The Good, The Bad, and the Ridiculous

SANS Penetration Testing Summit 2010

14 JUNE 2010

STACH&LIU

SANS

About Me

WHO IS THIS DUDE?

- Vinnie Liu
  Managing Partner @
  Stach & Liu
- Penetration testing professionally since 1999
- Background in Gov
  Intel, Big 4, F100

LEGES SINE MORIBUS VANAE

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

ERNST & YOUNG

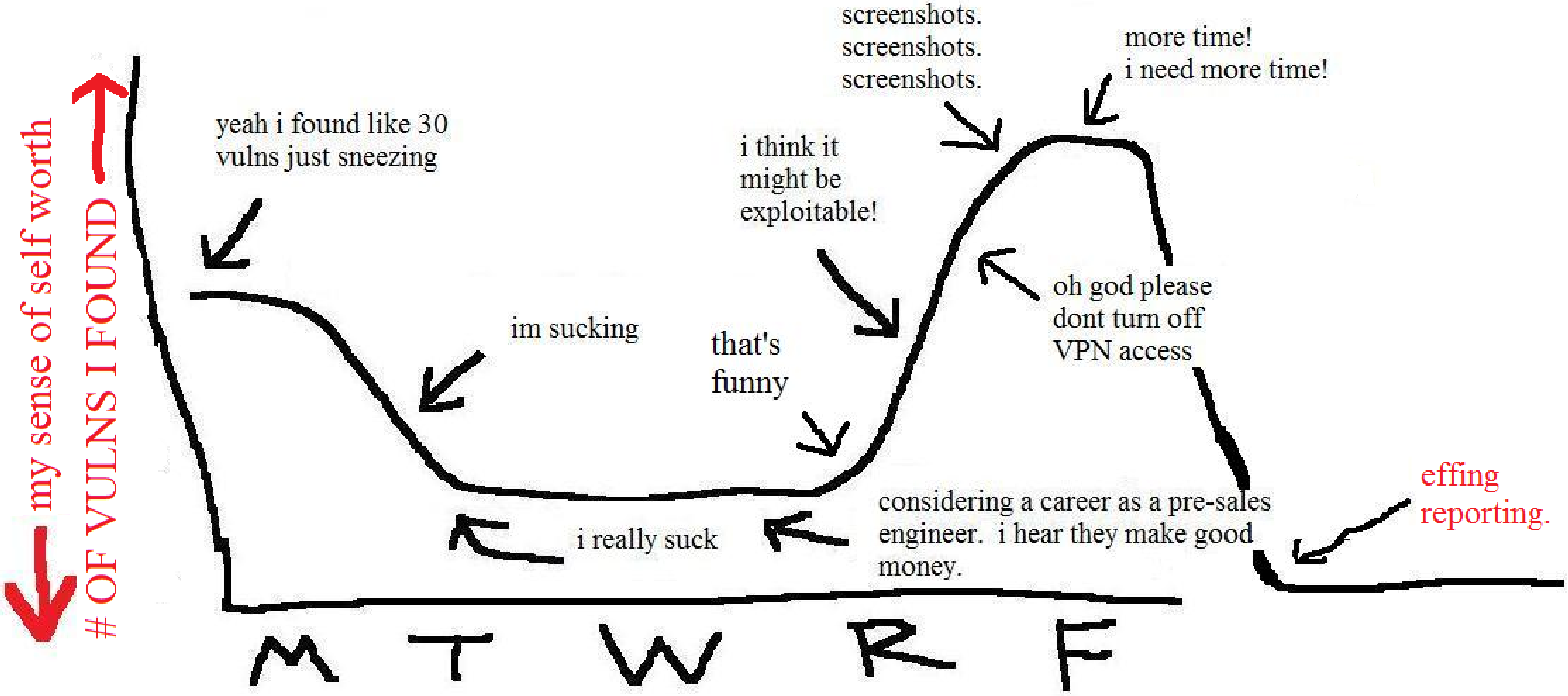
Honeywell

LOCKHEED MARTIN

Simulate a real world attack against a target network or application.

- EVERYBODY

Real World Pen Testing



It answers the question, “could someone break in?”

- ME

Types of Testing

JUST A FEW

- Penetration Testing
- Vulnerability Assessment
- Risk Assessment

Proficient

Advanced

Expert

Master

Proficient

80%

*I MADE THESE NUMBERS UP

Proficient Pen Testers

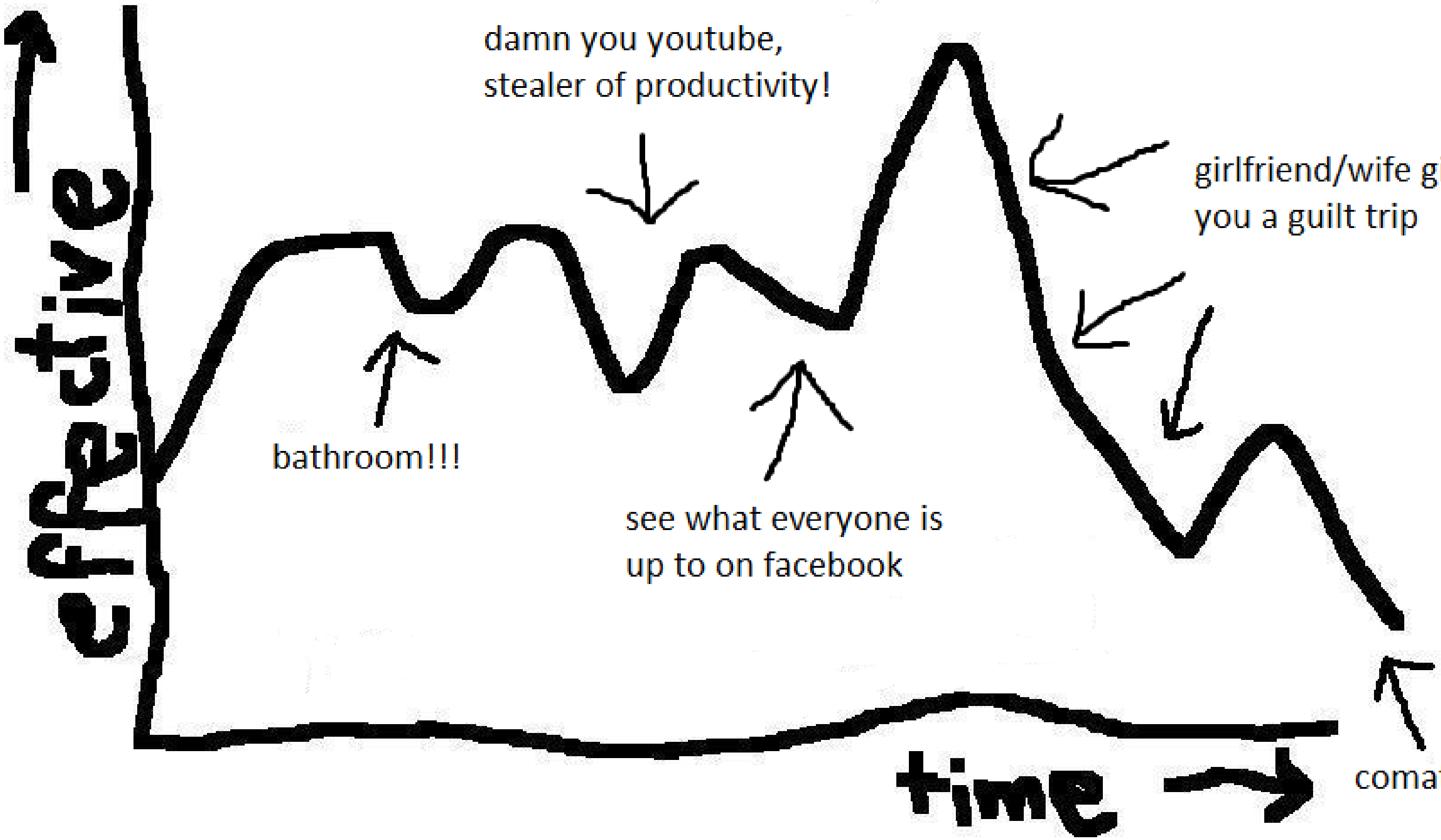
CANT HACK OUT OF A WET PAPER BAG

- Runs tools, validates results, adheres to checklist
- Standard vulnerability knowledge
- Performs simplistic "manual" testing

These aren’t the droids we’re looking for.

Over Reliance on Tools

Productivity



damn you youtube,
stealer of productivity!

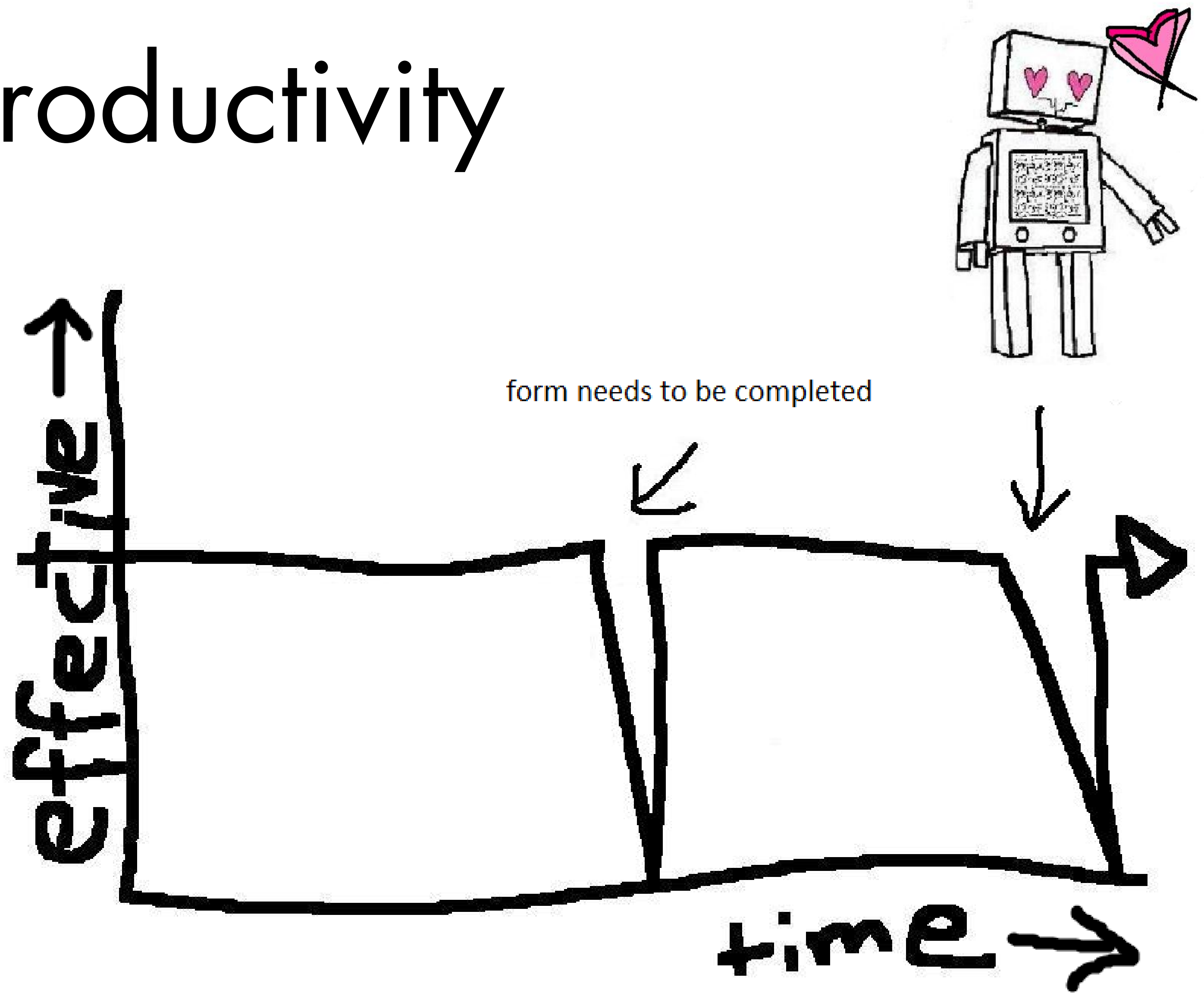
girlfriend/wife gives
you a guilt trip

bathroom!!!

see what everyone is
up to on facebook

comatose

Productivity



form needs to be completed

Advanced

15%

Advanced Pen Testers

BEYOND TOOLS

- Understand the nature of exploratory testing
- Passionate about learning on their own
- Able to perform more complex exploitation

How Do You Get Better?

Carbonated Taurine Drink.
Serve Ice Cold.
Red Bull
ENERGY DRINK
With Taurine. Vitalizes Body and Mind.

Expert

5%

Expert Pen Testers

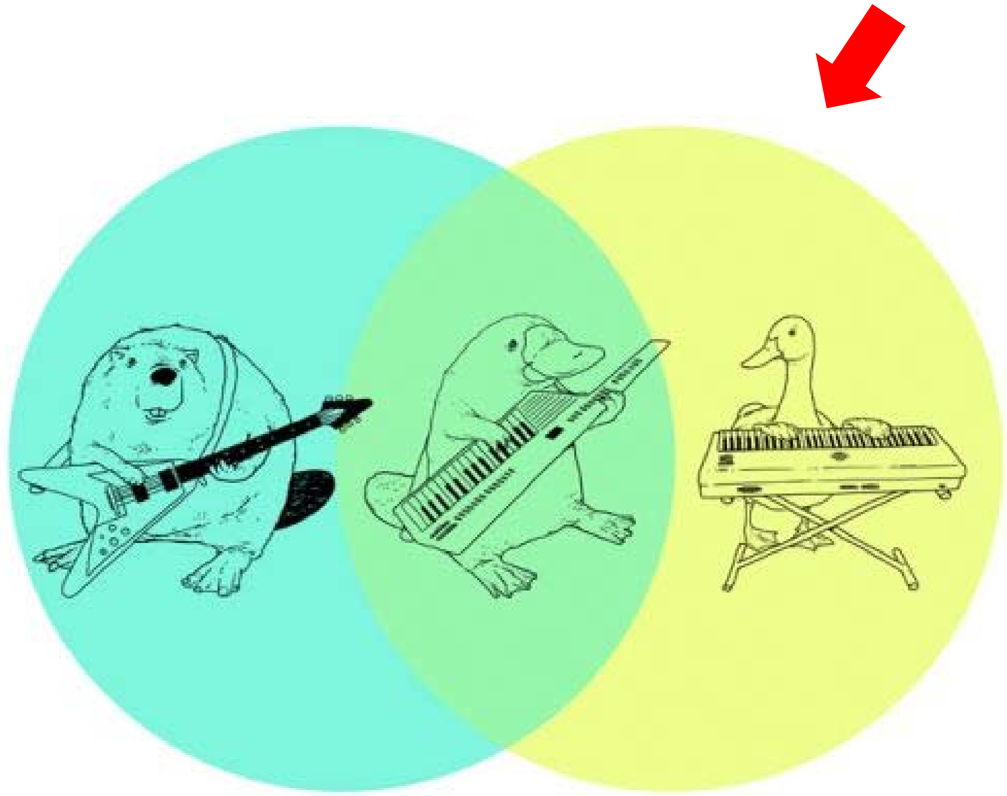
ARE NATURALS

- **Synthesize** disparate data points
- **Find patterns** in seemingly unrelated information
- **Build attack avenues** in their mind

STACH&LIU

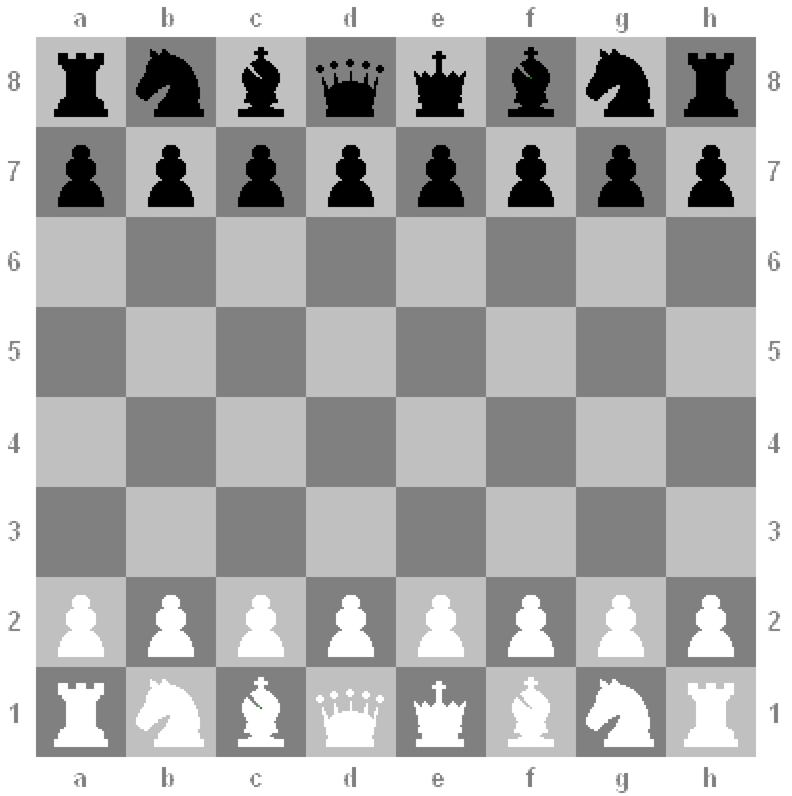
Synthesis and Patterns

CAN BE BOTH GOOD AND BAD



Attack Visualization

LIKE BOBBY FISCHER



Master

<1%

Until a man is twenty-five he still thinks, every so often, that under the right circumstances he could be the baddest motherf@*&! in the world. If [he] moved to a martial-arts monastery in China and studied real hard for ten years. If [his] family was wiped out by Columbian drug dealers and [he] swore [him]self to revenge…If [he] just dropped out and devoted [his] life to being bad.

Hiro used to feel that way, too, but then he ran into Raven. In a way, this is liberating. He no longer has to worry about being the baddest motherf@*&! in the world. The position is taken.

- SNOWCRASH

Master Pen Testers

ARE RELENTLESS

- They do all of the above…and they don’t give up.

Thank You

STACH&LIU

SANS