Hacking for your Security - Penetration Testing

Claus R. F. Overbeck - RedTeam Pentesting GmbH
claus.overbeck@redteam-pentesting.de
http://www.redteam-pentesting.de

November 6th, 2009
Entrepreneurial Marketing, RWTH Aachen, WIN

Agenda

1. RedTeam Pentesting, Dates and Facts
2. What is a Pentest
3. The Foundation Story
4. Marketing at RedTeam Pentesting

RedTeam Pentesting, Dates and Facts

- Founded in 2004
- Specialisation exclusively on penetration tests
- 8 penetration testers

"Laptop: a portable microcomputer having its main components (as processor, keyboard, and display screen) integrated into a single unit capable of battery-powered operation"

(merriam-webster.com - Merriam Webster Online)

"Laptop: A computer designed to allow employees to easily store vast amounts of customer data in the backseat of a taxicab"

(The Devil's Infosec Dictionary)

"Laptop: a portable microcomputer having its main components (as processor, keyboard, and display screen) integrated into a single unit capable of battery-powered operation"

(merriam-webster.com - Merriam Webster Online)

"Laptop: A computer designed to allow employees to easily store vast amounts of customer data in the backseat of a taxicab"

(The Devil's Infosec Dictionary)

What is a Pentest?

- ★ Attacking a network or product with the owner's consent
- ★ Question: How deeply can a real attacker penetrate the security?
- ★ Same methods as the "bad guys"
- ★ Conducted from the attacker's perspective
- ★ Individualised search of security vulnerabilities by experts
- ★ Detailed documentation from the beginning

RWTH Research Group “RedTeam”

- Founded December 2004 at the RWTH Aachen University
- Research group at the chair of Dependable Distributed Systems (Prof. Felix Freiling)
- All participants in the group already have many years of experience in IT security
- Research question: How to conduct efficient penetration tests resulting in the highest benefit for the client

RWTHAACHEN
UNIVERSITY

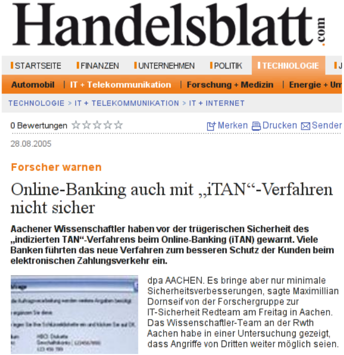
RWTH Research Group “RedTeam”

- The research group is informally called *Red Team*: a term describing the opposing force in military simulations
- First pentests of chairs at the RWTH (free of charge)
- Many are shocked how vulnerable they are

RWTH AACHEN UNIVERSITY

RWTH Research Group “RedTeam”

- The methodology used in the pentests is positively received
- The word spreads that “RedTeam” identifies security weaknesses of practical relevance in a short time
- Parallel research of security vulnerabilities generates the first press coverage: ITAN



Handelsblatt.com

28.08.2005

Forscher warnen

Online-Banking auch mit „iTAN“-Verfahren nicht sicher

Aachener Wissenschaftler haben vor der trügerischen Sicherheit des „indizierten TAN“-Verfahrens beim Online-Banking (iTAN) gewarnt. Viele Banken führten das neue Verfahren zum besseren Schutz der Kunden beim elektronischen Zahlungsverkehr ein.

dpa AACHEN. Es bringe aber nur minimale Sicherheitsverbesserungen, sagte Maximillian Dornseif von der Forschergruppe zur IT-Sicherheit Redteam am Freitag in Aachen. Das Wissenschaftler-Team an der Rwth Aachen habe in einer Untersuchung gezeigt, dass Angriffe von Dritten weiter möglich seien.

RWTH Research Group “RedTeam”

- The interest in RedTeam’s work remains high
- Prospective customers are willing to pay for the service
- In the middle of 2005: the chair moves to the University of Mannheim
- RedTeam has two choices: either quit or start a company

UNIVERSITÄT
MANNHEIM

RedTeam Pentesting

- ★ The problem: an adequate legal form
- ★ Risk of liability
- ★ Founding a company takes time RedTeam does not have ⇒ Nomis Development GmbH lets RedTeam work as an independent divison
- ★ Needs an official name, “RedTeam” is too generic ⇒ The new name: *RedTeam Pentesting*

Financing

- The next issue: How to finance the new company
- RedTeam Pentesting's advantage: no need to finance anything in advance
  - No machines
  - No producer goods
  - No suppliers
  - (Almost) no external service providers
- Pentests belong to the service sector
- Most valuable assets of the company: Its employees
  ⇒ Intellectual work

Financing

- ★ Biggest costs at the beginning:
  - ★ Fixed costs for rent, telephone, internet...
  - ★ Travel costs
- ★ Later: Salaries. Good people in IT security are rare
- ★ Financing of the first months is covered from payed work during the time at the RWTH
- ★ No need for Venture Capital, EU Fundings etc.
  ⇒ No dependencies, no expectations, no regulations

Technology Centre Aachen

In late 2005, the first offices at the TZA are rented

- Focus on technology-oriented companies
- Inexpensive rent
- Availability of small offices
- Flexible (even with unusual demands)
- Direct access by autobahn
- Already existing infrastructure:
  - Reception
  - Cafeteria
  - Conference rooms
  - Site security in the evening/night

RedTeam Pentesting GmbH

- The trademark RedTeam Pentesting gets more and more established
- RedTeam Pentesting starts its own company in parallel to its day-to-day business
- *RedTeam Pentesting GmbH* is in the course of formation as of December 2006
- Fully established as of January 1st, 2007

RedTeam Pentesting GmbH Today

- Working worldwide
- Medium to large companies and international corporations
- Small companies with special security interests
- Branches of trade: industry, banks and insurance companies, trading business, operators of data centers, public administration...
- Press coverage in online and print media, radio and TV
- Expanded to bigger offices at the TZA

What is Marketing?

- ★ Who is your customer?
- ★ What does she want/need?
- ★ Design your product/service to your customer's needs.
- ★ Communicate the value of your product/service to your customer.

RedTeam Pentesting

- ★ Seriousness
- ★ Specialisation exclusively on penetration tests
- ★ Teamwork
- ★ Discretion
- ★ Transfer of know-how

Thank you for listening. Questions?