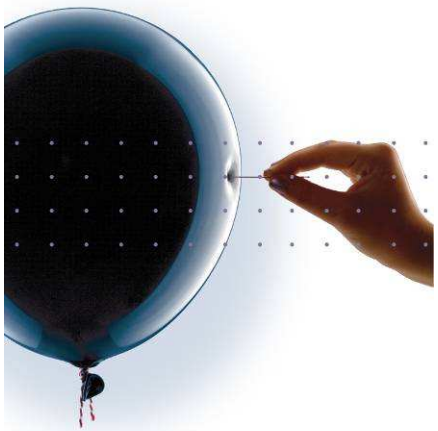
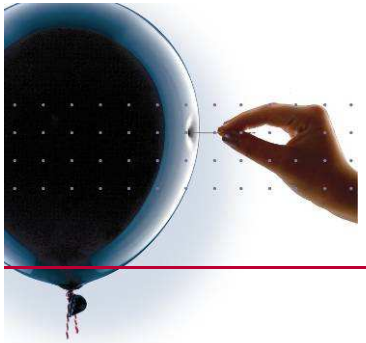


ps_testWare
Your devil's advocate

Modern information gathering

Dave van Stein

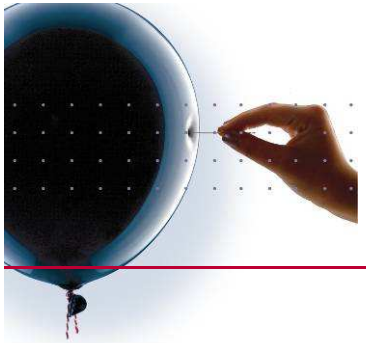
9 april 2009



Who Am I

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

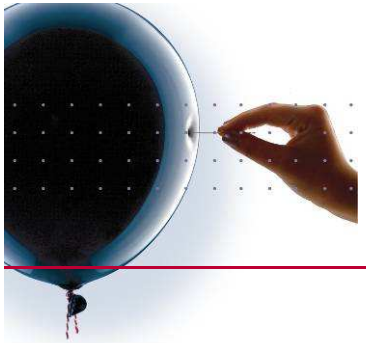
ps_testWare
Your devil's advocate



Agenda

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

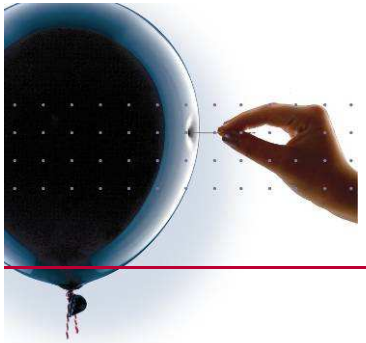
ps_testWare
Your devil's advocate



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

ps_testware
Your devil's advocate

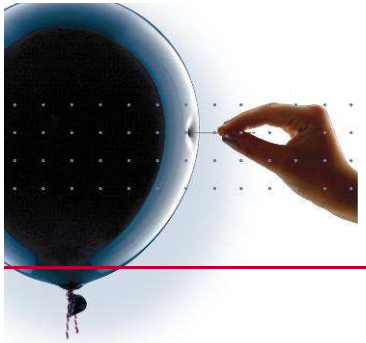


Intermezzo: How to hack

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

(simplified procedure)

ps_testWare
Your devil's advocate

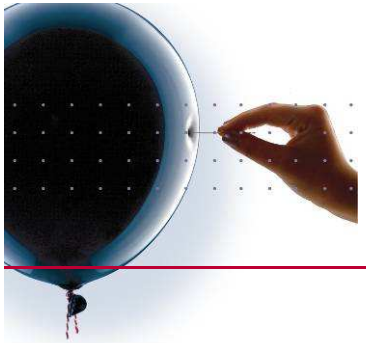


Information Gathering

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

- Not only identifying risks, but also risk on exposure and exploiting

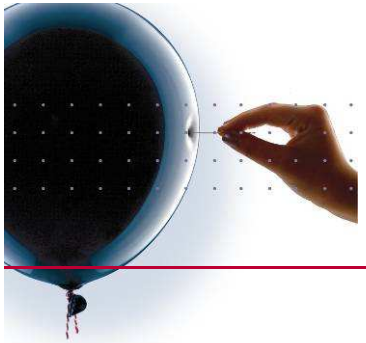
ps_testWare
Your devil's advocate



Passive Reconnaissance

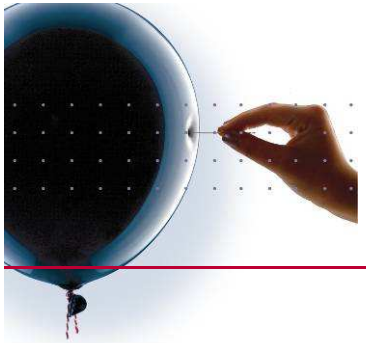
- Reconnaissance:
  - Information gathering, fingerprinting
  - Gaining information about a target

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



Sources of information

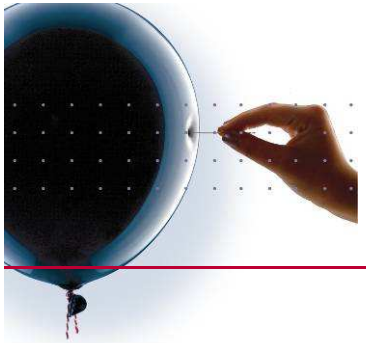
- Public records
  - WHOIS: information about owner
  - DNS : information about IP adresses
  - Necessary for network functionality
- Search engines
  - Often little restrictions on websites
  - Cache all information gathered



Tools

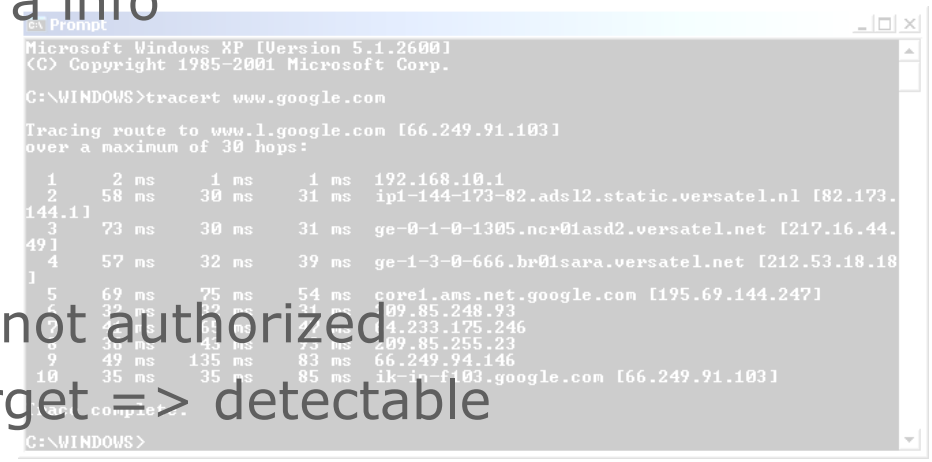
- What do you need ?
  - Webbrowser
  - Internet access
  - Creativity
- Advanced and Automated scanning:
  - Specialized (offline) Tools

ps_testWare
Your devil's advocate

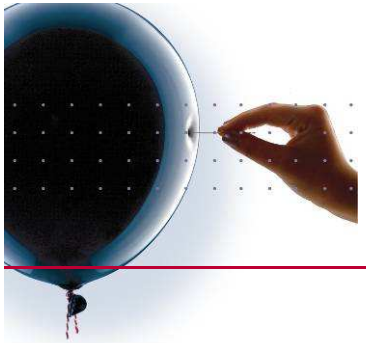


‘Classic’ Domain Scanning

- 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



ps_testWare
Your devil’s advocate

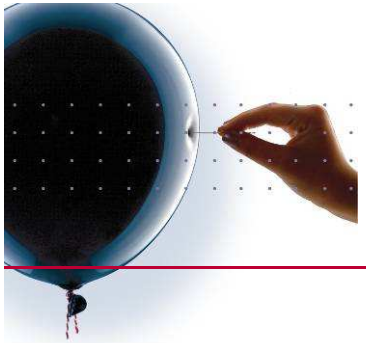


‘Modern’ Domain Scanning

- Various websites
  - Anonymous
  - Combination of techniques
  - Sort results for nice presentation
- Search engine ‘tweaking’
  - Additional information linked to domain

→ Some examples

ps_testware
Your devil’s advocate

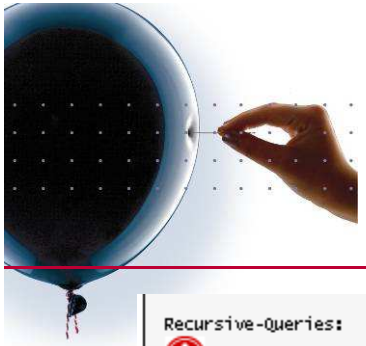


Domain Scanning: ServerSniff

Reports	IP-Tools	Nameserver	Webserver

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

ps_testware
Your devil's advocate



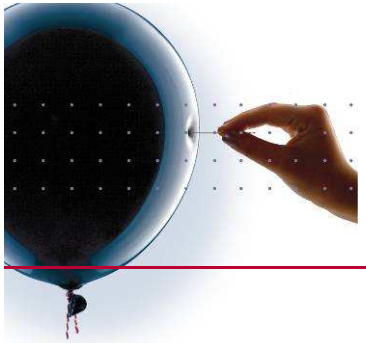
Domain Scanning: Server Sniff

```
Recursive-Queries:
ns1.secure.net. YES - recursive queries allowed!
ns2.secure.net. YES - recursive queries allowed!

NS-AXFR:
ns1.secure.net.: anonymous Zonetransfer (AXFR) allowed!!
ns2.secure.net.: anonymous Zonetransfer (AXFR) allowed!!
owasp.org. 86400 IN SOA ns1.secure.net. hostmaster.secure.net. 2007080332 86400 7200 2592000 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 ASPMX2.GOOGLEMAIL.COM.
owasp.org. 86400 IN MX 30 ASPMX3.GOOGLEMAIL.COM.
owasp.org. 86400 IN MX 30 ASPMX4.GOOGLEMAIL.COM.
owasp.org. 86400 IN MX 30 ASPMX5.GOOGLEMAIL.COM.
owasp.org. 86400 IN MX 10 ASPMX.L.GOOGLE.COM.
owasp.org. 86400 IN MX 20 ALT1.ASPMX.L.GOOGLE.COM.
owasp.org. 86400 IN MX 20 ALT2.ASPMX.L.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
google6912a08c3a8cdf0b.owasp.org. 86400 IN CNAME GOOGLE.COM.
jobs.owasp.org. 86400 IN CNAME owasp.org.
lists.owasp.org. 86400 IN A 216.48.3.22
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 127.0.0.1
mail.owasp.org. 86400 IN CNAME ghs.GOOGLE.COM.
old.owasp.org. 86400 IN A 216.48.3.19
registration.owasp.org. 86400 IN CNAME owasp.org.
stage.owasp.org. 86400 IN CNAME owasp.org.
voip.owasp.org. 86400 IN A 216.48.3.22
webmail.owasp.org. 86400 IN A 216.48.3.24
www.owasp.org. 86400 IN CNAME owasp.org.
owasp.org. 86400 IN SOA ns1.secure.net. hostmaster.secure.net. 2007080332 86400 7200 2592000 86400
```

```
owasp.org. 86400 IN MX
*.owasp.org. 86400 IN CNA
austin.owasp.org. 86400 I
blogs.owasp.org. 86400 IN
calendar.owasp.org. 8640
docs.owasp.org. 86400 IN
es.owasp.org. 86400 IN A
google6912a08c3a8cdf0b.ow
jobs.owasp.org. 86400 IN
```


ps_testware
Your devil's advocate



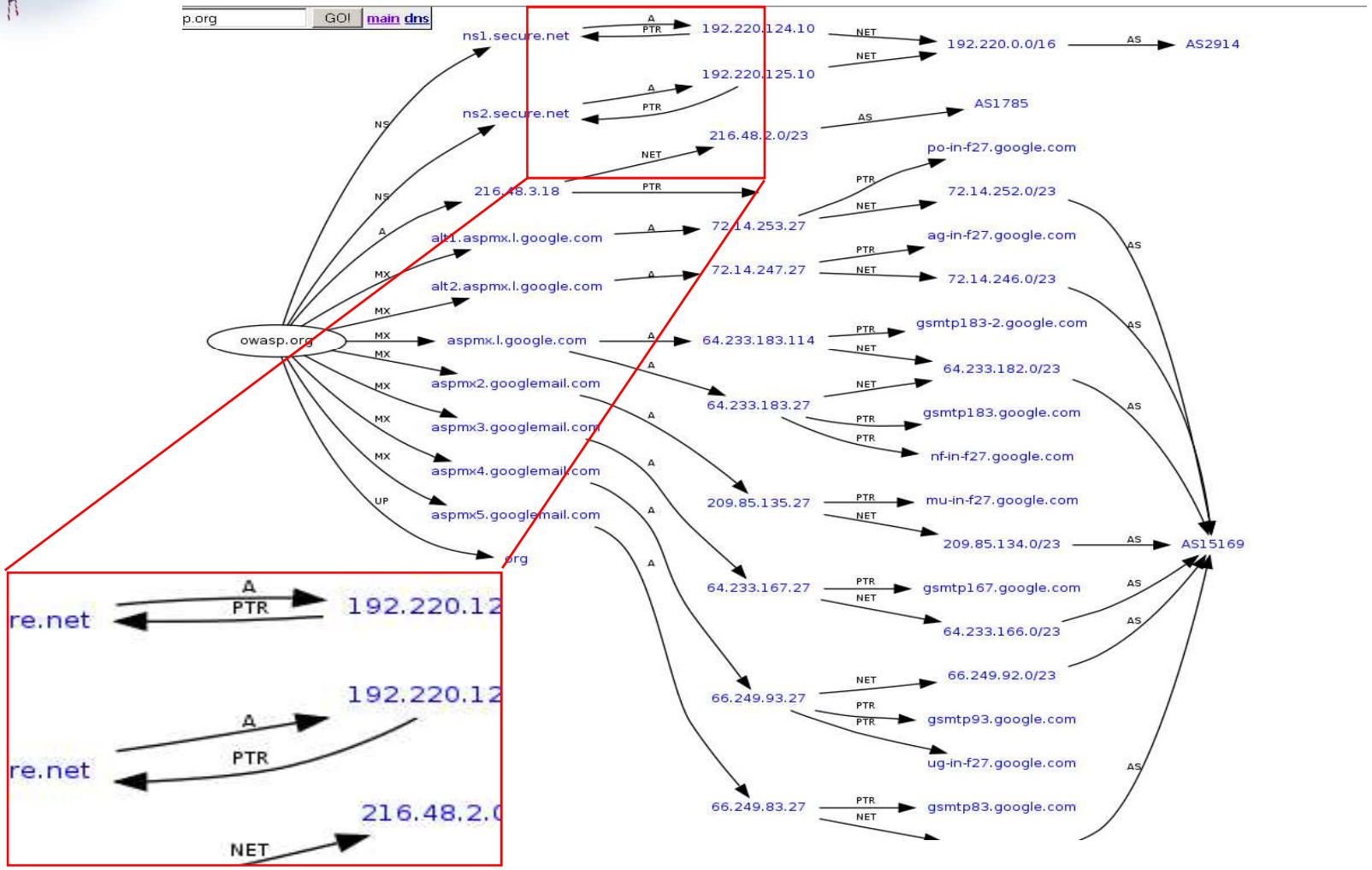
Domain Scanning: Robtex

- Domain 'Swiss Army Knife'
  - Provides ALL information linked to a domain

base	record	name	ip	reverse	route	as
owasp.org	a		216.48.3.18		216.48.2.0/23 Proxy-registered route object	AS1785 FASTNET-ASN-
	ns	ns1.secure.net	192.220.124.10	-	192.220.0.0/16 VRIO-192-220	AS2914 NTTC GIN AS N
		ns2.secure.net	192.220.125.10	-		
	mx	alt1.aspmx.l.google.com	72.14.253.27	po-in-f27.google.com	72.14.252.0/23 Google	AS15169 Google , Inc
		alt2.aspmx.l.google.com	72.14.247.27	ag-in-f27.google.com	72.14.246.0/23 Google	
		aspmx.l.google.com	64.233.183.27	gsmtp183.google.com	64.233.182.0/23 Google	
				nf-in-f27.google.com		
			64.233.183.114	gsmtp183-2.google.com		
		aspmx2.googlemail.com	209.85.135.27	mu-in-f27.google.com	209.85.134.0/23 Google	
		aspmx3.googlemail.com	64.233.167.27	gsmtp167.google.com	64.233.166.0/23 Google	
		aspmx4.googlemail.com	66.249.93.27	gsmtp93.google.com	66.249.92.0/23 Google	
				ug-in-f27.google.com		
		aspmx5.googlemail.com	66.249.83.27	gsmtp83.google.com	66.249.82.0/23 Google	
org	ptr		66.35.111.73	-	66.35.111.0/24	AS14955 N-V-C Northe
	ns	d0.org.afilias-nst.org	199.19.57.1	-	199.19.57.0/24 REACH (Customer Route)	AS12041 AFILIAS NST anycast from several p
		tld1.ultradns.net	204.74.112.1	-	204.74.112.0/24 UltraDNS	AS12008 UNSPECIFIED
		tld2.ultradns.net	204.74.113.1	-	204.74.113.0/24 UltraDNS	
		a0.org.afilias-nst.info	199.19.56.1	-	199.19.56.0/24 REACH (Customer Route)	
					199.19.54.0/24 REACH (Customer	AS12041 AFILIAS NST

ps_testware
Your devil's advocate

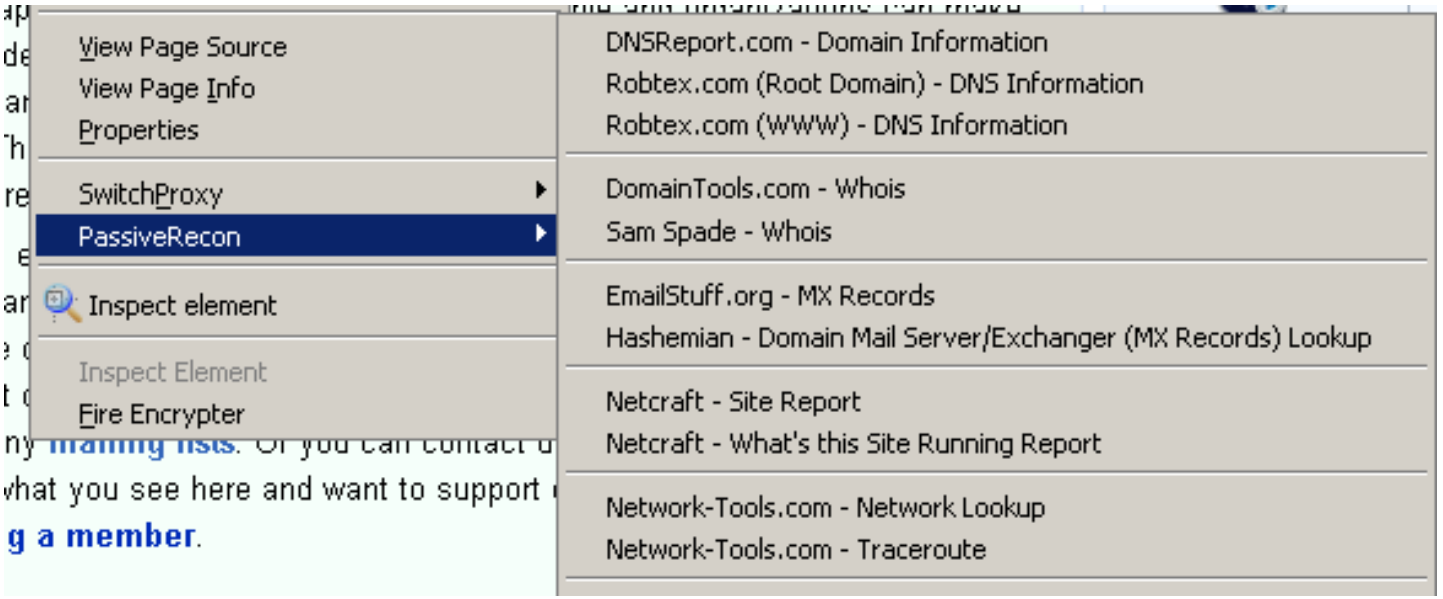
Domain scanning: Robtex



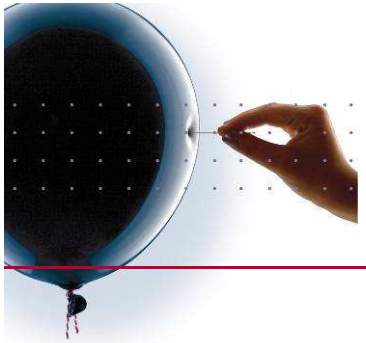
ps_testware
Your devil's advocate

Domain Scanning ‘on-the-fly’

- Passive Recon (Firefox add-on)

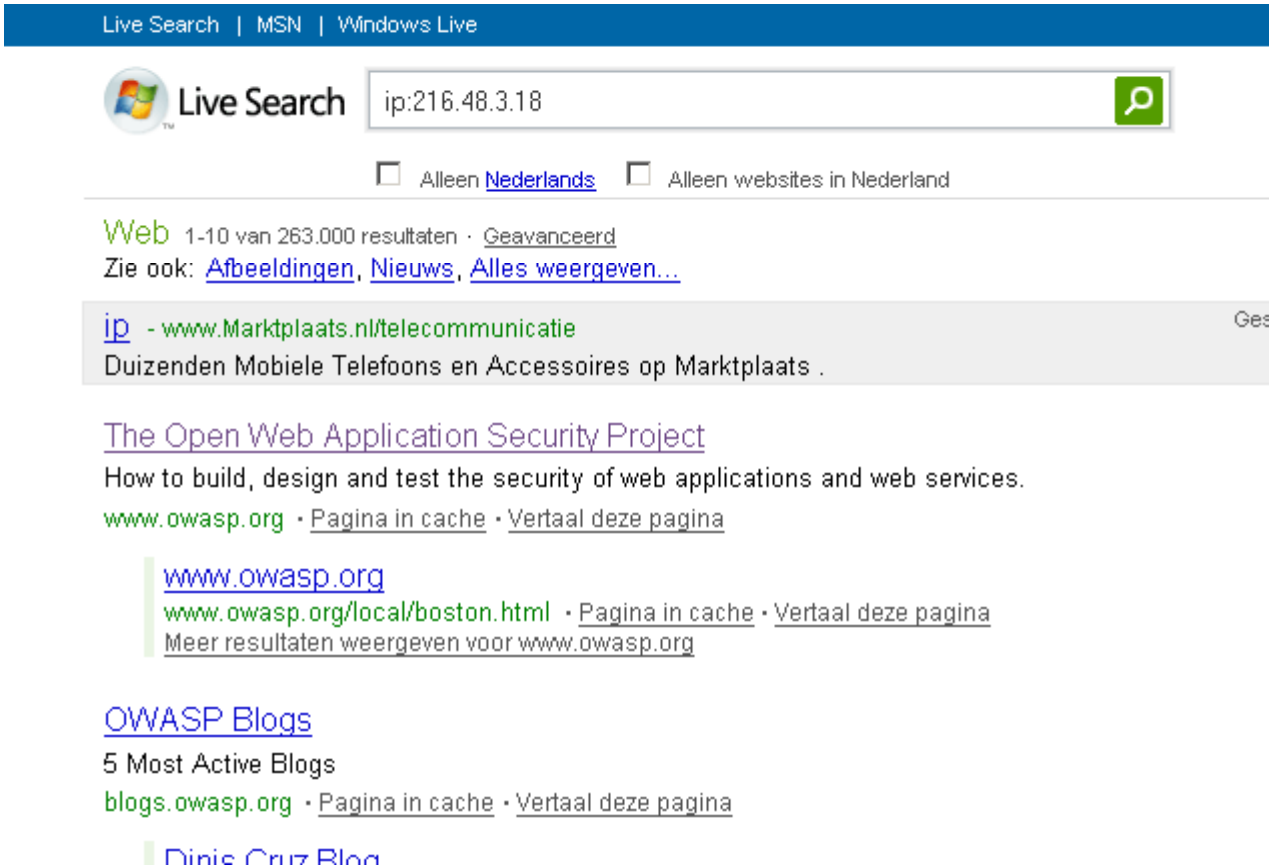


ps_testware
Your devil’s advocate



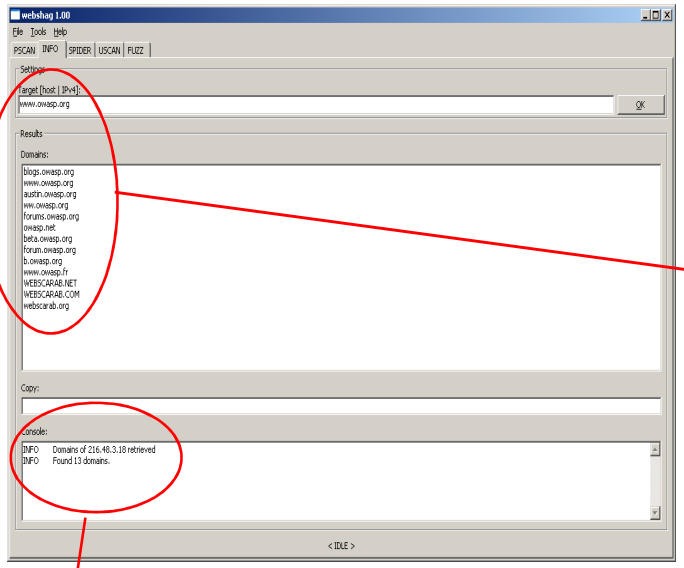
Domain Scanning: Live search

- Finds subdomains with *'IP:x.x.x.x'*



ps_testware
Your devil's advocate

Live search automated: Webshag



Target [host | IPv4]:

www.owasp.org

Results

Domains:

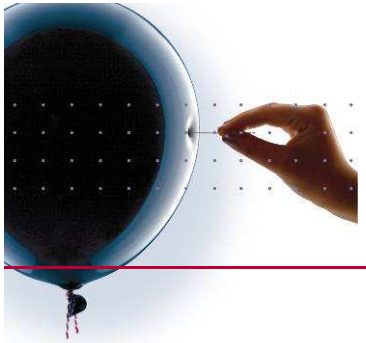
blogs.owasp.org
www.owasp.org
austin.owasp.org
ww.owasp.org
forums.owasp.org
owasp.net
beta.owasp.org
forum.owasp.org
b.owasp.org
www.owasp.fr
WEBSCARAB.NET
WEBSCARAB.COM
webscarab.org

Copy:

Console:

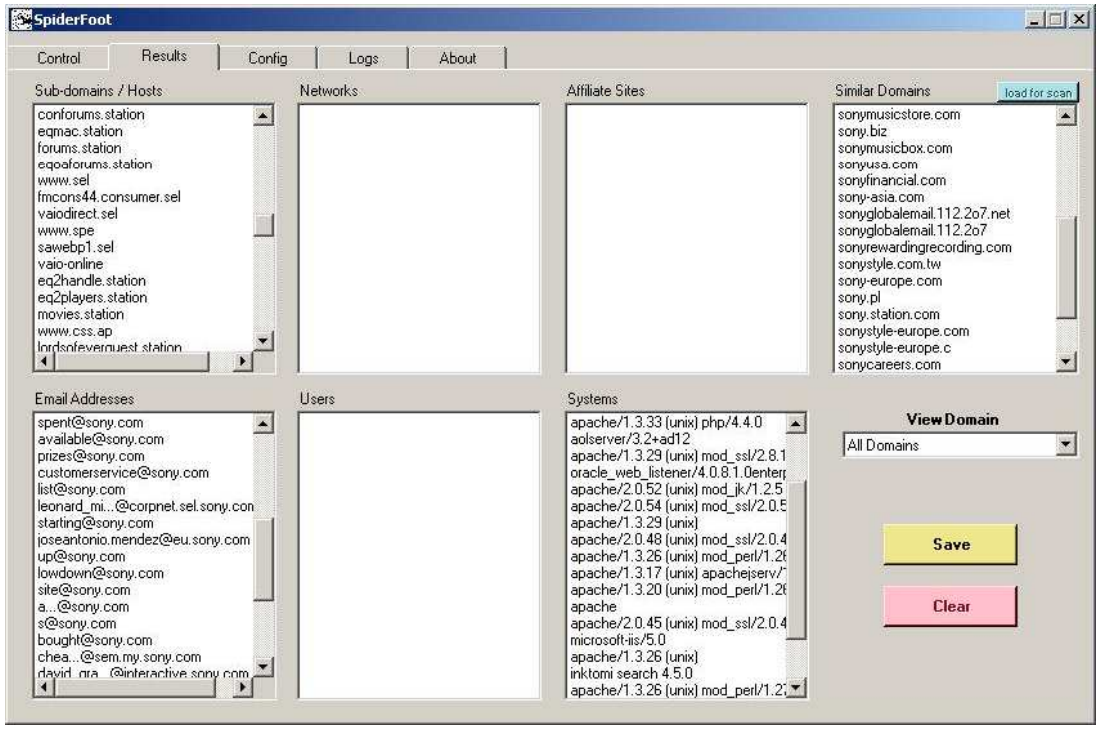
INFO Domains of 216.48.3.18 retrieved
INFO Found 13 domains.

ps_testWare
Your devil's advocate

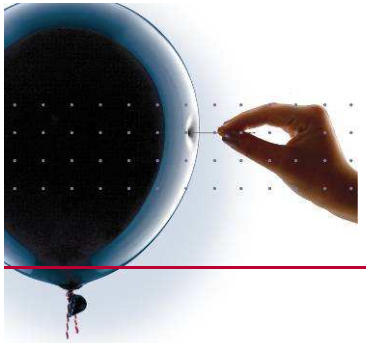


Other tools

- Spiderfoot / Wikto
  - Combine DNS / Google / Live Search / Yahoo
  - Subdomains
  - Directories
  - IP's
  - Email adressess
  - Usernames
  - Systems in use



ps_testware
Your devil's advocate



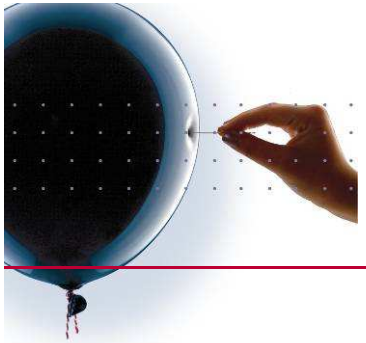
Maltego

- 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

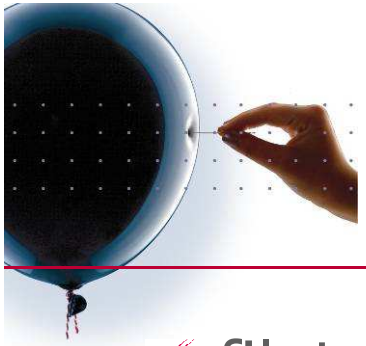
ps_testWare
Your devil's advocate



Modern Domain Scanning

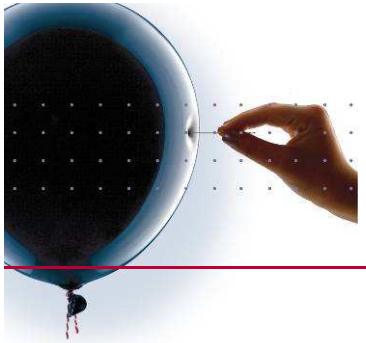
- Anonymous
- Both online and offline
- Highly automated
- Graphical network mapping in less than 10 minutes !
- Lots of additional information

ps_testWare
Your devil's advocate



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.

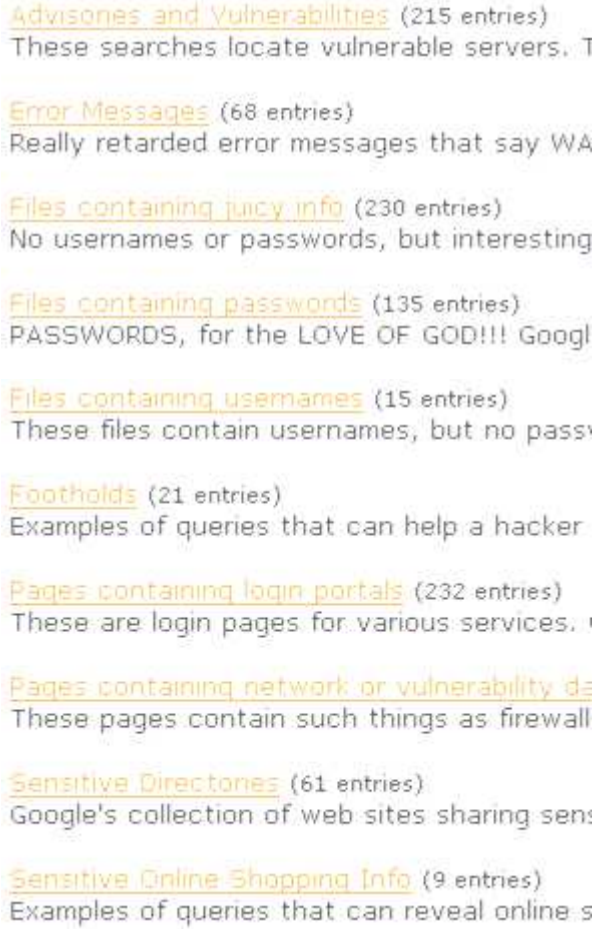


Google Hacking Database

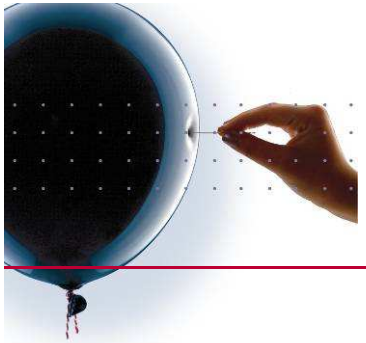
- www.johnny.ihackstuff.com

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

- Collection of queries for finding 'interesting' stuff
- Regular updates



ps_testWare
Your devil's advocate



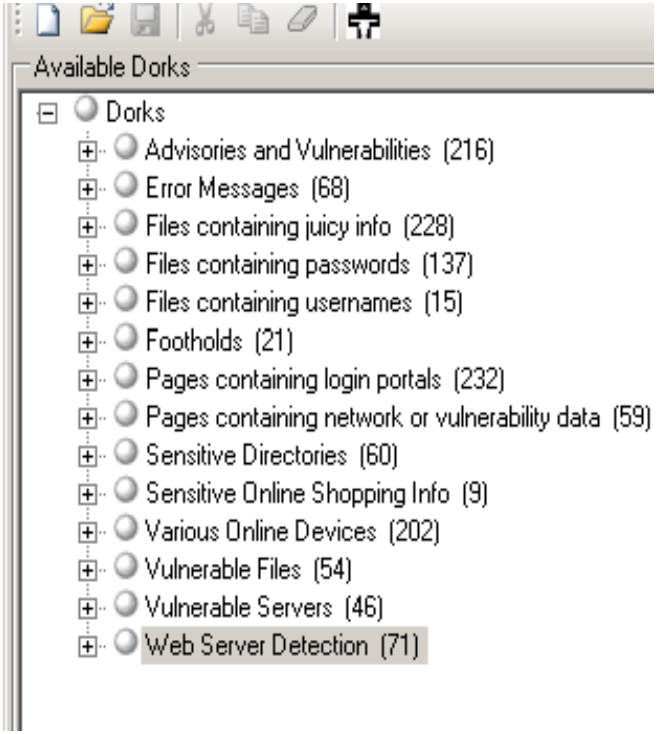
GHD applications

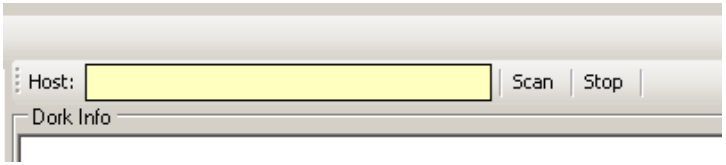
- Goolag scanner

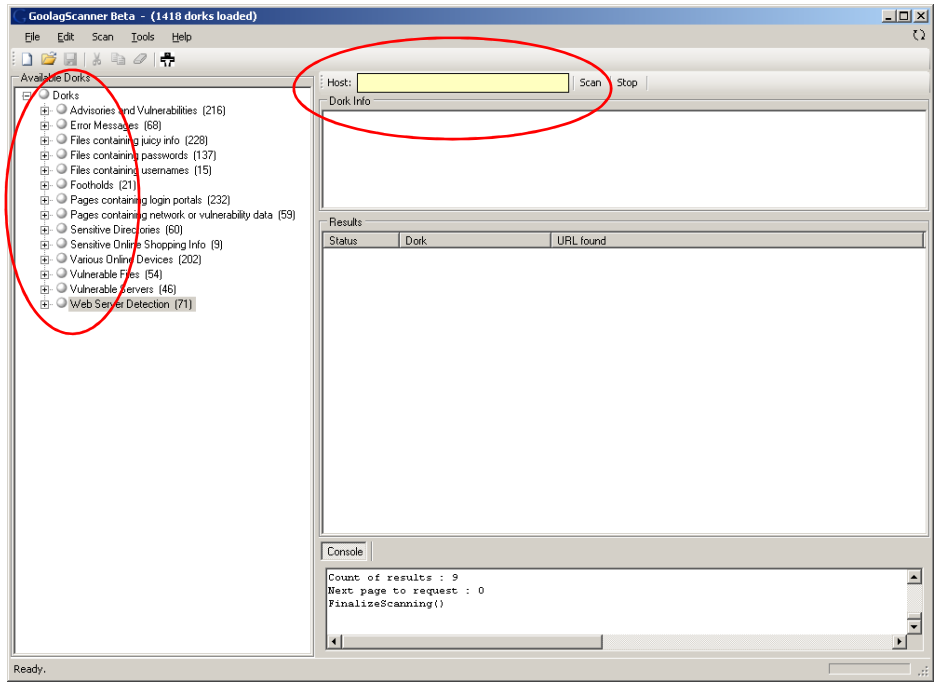
  Goolag Scanner is a Web auditing tool. It works by exploiting data- retention practices of popular search engines.

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

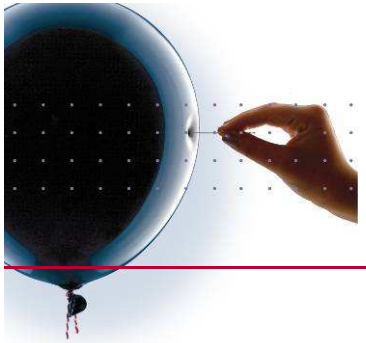
Goolag scanner





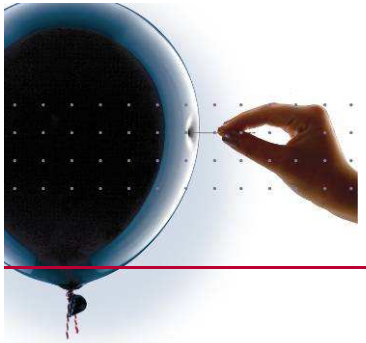


ps_testWare
Your devil's advocate



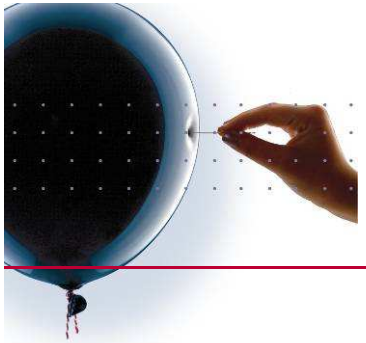
More applications

- Modern vulnerability scanners use GHD:
  - IBM Rational Appscan
  - Acunetix Vulnerability Scanner
  - Others
- Several Firefox plug-ins for “on-the-fly” scanning



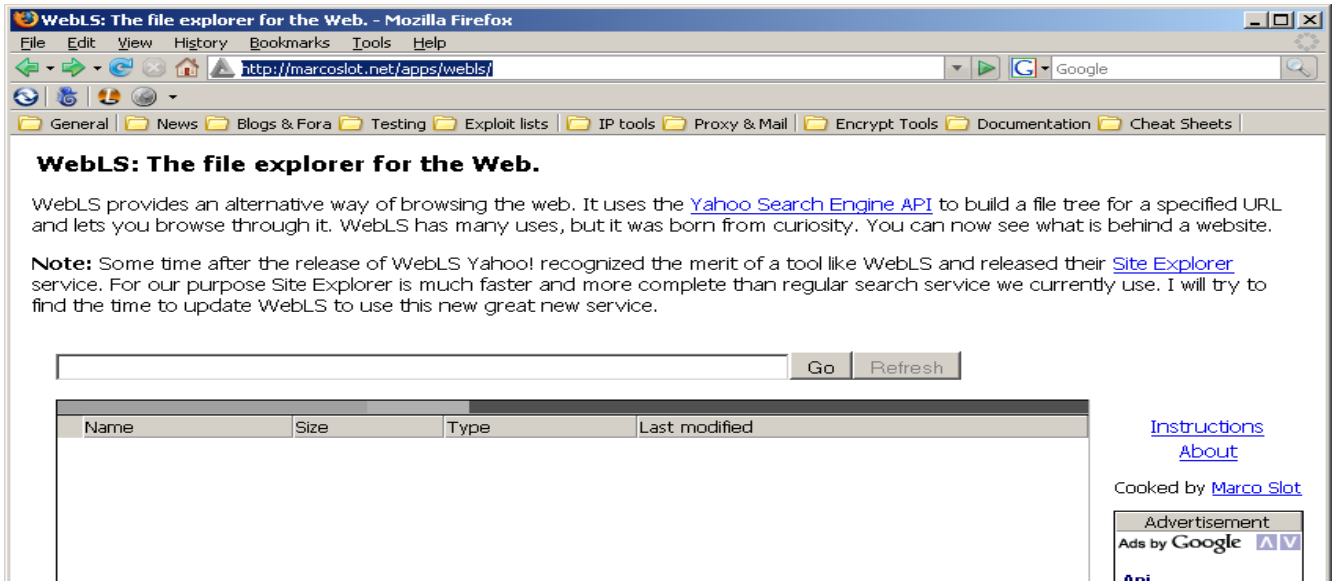
Google Hacking Database

- 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

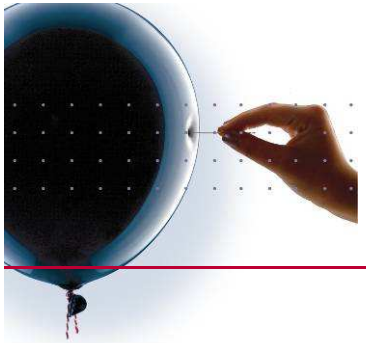


Yahoo search: file explorer

- File explorer for the web



ps_testware
Your devil's advocate



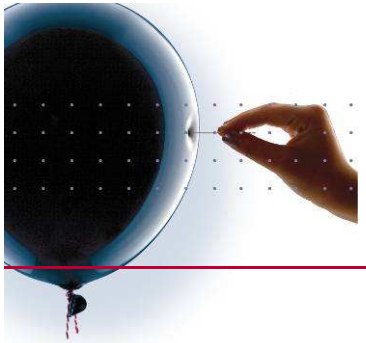
Yahoo search: file explorer

- Examples

Name	Size	Type	Last modified
.	0kB		
index.php	17kB	text/html	Thu, 10 Jul 2008 07:00:00 GMT

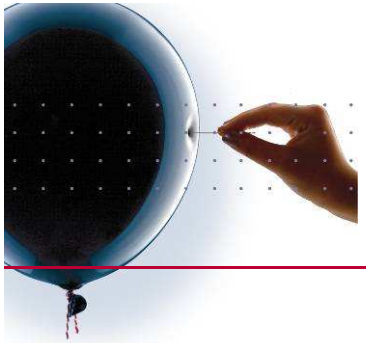
Name	Size	Type	Last modified
.	0kB		
be			
data			
news			
references			
styles			
function.mysql-list-tables	0kB	text/html	Wed, 18 Jun 2008 07:00:00 GMT
index.php	8kB	text/html	Wed, 16 Jul 2008 07:00:00 GMT

ps_testWare
Your devil's advocate



Other tools

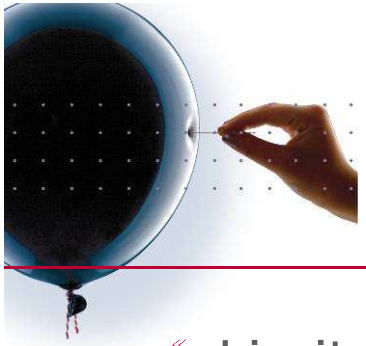
- Metagoofil : extract metadata from documents on website
  - User names, server names, path locations, sofware + versions, MAC adresses (!)
- Wikiscanner : check comments made on Wikipedia by company or domain
  - Company IP ranges
- Several “Social Site” extractors
  - Linkedin, twitter, hyves, etc, etc, etc



Conclusions

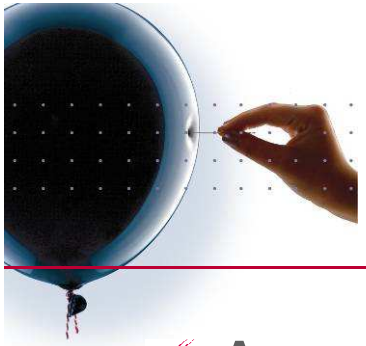
- What search engines see, hackers can abuse
- Many tools are freely available
- Networks can be mapped with much detail in minutes
- Much information about your company, systems and users available on internet

ps_testWare
Your devil's advocate



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.

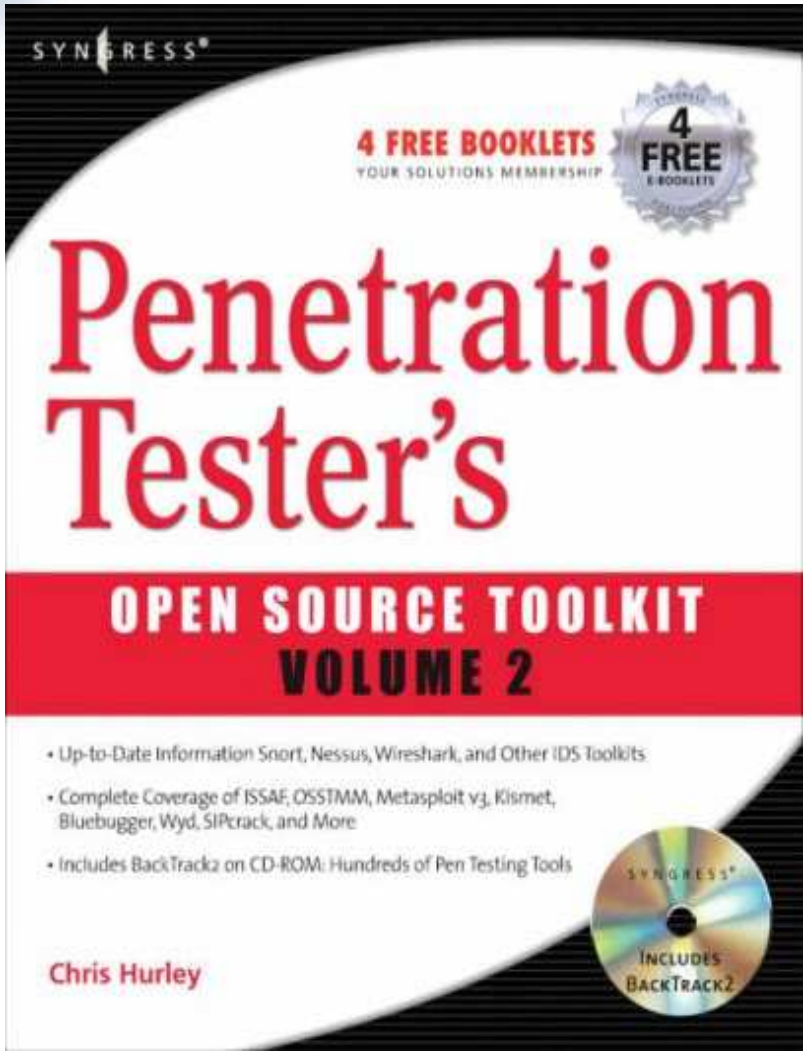


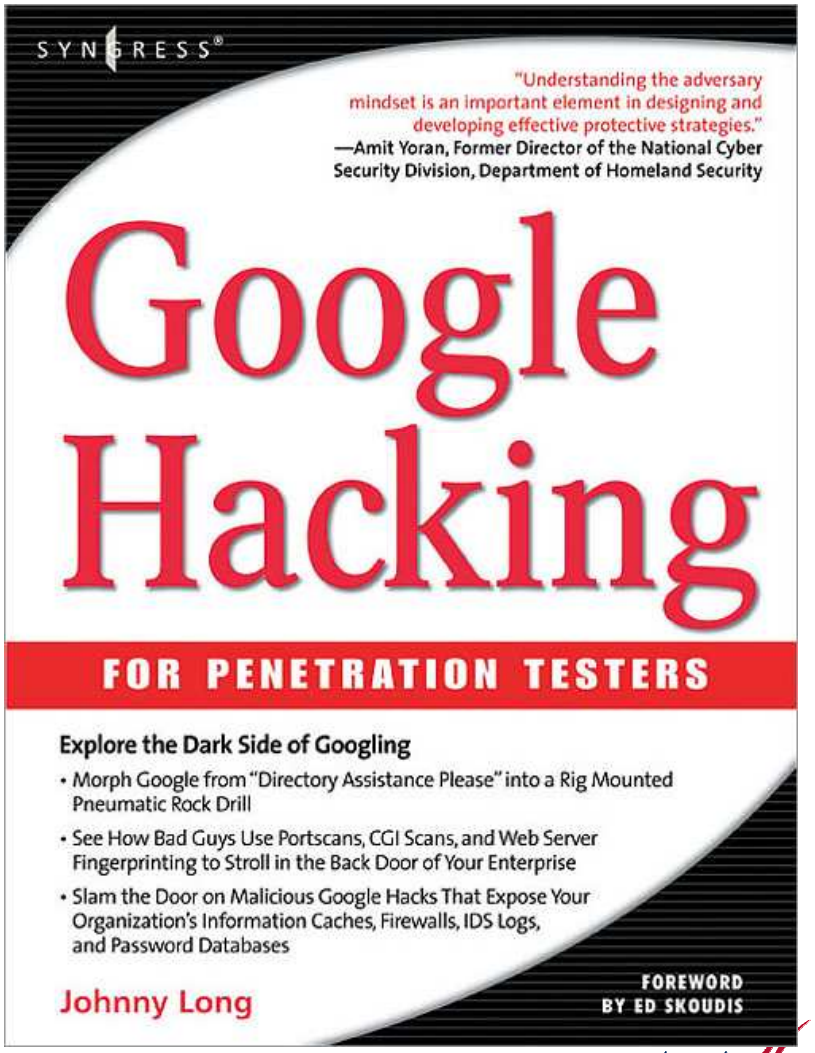
Remedies (2/2)

- Awareness
  - Be aware of all possible sources of information. Create awareness among employees. Assume all information will possibly abused
- Clean documents
  - Remove al 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.

ps_testWare
Your devil's advocate

Interesting books on the subject





ps_testWare
Your devil's advocate