Modern information gathering

Dave van Stein
9 april 2009
Who Am I

✓ Dave van Stein
✓ 34 years
✓ Functional tester > 7 years
✓ Specializing in (Application) Security Testing
✓ “Certified Ethical Hacker”
Agenda

- Goal of the presentation
- What is Information Gathering?
- Domain scanning
- Search engine ‘abuse’
- Other tools
- Some Social Engineering
- Remedies
- Conclusions
Goal of this presentation

✓ Give insight in amount of information anonymously available on internet about your system (and users)

✓ Give insight in the amount and possibilities of tools freely available
Intermezzo: How to hack

✓ Identify entrypoint
✓ Gain access
✓ Secure access
✓ Do stuff
✓ Clear up the mess
✓ Come back another time

(simplified procedure)
Information Gathering

✓ Information gathering scans for:
  - Domains and subdomains
  - IP addresses
  - Applications and technologies
  - Hotspots (known vulnerabilities)
  - Usernames and passwords
  - Sensitive information

✓ Not only identifying risks, but also risk on exposure and exploiting
Passive Reconnaissance

- Information gathering, fingerprinting
- Gaining information about a target

Passive

- Without making contact with target
- No direct scanning, no intrusion
- No logging and no alarm triggering!
Sources of information

✓ Public records
  - WHOIS: information about owner
  - DNS: information about IP addresses
  - Necessary for network functionality

✓ Search engines
  - Often little restrictions on websites
  - Cache all information gathered
Tools

✔️ What do you need?
  - Webbrowser
  - Internet access
  - Creativity

✔️ Advanced and Automated scanning:
  - Specialized (offline) Tools
'Classic' Domain Scanning

✔ Steps involved:
- Get network information with ping and traceroute
- Get DNS information with WHOIS and LOOKUP
- Do DNS zone transfer for subdomains
- Download website for extra info
- Scan servers

✔ Problems:
- DNS zone transfers often not authorized
- Active connection with target => detectable
‘Modern’ Domain Scanning

✓ Various websites
  – Anonymous
  – Combination of techniques
  – Sort results for nice presentation

✓ Search engine ‘tweaking’
  – Additional information linked to domain

→ Some examples
Server Sniff
- NS reports
- Domain reports
- Subdomains
- Various (trace)routes
- Various ping types
- Shows robots.txt
- Anonymous!
Domain Scanning: Server Sniff

Recursive Queries:

- ns1.secure.net. YES - recursive queries allowed!
- ns2.secure.net. YES - recursive queries allowed!

NS-AVRP:

- ns1.secure.net: Anonymous ZoneTransfer (AVRP) allowed!!
- ns2.secure.net: Anonymous ZoneTransfer (AVRP) allowed!!

owasp.org. 86400 IN SOA ns1.secure.net. hostmaster.secure.net. 200708332 86400 7200 2192000 86400
owasp.org. 86400 IN A 216.48.3.18
owasp.org. 86400 IN NS ns2.secure.net.
owasp.org. 86400 IN NS ns1.secure.net.
owasp.org. 86400 IN MX 30 ASPMCL.GOOGLE.COM.
owasp.org. 86400 IN MX 30 ASPMCL.GOOGLE.COM.
owasp.org. 86400 IN MX 30 ASPMCL.GOOGLE.COM.
owasp.org. 86400 IN MX 30 ASPMCL.GOOGLE.COM.
owasp.org. 86400 IN MX 10 ASPMCL.GOOGLE.COM.
owasp.org. 86400 IN MX 10 ALTL2.ASPMCL.GOOGLE.COM.
owasp.org. 86400 IN MX 20 ALTL2.ASPMCL.GOOGLE.COM.
owasp.org. 86400 IN MX 20 ALTL2.ASPMCL.GOOGLE.COM.
owasp.org. 86400 IN MX 20 ALTL2.ASPMCL.GOOGLE.COM.
owasp.org. 86400 IN MX 20 ALTL2.ASPMCL.GOOGLE.COM.
owasp.org. 86400 IN MX 20 ALTL2.ASPMCL.GOOGLE.COM.
owasp.org. 86400 IN MX 20 ALTL2.ASPMCL.GOOGLE.COM.
owasp.org. 86400 IN MX 20 ALTL2.ASPMCL.GOOGLE.COM.

OWASP.org. 86400 IN CNAME owasp.org.
austin.owasp.org. 86400 IN CNAME owasp.org.
blogs.owasp.org. 86400 IN CNAME owasp.org.
calendar.owasp.org. 86400 IN CNAME ghs.GOOGLE.COM.
docs.owasp.org. 86400 IN CNAME ghs.GOOGLE.COM.
es.owasp.org. 86400 IN A 216.48.3.18
google6912a08e29cde3c6.owasp.org. 86400 IN CNAME GOOGLE.COM.
jobs.owasp.org. 86400 IN CNAME owasp.org.
lists.owasp.org. 86400 IN MX 10 lists.owasp.org.
lists.owasp.org. 86400 IN MX 20 mailhost.rdurkee.com
localhost.owasp.org. 86400 IN A 216.48.3.12
mail.owasp.org. 86400 IN CNAME ghs.GOOGLE.COM.
old.owasp.org. 86400 IN A 216.48.3.12
registration.owasp.org. 86400 IN CNAME owasp.org.
staging.owasp.org. 86400 IN CNAME owasp.org.
www.owasp.org. 86400 IN A 216.48.3.22
webmail.owasp.org. 86400 IN A 216.48.3.24
owasp.org. 86400 IN SOA ns1.secure.net. hostmaster.secure.net. 200708332 86400 7200 2192000 86400

Copyright © 2008 ps_testware
## Domain Scanning: Robtex

- **Domain ‘Swiss Army Knife’**
  - Provides ALL information linked to a domain

<table>
<thead>
<tr>
<th>base</th>
<th>record</th>
<th>name</th>
<th>ip</th>
<th>reverse</th>
<th>route</th>
<th>as</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>a</td>
<td>ns1.secure.net</td>
<td>216.48.3.18</td>
<td></td>
<td>216.48.2.0/23 Proxy-registered route object</td>
<td>AS1785 FASTINET-ASN</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ns2.secure.net</td>
<td>192.220.124.10</td>
<td></td>
<td>192.220.0.0/16 VROID-192-220</td>
<td>AS2934 NITC GEN ASN</td>
</tr>
<tr>
<td></td>
<td></td>
<td>aspxx1.google.com</td>
<td>64.233.183.27</td>
<td>smtp103.google.com</td>
<td>64.233.182.0/23 Google</td>
<td>AS15169 Google, Inc</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>64.233.183.114</td>
<td>smtp186-2.google.com</td>
<td>64.233.182.0/23 Google</td>
<td>AS15169 Google, Inc</td>
</tr>
<tr>
<td></td>
<td></td>
<td>aspxx2.googlemail.com</td>
<td>209.85.135.27</td>
<td>smtp186-2.google.com</td>
<td>209.85.134.0/23 Google</td>
<td>AS15169 Google, Inc</td>
</tr>
<tr>
<td></td>
<td></td>
<td>aspxx3.googlemail.com</td>
<td>209.85.135.27</td>
<td>smtp186-2.google.com</td>
<td>209.85.134.0/23 Google</td>
<td>AS15169 Google, Inc</td>
</tr>
<tr>
<td></td>
<td></td>
<td>aspxx4.googlemail.com</td>
<td>209.85.135.27</td>
<td>smtp186-2.google.com</td>
<td>209.85.134.0/23 Google</td>
<td>AS15169 Google, Inc</td>
</tr>
<tr>
<td></td>
<td></td>
<td>aspxx5.googlemail.com</td>
<td>209.85.135.27</td>
<td>smtp186-2.google.com</td>
<td>209.85.134.0/23 Google</td>
<td>AS15169 Google, Inc</td>
</tr>
<tr>
<td>org</td>
<td>ptr</td>
<td>dl0.org.afilias-nst.org</td>
<td>66.35.111.73</td>
<td></td>
<td>66.35.111.24</td>
<td>AS14955 N-V-C Norte</td>
</tr>
<tr>
<td></td>
<td></td>
<td>tild1.ultradns.net</td>
<td>204.74.112.1</td>
<td></td>
<td>204.74.111.24 UltraDNS</td>
<td>AS12041 AFILIAS NST</td>
</tr>
<tr>
<td></td>
<td></td>
<td>tild2.ultradns.net</td>
<td>204.74.113.1</td>
<td></td>
<td>204.74.113.24 UltraDNS</td>
<td>AS12041 AFILIAS NST</td>
</tr>
<tr>
<td></td>
<td>ns</td>
<td>a0.org.afilias-nst.info</td>
<td>199.19.56.1</td>
<td></td>
<td>199.19.56.0/24 REACH (Customer Route)</td>
<td>AS12041 AFILIAS NST</td>
</tr>
<tr>
<td></td>
<td></td>
<td>as1.org.afilias-nst.org</td>
<td>199.19.56.1</td>
<td></td>
<td>199.19.56.0/24 REACH (Customer Route)</td>
<td>AS12041 AFILIAS NST</td>
</tr>
</tbody>
</table>

Copyright © 2008 ps_testware
Domain scanning: Robtexit

Copyright © 2008 ps_testware
Domain Scanning ‘on-the-fly’

✔ Passive Recon (Firefox add-on)
Domain Scanning: Live search

✔ Finds subdomains with 'IP:x.x.x.x'

Live Search | MSN | Windows Live

Live Search ip:216.48.3.18

[ ] Alleen Nederlands  [ ] Alleen websites in Nederland

Web 1-10 van 263.000 resultaten · Geavanceerd
Zie ook: Afbeeldingen, Nieuws, Alles weergeven...

ip - www.Marktplaats.nl/telecommunicatie
Duizenden Mobiele Telefoons en Accessoires op Marktplaats.

The Open Web Application Security Project
How to build, design and test the security of web applications and web services.
www.owasp.org · Pagina in cache · Vertaal deze pagina

www.owasp.org
www.owasp.org/local/boston.html · Pagina in cache · Vertaal deze pagina
Meer resultaten weergeven voor www.owasp.org

OWASP Blogs
5 Most Active Blogs
blogs.owasp.org · Pagina in cache · Vertaal deze pagina

Dina Cruz Blog
Live search automated: Webshag

Target [host | IPv4]:
www.owasp.org

Results:
- blogs.owasp.org
- www.owasp.org
- austin.owasp.org
- www.owasp.org
- forums.owasp.org
- owasp.net
- beta.owasp.org
- forum.owasp.org
- b.owasp.org
- www.owasp.fr
- WEBSCARAB.NET
- WEBSCARAB.COM
- webscarab.org

Copy:

Console:
INFO  Domains of 216.48.3.18 retrieved
INFO  Found 13 domains.
Other tools

- Spiderfoot / Wikto
  - Combine DNS / Google / Live Search / Yahoo
- Subdomains
- Directories
- IP’s
- Email addresses
- Usernames
- Systems in use
Maltego

✓ Intelligence and forensics tool

✓ Connects many different sources of info
✓ Represents in graphical way
✓ Very extensive capabilities

✓ Too much to cover in this presentation
✓ http://www.paterva.com/maltego
Modern Domain Scanning

✔ Anonymous
✔ Both online and offline
✔ Highly automated
✔ Graphical network mapping in less than 10 minutes!
✔ Lots of additional information
Google Advanced search

✓ filetype: (or ext:)
  - Find documents of the specified type.
    *E.g. PDF, XLS, DOC*

✓ intext:
  - The terms must appear in the text of the page.

✓ intitle:
  - The terms must appear in the title of the page.

✓ inurl:
  - The terms must appear in the URL of the page.
Google Hacking Database

✓ www.johnny.ihackstuff.com
   (edit: http://johnny.ihackstuff.com/ghdb.php)

✓ Collection of queries for finding ‘interesting’ stuff

✓ Regular updates

Advisories and Vulnerabilities (215 entries)
These searches locate vulnerable servers.

Error Messages (68 entries)
Really retarded error messages that say WA

Files containing juicy info (230 entries)
No usernames or passwords, but interesting

Files containing passwords (135 entries)
PASSWORDS, for the LOVE OF GOD!!! Google

Files containing usernames (15 entries)
These files contain usernames, but no passwords!

Footholds (21 entries)
Examples of queries that can help a hacker

Pages containing login portals (232 entries)
These are login pages for various services.

Pages containing network or vulnerability info
These pages contain such things as firewall

Sensitive Directories (61 entries)
Google’s collection of web sites sharing sen-

Sensitive Online Shopping Info (9 entries)
Examples of queries that can reveal online s
GHD applications

✓ Goolag scanner

Goolag Scanner is a Web auditing tool. It works by exploiting data-retention practices of popular search engines.

- Contains Google Hacking Database
- Automated Google queries
- Automated result interpretation
- Single host or general scan
Goolag scanner

Available Dorks

- Advisories and Vulnerabilities (216)
- Error Messages (68)
- Files containing juicy info (228)
- Files containing passwords (137)
- Files containing usernames (15)
- Footholds (21)
- Pages containing login portals (232)
- Pages containing network or vulnerability data (59)
- Sensitive Directories (60)
- Sensitive Online Shopping Info (9)
- Various Online Devices (202)
- Vulnerable Files (54)
- Vulnerable Servers (46)
- Web Server Detection (71)
More applications

- Modern vulnerability scanners use GHD:
  - IBM Rational Appscan
  - Acunetix Vulnerability Scanner
  - Others

- Several Firefox plug-ins for “on-the-fly” scanning
Google Hacking Database

✔ Possible results of GHD:
  – Identify systems in use (including version)
  – Identify known exploits
  – Locations of sensitive information
  – User-id’s & passwords
  – Logging files
  – Many other things
Yahoo search: file explorer

File explorer for the web


WebLS provides an alternative way of browsing the web. It uses the Yahoo Search Engine API to build a file tree for a specified URL and lets you browse through it. WebLS has many uses, but it was born from curiosity. You can now see what’s behind a website.

Note: Some time after the release of WebLS Yahoo recognized the merit of a tool like WebLS and released their Site Explorer service. For our purpose Site Explorer is much faster and more complete than regular search engine we currently use. I will try to find the time to update WebLS to use this new great new service.
Yahoo search: file explorer

Examples

<table>
<thead>
<tr>
<th>Name</th>
<th>Size</th>
<th>Type</th>
<th>Last modified</th>
</tr>
</thead>
<tbody>
<tr>
<td>index.php</td>
<td>17kB</td>
<td>text/html</td>
<td>Thu, 10 Jul 2008 07:00:00 GMT</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Size</th>
<th>Type</th>
<th>Last modified</th>
</tr>
</thead>
<tbody>
<tr>
<td>be</td>
<td>0kB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>data</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>news</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>references</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>styles</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>function.mysql-List-Tables</td>
<td>0kB text/html</td>
<td>Wed, 18 Jun 2008 07:00:00 GMT</td>
<td></td>
</tr>
<tr>
<td>index.php</td>
<td>8kB</td>
<td>text/html</td>
<td>Wed, 16 Jul 2008 07:00:00 GMT</td>
</tr>
</tbody>
</table>
Other tools

✓ Metagoofil : extract metadata from documents on website
  – User names, server names, path locations, sofware + versions, MAC adresses (!)

✓ Wikiscanner : check comments made on Wikipedia by company or domain
  – Company IP ranges

✓ Several “Social Site” extractors
  – Linkedin, twitter, hyves, etc, etc, etc
Conclusions

✔ What search engines see, hackers can abuse

✔ Many tools are freely available

✔ Networks can be mapped with much detail in minutes

✔ Much information about your company, systems and users available on internet
Remedies (1/2)

✔ Limit access
  - Allow search engines only to see what they need to see. Make sure unauthorized users are not able to look into or even see files they do not need to see. Force possible intruders to use methods that can be scanned and monitored.

✔ Use the tools of hackers
  - Scan your systems with the tools hackers use and check the information that is found. Scan for error messages and other things that reveal information about the system and services and remove them.

✔ Check what spiders can see
  - Use a spider simulator to check what spiders can see and if your application still functions correctly.
Remedies (2/2)

✓ Awareness
  - Be aware of all possible sources of information. Create awareness among employees. Assume all information will possibly abused

✓ Clean documents
  - Remove all metadata from documents before publishing.

✓ Audit frequently
  - Keep your knowledge up-to-date and scan regularly for information that can be found about your systems or hire professionals do to it for you.
Interesting books on the subject

Penetration Tester’s Open Source Toolkit Volume 2
Chris Hurley

Google Hacking for Penetration Testers
Johnny Long

Copyright © 2008 ps_testware