

Interner Angriff auf ein Netzwerk

**Vortrag und „vorgetäuschter“ Erfahrungsbericht einer
Netzwerkanalyse in einem beispielhaften Netzwerk ...**

**Gesellschaft für Informatik,
Regionalgruppe Dortmund,**

14. Februar 2005

Interner Angriff auf ein Netzwerk

Vortrag und „vorgetäuschter“ Erfahrungsbericht einer Netzwerkanalyse in einem beispielhaften Netzwerk ...

... und Diskussionsgrundlage.

Überblick

- Zum Problem des echtes Erfahrungsberichtes
- Die Werkzeuge:
 - Ablaschen
 - spezielles Ablaschen
 - Analyse
 - Kompromittieren
- Beispiele, Beispiele, Beispiele

Gewählte Beispiele

- SMTP-Dienst ablauschen
- Diebstahl einer beliebigen Datei beim „Runterladen“
- Was hat der Kollege gedruckt?
- Administratives auf unserem Switch
- Schutzeinrichtungen im Dienste der „dunklen Seite“
- gutes Beispiel der Verschlüsselung anhand der Standardanwendungen
 - WWW per https
 - Shellzugriff per ssh

Problem 1:
switched networks

Lösung 1:
ARP-Spoofing

Problem 2:
Verschlüsselung

Lösung 2:
**(statistische)
Gefahrenanalyse**

- Abhören - Vorteile:

- Keine Beeinflussung des Netzwerkes, da es sich um ein rein passives Verfahren handelt
- Ermöglicht die schnelle Erstellung einer Übersicht

- Abhören - Nachteile:

- Analysiert nur einen geringen Teil des Netzwerkverkehrs, da ein reines Abhören in Netzwerken mit Switching-Techniken nicht möglich ist.

- spezielles Abtauschen - Vorteile:

- Keine Beeinflussung des Netzwerkes, da es sich um ein rein passives Verfahren handelt
- Ermöglicht auch in Netzwerken mit reiner Switching-Technik die genaue Analyse eines Netzwerksegmentes
- Besonders für die Messung an einzelnen Servern geeignet

- spezielles Abtauschen - Nachteile:

- Der Anschluss des Analyserechners ist mit erhöhtem Aufwand verbunden, da erst ein „besonderer“ Anschlusspunkt gefunden und verbunden werden muss

- Analyse - Vorteile:

- **Gute Analyseergebnisse aus einer „normalen“ Büroumgebung, kein exponierter Serverstandort nötig**
- **Firewall-Einstellungen innerhalb des Netzwerkes können zum Teil verifiziert werden**
- **Gute Testmöglichkeit für bereits installierte Einbruchserkennungssysteme (IDS)**
- **Ungefährlich für ein robustes Netzwerk**

- Analyse - Nachteile:

- **Beinhaltet bereits verschiedene aktive Eingriffe in die Netzwerkübertragung, die unter ungünstigen Umständen die Funktionsfähigkeit beeinflussen können**

- Kompromittieren - Vorteile:

- **Ähnlich dem Verhalten eines typischen Angreifers auf das Netzwerk**
- **Gute Testmöglichkeit für bereits installierte Einbruchserkennungssysteme (IDS)**
- **Nach Absprache mit den Verantwortlichen ermöglicht diese Vorgehensweise die gezielte Untersuchung von besonders kritischen Systemen**

- Kompromittieren - Nachteile:

- **Beinhaltet aktive Eingriffe in die Netzwerkübertragung, die unter ungünstigen Umständen die Funktionsfähigkeit beeinflussen können**

dann folgte

Arbeit

und brachte folgende

Ergebnisse

Noch Fragen?

Markus Leist
leist@ikom-online.de

Ingenieurbüro IKOM
www.ikom-online.de
02151 / 9416-10

Vielen Dank für Ihre Aufmerksamkeit.

