A fresh new look into Information Gathering

Christian Martorella
IV OWASP MEETING SPAIN
Who am i ?

Christian Martorella

- Manager Auditoria S21sec
- CISSP, CISA, CISM, OPST, OPSA
- OWASP WebSlayer Project Leader
- OISSG, Board of Directors
- FIST Conference, Presidente
- Edge-Security.com
Information Gathering

“Denotes the collection of information before the attack. The idea is to collect as much information as possible about the target which may be valuable later.”
OSINT: Open Source INTElligence

“Is an information processing discipline that involves finding, selecting, and acquiring information from publicly available sources and analyzing it to produce actionable intelligence.”
Penetration test anatomy

- Information Gathering
- Discovery / Fingerprinting
- Vulnerability analysis
- Exploitation
- Reporting
Types of I.G

Passive

Active
I.G - Types of information

- Domain, subdomain/host names: dev.target.com
- User names: jdoe
- Email Accounts: jdoe@target.com
- Person names: John Doe
I.G what for?

- **Infrastructure:**
  - Information for discovering new targets, to get a description of the hosts (NS, MX, AS, etc), shared resources

- **People and organizations:**
  - For performing brute force attacks on available services, Spear phishing, social engineering, investigations, analysis, background checks, information leaks
How can we obtain this kind of info?
Obtaining **host and Domains** info - Classic

- Zone Transfer (active)
- Whois (passive)
- Reverse Lookup (active)
- BruteForce (active++)
- Mail headers (active)
- smtp (active++)
Zone-Transfer - DIG

request: dig @srv.weak.dns weak.dns -t AXFR

brad@rt001:/root$ dig @srvr.weak.dns -t AXFR weak.dns

; <<>> DiG 9.2.4 <<< @srvr.weak.dns -t AXFR weak.dns
;; global options:  printcmd
weak.dns. 3600 IN SOA ns.weak.dns. hostmaster.weak.dns. 2005061602
 3600 900 600000 3600
weak.dns. 3600 IN NS ns.weak.dns.
weak.dns. 3600 IN NS ns2.weak.dns.
weak.dns. 3600 IN NS some.weak.dns.
weak.dns. 3600 IN NS other.weak.dns.
weak.dns. 3600 IN MX 10 mail-in.weak.dns.
weak.dns. 3600 IN MX 200 relay1.weak.dns.
weak.dns. 3600 IN A x.x.x.x
filer0-501.weak.dns. 3600 IN A x.x.x.x
xxx-xx-xxx-xx.weak.dns. 3600 IN A x.x.x.x
xxx-xx-xxx-xx.weak.dns. 3600 IN A x.x.x.x
DNS bruteforce

Domain: target.com

Discoverd hosts:
afrodita
target
neo

Dictionary
afrodita ★
hermes ✗
matrix ✗
target ★
...
Mail Headers

Received: from smtp.example.com (6.Net-45-12-192.dynamicIP.example.net [192.12.45.6])
  by mail.example.org (Postfix) with ESMTP id 0AB0E147B1

Received: from smtp.example.com (smtp.example.com [172.18.5.21])
  by mx1.example.com (8.11.6/8.11.6) with ESMTP id i82sokwis;

Received: from vaio (172.16.1.100)
  by smtp.example.com (Postfix) with ESMTP id i82shwk;

X-Mailer: Microsoft Office Outlook, Build 11.0.5510

User-Agent: Thunderbird 1.5.0.7 (Windows/20060909)

X-Mailer: ColdFusion MX Application Server

X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.2962

X-Mailer: Evolution 2.2.3 (2.2.3-4.fc4)

X-Mailer: iPlanet Messenger Express 5.2 Patch 2 (built Jul 14 2004)
Obtaining **user info** - Classic

- Search engines (passive)
- Web pages (active)
New sources for I.G ...
Obtaining host and Domains info

- Search Engines (passive)
- Public PGP key servers (passive)
- serversniff.net and others (passive)
Obtaining **host and Domains** - Search engines **Passive**

---

**La Web**

La Web | Imágenes | Noticias | Maps | Grupos | Más |
--- | --- | --- | --- | --- | ---

**La Web** Resultados 1 - 10 de aproximadamente 13.100.000 de "nasa.gov". (0,04 segundos)

**NASA - Home** - [Traduce esta página]

The nasa.gov site requires that JavaScripts be enabled in your browser. ... Follow this link to go to the text only version of nasa.gov ...

www.nasa.gov - 69k - En caché - Páginas similares

**Space Shuttle**

**STEREO - The Sun in 3D**

**MULTIMEDIA**

**News - Highlights**

**Missions - Highlights**

Más resultados de nasa.gov

---

**Ciencia @ NASA**

Reportajes científicos sobre astronomía, ciencias espaciales, física y biología.

ciencia.nasa.gov - 17k - En cache - Páginas similares

---

**El Sol se voltea**

Actualizaciones sobre la misión de la sonda Ulises se pueden encontrar en Internet por el JPL en http://Alyssette.jpl.nasa.gov ...

---

**Imágenes Interactivas de Satélites Meteorológicos - Geostacionarios**

---

**The Space Place :: Inicio**

Informaciones, juegos, entretenimientos y curiosidades sobre el mundo espacial.

---

**Exploración de Marte: Reseña general**

El sol detrás del limbo de Marte Desde nuestra primera foto detallada de Marte tomada en 1965, viajes de sondas espaciales al planeta rojo han revelado un...

---

**subdomain**
Obtaining host and Domains info

The PGP public key servers are only intended to help the user in exchanging public keys.

http://keyserver.veridis.com/

Obtaining host and Domains info

subdomains
Obtaining **host and Domains**

Subdomainer

```
glast.gsfc.nasa.gov ===> 128.183.246.122
isscp.gsfc.nasa.gov ===> 169.154.204.82
aura.gsfc.nasa.gov ===> 128.183.212.218
www.cdscc.nasa.gov ===> 203.37.69.18
nightsky.jpl.nasa.gov ===> 128.149.224.62
microgravityuniversity.jsc.nasa.gov ===> 198.122.144.106
rapidfire.sci.gsfc.nasa.gov ===> 169.154.196.76
neat.jpl.nasa.gov ===> 137.78.178.64
earthobservatory.nasa.gov ===> 128.183.183.247
opensource.arc.nasa.gov ===> 128.102.182.85
climate.gsfc.nasa.gov ===> 128.183.182.137
nmma.msfc.nasa.gov ===> 198.122.199.248
www.wstf.nasa.gov ===> 130.135.110.42
asrs.arc.nasa.gov ===> 128.102.2.185
career.launch.jpl.nasa.gov ===> 128.149.128.44
echo.jpl.nasa.gov ===> 137.78.253.36
onearth.jpl.nasa.gov ===> 128.149.132.199
mediaarchive.ksc.nasa.gov ===> 198.119.202.51
education.gsfc.nasa.gov ===> 128.183.244.216
istp.gsfc.nasa.gov ===> 128.183.198.25
ghrc.msfc.nasa.gov ===> 198.122.199.239
sec.gsfc.nasa.gov ===> 128.183.169.196
esc.nasa.gov ===> 128.183.112.197
gen.gsfc.nasa.gov ===> 128.183.248.45
theamall.gsfc.nasa.gov ===> 128.183.16.143
ndrd.gsfc.nasa.gov ===> 128.183.102.288
```

```
liberacion:/tools/edge/edgesec/subdomainer root# ```
Once we have some host names, we can improve our dictionary using Google sets, and then try a brute force attack on the dns.
Obtaining host and Domains

Subdomainer
WikiScanner

- Company IP ranges
- Anonymous Wikipedia edits, from interesting organizations
- http://wikiscanner.virgil.gr/
WikiScanner - IP ranges

<table>
<thead>
<tr>
<th>IP Range</th>
<th>Name</th>
<th>Domain</th>
<th>Location</th>
<th>EN edits</th>
<th>DE edits</th>
<th>JA Edits</th>
</tr>
</thead>
<tbody>
<tr>
<td>171.159.129.0-160.231.255</td>
<td>Bank Of America</td>
<td>pacbell.net [web]</td>
<td>Concord, California, United States</td>
<td>1396</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>171.161.160.0-255</td>
<td>Bank Of America</td>
<td>pacbell.net [web]</td>
<td>Dallas, Texas, United States</td>
<td>990</td>
<td>8</td>
<td>0</td>
</tr>
<tr>
<td>171.159.64.0-255</td>
<td>Bank Of America</td>
<td>pacbell.net [web]</td>
<td>Walnut Creek, California, United States</td>
<td>827</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>171.161.224.0-255</td>
<td>Bank Of America</td>
<td>bankofamerica.com [web]</td>
<td>Charlotte, North Carolina, United States</td>
<td>605</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>171.191.65.0-196.96.255</td>
<td>Bank Of America</td>
<td>pacbell.net [web]</td>
<td>Concord, California, United States</td>
<td>223</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>171.161.96.0-255</td>
<td>Bank Of America</td>
<td>bankofamerica.com [web]</td>
<td>Pasadena, California, United States</td>
<td>199</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>171.158.6.0-159.63.255</td>
<td>Bank Of America</td>
<td>davita.com [web]</td>
<td>Concord, California, United States</td>
<td>103</td>
<td>38</td>
<td>0</td>
</tr>
<tr>
<td>171.160.233.0-161.95.255</td>
<td>Bank Of America</td>
<td>pacbell.net [web]</td>
<td>Concord, California, United States</td>
<td>82</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>171.159.128.0-255</td>
<td>Bank Of America</td>
<td>bankofamerica.com [web]</td>
<td>Chicago, Illinois, United States</td>
<td>22</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>63.148.5.0-63</td>
<td>Woori America Bank</td>
<td>qwest.net [web]</td>
<td>Flushing, New York, United States</td>
<td>19</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>206.229.105.0-63</td>
<td>First National Bank Of America</td>
<td>-</td>
<td>East Lansing, Michigan, United States</td>
<td>14</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>69.208.102.112-119</td>
<td>Mid America Bank</td>
<td>-</td>
<td>Chicago, Illinois, United States</td>
<td>9</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
WikiScanner - Wikipedia edits

Found 22 edits within 171.159.128.0-255

Submit your favorite edits to Wired's 27bstroke6.

<table>
<thead>
<tr>
<th>ip</th>
<th>title</th>
<th>diff</th>
<th>comment</th>
<th>time</th>
</tr>
</thead>
<tbody>
<tr>
<td>171.159.128.10</td>
<td>Bosch reaction [cur]</td>
<td>4928021</td>
<td></td>
<td>2004-06-25 14:10:03</td>
</tr>
<tr>
<td>171.159.128.10</td>
<td>Evangelical Lutheran Synod [cur]</td>
<td>13907709</td>
<td>/* History */</td>
<td>2005-03-30 16:13:13</td>
</tr>
<tr>
<td>171.159.128.10</td>
<td>Fencing [cur]</td>
<td>4821554</td>
<td>/* Notable modern fencers and fencing masters */</td>
<td>2004-07-23 19:16:12</td>
</tr>
<tr>
<td>171.159.128.10</td>
<td>IBM Rational ClearCase [cur]</td>
<td>4260457</td>
<td></td>
<td>2004-06-24 17:54:29</td>
</tr>
<tr>
<td>171.159.128.10</td>
<td>MediaWiki talk:RecentChangesText [cur]</td>
<td>4021222</td>
<td>/* Requested Articles */</td>
<td>2004-06-10 18:13:44</td>
</tr>
<tr>
<td>171.159.128.10</td>
<td>MOD (file format) [cur]</td>
<td>7042652</td>
<td>/* Software */</td>
<td>2004-09-21 15:54:12</td>
</tr>
<tr>
<td>171.159.128.10</td>
<td>Prior art [cur]</td>
<td>5147269</td>
<td>/* First-to-file systems */</td>
<td>2004-08-11 18:38:52</td>
</tr>
<tr>
<td>171.159.128.10</td>
<td>Terraforming [cur]</td>
<td>4263486</td>
<td>/* In fiction */</td>
<td>2004-06-24 19:54:23</td>
</tr>
<tr>
<td>171.159.128.10</td>
<td>Terraforming [cur]</td>
<td>4264707</td>
<td>/* History */</td>
<td>2004-06-24 21:45:24</td>
</tr>
<tr>
<td>171.159.128.10</td>
<td>Terraforming [cur]</td>
<td>4264749</td>
<td>/* Ethical issues */</td>
<td>2004-06-24 21:50:27</td>
</tr>
<tr>
<td>171.159.128.10</td>
<td>Vladimir Nazlymov [cur]</td>
<td>4810524</td>
<td></td>
<td>2004-07-23 22:17:46</td>
</tr>
<tr>
<td>171.159.128.10</td>
<td>Vladimir Nazlymov [cur]</td>
<td>4810835</td>
<td></td>
<td>2004-07-23 22:35:51</td>
</tr>
<tr>
<td>171.159.128.10</td>
<td>Vladimir Nazlymov [cur]</td>
<td>4810984</td>
<td></td>
<td>2004-07-23 22:36:34</td>
</tr>
</tbody>
</table>
Obtaining **user info** - New sources

- PgP key servers (passive)
- Social Networks (passive)
- Metadata (passive)
Obtaining **user info** - New sources

- **Social networks**

  LinkedIn is an online network of more than 15 million experienced professionals from around the world, representing 150 industries.
Obtaining user info - New sources

Current Job
Past Jobs
Education
Job description
Etc...
Obtaining user info - New sources
Obtaining user info - theHarvester

```
libe liber Julie Atwood
**** Pete Langlois
*The Megumi Nordby
*Coc Eric Dawson
*Edq Tobey Fitch
*cmc Solomon Eljashev
**** Conrad Klahn
Jennifer Dockery
Neil Saunders
Usaq Lance Hoffman
Roy Riccomini
Nick Hodge
Ellen Pellens
Bill Stevenson
Matthew Formica
Michael Agustin
Dave Falkenburg
Carsten Brinkschulte
Stewart Hopkirk
Exan Steve Flinn
Eric Shultz
Phil Kirschner
Noelle Gonzalez
libe Danese Cooper
Ben DeVries
Kathy Tafel
Joe Interisano
Mark Leabo
Gregor Purdy
Joe Jasinskas
Nicholas Volodimer
Kati Lechner
Pete Petras

Total results: 71
```

liberation:/tools/edge/edgesec/theHarvester root#
Obtaining **Emails** - theHarvester

```
liberacion:/tools/edge/edgesec/theHarvester root# python theHarvester.py -d "nasa.gov" -l 100 -b google

****************************************************
TheHarvester Ver. 1.4  *
*Coded by laramies  *
*Edge-Security Research  *
*cmartorella@edge-security.com  *
****************************************************

Searching for nasa.gov in google:

Total results: 12700000
Limit: 100
Searching results: 0

Accounts found:

jim.arnold@msfc.nasa.gov
paul.meyer@msfc.nasa.gov
globus@nas.nasa.gov
help@sti.nasa.gov
earthweb@mail.nasa.gov
histinfo@hq.nasa.gov
E.Larko@nasa.gov
steven.m.graham.2@gsfc.nasa.gov
starchild@heasarc.gsfc.nasa.gov
espendak@gsfc.nasa.gov
piercedagnes.gsfc.nasa.gov
access@mail.arc.nasa.gov

Total results: 12
liberacion:/tools/edge/edgesec/theHarvester root#  
```
Online tools

- ServerSniff.net:
  - NameServers reports (NS)
  - Autonomous Systems reports (AS)
  - Virtual hosts
Serversniff  MX and NS Graphs
Obtaining more data - New sources

**Metadata**: is data about data.

Is used to facilitate the understanding, use and management of data.
Obtaining more data - New sources
- Metadata

Provides basic information such as the author of a work, the date of creation, links to any related works, etc.
# Metadata - Dublin Core (schema)

<table>
<thead>
<tr>
<th>Content &amp; about the Resource</th>
<th>Intellectual Property</th>
<th>Electronic or Physical manifestation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>Author or Creator</td>
<td>Date</td>
</tr>
<tr>
<td>Subject</td>
<td>Publisher</td>
<td>Type</td>
</tr>
<tr>
<td>Description</td>
<td>Contributor</td>
<td>Format</td>
</tr>
<tr>
<td>Language</td>
<td>Rights</td>
<td>Identifier</td>
</tr>
<tr>
<td>Relation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Coverage</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Metadata - example

software - Adobe ImageReady
size - 1501x391
mimetype - image/png

software - www.inkscape.org
size - 1501x379
mimetype - image/png
EXIF Exchangeable Image File Format

- GPS coordinates
- Time
- Camera type
- Serial number

Sometimes unaltered original photo can be found in thumbnail Online exif viewer.
Metadata - EXIF - Harry Pwner

Deathly EXIF?
So where can we get interesting metadata?
Ok, I understand metadata... so what?
Metagoofil

- Metagoofil is an information gathering tool designed for extracting metadata of public documents (pdf, doc, xls, ppt, etc) availables in the target/victim websites.
Metagoofil

- User names
- Workers names
- Server names
- Paths
- Software versions + Date
- Mac Address
[PPT] **Annual Procurement Report**
File Format: Microsoft Powerpoint - View as HTML
1. 2. Source: Code 210. * Includes NASA HQ. NASA GSFC* Procurement Personnel ...
[URL] www.gsfc.nasa.gov/APRFY20031.ppt - Similar pages

[PPT] **www.nasa.gov/ppt/47355main_Headquar.ppt**
File Format: Microsoft Powerpoint - View as HTML
NASA NPG 7120.5A Town Hall. Agenda: Welcome and Introductions - Chris Christensen;
Agency Perspective - General Dailey; NPG 7120.5A Overview - Carolyn ...
Similar pages

[PPT] **MAGNETIC FIELD USES SOUND WAVES TO IGNITE SUN'S RING OF FIRE**
File Format: Microsoft Powerpoint - View as HTML
MAGNETIC FIELD USES SOUND WAVES TO IGNITE SUN'S RING OF FIRE. Stuart
Jeffries, University of Hawaii. HI. Viggo Hansteen, University of Oslo, Norway ...
[URL] www.nasa.gov/ppt/178222main_nasa_press_no_comment.ppt - Similar pages

[PPT] **www.nasa.gov/ppt/119097main_Marks.ppt**
File Format: Microsoft Powerpoint - View as HTML
1. NOAA 2005 Hurricane Field Program — Intensity Forecast Experiment (IFEX) Frank Marks
NOAA/AOML Hurricane Research Division ...
Similar pages

[PPT] **www.nasa.gov/ppt/118984main_heymsfield_telcon_slid...**
File Format: Microsoft Powerpoint - View as HTML
ER-2 Doppler Radar (EDOP), Cloud Radar System (CRS), MODIS Airborne Simulator (MAS),
Advanced Microwave Precipitation Radiometer (AMPR) / Lightning ...
Metagoofil

Downloaded files

ppt 1

ppt 2

ppt 3

ppt n

libextractor / filtering

Results.html
http://lwscience.gsfc.nasa.gov/Townsend_LWSWG.ppt

Local copy Open

Important metadata:

mimetype - application/vnd.ms-powerpoint
paragraph count - 181
last saved by - Lt
creation date - 2004-04-03T23:16:58Z
title - PowerPoint Presentation
word count - 974
creator - Lt
date - 2004-04-06T12:42:45Z
generator - Microsoft PowerPoint

http://saber.larc.nasa.gov/03SABER_non_LTE_algo_approach.ppt

Local copy, failed download :

http://larc.nasa.gov/library/Analysis_L7ImageryPurchases_110501.ppt

Local copy Open

Important metadata:

mimetype - application/vnd.ms-powerpoint
paragraph count - 123
last saved by - BMK52
template - C:\Documents and Settings\m10282\Application Data\Microsoft\Templates\mtak_briefing.pot
creation date - 2001-09-21T21:26:00Z
title - TitleHere
word count - 520
page count - 3
creator - Nitrotek Systems
date - 2001-11-08T13:26:22Z
generator - Microsoft PowerPoint 4.0

http://gsfetechology.gsfc.nasa.gov/Code550procurement02012005.ppt
### MetaGoofil - results

1. **http://weboflife.nasa.gov/1202.doc**
   - Local copy: Open
   - Important metadata:
     - **Mimetype**: application/msword
     - **Revision history**: Revision #0: Author 'Philip T. Metzger' worked on
     - **Language**: U.S. English
     - **Paragraph count**: 2
     - **Line count**: 10
     - **Last saved by**: Philip T. Metzger
     - **Character count**: 1258
     - **Template**: Normal.dot
     - **Creation date**: 2005-01-03T13:33:00Z
     - **Title**: Penetrometer Testing of Transparent Granular Medium
     - **Word count**: 220
     - **Page count**: 1
     - **Creator**: Naahiro Toiya
     - **Date**: 2005-01-03T13:33:00Z
     - **Generator**: Microsoft Word 10.0

2. **http://weboflife.nasa.gov/0704.doc**
   - Local copy: Open
   - Important metadata:
     - **Mimetype**: application/msword
     - **Revision history**: Revision #0: Author 'Philip T. Metzger' worked on
     - **Language**: U.S. English
     - **Paragraph count**: 2
     - **Line count**: 8
     - **Last saved by**: Philip T. Metzger
     - **Character count**: 1004
     - **Template**: Normal.dot
     - **Creation date**: 2005-01-03T17:01:00Z
     - **Title**: Rapid Relaxation of a Granular Step
     - **Word count**: 175
     - **Page count**: 1
     - **Creator**: ekadrolili
     - **Date**: 2005-01-03T17:01:00Z
     - **Generator**: Microsoft Word 10.0
<table>
<thead>
<tr>
<th>URL</th>
<th>Local copy</th>
<th>Important metadata</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://imdc.nasa.gov/IMDCPrework.xls">http://imdc.nasa.gov/IMDCPrework.xls</a></td>
<td>Open</td>
<td>mimetype = application/vnd.ms-excel&lt;br&gt;last saved by = jehulanajones&lt;br&gt;creation date = 2006-08-11T18:35:34Z&lt;br&gt;title = Mission Requirements&lt;br&gt;creator = tawhiter&lt;br&gt;date = 2005-10-24T15:51:95Z&lt;br&gt;generator = Microsoft Excel</td>
</tr>
<tr>
<td><a href="http://www.nasa.gov/xls/151027main_121TVSked.xls">http://www.nasa.gov/xls/151027main_121TVSked.xls</a></td>
<td>Open</td>
<td>mimetype = application/vnd.ms-excel&lt;br&gt;last saved by = IMIT-ODIN&lt;br&gt;subject = STS-89 TV Schedule&lt;br&gt;creation date = 1997-02-05T21:58:03Z&lt;br&gt;title = STS TV Sked&lt;br&gt;creator = Eileen Walsh&lt;br&gt;date = 2005-06-29T18:58:27Z&lt;br&gt;generator = Microsoft Excel</td>
</tr>
<tr>
<td><a href="http://www.nasa.gov/xls/163559main_LunarExplorationObjectives.xls">http://www.nasa.gov/xls/163559main_LunarExplorationObjectives.xls</a></td>
<td>Open</td>
<td>mimetype = application/vnd.ms-excel&lt;br&gt;last saved by = Aurey Schaifer&lt;br&gt;creation date = 2006-06-19T14:20:24Z&lt;br&gt;creator = IMIT-ODIN&lt;br&gt;generator = Microsoft Excel</td>
</tr>
</tbody>
</table>
http://www.nasa.gov/doc/47147main_pmsepstruc.doc

Local copy Open

Important metadata:

mimetype - application/msword
revision history - Revision #9: Author 'Jennifer Romeo' worked on 'romeo HD:Documents:Articles & News:Articles_PMSEPs\PMSEP & Conference Structure'
revision history - Revision #8: Author 'jiater' worked on '\\RGINTS\NasaShared\PMSEP\PMSEP & Conference Structure'
revision history - Revision #7: Author 'John Newcomb' worked on 'C:\My Documents\Scientific Man\Current Programs'
revision history - Revision #6: Author 'Edutech User' worked on 'C:\My Documents\PMSEP Detailed Structure 8-9-02'
revision history - Revision #5: Author 'Edutech User' worked on 'C:\My Documents\PMSEP Detailed Structure 8-9-02'
revision history - Revision #4: Author 'Edutech User' worked on 'C:\My Documents\PMSEP Detailed Structure 8-7-02'
revision history - Revision #3: Author 'Edutech User' worked on 'C:\My Documents\PMSEP Detailed Structure 8-7-02'
revision history - Revision #2: Author 'Edutech User' worked on 'C:\WINDOWS\Temporary Internet Files\OLK4\PMSEP Detailed Structure 8-7-02'
revision history - Revision #1: Author 'Edutech User' worked on 'C:\Documents and Settings\krobinson\Application Data\Microsoft\Windows NT\CurrentVersion\Run\mets.exe'
revision history - Revision #0: Author 'Edutech User' worked on 'C:\Documents and Settings\krobinson\Application Data\Microsoft\Windows NT\CurrentVersion\Run\mets.exe'

language - U.S. English
paragraph count - 13
line count - 55
last saved by - Jennifer Romeo
character count - 6717
template - Normal
creation date - 2002-08-12T14:24:00Z
title - CONFERENCE STRUCTURE
word count - 1178
page count - 5
creator - John Newcomb
date - 2002-08-12T14:24:00Z
generator - Microsoft Word 9.0
Metagoofil - results

Path Disclosure:

C:\Documents and Settings\baltner\Application Data\Microsoft\Word
C:\ISEM\MyProjects\XLCTIO\projectPlan\C:\Documents and Settings\benedic\My Documents\XML\NASA XML\XML Business Case\Final Business Case

Normal
C:\WINNT\Personal\U:\users\smarucci\AI\Writing\Internet\HOMEPAGE\cs\U:\code_hk\Competitive Sourcing\Ten Year Look Back\C:\Documents and Settings\jlecren\Application Data\Microsoft\Word\C:\My Documents\ZLdp\Website\2005 Web Site Update\Reports\C:\My Documents\ZLdp\2005-06\Orientation\Participants\Orientation Binder\Section D Reports\C:\My Documents\ZLdp\2005-06\Orientation\Participants\Orientation Binder\Section D\C:\My Documents\ZLdp\2004-05\Orientation\Participants\Orientation Binder\Section D\C:\My Documents\ZLdp\Website\2004 Update\1 Reports\C:\Documents and Settings\benedic\Application Data\Microsoft\Word\C:\Documents and Settings\benedic\My Documents\XML\NASA XML\NASA XML Project Plan\NASA XML Project Plan Revision\\RGINTS\NASAshared\PMSEP\PMSEP 6\Structure\C:\My Documents\Scientific Man\Current Programs\EduTech Work\PMSEP Folder\Structure\Present Structure\C:\My Documents\C:\WINNT\Temporary Internet Files\OLK4\C:\Documents and Settings\krobinson\Application Data\Microsoft\Word\U:\users\kbayer\TOY03\C:\Documents and Settings\u4ri9mah\My Documents\Rocket Blast\KSC Meeting\C:\Documents and Settings\u4ri9mah\Application Data\Microsoft\Word\C:\Documents and Settings\pcurto\Desktop\N:\A:\C:\Documents and Settings\akeneddy\My Documents\Data\attach\U:\users\kbayer\DATA\Word\Macintosh HD:Users\mis\Documents\student travel:Hemispheresapp\Macintosh HD:Documents\student travel:Hemispheresapp\Macintosh HD:Documents\student travel:astrobiosis workshop:ABstudentapp\Macintosh HD:Users\mis\Desktop:astrobiosis workshop:ABstudentapp\C:\Documents and Settings\lucero james\Desktop\C:\Documents and Settings\ceccilia desktop\E\Desktop\FY03FDP\Descrip\C:\Documents and Settings\ceccilia desktop\E\Desktop\FY03FDP\E:\ACE\CECILIA\Word8998\P09\Aug99\\Gwen Young:Desktop Folder\Gwen\C:\Program Files\Microsoft Office\Templates\Presentation Designs\D:Microsoft Office\Templates\Presentation Designs\C:\Program Files\Office2K\Templates\Presentation Designs\Macintosh HD:Users:pmhughes:Documents:PH's Docs:*Peter's Data*:*GSFC R&TD:*:FY07 R&T Planning:FY07 IntegInv
Metagoofil & Linkedin results

- Now we have a lot of information, what can I do?
  - User profiling
  - Spear Phishing / Social Engineering
  - Client side attacks
Using results

- User profiling

- Dictionary creation for John Doe

```
john.doe
jdoe
j.doe
johndoe
johnd
john.d
jd
doe
doe
john
```

ATTACK!
Tool developed by Michal Zalewski, this tool will extract comments and "Track changes" from Word documents.


Finally, Microsoft is an enduring company that's not going out of business (unlike many Linux vendors). We're committed to providing IT flexibility and growth options to our customers so they can continue to rely on their Microsoft-based IT infrastructure to quickly respond to a competitive marketplace.
Target information:

- Email account
- Google Finance, Reuters
- pipl.com
- Usercheck.com
Google Finance & Reuters

**Officers and directors**

- **Kenneth D. Lewis**: Chairman of the Board, President, Chief Executive Officer
- **Joe L. Price**: Chief Financial Officer
- **Barbara J. Desoer**: President of the New Bank of America Mortgage, Home Equity & Insurance Services Business
- **Liam E. McGee**: President - Global Consumer and Small Business Banking
- **Brian T. Moynihan**: President - Global Corporate and Investment Banking
- **Keith T. Banks**: President - Global Wealth and Investment Management
- **Bruce L. Hammonds**: President - Global Card Services
- **Craig R. Rosato**: Chief Accounting Officer
- **J. Steele Alphin**: Chief Administrative Officer
- **Amy Woods Brinkley**: Global Risk Executive

**Summary**

<table>
<thead>
<tr>
<th>Name</th>
<th>Age</th>
<th>Since</th>
<th>Current Position</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desoer, Barbara</td>
<td>55</td>
<td>2008</td>
<td>President of the New Bank of America Mortgage, Home Equity &amp; Insurance Services Business</td>
</tr>
<tr>
<td>Banks, Keith</td>
<td>52</td>
<td>2007</td>
<td>President - Global Wealth and Investment Management</td>
</tr>
<tr>
<td>Moynihan, Brian</td>
<td>48</td>
<td>2007</td>
<td>President - Global Corporate and Investment Banking</td>
</tr>
<tr>
<td>McGee, Liam</td>
<td>53</td>
<td>2004</td>
<td>President - Global Consumer and Small Business Banking</td>
</tr>
<tr>
<td>Hammonds, Bruce</td>
<td></td>
<td>2008</td>
<td>President - Global Card Services</td>
</tr>
<tr>
<td>Sloan, O. Temple</td>
<td>69</td>
<td>2006</td>
<td>Lead Director</td>
</tr>
<tr>
<td>Brinkley, Amy</td>
<td>52</td>
<td>2008</td>
<td>Global Risk Executive</td>
</tr>
<tr>
<td>Massey, Walter</td>
<td>70</td>
<td>1998</td>
<td>Director</td>
</tr>
<tr>
<td>Spangler, Meredith</td>
<td></td>
<td>1988</td>
<td>Director</td>
</tr>
<tr>
<td>Ward, Jacquelyn</td>
<td>70</td>
<td>1994</td>
<td>Director</td>
</tr>
<tr>
<td>Mitchell, Patricia</td>
<td>65</td>
<td>2001</td>
<td>Director</td>
</tr>
<tr>
<td>Gifford, Charles</td>
<td>65</td>
<td>2005</td>
<td>Director</td>
</tr>
<tr>
<td>Barnet, William</td>
<td>65</td>
<td>2004</td>
<td>Director</td>
</tr>
<tr>
<td>Collins, John</td>
<td>61</td>
<td>2004</td>
<td>Director</td>
</tr>
<tr>
<td>Countryman, Gary</td>
<td>68</td>
<td>2004</td>
<td>Director</td>
</tr>
<tr>
<td>May, Thomas</td>
<td>60</td>
<td>2004</td>
<td>Director</td>
</tr>
<tr>
<td>Ryan, Thomas</td>
<td>55</td>
<td>2004</td>
<td>Director</td>
</tr>
<tr>
<td>Franks, Tommy</td>
<td>62</td>
<td>2005</td>
<td>Director</td>
</tr>
<tr>
<td>Bramble, Frank</td>
<td>59</td>
<td>2006</td>
<td>Director</td>
</tr>
<tr>
<td>Tillman, Robert</td>
<td>64</td>
<td>2005</td>
<td>Director</td>
</tr>
<tr>
<td>Lozano, Monica</td>
<td>51</td>
<td>-</td>
<td>Director</td>
</tr>
</tbody>
</table>
Searching for a target
Using results

- Password profiling

Dictionary creation: words from the different user sites

- magic
- serra angel
- necropotence
- Shivan dragon
- elf
- brainstorm
- ...
- ...

Brute force ATTACK
There are more ways to get info.
Kyle Doyle's Facebook profile makes it quite obvious he was not off work for a 'valid medical reason'.
All together - Maltego

Maltego is “the only” professional Information Gathering tool.

“Information is power
Information is Maltego”
Maltego
Conclusions

- Clean your files before distribution
- Web applications should clean files on upload (if it’s not needed)
- Web applications should try to represent the information in a nonlicable way :/
- Be careful what you post/send
References

- www.edge-security.com
- blog.s21sec.com
- www.s21sec.com
- carnal0wnage.blogspot.com
- www.gnunet.org/libextractor
- lcamtuf.coredump.cx/strikeout/
- www.paterva.com
Thank you for coming

cmartorella@s21sec.com
cmartorella@edge-security.com