Vienna University of Technology
Department of Software Technology
and Interactive Systems (IFS)

Mag. Dipl.-Ing. Dr. techn. Edgar Weippl
Dipl.-Ing. Mag. Andreas Tomek

TU WIEN

188.337 VU 2.0 Practical Aspects of IT-Security

2. Termin: 2006-03-13

Nachname					
Vorname					
Matrikelnummer		Studienkennzahl		Punkte		Note	

Füllen Sie die obigen Felder aus (Name, Matrikelnummer) und geben Sie die Studienkennzahl der Studienrichtung an, für die Sie diese Prüfung ausgestellt haben wollen. Mit den Fragen auf den nächsten drei Seiten gibt gesamt 40 Punkte zu erreichen.

Viel Glück!

Hinweis: Ein Verlassen der Prüfung nachdem Sie die Angaben bekommen bzw. gesehen haben, ohne Abgabe der Ausarbeitung, wird als negativer Antritt gewertet (Hochschulstudiengesetz).

Wenn Sie Ihre Studienkennzahl auf diesem Bogen falsch angeben, kann kein Zeugnis ausgestellt werden.

1. Welche Phasen umfasst ein Penetrationstest? Was muss in der Planung und Durchführung besonders beachtet werden? Nennen Sie für jede Phase zumindest ein Tool! (5 Punkte)

2. Was ist 802.1x, wie funktioniert die Authentifizierung, welche Vorteile bietet es? Beschreiben Sie mind. 2 Abarten von EAP und deren Vor-/Nachteile! (4 Punkte)

3. Was ist ein Honeypot und welche Funktion hat er? Wie lassen sich Honeypots grob einteilen und klassifizieren? Was unterscheidet ein Honeynet davon? (4 Punkte)

4. Was ist Portknocking? Stellen Sie das Verfahren grafisch dar und beschreiben Sie es! Welche Probleme (mind. 5) haben die klassischen Port Knocking Verfahren? Wie versucht SIG^2 diese Probleme zu beheben? (5 Punkte)

5. Zeichnen Sie die wichtigsten Komponenten eines Standard IPS Systems und erklären Sie deren Funktionen! Wo liegen die Unterschiede zwischen einem IPS und einem IDS? (5 Punkte)

6. Vergleichen und nennen Sie zumindest 5 wesentliche Unterscheidungsmerkmale zwischen einem Hacker und einem Penetrationstester. Welche Arten von Penetrationstests gibt es? (3 Punkte)

7. Welche Analysis Schemes gibt es im Intrusion Analysis Process und wie funktionieren sie? (1 Punkte pro Scheme und Erklärung, max. 5 Punkte)

8. Wie kann TTL möglicherweise verwendet werden, um ein IDS zu täuschen (+ Grafik)? (3 Punkte)

9. Was ist ein Datenbank Rootkit und welche Problematik wirft es auf? Wie könnte ein solches unter Oracle aussehen? (3 Punkte)

10. Was ist bei der Anfertigung von Kopien von digitalem Beweismaterial zu beachten? (Art der Kopie) Zwischen welchen Arten von (forensischer) Reconstruction wird unterschieden? Charakterisieren Sie die verschiedenen Arten kurz. (3 Punkte)