Online-Voodoo: Mehr finden, mehr sehen, mehr wissen.

Effektive Recherche im Internet

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

Zukunftskongress – Ethik 2.0 – Schöne neue Online-Welt
29. September 2007, Heidelberg

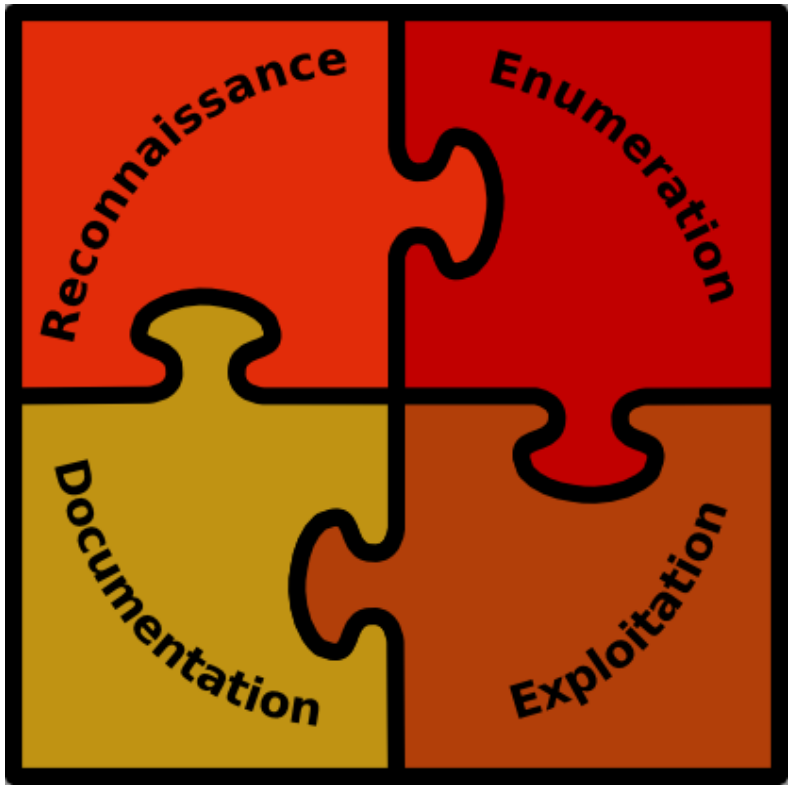
Über den Vortrag

- ★ Gute (Online-)Recherche ist unerlässlich
- ★ Anregung zum Selberdenken und kreativ sein
- ★ Nicht nur Suchmaschinen ⇒ gesamter Onlinebereich
- ★ Viele Livedemos
- ★ Seien Sie interaktiv ⇒ Workshop

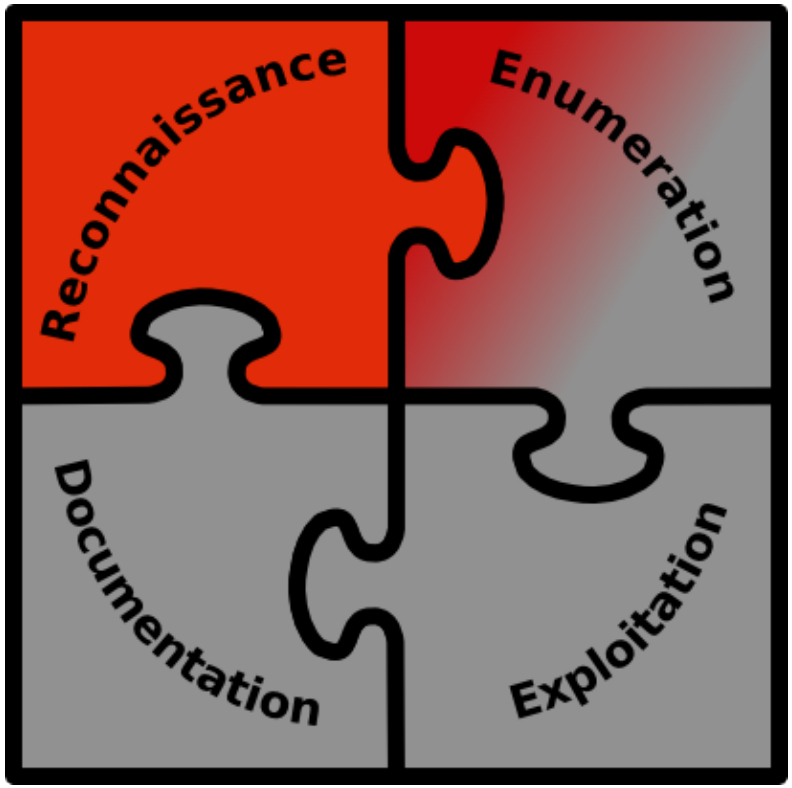
RedTeam Pentesting, Daten & Fakten

- ★ Penetrationtests: „IT-Sicherheit aus Angreiferperspektive“
- ★ Spezialisierung ausschließlich auf Penetrationtests
- ★ 7 Penetrationtester (Stand Anfang 2007)
- ★ Europaweite Durchführung von Penetrationtests

Ablauf eines Pentests



In diesem Workshop



Rechtliches

- ★ Pentest ⇔ Recherche
- ★ Strafrechtliche Konsequenzen
- ★ Zivilrechtliche Konsequenzen
- ★ Damoklesschwert neuer §202c

Rechtliches

§202c (1): Vorbereiten des Ausspähens und Abfangens von Daten

Wer eine Straftat nach §202a oder §202b vorbereitet, indem er

1. *Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten (§202a Abs. 2) ermöglichen, oder*
2. *Computerprogramme, deren Zweck die Begehung einer solchen Tat ist, herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.*

Warum Online-Recherche?

Warum ist eine gute Online-Recherche wichtig?

- ★ Es findet sich *alles* im Internet
- ★ Was einmal im Internet ist, *bleibt* im Internet
- ★ Man muss es nur finden!

Beispiel: Juli 2007, Irak

Beispiel: Juli 2007, Irak

Associated Press hacks who carried out the investigation suggested that less tech-savvy people in the US military-industrial complex thought it safe to put the files on open FTP (File Transfer Protocol) machines because they were not crawled by search-engine bots and thus could not be Googled. However, the AP scribes could get to the files in many cases by simply substituting "ftp" for "http" in their browser address bars.

The Register, 16.07.2007

Beispiel: Juli 2007, Irak

FTP search v3.4

www.FTPSearch.net

Die Basics: Suchmaschinen

- ★ Es gibt nicht nur Google
- ★ Yahoo!, MSN, AllTheWeb, Altavista, Ask.com ...
- ★ In die Hilfe schauen!
- ★ Meta-Suchmaschinen durchsuchen mehrere Suchmaschinen auf einmal (z.B. MetaCrawler)

⇒ Demo

Die Basics: Suchmaschinen

- ★ Es gibt nicht nur Google
- ★ Yahoo!, MSN, AllTheWeb, Altavista, Ask.com ...
- ★ In die Hilfe schauen!
- ★ Meta-Suchmaschinen durchsuchen mehrere Suchmaschinen auf einmal (z.B. MetaCrawler)

$\Rightarrow$ **Demo**

Kreativ Suchen

⇒ Demo

Kreativ Suchen

⇒ **Demo**

Suchmaschinen der anderen Art

- Social Bookmarking
  - Del.icio.us
  - Mr. Wong
- spezialisierte Suchmachinen
  - Google Co-Op: eBook Search / eBookSearchr
  - Google Groups
  - Technorati
  - Gmane
- Es existieren spezialisierte Suchmaschinen für jeden Bedarf

⇒ Benutzen Sie Suchmaschinen zum Finden von Suchmaschinen!

⇒ Demo

Suchmaschinen der anderen Art

- Social Bookmarking
  - Del.icio.us
  - Mr. Wong
- spezialisierte Suchmachinen
  - Google Co-Op: eBook Search / eBookSearchr
  - Google Groups
  - Technorati
  - Gmane
- Es existieren spezialisierte Suchmaschinen für jeden Bedarf

⇒ Benutzen Sie Suchmaschinen zum Finden von Suchmaschinen!

⇒ **Demo**

Öffentliche Datenbanken

- ★ Der Fall Atze Schröder
  ⇒ Deutsches Marken- und Patentamt `http://www.dpma.de`
- ★ Änderungen in der Wikipedia
  ⇒ Wikipedia-Scanner `http://wikiscanner.virgil.gr`

⇒ **Demo**

Öffentliche Datenbanken

- ★ Der Fall Atze Schröder
  ⇒ Deutsches Marken- und Patentamt `http://www.dpma.de`
- ★ Änderungen in der Wikipedia
  ⇒ Wikipedia-Scanner `http://wikiscanner.virgil.gr`

⇒ **Demo**

Web 2.0: User Generated Content

Social Networks

- ★ Xing
- ★ MySpace
- ★ Facebook
- ★ StudiVZ
- ★ StayFriends
- ★ Orkut

Inhaltsanbieter

- ★ YouTube
- ★ Google Video
- ★ Google Maps/Earth
- ★ Flickr
- ★ Ebay

Personenrecherche

- Jeder hinterlässt Spuren im Netz
- Die ersten Suchmaschinen spezialisieren sich darauf, diese zusammenzutragen
  - Spock.com `http://www.spock.com`
  - Pipl `http://www.pipl.com`
  - Maltego `http://www.paterva.com`

⇒ Demo

Personenrecherche

- Jeder hinterlässt Spuren im Netz
- Die ersten Suchmaschinen spezialisieren sich darauf, diese zusammenzutragen
  - Spock.com `http://www.spock.com`
  - Pipl `http://www.pipl.com`
  - Maltego `http://www.paterva.com`

$\Rightarrow$ **Demo**

Internet-Archive

Was einmal im Internet ist, *bleibt* im Internet

- ★ Google Cache
- ★ Coral Cache `http://www.coralcdn.org`
- ★ Archive.org `http://www.archive.org`

⇒ Demo

Internet-Archive

Was einmal im Internet ist, *bleibt* im Internet

- ★ Google Cache
- ★ Coral Cache `http://www.coralcdn.org`
- ★ Archive.org `http://www.archive.org`

⇒ **Demo**

Exkurs: GPG/PGP

- ★ *GNU Privacy Guard*, *Pretty Good Privacy*
- ★ Verschlüsselung und Signierung von E-Mails/Dateien
- ★ Problem: Jeder kann unter beliebigem Namen einen neuen Schlüssel erstellen
- ★ Eine Lösung: *Web of Trust*
- ★ Feststellen von Verbindungen zwischen Personen

⇒ Demo

Exkurs: GPG/PGP

- ★ *GNU Privacy Guard*, *Pretty Good Privacy*
- ★ Verschlüsselung und Signierung von E-Mails/Dateien
- ★ Problem: Jeder kann unter beliebigem Namen einen neuen Schlüssel erstellen
- ★ Eine Lösung: *Web of Trust*
- ★ Feststellen von Verbindungen zwischen Personen

⇒ **Demo**

Internet-Tauschbörsen

The Register » Security »

Classified Dutch military documents found on P2P site

Classified U.S. military info available over P2P

By Jaikumar Vijayan, Computerworld, 07/25/07

The Register » Security » Enterprise Security »

Pfizer worker data leaked via P2P

66,000 Names and Personal Details Leaked On P2P

⇒ Demo

Internet-Tauschbörsen

The Register » Security »

Classified Dutch military documents found on P2P site

Classified U.S. military info available over P2P

By Jaikumar Vijayan, Computerworld, 07/25/07

The Register » Security » Enterprise Security »

Pfizer worker data leaked via P2P

66,000 Names and Personal Details Leaked On P2P

⇒ **Demo**

Anonyme Netze

- Das *World Wide Web* ist nicht das einzige Hypertext-System im Internet
- Anonyme Netze, um Inhalte frei veröffentlichen zu können (z.B. aus Angst vor Repressalien ⇒ China)
  - Freenet Freesites `http://www.freenetproject.org`
  - I2P eepSites `http://www.i2psites.com`

⇒ Demo

Anonyme Netze

- Das *World Wide Web* ist nicht das einzige Hypertext-System im Internet
- Anonyme Netze, um Inhalte frei veröffentlichen zu können (z.B. aus Angst vor Repressalien ⇒ China)
  - Freenet Freesites `http://www.freenetproject.org`
  - I2P eepSites `http://www.i2psites.com`

⇒ **Demo**

Hinter den Kulissen: HTML-Quellcode

- Webseiten sind in *HyperText Markup Language* (HTML) geschrieben
- HTML ist Text ⇒ Von Menschen lesbar
  - Auskommentierter Inhalt
  - Versteckte Verzeichnisse
  - Nicht angezeigte Formularfelder (*Hidden Fields*)
  - Verzeichnisse und Dateien, die nicht von Suchmaschinen indexiert werden sollen (`robots.txt`)

⇒ Demo

Hinter den Kulissen: HTML-Quellcode

- Webseiten sind in *HyperText Markup Language* (HTML) geschrieben
- HTML ist Text ⇒ Von Menschen lesbar
  - Auskommentierter Inhalt
  - Versteckte Verzeichnisse
  - Nicht angezeigte Formularfelder (*Hidden Fields*)
  - Verzeichnisse und Dateien, die nicht von Suchmaschinen indexiert werden sollen (`robots.txt`)

⇒ **Demo**

Vom Client zum Server: Serverlogs

- ★ Beispiel Webserver
- ★ Interessant: IP-Adressen
- ★ Geographische Zuordnung
  ⇒ GeoIP `http://www.maxmind.com/app/locate_ip`
- ★ Welche Domain gehört zu dieser Adresse?
  ⇒ `DNS Reverse Lookup`
- ★ Welche Informationen gibt es zu dieser Domain?
  ⇒ `WHOIS`
- ★ Online z.B. `http://ping.eu`

⇒ Demo

Vom Client zum Server: Serverlogs

- ★ Beispiel Webserver
- ★ Interessant: IP-Adressen
- ★ Geographische Zuordnung
  ⇒ GeoIP `http://www.maxmind.com/app/locate_ip`
- ★ Welche Domain gehört zu dieser Adresse?
  ⇒ `DNS Reverse Lookup`
- ★ Welche Informationen gibt es zu dieser Domain?
  ⇒ `WHOIS`
- ★ Online z.B. `http://ping.eu`

⇒ **Demo**

Mail-Header

E-Mails bestehen nicht nur aus dem Nachrichtentext

```
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]) with ESMTP; Wed,
 18 Jan 2006 09:50:06 +0100
Received: from [redacted].intern ([7.37.23.247])
        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
```

Beteiligte Mailserver, Absendedatum, Bounce-Informationen, Benutzerdefinierte Einträge . . .

Vorsicht: Header lassen sich fälschen!

Mehr sehen: Versteckte Informationen in Dateien

- Viele Dateiformate enthalten „versteckte“ Zusatzinformationen (*Metainformationen*)
- MS Word `.doc`-Dateien
  - Word Version
  - Autoren
  - Undo-History

⇒ Demo

Mehr sehen: Versteckte Informationen in Dateien

- Viele Dateiformate enthalten „versteckte“ Zusatzinformationen (*Metainformationen*)
- MS Word `.doc`-Dateien
  - Word Version
  - Autoren
  - Undo-History

⇒ **Demo**

Mehr sehen: Versteckte Informationen in Dateien

Die Lösung: PDF-Datei?

Mehr sehen: Versteckte Informationen in Dateien

Die Lösung: PDF-Datei?

```
$ strings Bewerbung.pdf | grep -o -E '(Mi.*\.doc|T.*\.pdf)'
Title( Praktikum .pdf
Title(abi2.pdf
Title(abi1.pdf
Title( dienstzeugnis.pdf
Title( arbeitszeugnis.pdf
Title( .pdf
Title( .pdf
Title(Notenspiegel .pdf
Microsoft Word - Praktikum .doc
```

Textschwärzungen

Wenn [redacted], dann richtig.

⇒ Demo

Textschwärzungen

Wenn schwärzen, dann richtig.

$\Rightarrow$ **Demo**

Ich sehe was, was du nicht siehst

- Metainformationen in Bildern
- *Exchangeable Image File Format* (Exif)
  - Hersteller, Modell, Seriennummer der Kamera
  - Datum, Uhrzeit der Aufnahme
  - Name, Version der Bildbearbeitungssoftware
  - Vorschaubild
  - ...
- Beispiel Juli 2007: Seriennummer der Kamera in illegal abfotografiertem Harry Potter-Buch

Bildausschnitte

Quelle: Dr. jur. Maximillian Dornseif

http://www.redteam-pentesting.de/advisories/rt-sa-2005-008.php?lang=de

Bildausschnitte

Quelle: Dr. jur. Maximillian Dornseif

http://www.redteam-pentesting.de/advisories/rt-sa-2005-008.php?lang=de

Ausgeschnittene Personen

Quelle: Dr. jur. Maximillian Dornseif

http://www.redteam-pentesting.de/advisories/rt-sa-2005-008.php?lang=de

Ausgeschnittene Personen

Quelle: Dr. jur. Maximillian Dornseif

http://www.redteam-pentesting.de/advisories/rt-sa-2005-008.php?lang=de

Ausgeschnittene Personen

Quelle: Dr. jur. Maximillian Dornseif

http://www.redteam-pentesting.de/advisories/rt-sa-2005-008.php?lang=de

Ausgeschnittene Personen

Quelle: Dr. jur. Maximillian Dornseif

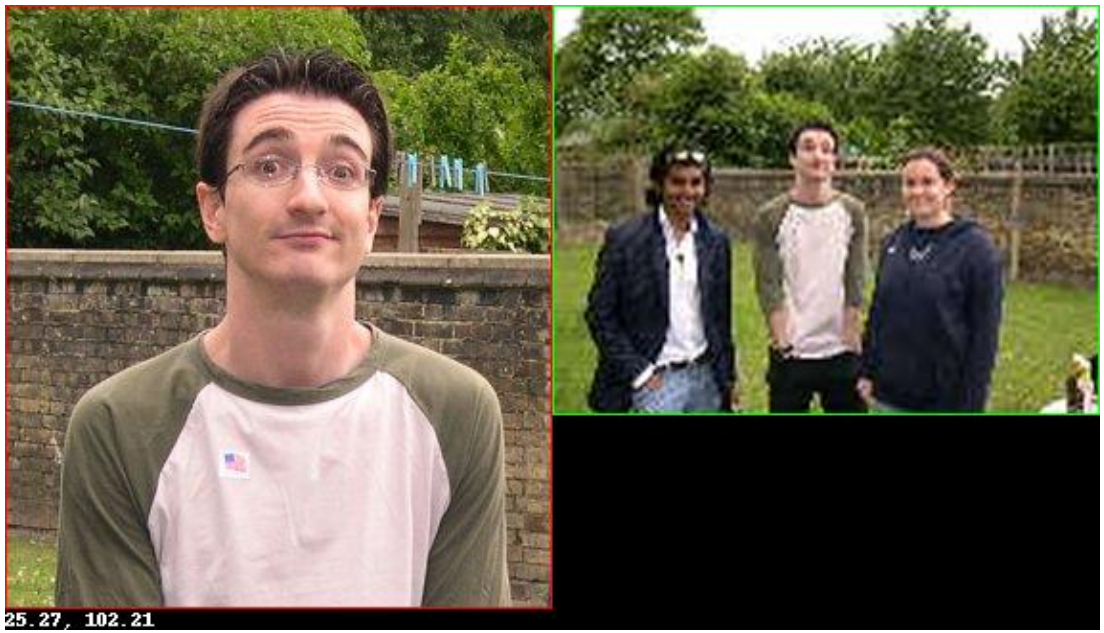
http://www.redteam-pentesting.de/advisories/rt-sa-2005-008.php?lang=de

Ausgeschnittene Personen

Quelle: Dr. jur. Maximillian Dornseif

http://www.redteam-pentesting.de/advisories/rt-sa-2005-008.php?lang=de

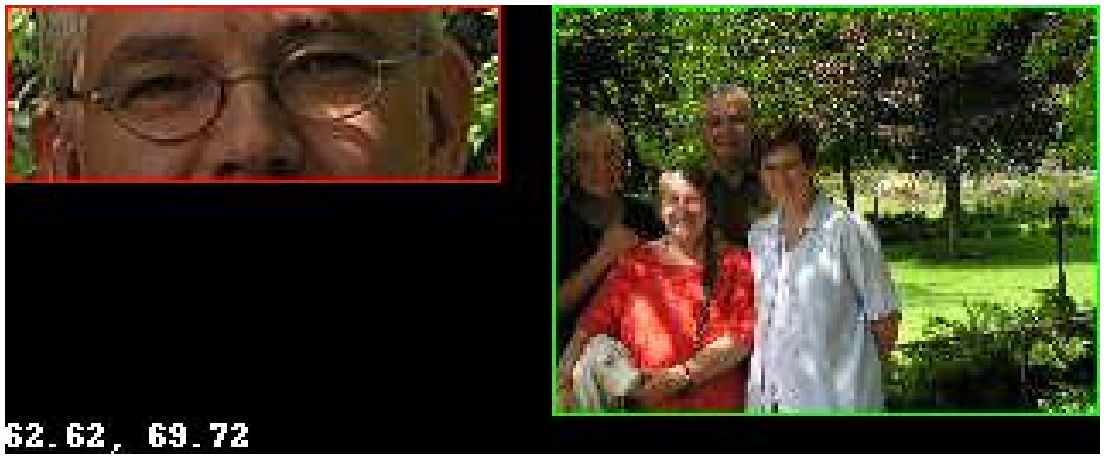
Ausgeschnittene Personen



Quelle: Dr. jur. Maximillian Dornseif

http://www.redteam-pentesting.de/advisories/rt-sa-2005-008.php?lang=de

Ausgeschnittene Personen



Quelle: Dr. jur. Maximillian Dornseif

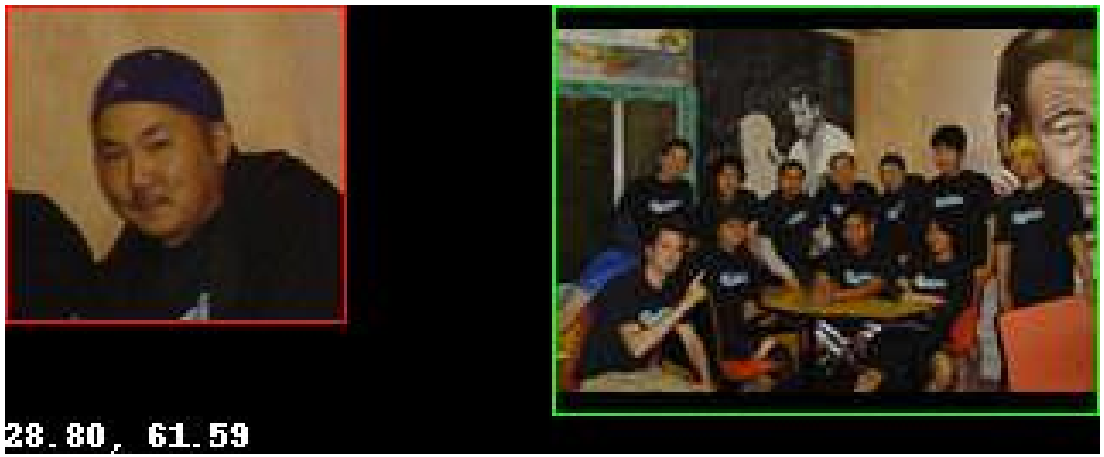
http://www.redteam-pentesting.de/advisories/rt-sa-2005-008.php?lang=de

Ausgeschnittene Personen

Quelle: Dr. jur. Maximillian Dornseif

http://www.redteam-pentesting.de/advisories/rt-sa-2005-008.php?lang=de

Ausgeschnittene Personen



Quelle: Dr. jur. Maximillian Dornseif

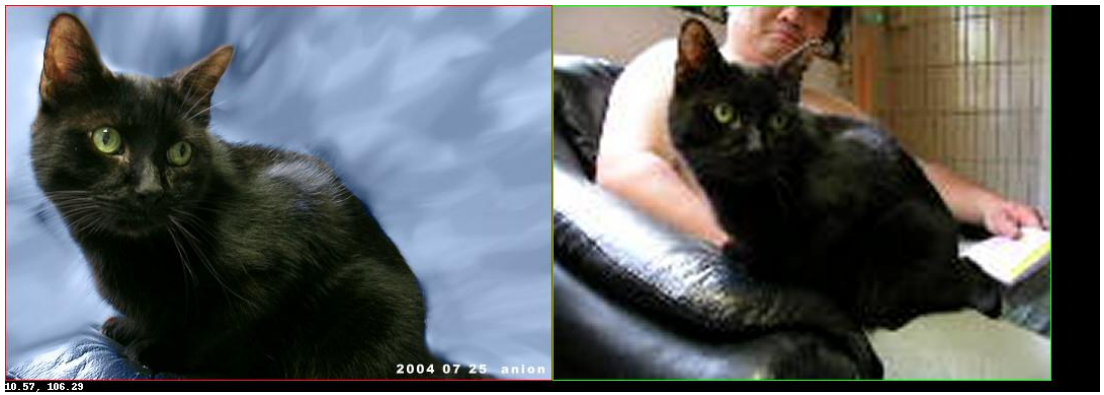
http://www.redteam-pentesting.de/advisories/rt-sa-2005-008.php?lang=de

Verschwundener Text

Quelle: Dr. jur. Maximillian Dornseif

http://www.redteam-pentesting.de/advisories/rt-sa-2005-008.php?lang=de

Bildmanipulationen



Quelle: Dr. jur. Maximillian Dornseif

http://www.redteam-pentesting.de/advisories/rt-sa-2005-008.php?lang=de

Bildmanipulationen

Quelle: Dr. jur. Maximillian Dornseif

http://www.redteam-pentesting.de/advisories/rt-sa-2005-008.php?lang=de

Bildmanipulationen

Quelle: Dr. jur. Maximillian Dornseif

http://www.redteam-pentesting.de/advisories/rt-sa-2005-008.php?lang=de

Erkennen von Bildmanipulationen

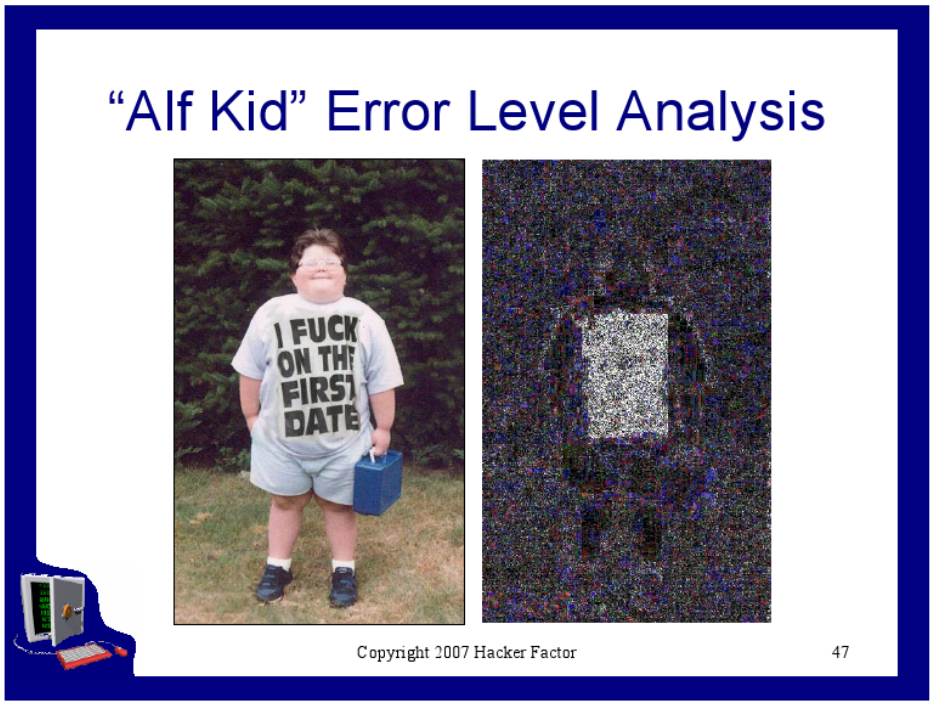
- ★ Kann man Bildmanipulationen erkennen?
- ★ ⇒ Vortrag von Dr. Neal Krawetz auf der BlackHat 2007

Alf Kid

Quelle: Dr. Neal Krawetz, BlackHat USA 2007

http://www.hackerfactor.com/papers/bh-usa-07-krawetz-wp.pdf

Alf Kid



Quelle: Dr. Neal Krawetz, BlackHat USA 2007

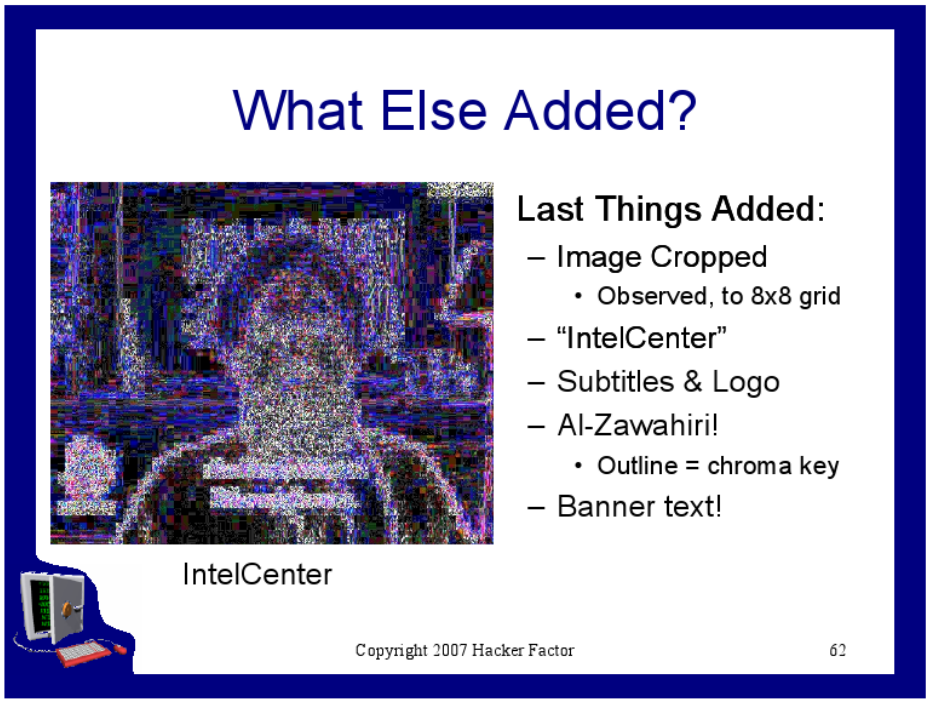
http://www.hackerfactor.com/papers/bh-usa-07-krawetz-wp.pdf

Al-Zawahiri

Quelle: Dr. Neal Krawetz, BlackHat USA 2007

http://www.hackerfactor.com/papers/bh-usa-07-krawetz-wp.pdf

Al-Zawahiri



Quelle: Dr. Neal Krawetz, BlackHat USA 2007

http://www.hackerfactor.com/papers/bh-usa-07-krawetz-wp.pdf

Festplatten

- ★ Daten auf Festplatten zu löschen ist nicht trivial
- ★ „Normales“ Löschen markiert Daten nur mit: „Zum Überschreiben freigegeben“
- ★ Bis zum Überschreiben sind die Daten jedoch noch vorhanden

Festplatten

heise online · c't · iX · Technology Review · Telepolis · mobil · Security · Netze · heise open

heise online

news 07.04.2005 17:53

<< Vorige | Nächste >>

Sie sind Gast
Einloggen | Registrieren

Suche ...

7-Tage-News
News-Archiv
News unterwegs
Newsletter
News einbinden

Telefontarife

Mitarbeiter versteigerte sieben Festplatten mit Polizeidaten vorlesen

Das Rätselraten um die Herkunft der im Internet versteigerten Computer-Festplatte mit geheimen Polizeidaten ist zu Ende. Ein 45-jähriger Angestellter der Zentraldienste der Polizei habe gestanden, den Speicher unberechtigt über das Internet-Auktionshaus eBay versteigert zu haben, erklärte Brandenburgs Innenminister Jörg Schönbohm (CDU) heute in Potsdam. Das Arbeitsverhältnis mit dem Beschuldigten sei bereits beendet worden.

Quelle: Heise online

http://www.heise.de/newsticker/meldung/58353

Fazit

- ★ Online-Recherche ist mehr als Google benutzen
- ★ Werden Sie selbst kreativ!
- ★ Ungewollte Datenlecks passieren auch wichtigen Stellen
- ★ Manipuliert wird überall – schauen Sie zweimal hin bei Dokumenten, Bildern etc.

Es findet sich alles im Internet ⇒ und täglich kommt mehr dazu. . .

Fazit

- ★ Online-Recherche ist mehr als Google benutzen
- ★ Werden Sie selbst kreativ!
- ★ Ungewollte Datenlecks passieren auch wichtigen Stellen
- ★ Manipuliert wird überall – schauen Sie zweimal hin bei Dokumenten, Bildern etc.

Es findet sich alles im Internet ⇒ und täglich kommt mehr dazu. . .

Fragen?

Vielen Dank für Ihre Aufmerksamkeit!

–

Offene Diskussion