Stefan Friedli

THE 99¢ HEART SURGEON DILEMMA

Hi, I’m Stefan.

BSides Vienna

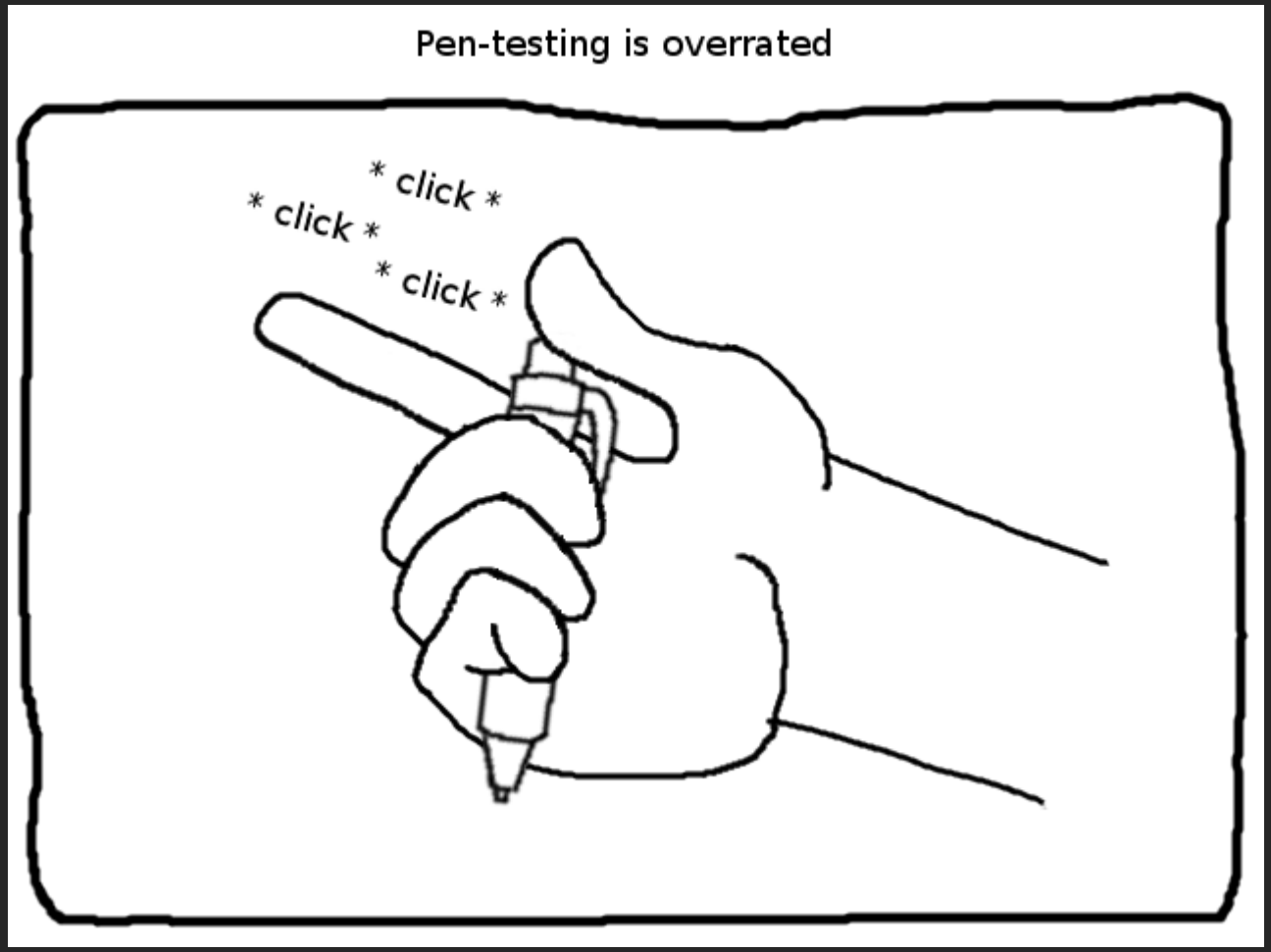
Switzerland

CNN, 25.09.2001

Please note that the views and opinions expressed during this presentation are my own and not necessarily my employers.

The 99¢ heart surgeon dilemma

Pen Testing?



Judging a painter is easy...

Good

Bad

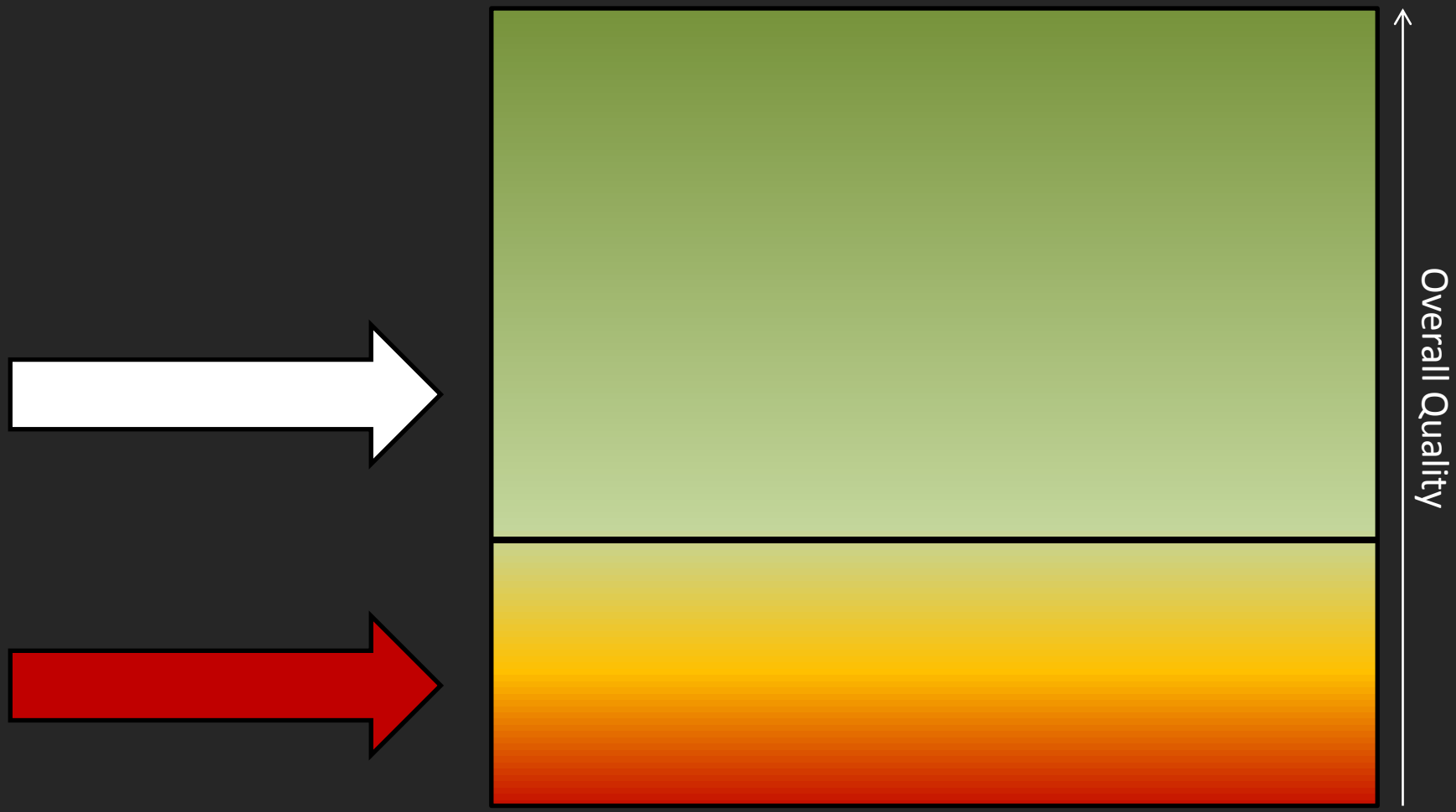
This is how most of our clients see **us**

Good

Bad


PENETRATION TESTING
EXECUTION STANDARD
PTES

Killing «bad» pentesting



5173 Pages


«Due to copyright reasons, all of our documents are print-only by default. If you would like to purchase an electronic version at additional cost, please contact our sales staff.»*
Redacted
* Translated from German

Bombs?!

Cross Site Scripting in

„http://intranet.[redacted]/web/search.aspx“

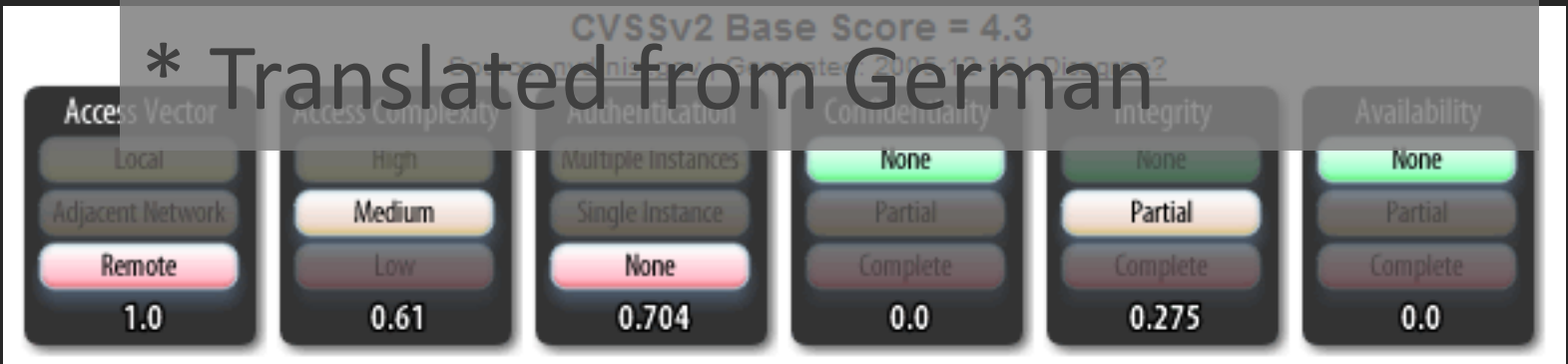
Durch die fehlerhafte Eingabevalidierung des Parameters „s“ kann beliebiger Scriptcode zur Ausführung gebracht werden.

«Due to the incorrect input validation of the parameter «s», arbitrary script code can be executed.»

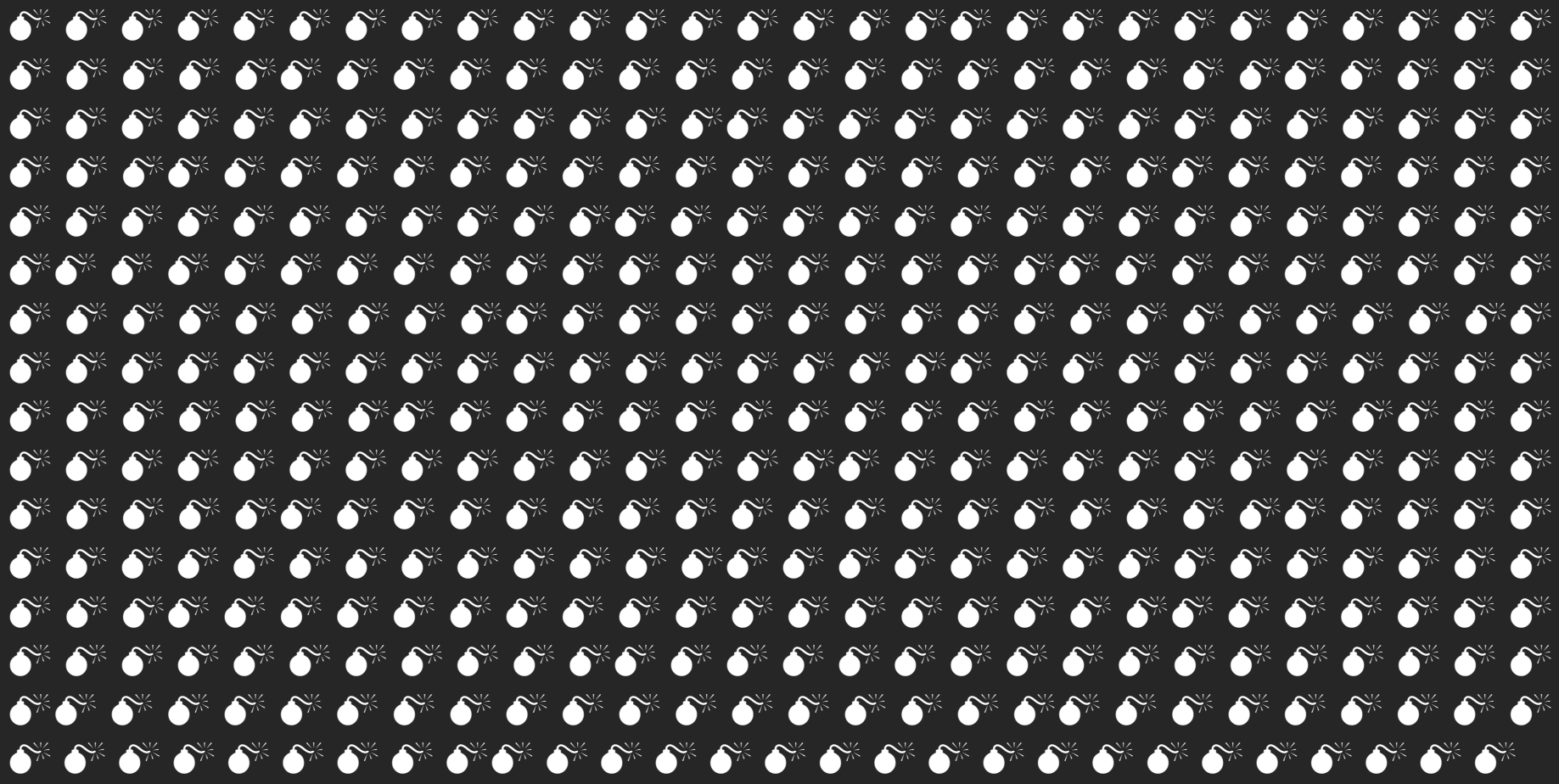
Impact Metrics?

«The amount of bombs depends on the danger the vulnerability causes. (...) There is no upper limit.»*

* Translated from German



MS08-067: Microsoft Windows Server Service RPC Handling Remote Code Execution Vulnerability



Fat Fingers

We tested the complete IP range [redacted].231.[redacted].1/24 supplied by the customer.

Based on the results, we can clearly state that the target range has a high level of security, since no services are supplied and only few hosts are available from the internet.

10.231.0.1/24

- 10.213.0.1/24

---

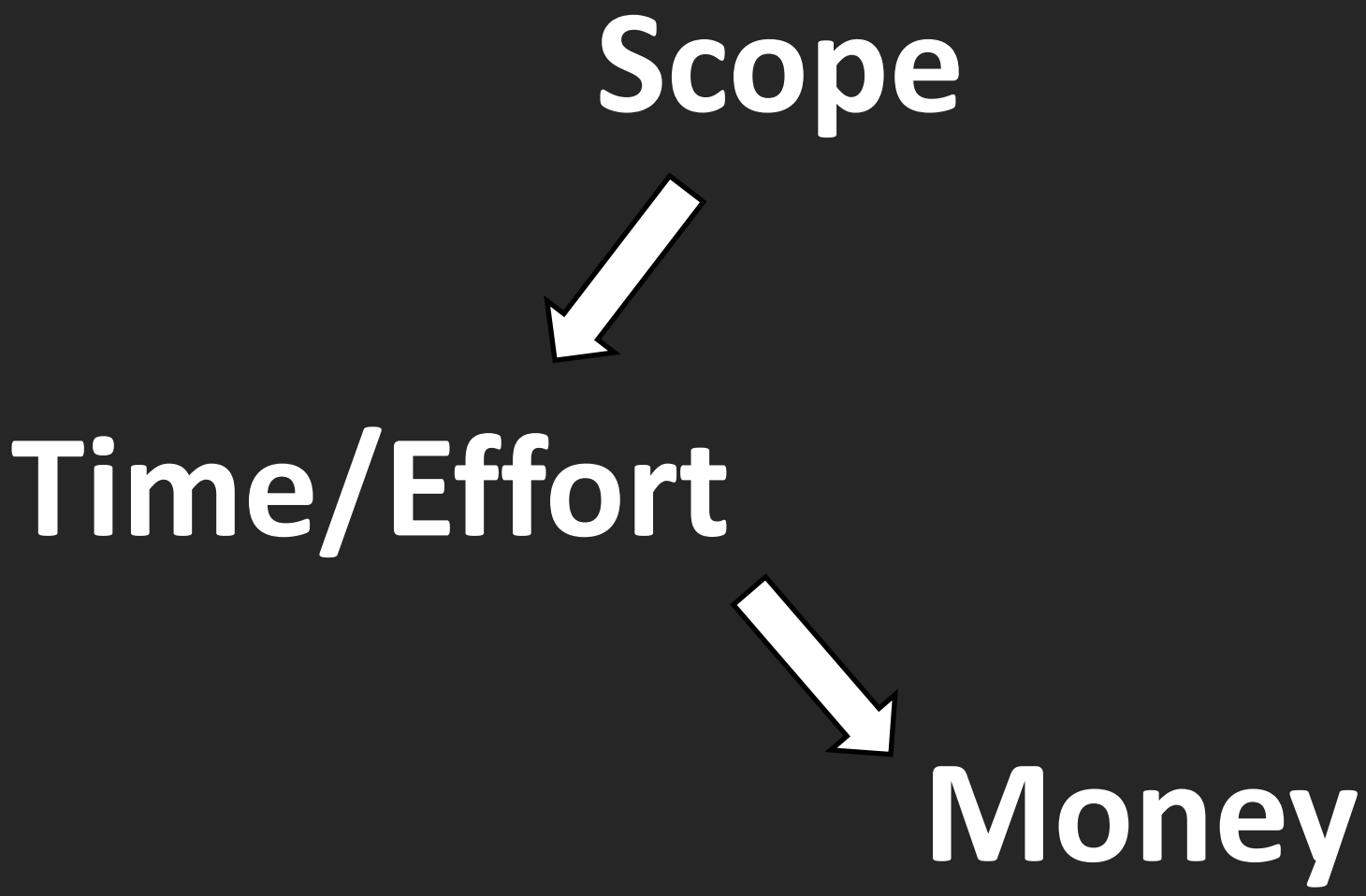
9 Days – Wasted.

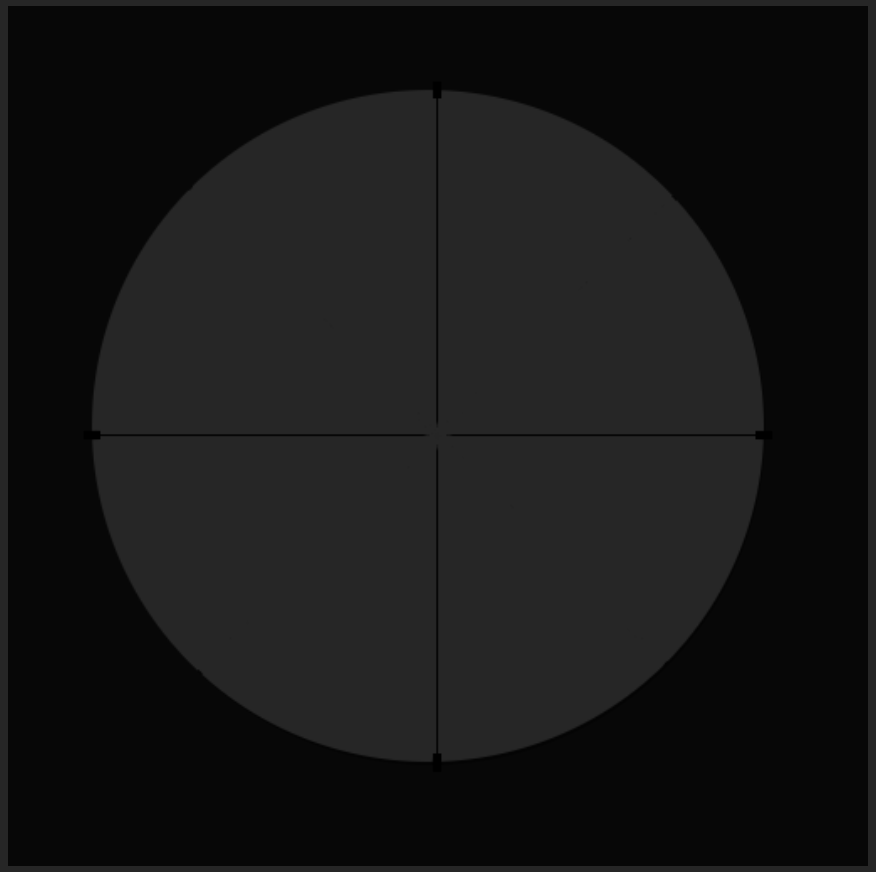
How can we improve?

SCOPE!

Things that don’t exist:

- Unicorns
- Imaginary childhood friends
- A decent Metallica album after 1991
- **«No Scope»**


Scope
Time/Effort
Money

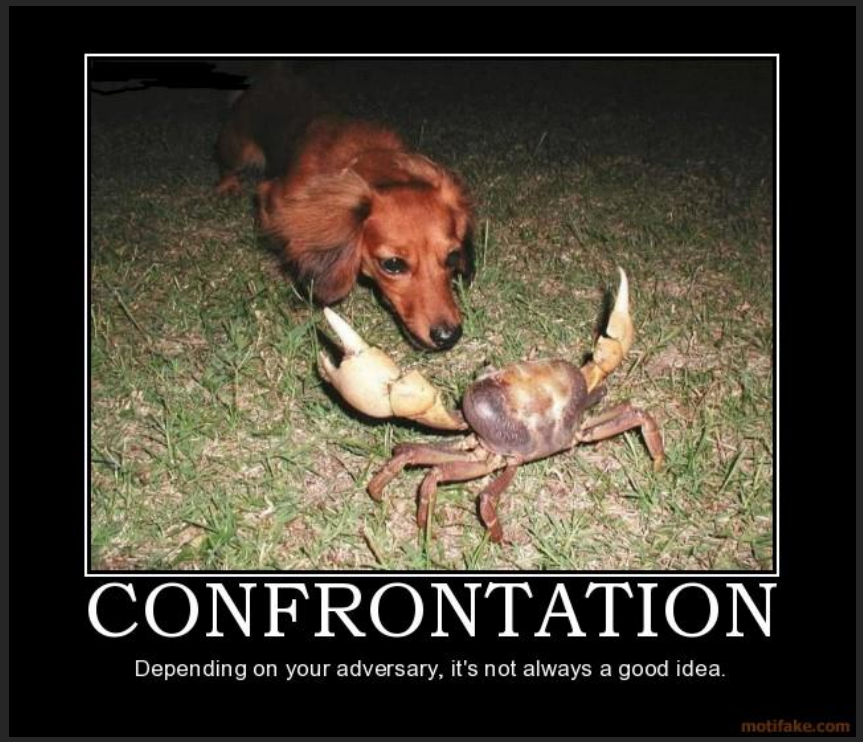


Out of Scope

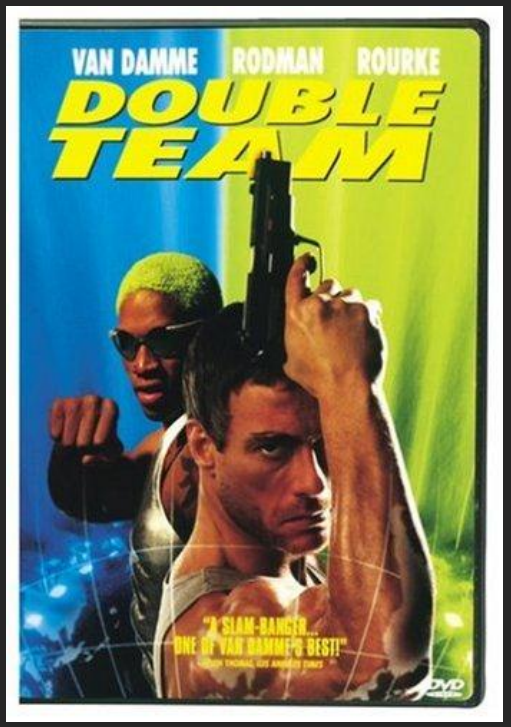
Work with the client.

Things get a lot easier...

Confrontation



Working together



Talk to the suits.

Scanning is stupid.

Scanner Monkey Mode

run nmap
run nessus/nexpose
run Metasploit/Core/Canvas
db_autopwn (...)
Root as much as you can.

Real World Mode

Send well-crafted phishing mail
Compromise client
Beacon out on tcp/443
Exfiltrate data

Get to the heart of the company.

Scratching on the surface...

Help killing bad pentesting.
http://www.pentest-standard.org

Check out the PTES-G!

... and come party with us at Blackhat/Defcon/BSidesLV

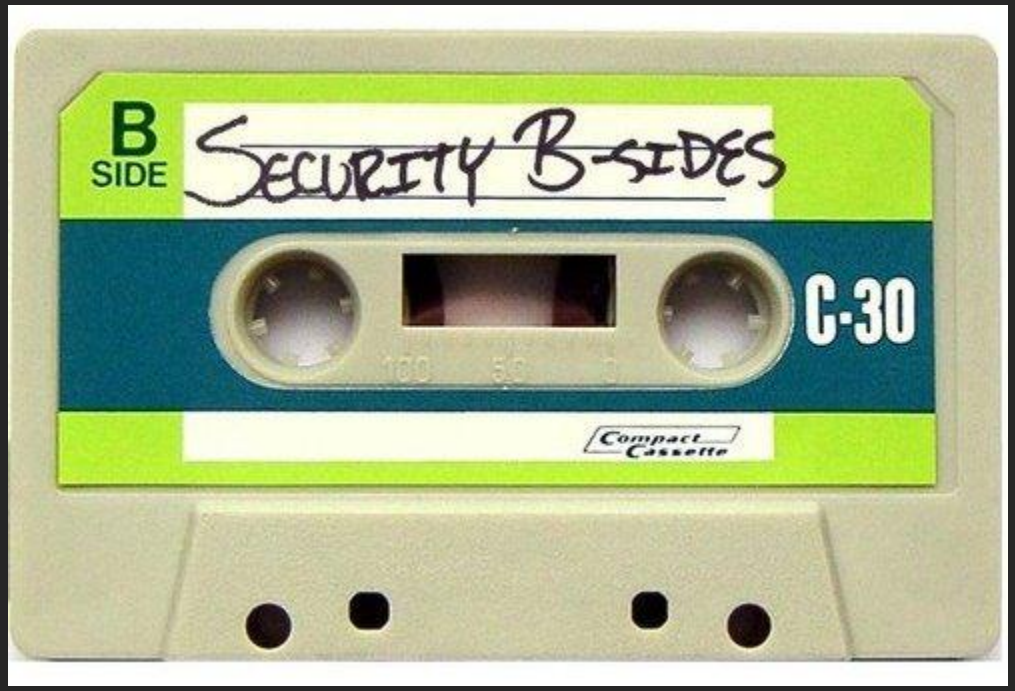
One last thing...

«We were unable to complete the task because it [the website] was too big.»

Thank you, Ben Jackson!

http://code.google.com/p/weblabyrinth/

Thank you.



The hashdays 2011 conference will be held on October 26th - 29th 2011
Lucerne, Switzerland
CFP is still open...