
# Ethical Hackers Are Your Best Friends

**Xavier Mertens - Principal Security Consultant**

**"If the enemy leaves a door open, you must rush in"**
**(Sun Tzu)**

# # whoami

- Xavier Mertens
- Not $VENDORS' best friend
- Interested in your $DATA!




# # whoami

/dev/random
Can't sleep, hackers will eat me!

Search

About Me | Disclaimer | Tools

## DNS Hijacking With Just One Mail

January 15, 2014 21:15 | 17 Comments | Xavier


This is not new but it still happens in 2014... Hijacking a website with just a small e-mail. Here are the facts. For a while, I'm hosting a friend's website. His website is quite old and it already moved from servers to servers depending on my deployed infrastructure. A few weeks ago, I notified my friend that a new change should occur asap: The website will be moved (again) to another IP address. Since the last server change, the domain name also moved and is now hosted by an ISP. My friend trusted me and suggested to contact directly the ISP. In this case, the ISP was the registrar and hosting the zone on its DNS servers at the same time! I followed the procedure and contacted the registrar as mentionned on dns.be:

**Registrar technical contacts**

| | |
|---|---|
| **Name** | Belgacom DNS Masters |
| **Organisation** | Belgacom sa/nv |
| **Language** | English |
| **Address** | boulevard du Roi Albert II 27<br>Koning Albert II laan 27<br>1030 Brussels<br>Belgium |
| **Phone** | +32.80023452 |

### Follow Me

### Upcoming Events

Stay tuned!

### Recent Posts

DNS Hijacking With Just One Mail

Building IP Reputation Lists from Snort Rules

Review: Mobile Security: How to Secure, Privatize and Recover Your Devices

OWASP Belgium Chapter Meeting Wrap-Up: Using Browsers Otherwise!

Twitter Used As Security Awareness Media: "FiveWordSecurityHorrors"

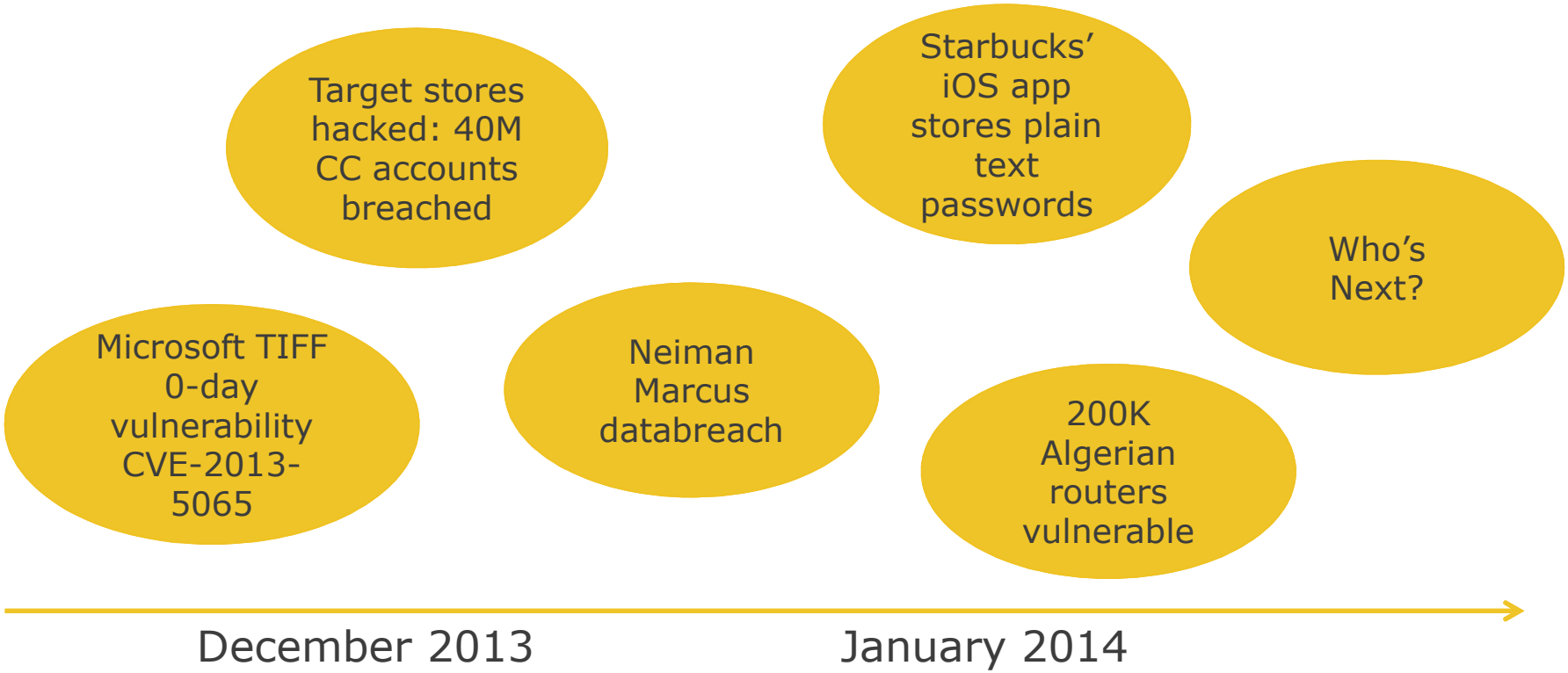
<warning>


</warning>

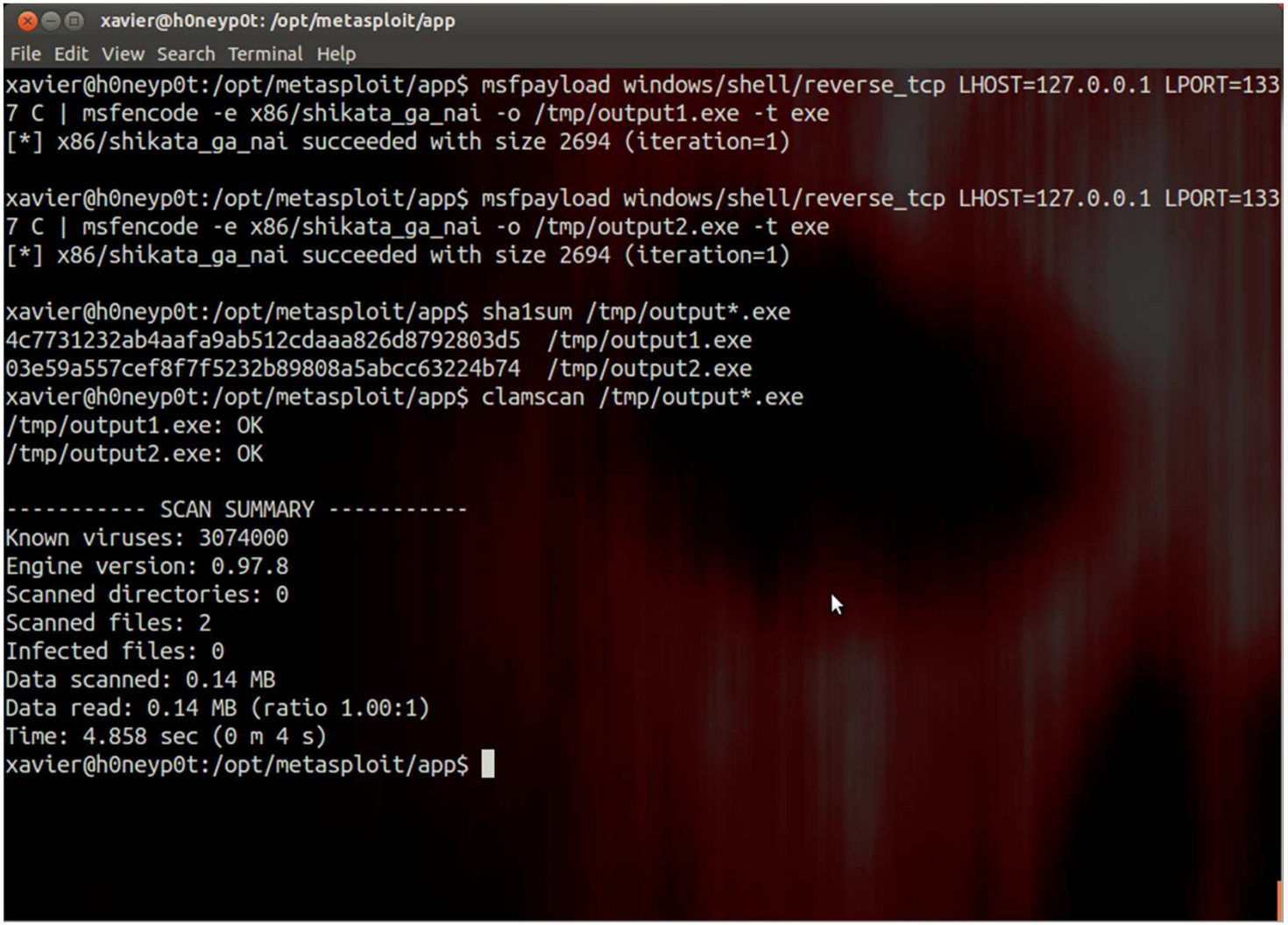
# Agenda

- **Introduction**
- We all fail
- Auditing VS. Pentesting
- How?
- Limitations!
- Conclusion

# Recent Events



# But I've An Antivirus...



# But I Also Have A Firewall...

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 0 | | Any | Any | Any Traffic | Any | accept | Log |

# And Many Other Stuff...

# Like Airplane Crashes

# The Weakest Link

# Security $VENDORS

- Bound to fail against **targeted** attacks
- Might increase the surface attack(1)
- Prone to broadcast a false sense of security

Our 2.0-NG-software deployed in the cloud will protect you against all APT…

(1) Turning your AV into a botnet - bit.ly/1aL7GcL

# “Ethic”

“A set of moral principles of right and wrong that are accepted by an individual or a social group”

# “Hacking”

“Practice of modifying computer hardware, software or any other electronic device to accomplish a goal outside of the creator’s original purpose. People who engage in computer hacking activities are often called ‘hacker’”. Hackers are good guys!

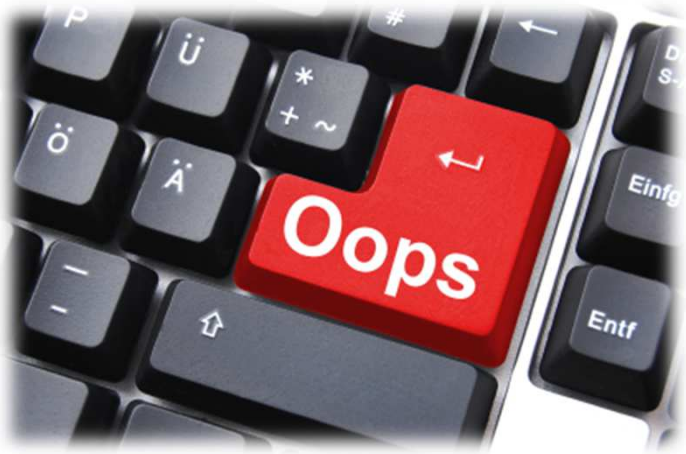
Ethical Hackers help you to find security holes in your infrastructure or process using the **same tools** and **techniques** as bad guys

# Agenda

- Introduction
- **We all fail**
- Auditing VS. Pentesting
- How?
- Limitations!
- Conclusion

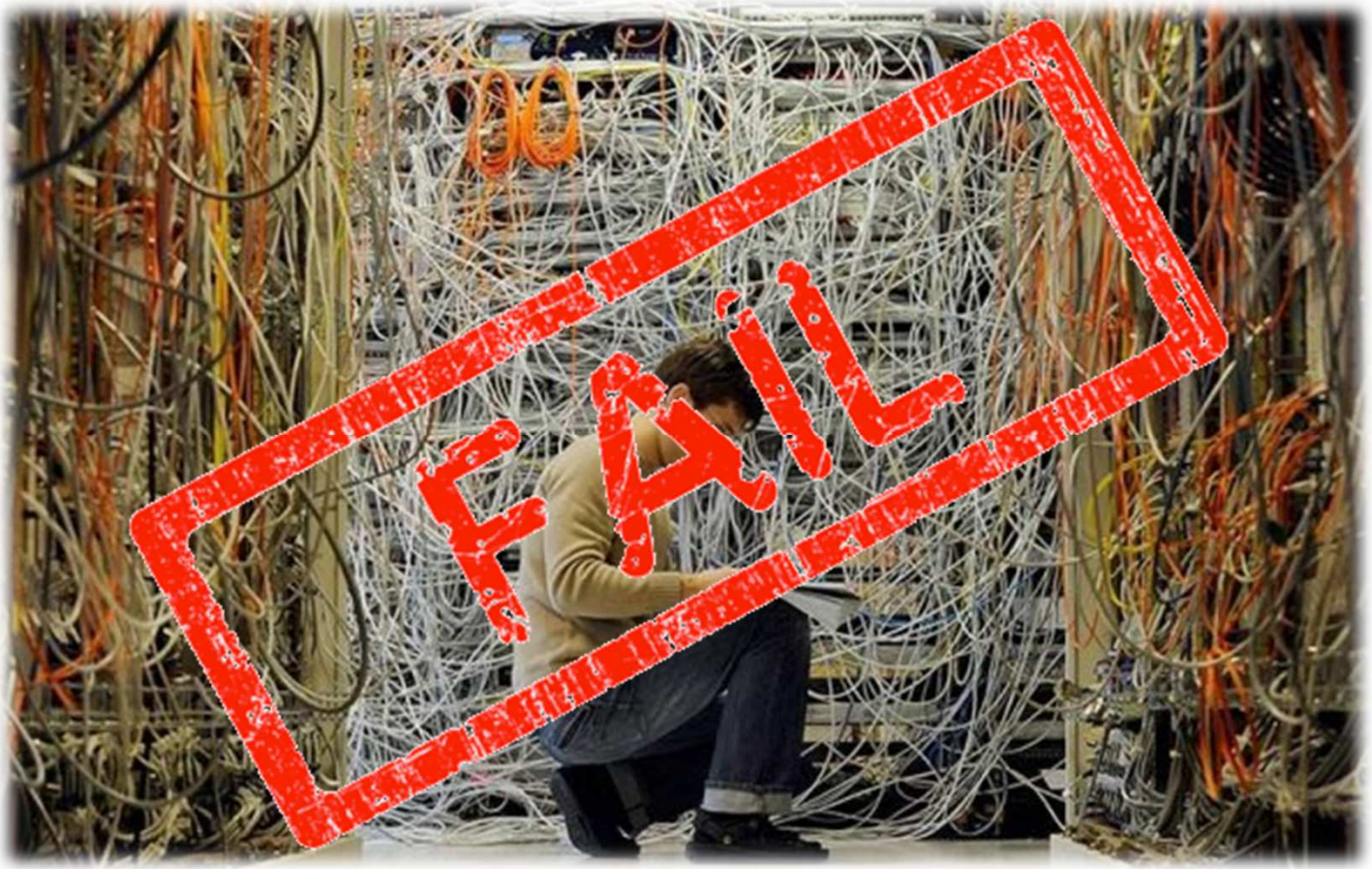
# People...

- The problem has been located between the keyboard and the chair
- Error is **human**
- Programs are written by humans, so they have **bugs**



# Misconfigurations

# Complexity



# Patching


The Register®
Biting the hand that feeds IT
Data Centre Software Networks Security Policy Business Jobs Hardware Science
Search site
SECURITY
Oracle spoils
patches
By Richard
16th January 2014
Follow
16
RELATED STORIES
If you're still waiting for Firefox on Windows 8, don't hold your breath
administrators who decided it
quiet week were wrong: Oracle
has
patches, and when you're finished, it'll
be time
for them.
Let's start
which among other things is taking another stab at securing
Java, fixing 36
authentication". All but one are client-side vulnerabilities, and ten of them are rated
by Oracle at 9.3 or 10 on its vuln scale.
MOST READ
COMMENTED
galaxy is INSIDE OUT. Just
pected, mutter boffins
sticks thumb in Microsoft's eye, extends
Windows 7 option for new machines
Mystery 'doughnut' materializes in front of
Mars rover: 'OH MY GOD! It wasn't there
before!'
ESA rejoices as comet-chasing Rosetta
probe wakes from 3-year nap
Although 'password' is no longer the #1
sesame opener, it's still STUPID
SPOTLIGHT
45
19
FAIL

# We are lazy!

# The Business

# Agenda

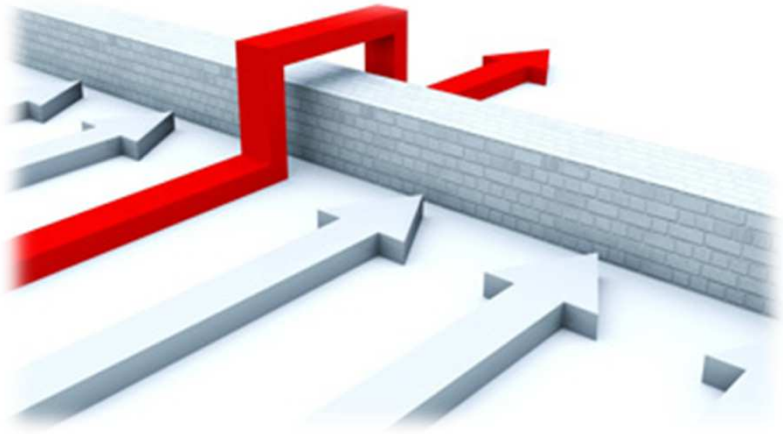
- Introduction
- We all fail
- **Auditing VS. Pentesting**
- How?
- Limitations!
- Conclusion

# Auditing

"Auditing is defined as a **systematic** and **independent** examination of data, statements, records and performances (in this case IT) of an enterprise for a **stated** purpose" (Source: wikipedia)

# Pentesting

"Pentesting is an act performed with a **specific goal** which determines the success status of the test. It can be **any** combination of **attack** methods depending on the goals and rules of engagement set" (Source: wikipedia)



# “It’s A Question of View”

Does you have a Web Application Firewall?

# Think As A Bad Guy

Will you trust this guy?

# But Look Like A Good Guy

And this one?

# Wait, Why Attacking Me?

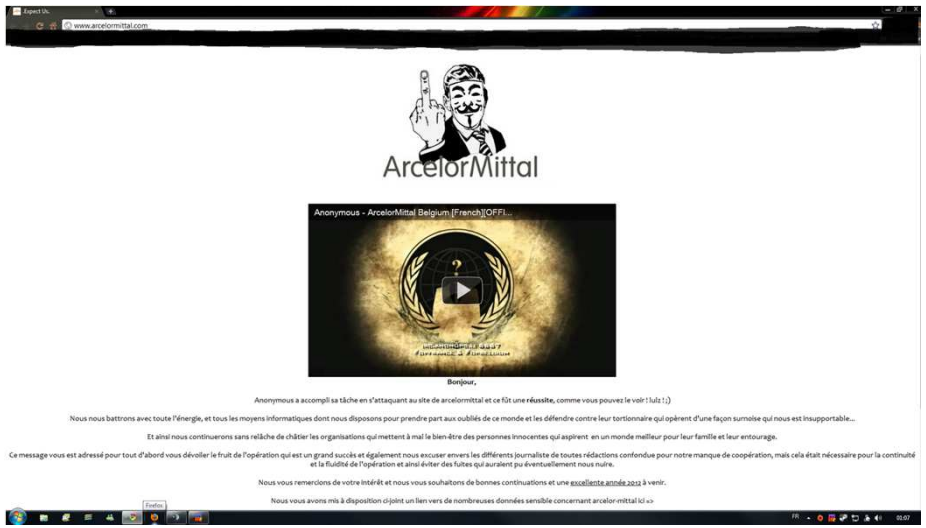
- Information is valuable!
  - Customers details
  - Financial information
  - Patent
- You’re not the end-target. Are you providing services to big customers? (pivot)

# Multiple Targets

- Anything that runs "code"
  - Computers, printers, webcams, phones, routers
- Hardware
  - Locks, cars, SCADA, scales

# Impacts

- Brand reputation

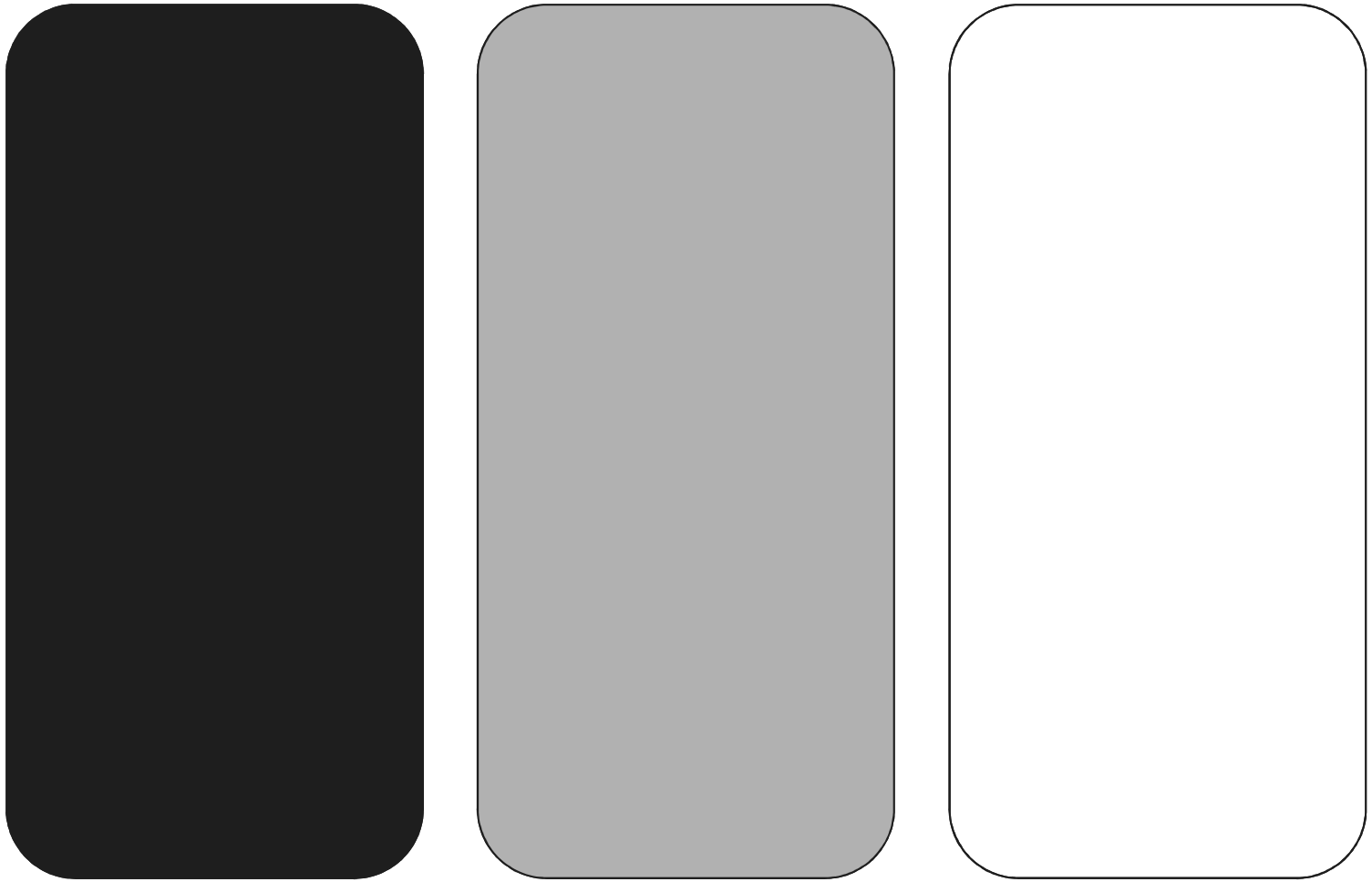



- Financial
  - Loss of revenue
  - EU Data Breach notification law soon?

# Agenda

- Introduction
- We all fail
- Auditing VS. Pentesting
- **How?**
- Limitations!
- Conclusion

# Different Approaches



# Step 0 – Engagement

# Step 1 – Public Info

- “You just have been indexed!”
- Google is your best friend!
  - site:mytarget.com "Microsoft OLE DB Provider for SQL Server“
  - site:mytarget.com "You have an error in your SQL syntax“
- OSINT

# Step 2 – Reconnaissance

- Scan your target
- Onsite visit & plug a computer
- Grab stuff on eBay
- Look for garbage

# Step 3 - Exploit

- Computers
  - Obsolete or internal software
- Humans
  - Drop USB keys
  - Send emails
  - Buy flowers (secretary) or goodies (techies) ;-)

# Step 4 - Attack

- Remain stealth
- Stay in
- Exfiltrate
- Cover your tracks

# Step 5 – Reporting

- After the fun, some homework!
- Address the management (a screenshot is worth a thousand words)
- Put risks levels on findings (be realistic)
- Use the report to define your security roadmap

# Agenda

- Introduction
- We all fail
- Auditing VS. Pentesting
- How?
- **Limitations!**
- Conclusion

# Bad Guy VS. Good Guy

- No scope constraint
- No time constraint
- No budget constraint
- No NDA
- Can be destructive
- Engaged resources are directly related to the target value

# Agenda

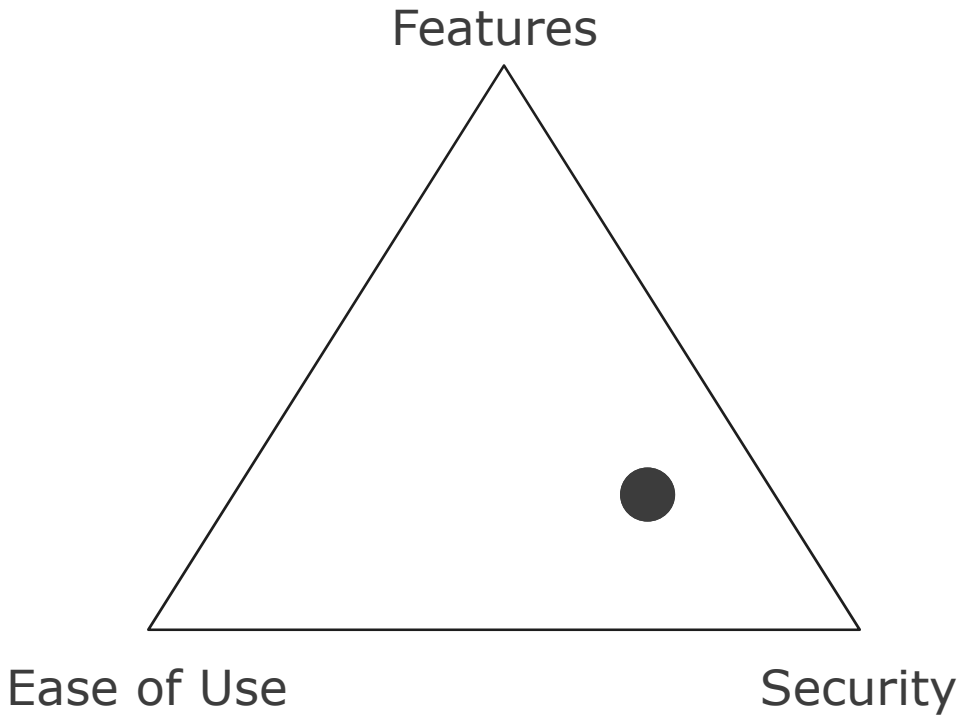
- Introduction
- Why we fail?
- Auditing VS. Pentesting
- How?
- Limitations!
- **Conclusion**

# Conclusion

- Security == Ability to resist to attacks
- Don’t ask “How?” but “When?”
- We live in a digital world run by analog managers
- Classic audit results might give a false sense of security
- Ask some help from ethical hackers!

# Conclusion

- Keep in mind the “security triangle”



**Thank You!**

Interested?
Contact your Account Manager for more information!