Googling for Malware and Bugs

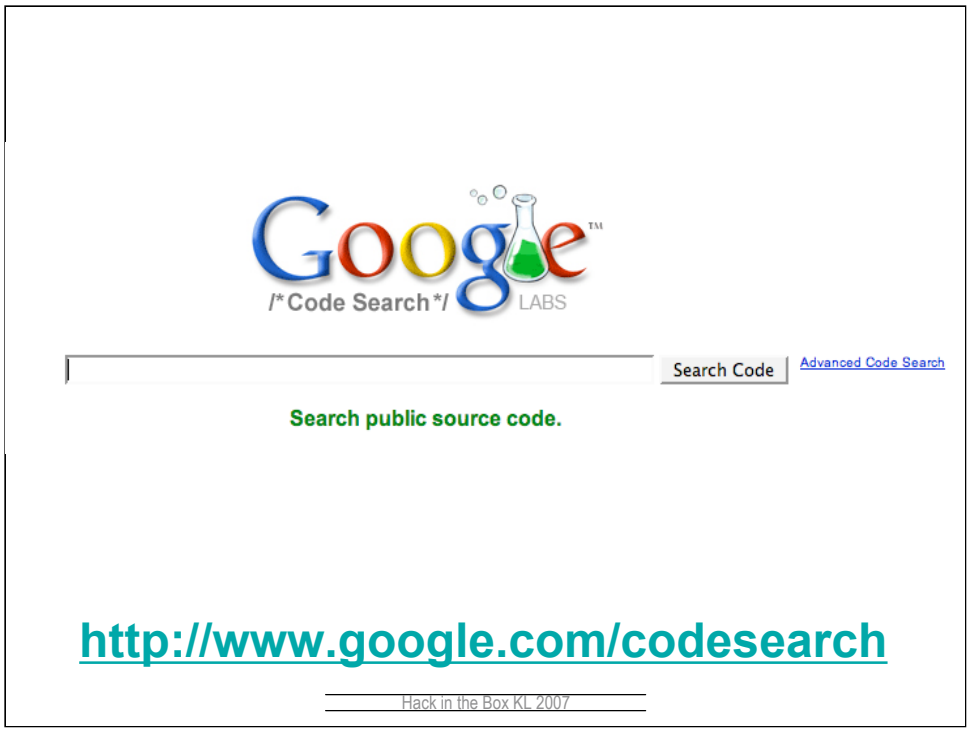
Jose Nazario
<jose@arbor.net>

Hack in the Box KL 2007

From slides given at HITB Malaysia 2007 in Sept.

For some additional “bullet points” around this topic, see http://monkey.org/~jose/presentations/umeet06/slides/


ARBOR
NETWORKS



Launched in October, 2006

Allows searching of source code

- Supports: Basic patterns, Search operators, Complex regular expressions

Indexes millions of source files They download so you don't have to

Similar to Koders http://www.koders.com/

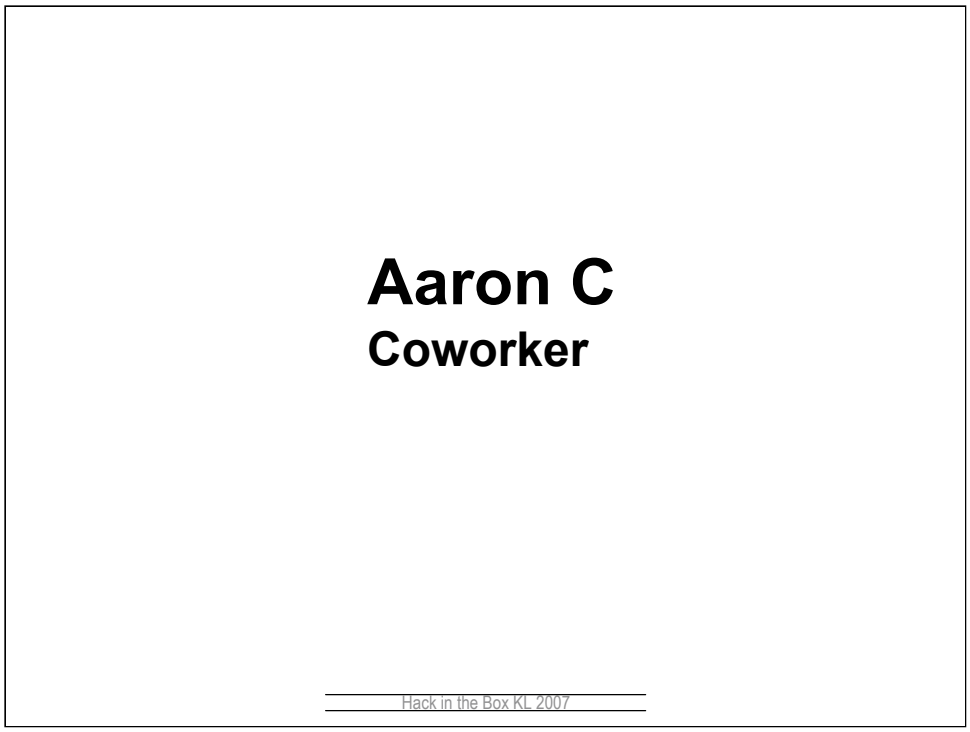
This is Google's cached copy of `./` from
http://marwww.in2p3.fr/~touchard/RTLinux.tar.bz2

Google is neither affiliated with the authors of this page nor responsible for its content.

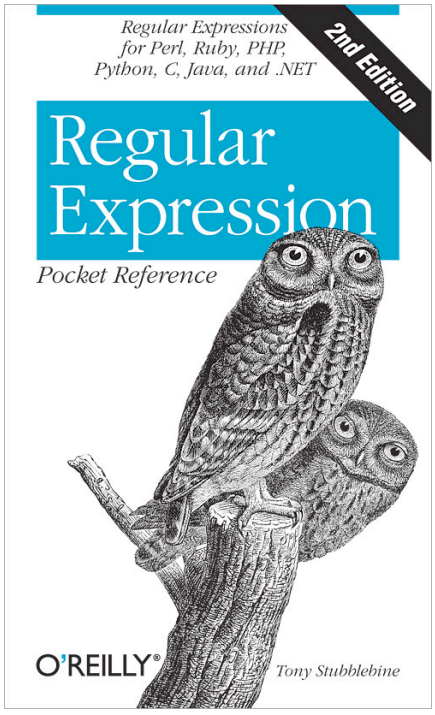
---

http://marwww.in2p3.fr/~touchard/RTLinux.tar.bz2/./

.Xresources
.adobe/
.bash_history
.bash_logout
.bash_profile
.bashrc
.cshrc
.cvspass
.fonts.cache-1
.fullcircle/
.gconf/
.gconfd/



Aaron blogged this up here:
http://asert.arbornetworks.com/2006/10/static-code-analysis-using-google-code-search/


Regular Expressions
for Perl, Ruby, PHP,
Python, C, Java, and .NET
2nd Edition
Regular
Expression
Pocket Reference
O'REILLY®
Tony Stubblebine

Regular Expression Basics

- . means any characters
- * means 0 or more characters
- X+ means one or more “X”
- X* means 0 or more “X”
- ^ anchors input to start of line
- $ anchors input to end of line
- [x-y] means a range of characters
- [^x] means “not x”
- (and) have meaning
- Escape special characters with \
  - \. To match a literal “.”
  - \(to match a “(“, \[, *, etc

lang:
license:
file:
package:

-lang:

& vs &&

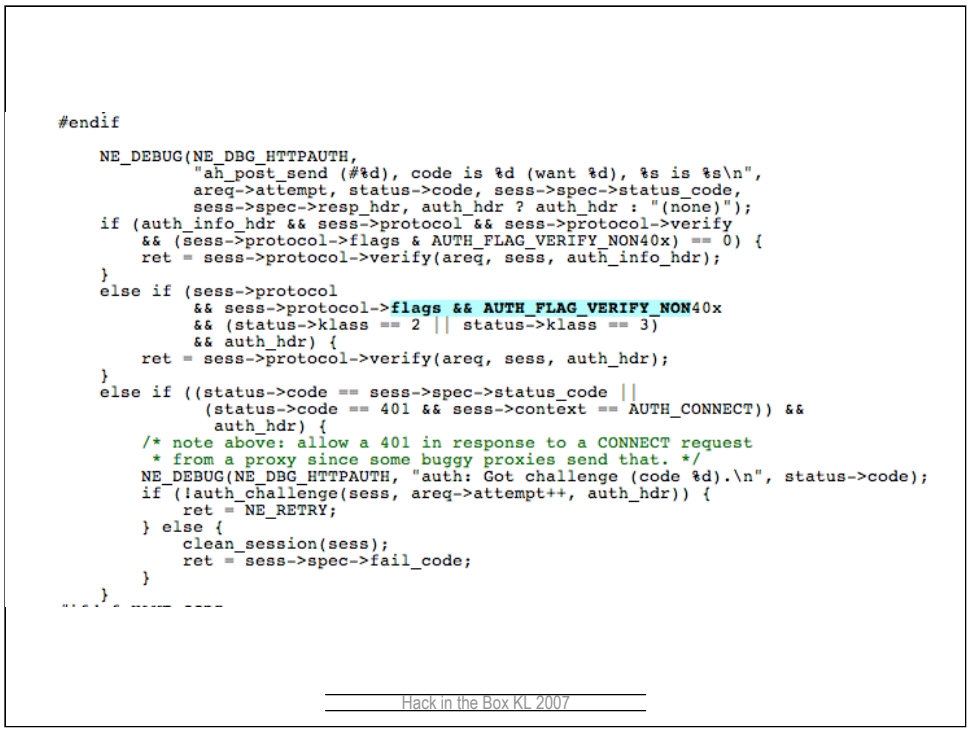
```
if (is_set && process) { … }
```

```
if (flags & FLAG_PROCESS) { … }
```

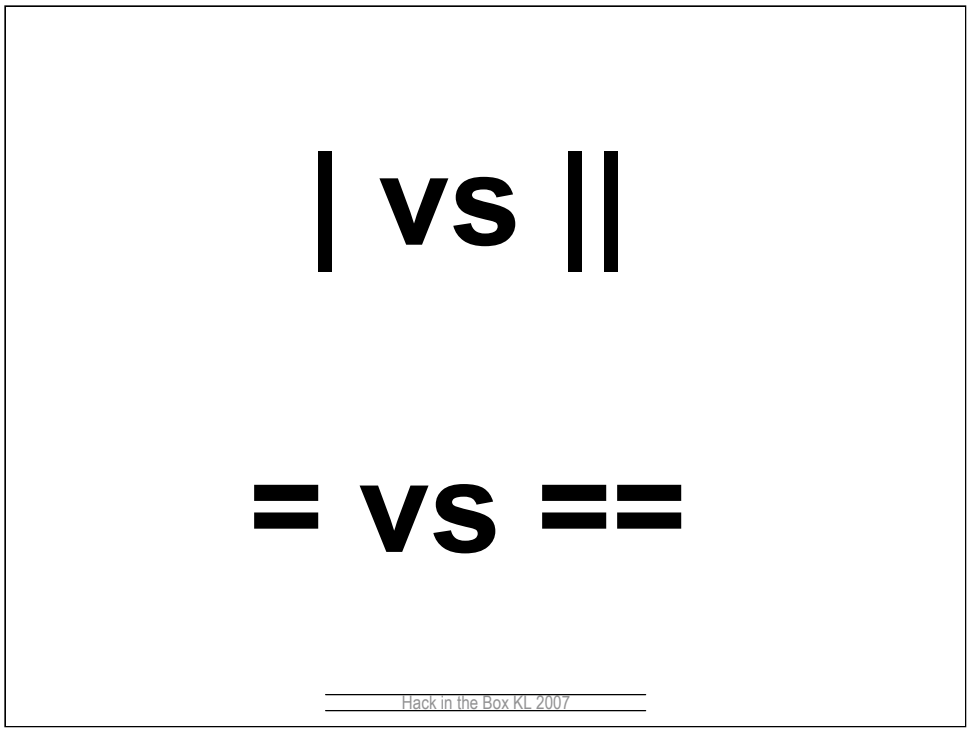
USUALLY

RARELY

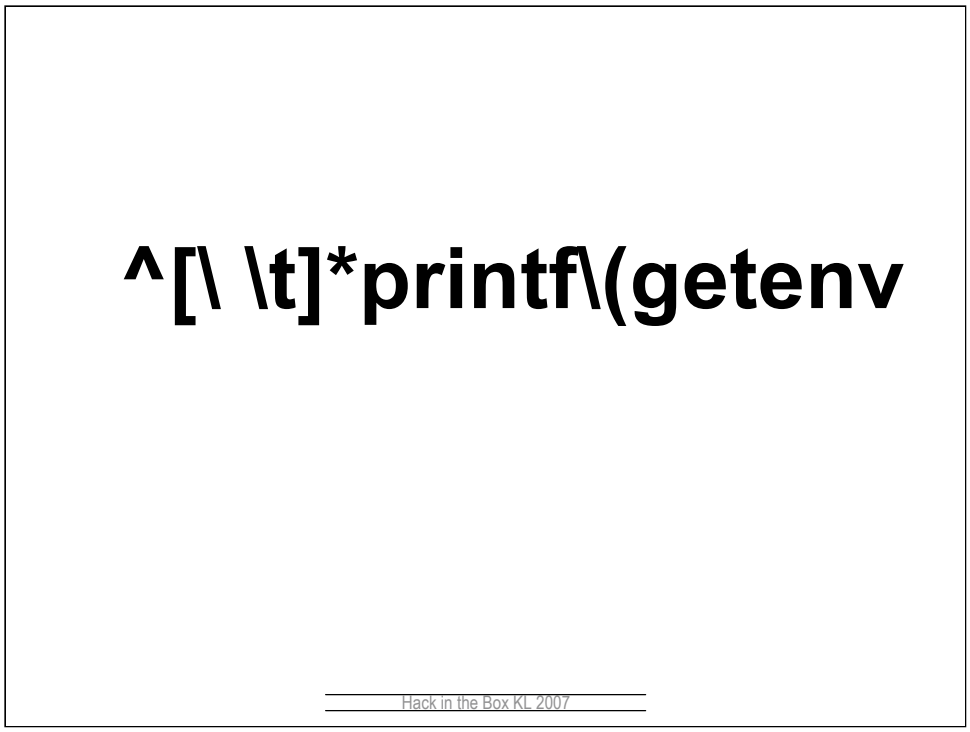
flags\ *&&\ *[A-Za-z_]*



Actual bug in neon, webdav tool. Causes authentication in some situations to not work properly.



More logic bugs directly caused by typos



Format string directly from user supplied input

strcat()

strcpy()

strcat\ *\(\ *.*\ *,\ * lang:c

http://www.google.com/codesearch?q=strcat%5C+*%5C%28%5C+*.*%5C+*%2C%5C+*+lang%3Ac&hl=en&btnG=Search+Code

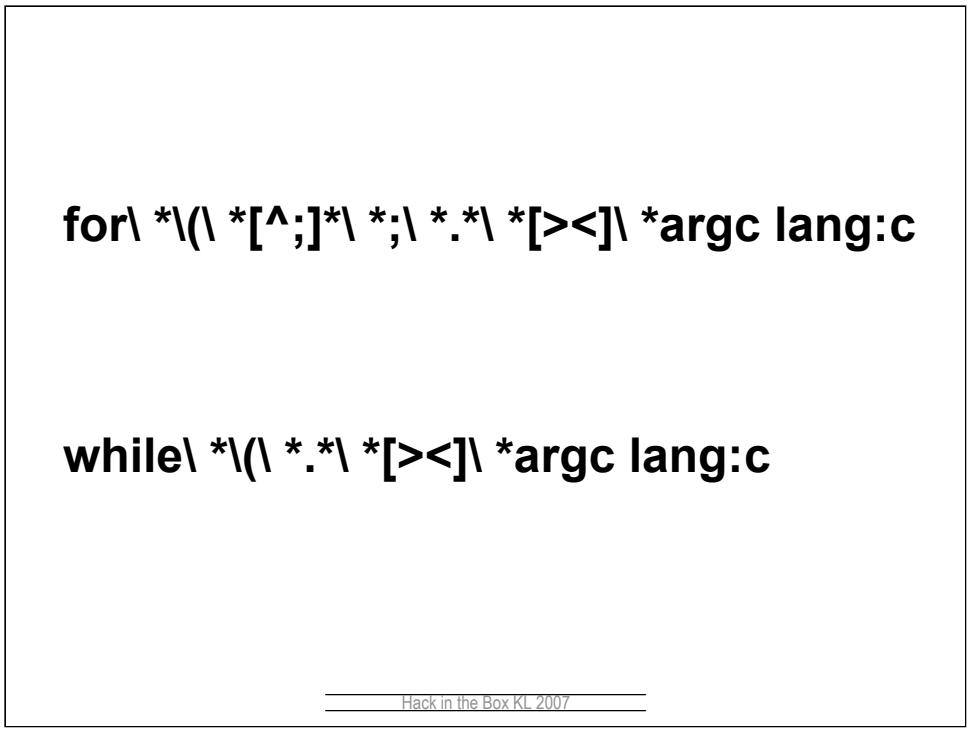
Results 1 - 10 of about 262,000.

http://www.google.com/codesearch?hl=en&lr=&q=strcpy%5C+*%5C%28%5C+*.*%5C+*%2C%5C+*+lang%3Ac&btnG=Search

Results 1 - 10 of about 640,000.

\[sizeof\(.*\)\]\ *=\ *’?\\?0′ ?;$

buf[sizeof(buf)] = '\0';



User-controlled loop counters

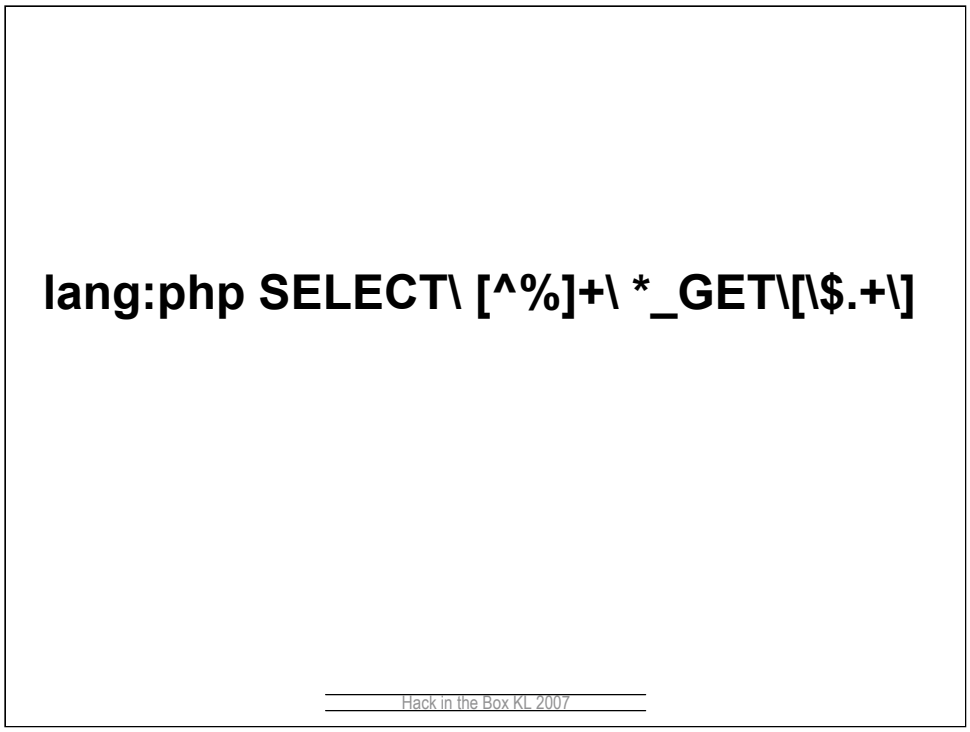
Look for priv'd code (local exploit) or remote code (ie system() called code in a web app)

Results 1 - 10 of about 59,100.

http://www.google.com/codesearch?hl=en&lr=&q=for%5C+*%5C%28%5C+*%5B%5E%3B%5D*%5C+*%3B%5C+*.*%5C+*%5B%3E%3C%5D%5C+*argc+lang%3Ac&btnG=Search

http://www.google.com/codesearch?hl=en&lr=&q=while%5C+*%5C%28%5C+*.*%5C+*%5B%3E%3C%5D%5C+*argc+lang%3Ac&btnG=Search

Results 1 - 10 of about 22,800.

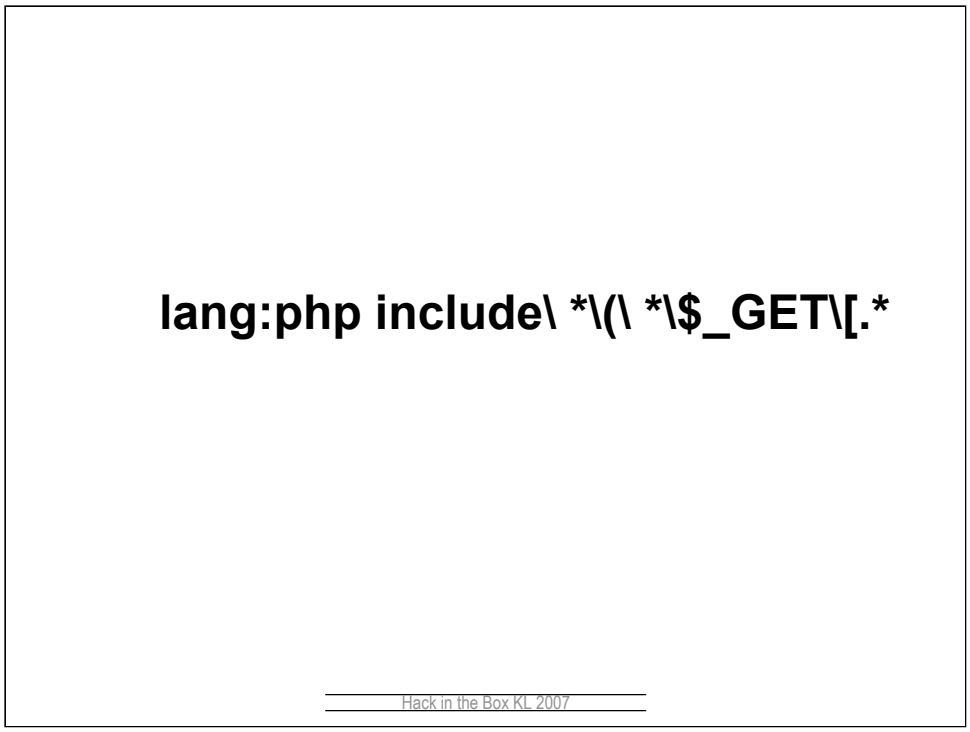


SQL injection

20 results

GET
POST

SELECT
DELETE
UPDATE



Remote file include

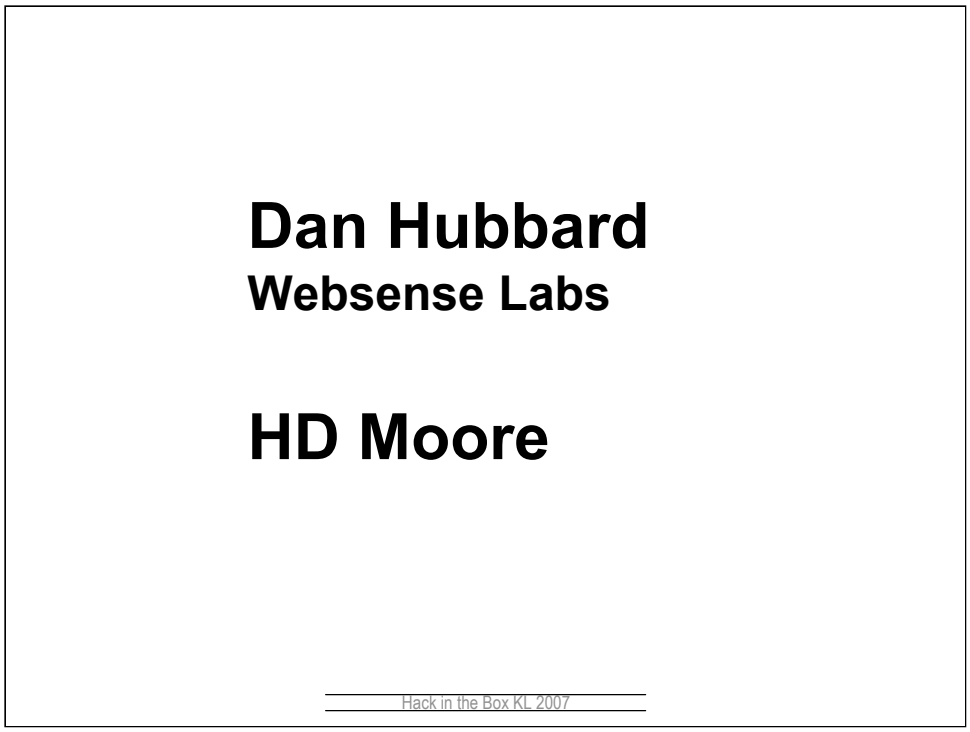
Cookies
XSS

PAM SMB

http://www.csn.ul.ie/~airlied/pam_smb/

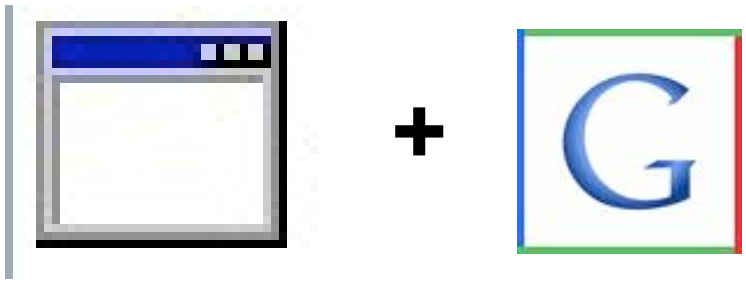
```
--- pam_smb_auth.c.orig 2006-10-05 14:33:14 -0400
+++ pam_smb_auth.c      2006-10-05 14:33:21 -0400
@@ -228,7 +228,7 @@
               error code for non-existant users -- alex */

            if ( ( !pw->pw_passwd ) && ( !p ) )
-             if ( flags && PAM_DISALLOW_NULL_AUTHTOK )
+             if ( flags & PAM_DISALLOW_NULL_AUTHTOK )
                return PAM_SUCCESS;

            pp = crypt(p, salt);
```

Googling for Malware



Also see http://metasploit.com/research/misc/mwsearch/index.html

Also see http://www.websense.com/securitylabs/blog/blog.php?BlogID=68 and related links



WINDOWS EXECUTABLE

32bit for Windows 95 and Windows NT

Technical File Information:

Image File Header

Signature: 00004550

Machine: Intel 386

Number of Sections: 0003

Time Date Stamp: 40152e57

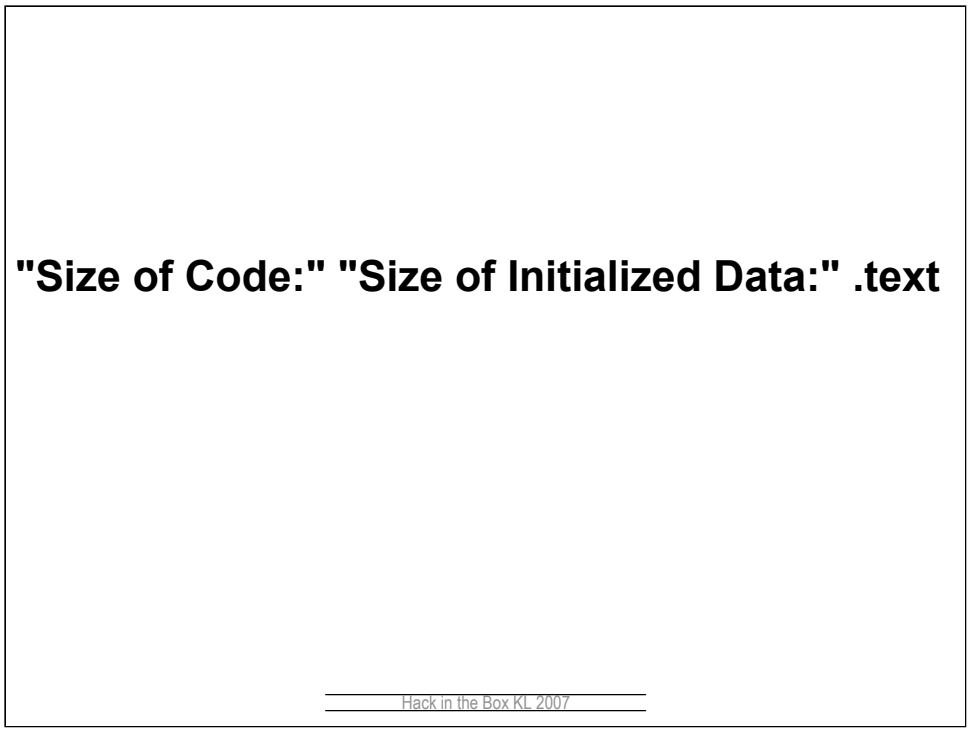
Symbols Pointer: 00000000

Number of Symbols: 00000000

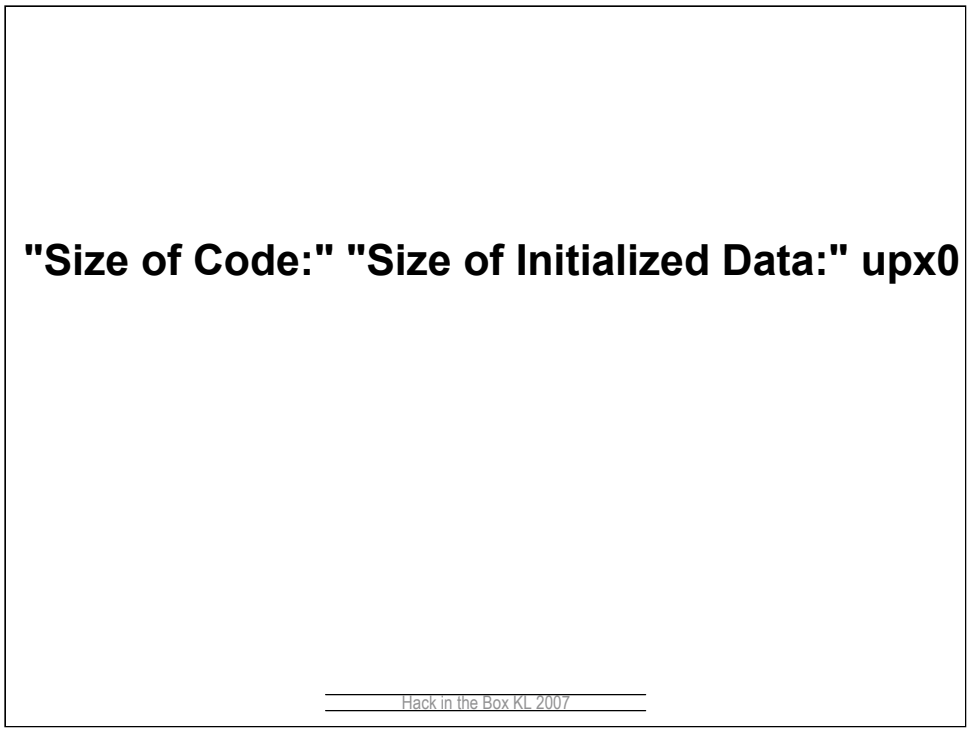
Size of Optional Header 00e0

Characteristics: Relocation info stripped from file.
File is executable (i.e. no unresolved external references).
Line numbers stripped from file.
Local symbols stripped from file.
32 bit word machine.

"Size of Code:" "Size of Initialized Data:" "32bit for Windows 95 and Windows NT "



Yields about 700 results, most of which are real EXEs



Yields about 20 valid results

URLOpen
URLDownloadToFile
InternetCrackUrlA

Some of the obvious ones don’t work; they may be blocked by google to prevent abuse

Some other things work; when in doubt use library names (ie for networking)

TimeDateStamp
SizeOfImage
AddressOfEntryPoint
SizeOfCode

40714098:00034200:00032f0e:00005000
3cc9d024:00033000:0002f001:0002a000
4011b0be:00013000:00001018:694c6461
4245cb17:00019000:00016fe0:00009000
406ec1d5:00036000:00033fce:00005000
41107b1d:00049000:00037d72:00038c00

http://www.abisource.com/mailinglists/abiword-dev/2005/Jun/att-0006/phone_number2.pif

http://gcc.gnu.org/ml/gcc-prs/2004-05/msg00001/the_message.com

http://lists.grok.org.uk/pipermail/full-disclosure/2006-July/047959.html

http://archives.neohapsis.com/archives/fulldisclosure/2006-07/0362.html

http://www.tavernmaker.de/download/TM_village_DEMO_1_0.tap

…


Terima kasih
Terima kasih
Terima kasih
Terima kasih
Terima kasih
Terima kasih
Terima kasih
Terima kasih
Terima kasih
Terima kasih
Terima kasih
Terima kasih
Hack in the Box KL 2007