Google attacks

I'm Feeling Lucky

We're in Vegas, right?

Patrick Chambet
Edelweb – ON-X Group
patrick.chambet@edelweb.fr
http://www.edelweb.fr
http://www.chambet.com
Planning

- General points
- Some examples
- Recommendations
- Conclusion
General Points

- Information gathering is the first step during a pen-test (or a real attack)
- A search engine is an obvious and common pen test tool
  - Passive
  - Stealth
  - Uses the huge “memory” of the Net
    - Google cache
    - Google groups
    - www.archive.org
Typical pen-test process

- Information gathering about the target
- Vulnerabilities identification
- Vulnerabilities exploitation
- Go further!
Planning

- General points
- Some examples
- Recommendations
- Conclusion
Some examples (1/7)

- Passive Web server identification
- Invisible corporate HTTP and FTP outgoing proxies detection
- SMTP headers
  - No need to send a fake mail to a non-existent user any more!
- Sensitive files gone offline but still present in Google cache
- Ex-employees, now in competing companies
Some examples (2/7)

<table>
<thead>
<tr>
<th>Google How To</th>
</tr>
</thead>
<tbody>
<tr>
<td>Special chars</td>
</tr>
<tr>
<td>&quot;foo1.foo2&quot; +foo -bar</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Useful Google keywords</th>
</tr>
</thead>
<tbody>
<tr>
<td>filetype:abc</td>
</tr>
<tr>
<td>site:foo.com</td>
</tr>
<tr>
<td>intext:foo</td>
</tr>
<tr>
<td>[all]intitle:footitle</td>
</tr>
<tr>
<td>[all]inurl:foo</td>
</tr>
<tr>
<td>link:www.foo.com</td>
</tr>
<tr>
<td>cache:www.foo.com/bar.html</td>
</tr>
<tr>
<td>related:www.foo.com/bar.html</td>
</tr>
<tr>
<td>phonebook:Bill Gates+WA</td>
</tr>
<tr>
<td>define:foo</td>
</tr>
</tbody>
</table>
Some examples (3/7)

- **Browsing a site “offline”**
  - `site:foo.com foo` → returns every cached page on the site
  - Stealth CGI scanner

- **Passwords**
  - "Index of" htpasswd / passwd
  - `filetype:xls username password email`
  - "WS_FTP.LOG"
  - "config.php"
  - `allinurl: admin mdb`
  - `service filetype:pwd (FrontPage)`
Some examples (4/7)

NTInfoScan

Results

NetBIOS

Share Information

Share Name : U:
Share Type : Default Disk Share
Comment :

Share Name : IPC$
Share Type : Default Pipe Share
Comment : Remote-IPC

WARNING - Null session can be established to \2\0\0\0\0\0\2\IPC$

Share Name : print$
Share Type : Disk
Comment :

WARNING - User's password is *****
Some examples (5/7)

Sensitive files / interesting attack data

- "robots.txt" "Disallow:" filetype:txt
- inurl:_vti_cnf (FrontPage files)
- allinurl:winnt/system32/
- allinurl:/msadc/Samples/selector/showcode.asp
- allinurl:/examples/jsp/snp/snoop.jsp
- allinurl:phpinfo.php
- ipsec filetype:conf
- intitle:"error occurred" ODBC request WHERE (SELECT|INSERT)
- "mydomain.com" nessus report
- "report generated by"
“Help me!” messages

“I have the net-to-net configuration:

\[\begin{align*}
\text{Localhost} & \rightarrow \text{Router} \rightarrow \text{Remotehost} \\
x.x.x.202 & \rightarrow x.x.x.31 \\
x.x.x.205 & \rightarrow x.x.x.32
\end{align*}\]

I work on Linux Red Hat 2.4.18 with x509 patched freeswan 1.99. I have updated my ipsec.conf configuration file with:

```
"conn net-to-net
    left=x.x.x.x
    (..)
"
```

The password is: (just kidding)

My problem is the following: (..)

Please, help me quickly!

Thanks a lot,

Jack"
Some examples (7/7)

- The cache can be used to cover one's tracks
- Search terms can be crafted to include known exploits in them
- Social engineering
  - Personal information about administrators and users
    - Hobbies
    - Skills
    - Expertise and motivation level
    - Friends
    - Etc.
Planning

- General points
- Some examples
- Recommendations
- Conclusion
Recommendations (1/2)

**On your webservers**
- Apply latest security patches and secure the server
- Disable directory browsing
- Don’t put sensitive information without authentication
- Do not rely on scripts/Java/ActiveX URL obfuscation
- Analyze Google queries that conducted to sensitive data on your site (HTTP logs) and modify your site
  - Web-based honeypots and honeytokens
Recommendations (2/2)

u Control Google content
  ŷ Information about your company
  ŷ Information about your users and employees
  ŷ Links pointing to your Web sites
  ŷ Organize a regular watch

u Ask Google to delete some search results from its cache
  ŷ http://www.google.com/remove.html
Conclusion

- Google is the pen-tester’s best friend
  - And also the attacker’s

- You have to pay attention to information leakage on the Web about you
  - A regular watch is necessary

- Do not hesitate to ask for modification or deletion of information about your company
Google
- Google APIs: http://www.google.com/apis/
- Remove results: http://www.google.com/remove.html

http://www.hackingspirits.com/eth-hac/papers/
Demystifying%20Google%20Hacks.pdf

“Googledorks”

http://www.searchlores.org/

http://www.theregister.co.uk/2001/11/28/the_google_attack_engine/

Athena tool
- http://www.buyukada.co.uk/projects/athena/