack/Buffer Overflows? Erklären sie die Vor- und Nachteile dieser Attacke. Skizzieren Sie den Aufbau des Stacks und erklären Sie was beim Buffer Overflow genau passiert.
[12 Punkte]
13. Welche Stack Overflow Schutzmechanismen gibt es? Nennen sie vier Möglichkeiten.
[4 Punkte]
- 1
 - 2
 - 3
 - 4