BlackHat
USA • EUROPE • ASIA
USA 2004

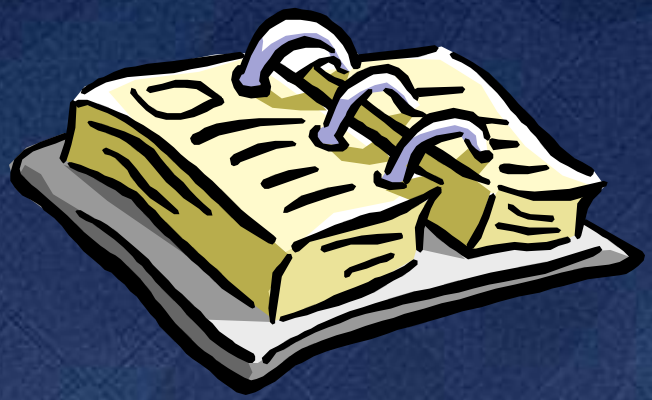
Google attacks

I'm Feeling Lucky

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

Planning

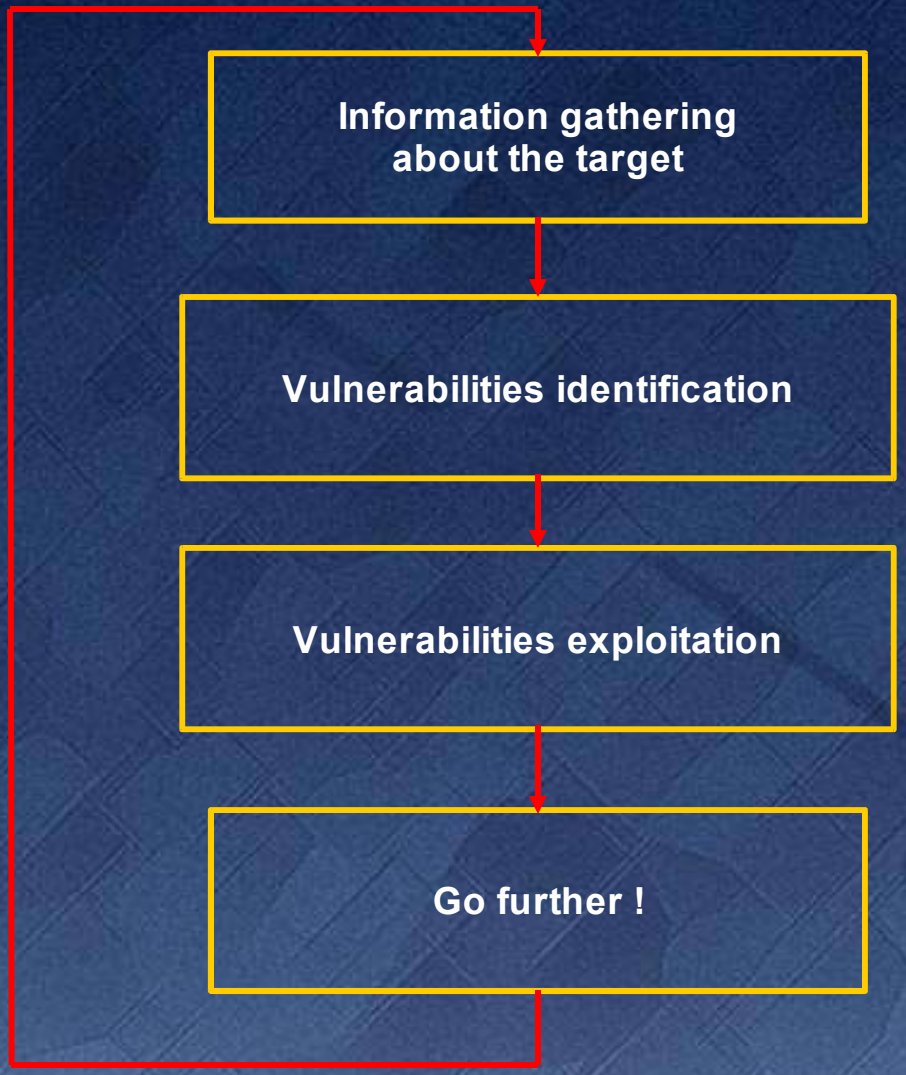
- General points
- Some examples
- Recommendations
- Conclusion



General Points

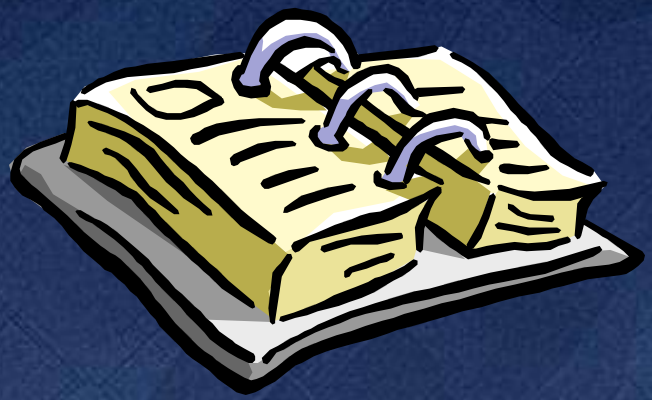
- Information gathering is the first step during a pen-test (or a real attack)
- The search engine is an obvious and common pen test tool
  - Passive
  - Stealth
  - Uses the huge “memory” of the Net
    - Google cache
    - Google groups
    - www.archive.org

Typical pen-test process



Planning

- General points
- Some examples
- Recommendations
- Conclusion



Some examples (1/5)

- 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 (2/5)

- Useful Google keywords
  - `"foo1 foo2"`
  - `filetype:123`
  - `site:foo.com`
  - `intext:foo`
  - `intitle:footitle`
  - `allinurl:foo`
- Passwords
  - `"Index of" htpasswd / passwd`
  - `filetype:xls username password email`
  - `"WS_FTP.LOG"`
  - `"config.php"`
  - `allinurl: admin mdb`
  - `service filetype:pwd` (FrontPage)

Some examples (3/5)

- Sensitive files / interesting attack data
  - `"robots.txt" "Disallow:" filetype:txt`
  - `inurl:_vti_cnf` (FrontPage files)
  - `allinurl:/msadc/Samples/selector/showcode.asp`
  - `allinurl:/examples/jsp/snp/snoop.jsp`
  - `allinurl:phpsysinfo`
  - `ipsec filetype:conf`
  - `intitle:"error occurred" ODBC request WHERE (SELECT|INSERT)`
  - `"mydomain.com" nessus report`
  - `"report generated by"`

Some examples (4/5)

- "Help me !" messages

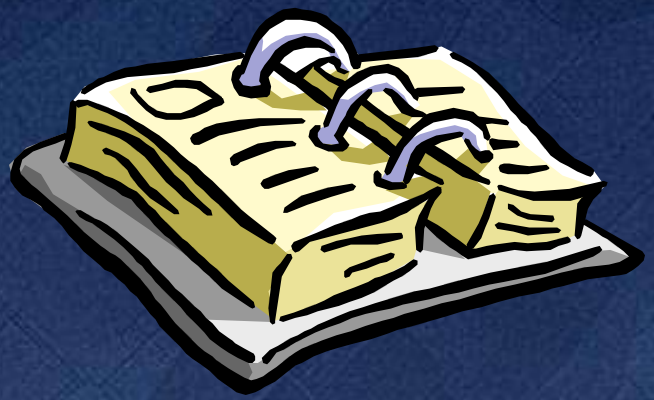
```
"I have the net-to-net configuration:

                  x.x.x.202    x.x.x.31
Localhost===============Router===============Remotehost
x.x.x.205                                      x.x.x.32

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 (5/5)

- 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

- You must control Google content
  - Information about your company
  - Information about your users and employees
  - Links pointing to your Web sites
  - Organize a regular watch
- You can ask Google to delete some search results from its cache
  - 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

Links

- Googledorks
  - http://johnny.ihackstuff.com/index.php?module=prodreviews
- 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/

Questions & Answers