

# Penetrationtests: Praxisnahe IT-Sicherheit

## Ihr Netzwerk aus der Angreiferperspektive

Jens Liebchen - RedTeam Pentesting GmbH
jens.liebchen@redteam-pentesting.de
http://www.redteam-pentesting.de

21. März 2007
Technologieforum Telekommunikation – IHK Aachen



# Februar 2007:

*„Verfassungsschutz: Spionage aus dem Reich der Mitte bedroht deutschen Mittelstand“ (heise online)*

*„Hacker nehmen IT-Lücken bei Firmen gezielt ins Visier“ (Financial Times Deutschland)*

*„Chinesen stehlen deutsches Know-how. Besonders mittelständische Unternehmen sind betroffen. Sie unterschätzen ihre Offenheit.“ (Hamburger Abendblatt)*

*„Hacker bedrohen verstärkt Betriebsgeheimnisse“ (Tagesschau)*

Und was ist mit Ihrem Unternehmen?

# Agenda

- Warum selbst ein Kopierer sicherheitsrelevant ist...

- RedTeam Pentesting
- Was sind Penetrationtests?
- Wie laufen Penetrationtests ab?
- Warum sind Penetrationtests gerade für KMUs sinnvoll?
- Typische Fehler aus Penetrationtests



# Über RedTeam Pentesting

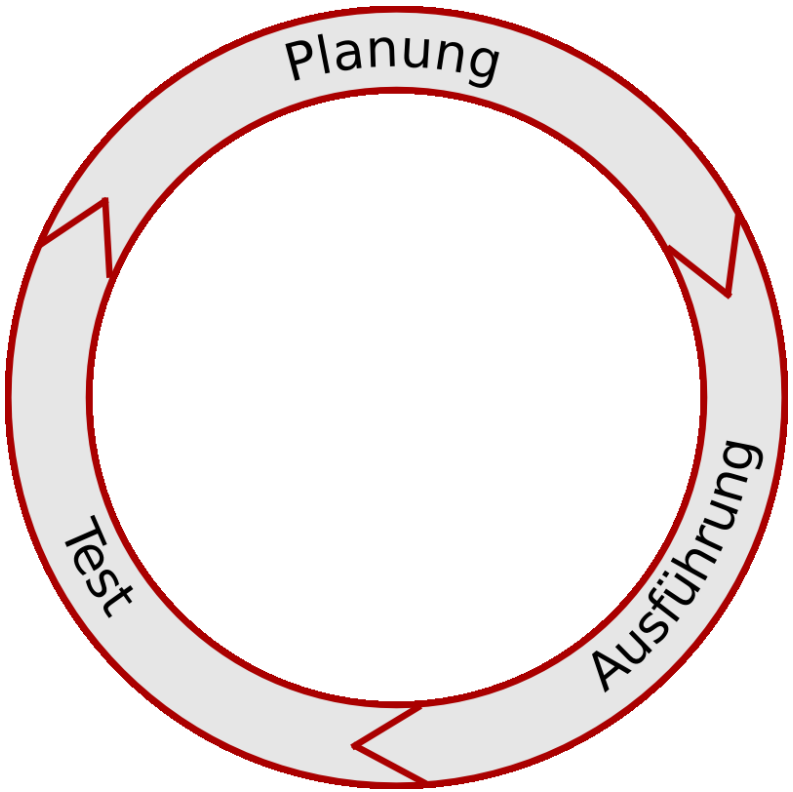
- ★ Über RedTeam Pentesting
- ★ Gründung 2004
- ★ Durchführung von Penetrationtests
- ★ Forschung im Bereich der IT-Sicherheit
- ★ Eine der wenigen auf Penetrationtests spezialisierten Firmen



# Was ist ein Pentest?

- ★ Angriff auf ein Netzwerk im Auftrag des Eigentümers
- ★ Fragestellung: Wie weit kann ein Angreifer eindringen?
- ★ Gleiche Methoden wie „die Bösen“
- ★ Vertraulichkeit (NDA)

# Motivation für die Durchführung eines Pentests





# Motivation für die Durchführung eines Pentests

- Wie sicher sind wir wirklich?
  - Realitätsnahe Überprüfung der eigenen Maßnahmen
  - Angst vor Industriespionage
  - Vorbeugung von „Betriebsblindheit“
  - Kontrollsystem vom Gesetz vorgeschrieben
- Indirekte Gründe
  - Werbung/Imagegewinn
  - Schutz der eigenen Kunden (netzwerkbasierende Produkte)



# Pentests – Eine Einordnung

- Pentest vs. Audit
- Die getesteten Netzwerke/Produkte sind in der Regel komplex:
  - Normalerweise nicht besonders verdeckt (viele Logmeldungen)
  - Pentests sind ergebnisorientiert



# Methodik

- ★ Black- und Whiteboxtesting
- ★ Externe oder interne Sichtweise
- ★ In der Praxis: Blackboxansatz meist erfolgreich



# Die vier Phasen

- ★ Reconnaissance
- ★ Enumeration
- ★ Exploitation
- ★ Documentation, Bericht und Vorstellung der Ergebnisse beim Kunden

Sehr idealisiert, in der Praxis oft vermischt. Hierdurch schnellere Ergebnisse für den Kunden.



# Reconnaissance (Aufklärung)

- ★ Nutzung öffentlicher Quellen
- ★ Insbesondere Suchmachinen
  - ★ Suchmaschinen indizieren fast alle Daten
  - ★ Viele Daten sind vertraulicher Natur
  - ★ Einmal ins Internet geratene Daten sind kaum noch zu entfernen

# Reconnaissance (Aufklärung)

Im Rahmen von Pentests wurde unter anderem gefunden...

- ★ Ein Counterstrike-Server, der durch alle Firewalls hindurch erreichbar im internen Netz stand
- ★ Interne Datenbanken inkl. gültiger Logins
- ★ Interne Sicherheitsrichtlinien (z.B. Aufbau der genutzten Passwörter)
- ★ „Versteckte“ Webapplikationen und nicht mehr genutzte veraltete Skripte



# Enumeration: Finden von Angriffsvektoren

- ★ Port scanning
- ★ (Verwundbare) Versionen von Diensten/Systemen feststellen
- ★ Konfigurationsfehler
- ★ Installierte Software auf neue Fehler untersuchen
- ★ Sonstige kreative Ideen

Aufgrund der Menge: Keine vollständige Suche, stattdessen genau wie ein echter Angreifer: „Hauptsache, rein!“



# Exploitation

Ausnutzen von Sicherheitslücken:

- ★ Verifizieren: Haben wir wirklich eine Lücke?
- ★ Was können wir durch Ausnutzen der Lücke erreichen?
- ★ Angriff, sofern Risiko des Angriffs nicht zu hoch (gerade bei Livesystemen)
- ★ Nach erfolgreichem Angriff startet wieder Reconnaissance



# Documentation

Der Abschlussbericht:

- Umfangreiche Dokumentation des gesamten Tests
  - Schwachstelle
  - Details
  - Risikoeinstufung
  - Lösungsvorschläge
- Managementkurzbericht
- ToDo-Liste: Was kann sofort gemacht werden?



# Resultate: Was bringt ein Pentest?

- ★ Schnelle Identifizierung von Schwachstellen
- ★ Überprüfung des Sicherheitskonzeptes mit Blick auf das Gesamtsystem
- ★ Risikoanalyse
- ★ Lösungsvorschläge
- ★ Awareness (auch bei nichttechnischem Personal)
- ★ Direkter Schulungseffekt



# Pentests für KMUs?

- ★ Kosten für einen (illegalen) Angriff bei KMUs sind sehr gering (zwischen 100 und 10.000 Euro)
- ★ Angriffe werden in KMUs normalerweise nie bemerkt (kein Risiko für potentielle Angreifer)
- ★ $\Rightarrow$ Industriespionage findet statt
- ★ Penetrationtests bieten die Möglichkeit, sehr schnell praxisnahe Fehler zu identifizieren
- ★ Schulungseffekte und Sicherheitsgewinn sind gerade in KMUs enorm
- ★ Kosten für Penetrationtests sind auf Grund des kleineren Testaufwands auch geringer

# Und der Kopierer?

- ★ Kopierer haben Festplatten
- ★ Netzwerkanschlüsse



# Die üblichen Verdächtigen Teil 1

- Veraltete Software
  - Insbesondere Software, die nicht im Online-Update des Systems ist
  - Nicht mehr vom Hersteller gepflegte Software/Betriebssysteme
- Schwache Passwörter
- Unsichere Konfiguration
  - Admins wird oft nicht genug Zeit gelassen um alles sicher zu konfigurieren
- Nur an den Außenrändern des Netzes Firewalls, IDS, etc.
- Zuviele Dienste auf einem Server
- Unnötige Dienste

# Die üblichen Verdächtigen Teil 2

- Windowsfreigaben im internen Netzwerk für alle les- und schreibbar
  - Bsp.: Userprofiles → Autostartordner...
- Unsicheres WLAN (gerne auch direkt im Firmennetz)
- „Verdächtiges“ wird nicht weitergemeldet
- Backups für alle lesbar
- Incident Response nicht vorhanden
- Schlechte physikalische Sicherheit

# Die üblichen Verdächtigen Teil 2

# Die üblichen Verdächtigen Teil 2



Vielen Dank für Ihre Aufmerksamkeit