Traps of Gold
Michael Brooks & Andrew Wilson
Caution. Please vet anything discussed with legal and management.
FRUSTRATION

http://www.flickr.com/photos/14511253@N04/4411497037/sizes/o/in/photostream/
Our entire defense strategy is REACTIVE... AKA, losing
Patch Management
Fixes known issues
Someone already pwned it
Already in Production!
Secure Development

Reduces Vulnerabilities

Expensive

Limited Effectiveness
Security Theater

Free groping at airport

You aren’t safer

Introduces vulnerabilities
But if they aren’t working...
What is missing?
Fight Back

http://www.flickr.com/photos/superwebdeveloper/5604789818/sizes/l/in/photostream/
We conclude that there exists no clear division between the offense and defense.
- USMC, Warfighting
Attackers are human too. They have:

• Finite time
• Imperfect tools
• Emotion / Ego / Bias
• Risk
So...

Attack them there.
“If I have seen further, it is only by standing on the shoulder of giants.
- Sir Isaac Newton
Traps of Gold

- IDS Systems
- Honeypots
- Exploits
Two Models of Warfare

Attrition

Maneuver
Stack the Deck

http://www.flickr.com/photos/jonathanrh/5817317551/sizes/o/in/photostream/
“To act in such a way that the enemy does not know what to expect.”
Server Banners
Who needs this?

File Extensions
The browser doesn’t care.

Default Files
Why leave these up?
If knowing is half the battle
Shut up.
Convince the enemy we are going to do something other than what we are really going to do.
Reduce what they can know

Lie about the rest.
Increase the noise by...

Blatantly lying.
Issues Identified

See updates after talk

Before

- Nikto

19

After

5462

That’s real though!
But that won't fool people...
Will it?
Some lies are better.
“The secrets of victory thus lie in the taking of initiative.”
It’s not about reaction

It’s about awareness and acting sooner.
Perceived

Actual

I made this up!

And I can watch for this.
I love it when a plan comes together.
-Hannibal
So far we’ve shown:
Misdirection
Shutting down tools
Increasing awareness
But...

Can we break it?
YES, WE CAN.
To recap.

Stop acting like this...
Start acting like this.

http://www.flickr.com/photos/kriztofor/3253758933/sizes/o/in/photostream/
Fight Back

http://www.flickr.com/photos/superwebdeveloper/5604789818/sizes/l/in/photostream/
Capture The Flag

http://ctf.doublethunk.org

The winner takes all