Hacking for your security - Penetration Testing

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

22. Februar 2006

„Wir wissen nicht, was für Lücken wir haben - deshalb juckt uns das nicht.“

Agenda

14:00 Uhr	Vorstellung Penetrationtests und Common Failures
ab ca. 15:00 Uhr	freie Diskussion und tiefergehende Fragestellungen

Über RedTeam

- Gegründet 2004
- Durchführung von Penetrationtests
- Teambasierte Arbeit
- Forschung im IT-Security Bereich und Veröffentlichung von Advisories
- 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)
- Endet mit ausführlichem Bericht für den Kunden
- Besonderheit bei RedTeam: Kein Test nach Norm

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)
- Endet mit ausführlichem Bericht für den Kunden
- Besonderheit bei RedTeam: Kein Test nach Norm

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)
- Endet mit ausführlichem Bericht für den Kunden
- Besonderheit bei RedTeam: Kein Test nach Norm

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)
- Endet mit ausführlichem Bericht für den Kunden
- Besonderheit bei RedTeam: Kein Test nach Norm

Methodik

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

Grundsätzliches

- Ein Pentest ist kein Audit
- Die getesteten Netzwerke sind in der Regel komplex, daher:
  - Normalerweise nicht besonders verdeckt (viele Logmeldungen)
  - Pentests sind ergebnisorientiert

Grundsätzliches

- Ein Pentest ist kein Audit
- Die getesteten Netzwerke sind in der Regel komplex, daher:
  - Normalerweise nicht besonders verdeckt (viele Logmeldungen)
  - Pentests sind ergebnisorientiert

Die vier Phasen

- Reconnaissance
- Enumeration
- Exploitation
- Bericht und Vorstellung der Ergebnisse beim Kunden

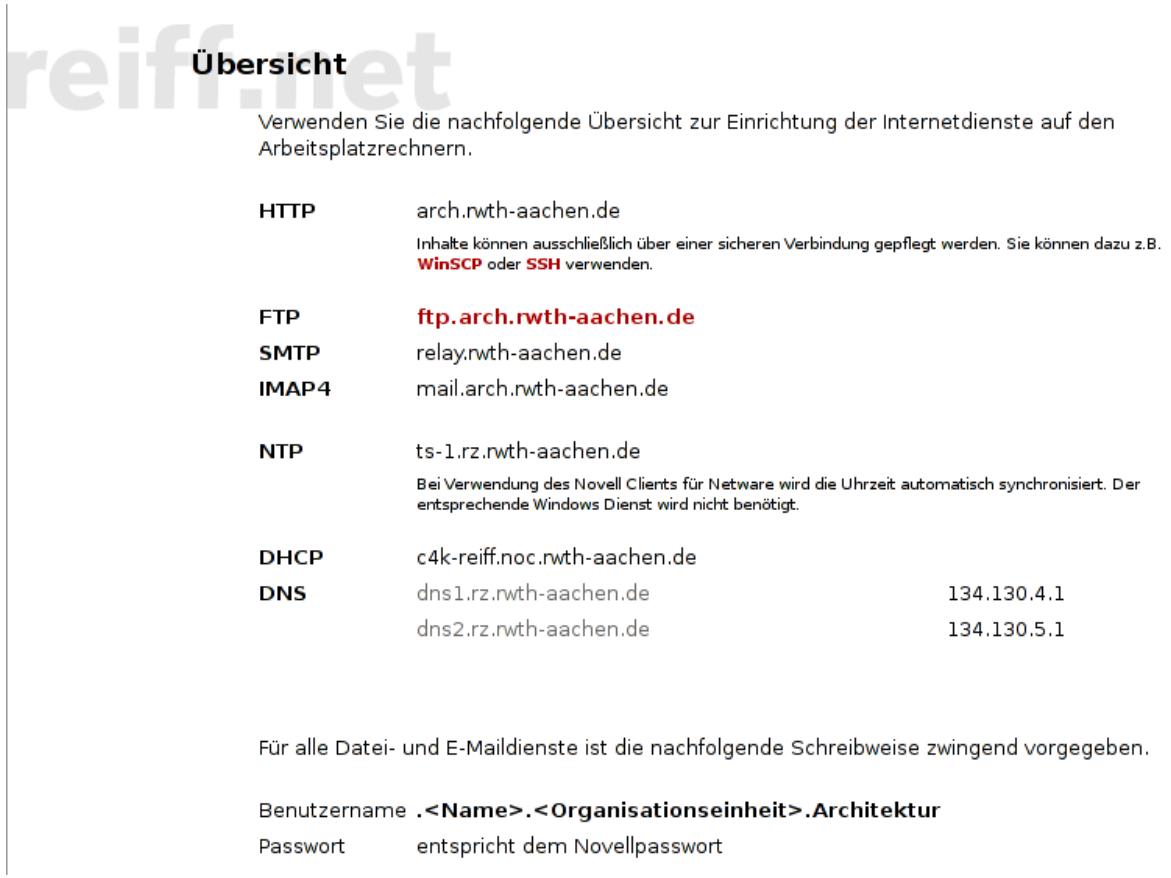
Sehr idealisiert, in der Praxis oft vermischt. Hierdurch schnellere Ergebnisse für den Kunden.

Reconnaissance (Aufklärung)

- Homepages
- Google
- DNS
- Whois

Reconnaissance (Aufklärung)

- Homepages
- Google
- DNS
- Whois



reiff.net

Übersicht

Verwenden Sie die nachfolgende Übersicht zur Einrichtung der Internetdienste auf den Arbeitsplatzrechnern.

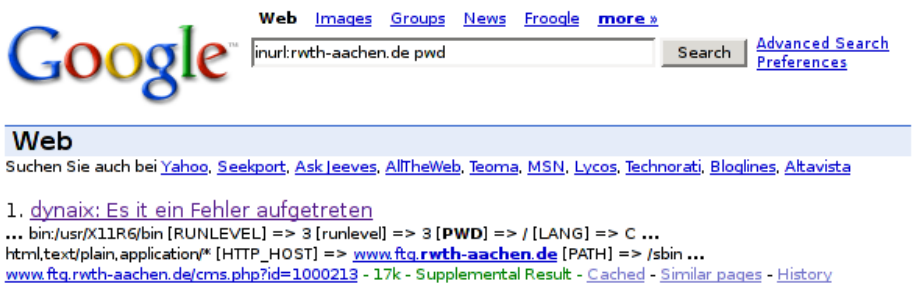
HTTP	arch.rwth-aachen.de	
	Inhalte können ausschließlich über einer sicheren Verbindung gepflegt werden. Sie können dazu z.B. **WinSCP** oder **SSH** verwenden.	
FTP	**ftp.arch.rwth-aachen.de**	
SMTP	relay.rwth-aachen.de	
IMAP4	mail.arch.rwth-aachen.de	
NTP	ts-1.rz.rwth-aachen.de	
	Bei Verwendung des Novell Clients für Netware wird die Uhrzeit automatisch synchronisiert. Der entsprechende Windows Dienst wird nicht benötigt.	
DHCP	c4k-reiff.noc.rwth-aachen.de	
DNS	dns1.rz.rwth-aachen.de	134.130.4.1
	dns2.rz.rwth-aachen.de	134.130.5.1

Für alle Datei- und E-Maildienste ist die nachfolgende Schreibweise zwingend vorgegeben.

Benutzername	**.<Name>.<Organisationseinheit>.Architektur**
Passwort	entspricht dem Novellpasswort

Reconnaissance (Aufklärung)

- Homepages
- Google
- DNS
- Whois



Reconnaissance (Aufklärung)

- Homepages
- Google
- DNS
- Whois

hostip	62.75.208.71
hostname	www.ftg.rwth-aachen.de
id	1000213
layers	Array ( )
license	1ccd07b1566727fe517ebbd49657287b
lng	german
page	page Object ([is_error] => [id] => 1000213)
password	084e0343a0486ff05530df6c705c8bb4

Reconnaissance (Aufklärung)

- Homepages
- Google
- DNS
- Whois

Reconnaissance (Aufklärung)

- Homepages
- Google
- DNS
- Whois

```
Received: from [redacted] ([redacted])
        by [redacted] (8.12.11/8.12.10) with ESMTP id k0I8o6Bc025086      for
        <kontakt@redteam-pentesting.de>; Wed, 18 Jan 2006 09:50:06 +0100 (MET)
Received: from [redacted] by [redacted] via smtpd
        (for [redacted] [redacted]) with ESMTP; Wed,
 18 Jan 2006 09:50:06 +0100
Received: from [redacted].intern ([7.87.28.247])
        by [redacted].intern (Lotus Domino Release 6.5.2)
        with ESMTP id 2006011809435671-5824515 ; Wed, 18 Jan 2006 09:43:56 +0100
Date: Wed, 18 Jan 2006 09:50:03 +0100
```

Reconnaissance (Aufklärung)

- Homepages
- Google
- DNS
- Whois

```
$ whois 7.37.23.247
Process query: '7.37.23.247'
Query recognized as IP.
Querying whois.arin.net:43 with whois.

OrgName:    DoD Network Information Center
OrgID:      DNIC
Address:    3990 E. Broad Street
City:       Columbus
StateProv:  OH
PostalCode: 43218
Country:    US

NetRange:   7.0.0.0 - 7.255.255.255
CIDR:       7.0.0.0/8
NetName:    DISANET7
NetHandle:  NET-7-0-0-0-1
Parent:
NetType:    Direct Allocation
Comment:    Defense Information Systems Agency
Comment:    DISA /D3
Comment:    11440 Isaac Newton Square
Comment:    Reston, VA 22090-5087 US
RegDate:    1997-11-24
Updated:    1998-09-26

RTechHandle: MIL-HSTMST-ARIN
RTechName:   Network DoD
RTechPhone:  +1-800-365-3642
RTechEmail:  HOSTMASTER@nic.mil

OrgTechHandle: MIL-HSTMST-ARIN
OrgTechName:   Network DoD
OrgTechPhone:  +1-800-365-3642
OrgTechEmail:  HOSTMASTER@nic.mil
```

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

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

Joker

Was sind Joker, wofür braucht man die?

- Zeit/Geld sparen
- Software könnte in Zukunft verwundbar sein
- Angreifer könnten einen eigenen Exploit entwickeln
- Testen von Second-Line-Defense

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)

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)

Resultate: Was bringt ein Pentest?

- Zeigt punktuell relevante Schwachstellen(klassen) auf
- Was steht im Bericht?
- Wie nutzt man die Ergebnisse des Pentests?

Resultate: Was bringt ein Pentest?

- Zeigt punktuell relevante Schwachstellen(klassen) auf
- Was steht im Bericht?
- Wie nutzt man die Ergebnisse des Pentests?

Resultate: Was bringt ein Pentest?

- Zeigt punktuell relevante Schwachstellen(klassen) auf
- Was steht im Bericht?
- Wie nutzt man die Ergebnisse des Pentests?

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 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 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 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 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 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

- 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

- 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

- 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

- 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

- 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

Fragen / freie Diskussion