Iterative Kompromittierungsgraphverfeinerung als methodische Grundlage für Netzwerkpenetrationstests

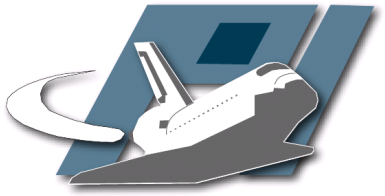
Felix C. Freiling – freiling@informatik.uni-mannheim.de
Universität Mannheim
Jens Liebchen – jens.liebchen@redteam-pentesting.de
RedTeam Pentesting GmbH

Sicherheit 2008, Saarbrücken, 4. April 2008

Über die Autoren

Felix C. Freiling

- ★ Universität Mannheim
- ★ Pi1 – Laboratory for Dependable Distributed Systems



Pi1 - Laboratory for Dependable Distributed Systems

Jens Liebchen

- ★ RedTeam Pentesting GmbH
- ★ Spezialisierung auf Penetrationstests

Über Penetrationstest

Penetrationstest

Ein *Penetrationstest* bezeichnet die Sicherheitsüberprüfung eines IT-Systems durch einen kontrollierten Angriff.

Arten von Penetrationstests

- ★ *Produktpenetrationstests*: Überprüfung eines (sicherheitsrelevanten) Produkts auf Schwachstellen
- ★ *Netzwerkpenetrationstests*: Kontrollierter Angriff auf ein Firmennetzwerk oder zumindest Teile davon

Über Penetrationstest

Penetrationstest

Ein *Penetrationstest* bezeichnet die Sicherheitsüberprüfung eines IT-Systems durch einen kontrollierten Angriff.

Arten von Penetrationstests

- ★ *Produktpenetrationstests*: Überprüfung eines (sicherheitsrelevanten) Produkts auf Schwachstellen
- ★ *Netzwerkpenetrationstests*: Kontrollierter Angriff auf ein Firmennetzwerk oder zumindest Teile davon

Schlüsselfaktoren bei Penetrationstests

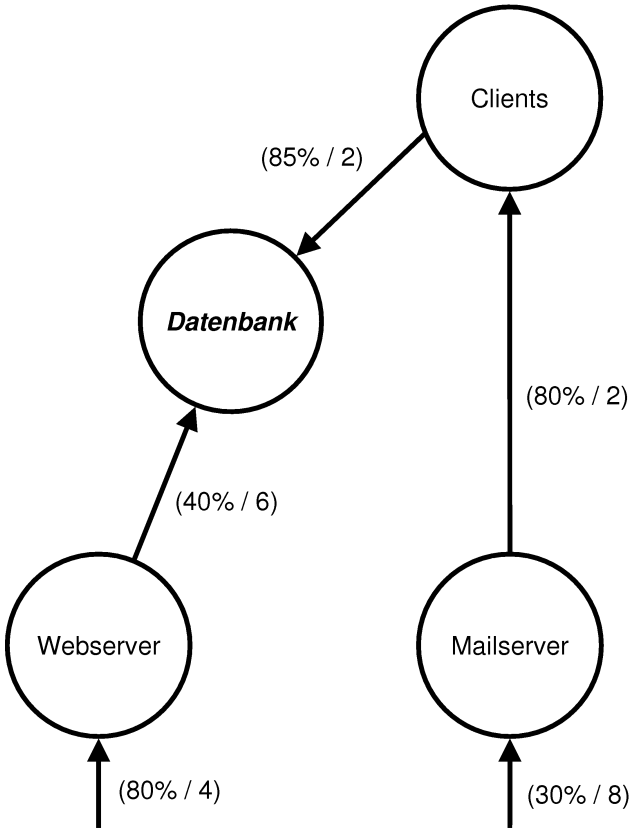
Eine wichtige Rolle für erfolgreiche Penetrationstests in der Praxis spielen:

- ★ Realistische Angreiferannahmen
- ★ Kreativität
- ★ Individualität eines Penetrationstests

Wissenschaftlicher Stand

- ★ BSI, NIST, OSSTMM, etc.
- ★ Literatur zu Angriffsvektoren sehr schnell veraltet und immer unvollständig
- ★ Kaum Informationen zur Dauer eines Penetrationstests
- ★ Problem: Keine Beauftragung eines Penetrationstests ohne definierte Kosten!

Kompromittierungsgraphen



Definition

$$G = (V, E) \quad \text{(Graph)}$$

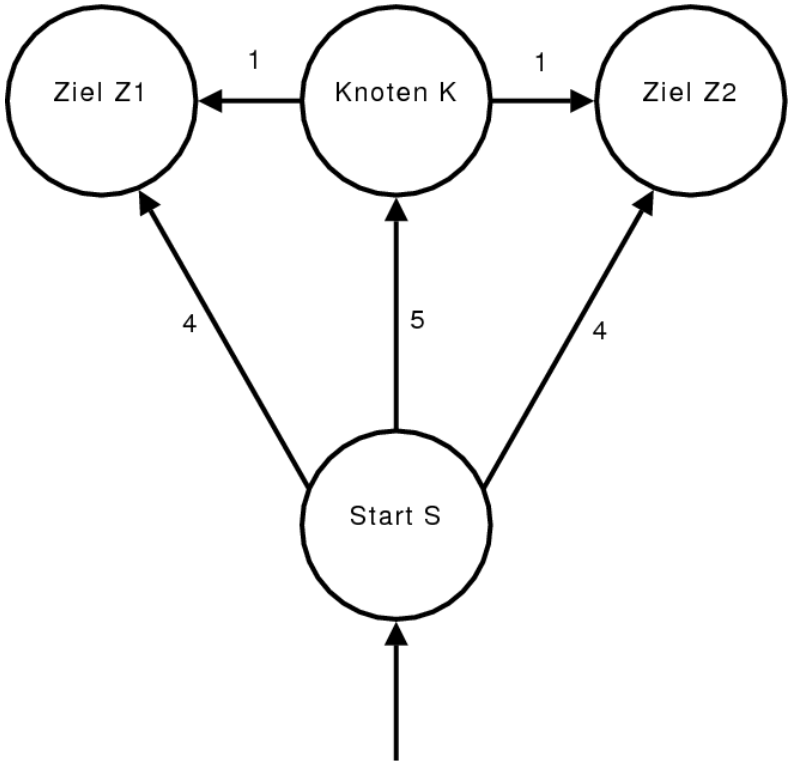
$$S \subseteq V \quad \text{(Startknoten)}$$

$$Z \subseteq V \quad \text{(Zielknoten)}$$

$$b : E \to \mathbb{R}^{>0} \times \mathbb{R}^{>0} \quad \text{(Bewertung)}$$

$$k(e) = \alpha \cdot \frac{t}{p} \quad \text{(Normierung)}$$

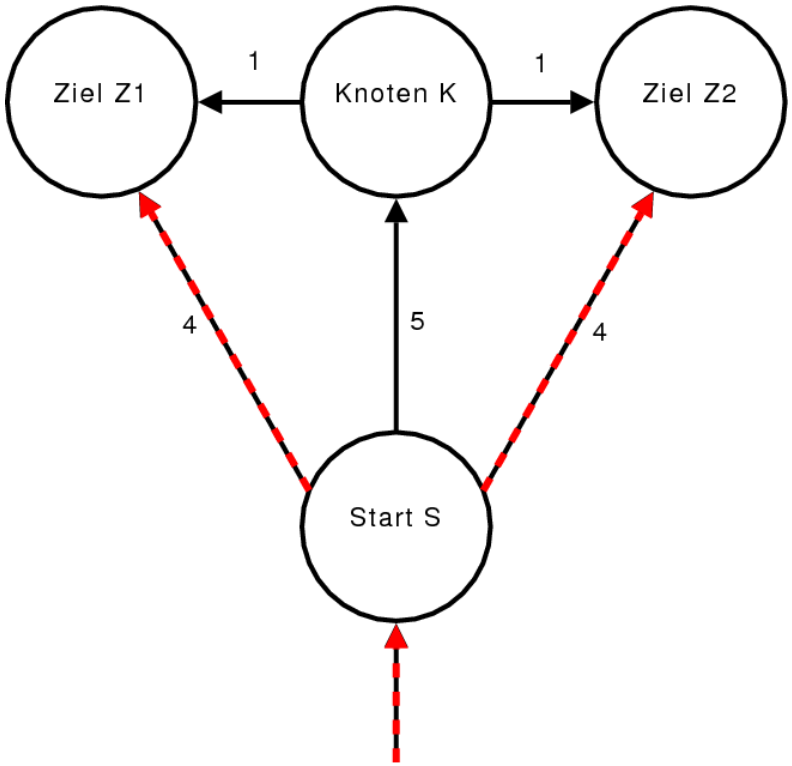
Kompromittierungspfade



Kompromittierungspfad

Ein *Kompromittierungspfad* in einem Kompromittierungsgraph $G = (V, E)$ ist ein Folge $v_1, v_2, \ldots, v_k$ von Knoten aus G so dass $v_1 \in S$, $v_k \in Z$ und für alle $0 < i \leq k$ gilt: $(v_{i-1}, v_i) \in E$.

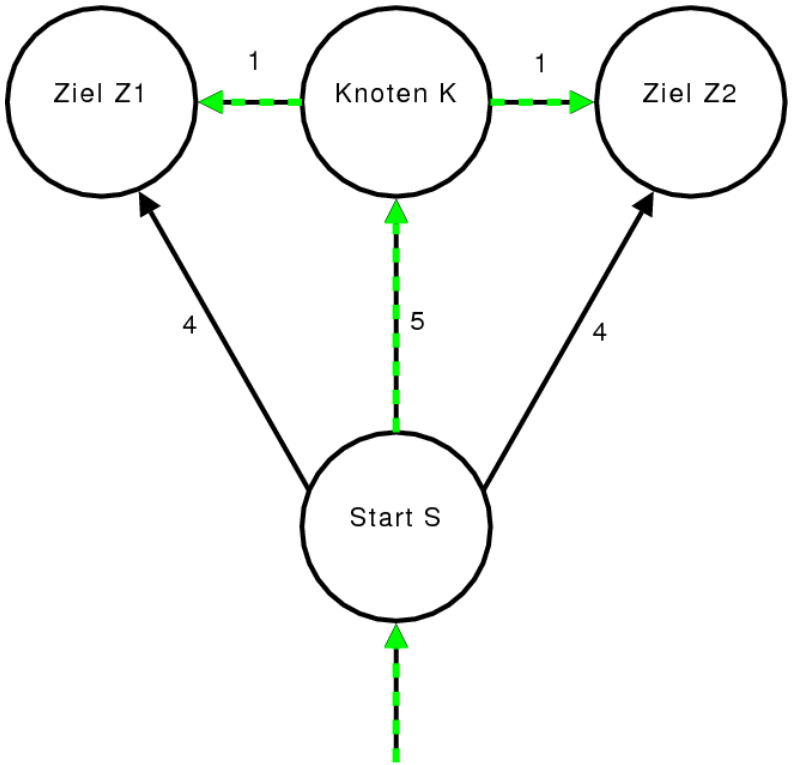
Kompromittierungspfade



Kosten:

Gesamtkosten für alle Zielsysteme: 8

Kompromittierungspfade



Kosten:

Gesamtkosten für alle Zielsysteme: **7**

Berechnungsaufwand

Die Berechnung der Kosten ist ein bekanntes Graphenproblem der Informatik, das *gerichtete Steinerbaumproblem*

- ★ Leider NP-schwer
- ★ Gute Approximationslösungen sind vorhanden
- ★ In der Praxis von Penetrationstests: Verhältnismäßig wenige Knoten und nur wenige Ziele (oft $|Z| = 1$), dann „leicht“ lösbar

Abschätzung einer sinnvollen Testdauer

Mit Hilfe der Kompromittierungspfade kann eine Testdauer nur auf Grund eines ersten Bildes des Netzwerks abgeschätzt werden.

- ★ Abschätzung vor eigentlicher Auftragsvergabe möglich
- ★ Genauigkeit steht und fällt mit den Erfahrungen der abschätzenden Pentester (insbesondere schwierig: Abschätzung der Kosten einzelner Teilpfade)

Kompromittierungspfade während des Pentests

Direktes Vorgehen anhand von Kompromittierungspfaden nicht sinnvoll. Besser:

- ★ Möglichst schnelle Tests vorziehen
- ★ Erst „überraschende“ Schwachstellen suchen
- ★ ⇒ Iterative Verfeinerung des Kompromittierungsgraphen
- ★ (Außer Start- und Zielknoten muss kein Zusammenhang zwischen zwei Iterationsstufen bestehen)

Kompromittierungspfade während des Pentests

Anpassung der Kostenfunktion zur Nutzung während des Penetrationstests:

Neue Kostenfunktion

$$kosten_z(E) = \alpha \cdot \frac{t}{p^z} \qquad \texttt{(Normierung)}$$

Vereinbare Ziele

- ★ Eine möglichst breite Sichtweise garantiert das Aufdecken von vielen verschiedenen Schwachstellen
- ★ Das Erreichen der vereinbarten Ziele garantiert die gewünschte Testtiefe

Diskussion

- ★ Zumindest ein erster Ansatz für Abschätzungen und Vorgehen bei Pentests
- ★ Abschätzungen bei Pentests sind erfahrungsabhängig
- ★ Auch Kompromittierungspfade lösen diese Abhängigkeit nicht
- ★ NDAs verhindern Analyse von echten Penetrationstests
- ★ Untersuchung der möglichen Evaluierung mit Hilfe von studentischen Praktika läuft $\Rightarrow$ Problem: Fehlende Erfahrung für Abschätzungen

Diskussion

Vielen Dank!