

# ***Red Teaming***

*15 Minuten die Welt aus der Sicht eines Angreifers erleben*

***René Freingruber***

*Information Security Auditor,  
Kapsch BusinessCom*

# About me



- > 7 years experience as pentester / red teamer / researcher
- > Twitter: [@ReneFreingruber](https://twitter.com/ReneFreingruber)
- > Staatsmeister Cyber Security Austria 2019
- > Research topics:
  - 2014: Bypassing EMET
    - 31C3, DeepSec, ZeroNights, RuxCon, ToorCon, NorthSec
  - 2015: Bypassing Application Whitelisting
    - CanSecWest, DeepSec, Hacktivity, NorthSec, IT-SeCX, Bsidess Vienna, QuBit
  - 2016: Hacking companies via firewalls
    - DeepSec, Bsidess Vienna, DSS ITSEC, IT-SeCX (lightning talks Recon EU and hack.lu)
  - 2017 & 2018: Fuzzing talks & workshops
    - DefCamp, Heise DevSec, IT-SeCX, Bsidess Vienna, RuhrSec, BruCon, Hack.lu

# Security Audit & Assessment Team



# ***Security Audit & Assessment Team***



**+80 Security Systems Engineers**

```
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64
64 bytes from 127.0.0.1: icmp_seq=5 ttl=64
^C
--- 127.0.0.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 0.07ms
rtt min/avg/max/mdev = 0.021/0.028/0.044/0.011ms

[root@chad]~# nslookup kapsch.net
Server:          192.168.124.2
Address:         192.168.124.2#53

Non-authoritative answer:
Name:   kapsch.net
Address: 148.198.3.2

[root@chad]~## ping kapsch.net
[root@chad]~# ping kapsch.net
PING kapsch.net (148.198.3.2) 56(84) bytes of data:
^C
--- kapsch.net ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 0.76ms

[x]-[root@chad]~# ./hack.exe kapsch.net
trying to hack....
target is secure!
no hacking possible!

[root@chad]~#
```



# *This talk is about flaws and mistakes*

# Test Test Test !

> Performing tests is nowadays mandatory:

- Programmers → Unit Tests, Website audits, ...
- Admins → Internal Audits, Test Backups, Netflix “Chaos Monkey”, ...
- End Users → Social Engineering Audits, ...

# Emergency tests!

- > IT unrelated areas also test the emergency!
  - Fire department regularly perform tests
  - Police special forces regularly perform tests



**kapsch** >>>  
challenging limits

# ***Threat Detection***



# Threat Detection

- > Companies buy expensive threat intelligence software which can \*insert fancy marketing word\* and which solves \*insert fancy marketing word\* ...
- > **BUT: Nearly nobody verifies if the system is really working**
  - Does it alert in emergency?
  - Can it detect real-world attacks?
  - How long does it take until someone reacts to the alert?
  - How simple is it to stay under the radar?

# Who should do red teaming?

## > Requirements:

- A base level of security should be established
- Threat detection capabilities

## > The advantages are:

- Check if the system can detect real-world attacks
- Identify blind spots in monitoring solutions and security strategies
- Training for administrators for emergency



## ***Scenario 1: Unimportant system***

# Scenario 1: Unimportant system

- OSINT revealed an unaesthetic looking website, hosted in the cloud
  - Never tested, company: “standalone and old website → useless for hackers”
1. Default credentials guessed based on documentation
  2. Cleartext password from admin from 2011 found in FileZilla cache
  3. Password bruteforce based on identified password pattern to get access
    - Was not detected because only this “service was not monitored” (and no multi factor authentication...)
  4. SSH backdoored → All company passwords obtained in a week



**kapsch** >>>  
challenging limits

## ***Scenario 2: Password Spray***

# Scenario 2: Password spray

- OSINT + quick pentest for low hanging fruits during first days lead to nothing
  
- 1. OSINT revealed lots of users (LinkedIn, Xing, Research Gate, ...)
- 2. Service with LDAP authentication but which does not support MFA (multi factor authentication) was identified
- 3. Password spray with “Sommer2019”, “Sommer2019!”, “Password2019!”, “Sommer19”, “<CompanyName>2019” was done
  - Monitoring solution could just detect bruteforce, no password spray ...
- 4. ~20 User accounts compromised → Full domain compromise



## ***Scenario 3: Phishing against 2-factor authentication***

# Scenario 3: Phishing against 2-factor authentication

> Phishing is the most effective entry point!

> Scenarios:

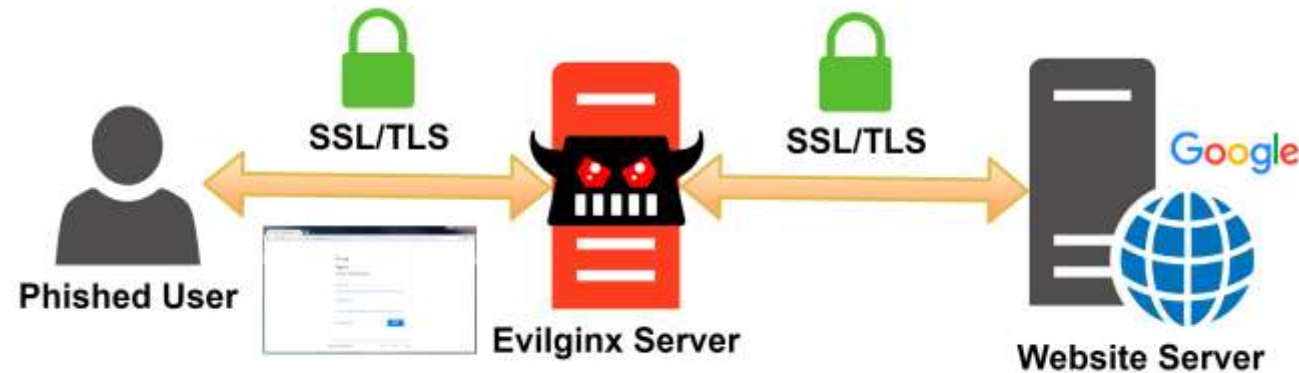
- Student survey → Name of AV and security products, OS version, ...
- Inside the target building install a poster with a contest to win Sodexo vouchers
- Send a link to a phishing site which shows the companies Christmas bonus
- .... (be creative)



# Scenario 3: Phishing against 2-factor authentication

> Bypass multi-factor authentication with:

- evilginx2
- Modlishka



source: <https://breakdev.org/evilginx-2-next-generation-of-phishing-2fa-tokens/>

> Other useful technique to bypass sandbox solutions

- HTML smuggling, Domain Fronting, Azure Information Protection, ...

# Scenario 3: Phishing against 2-factor authentication



Von: Microsoft Exchange [mailto:msexchange@outlook.com]  
Gesendet: Mittwoch, 04. Mai 2016 16:53  
An: [Redacted]  
Betreff: Ihre Mailbox ist fast voll

## Ihre Mailbox ist fast voll.

945MB  950MB

In Verwendung Verfügbar

Ihr Administrator hat den Speicherplatz bereits erweitert. Um die Erweiterung abzuschließen, navigieren Sie über den folgenden Link zu Ihrem Exchange Webportal: <https://mail.kapsch.net/owa>

Nach dem Login werden Sie aufgefordert, die Speichererweiterung zu bestätigen.

Gesendet von Microsoft Exchange Server

mail.kapsch.net:ssl3.at?rid=98847d6c3541d

entesting Malware Analysis

Domain\user name:   
Password:   
Sign in

Connected to Microsoft Exchange  
© 2010 Microsoft Corporation. All rights reserved.

Submitted Data May 4th 2016 5:36

View Details

Parameter	Value(s)
destination	https://mail.kapsch.net:ssl3.at/owa/
flags	0
forcedownlevel	0
isUtf8	1
password	Klartext/PW
trusted	0
username	Domänenbenutzer



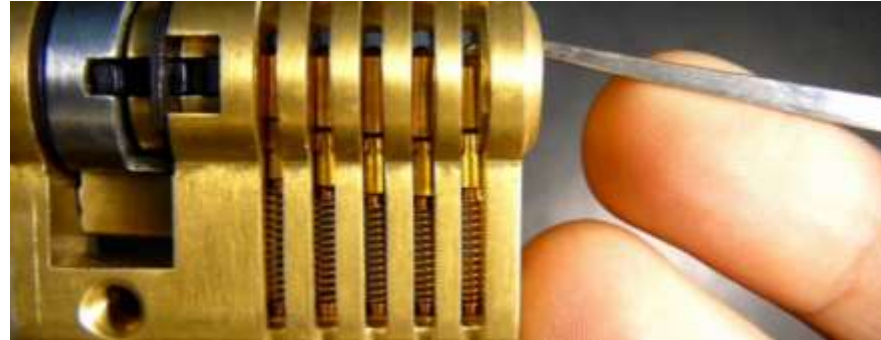
**kapsch** >>>  
challenging limits

# ***Scenario 4: Physical Entrance & Hardware Hacking***

# Scenario 4: Physical Entrance

## > LockPicking

- Door lock bypass tools

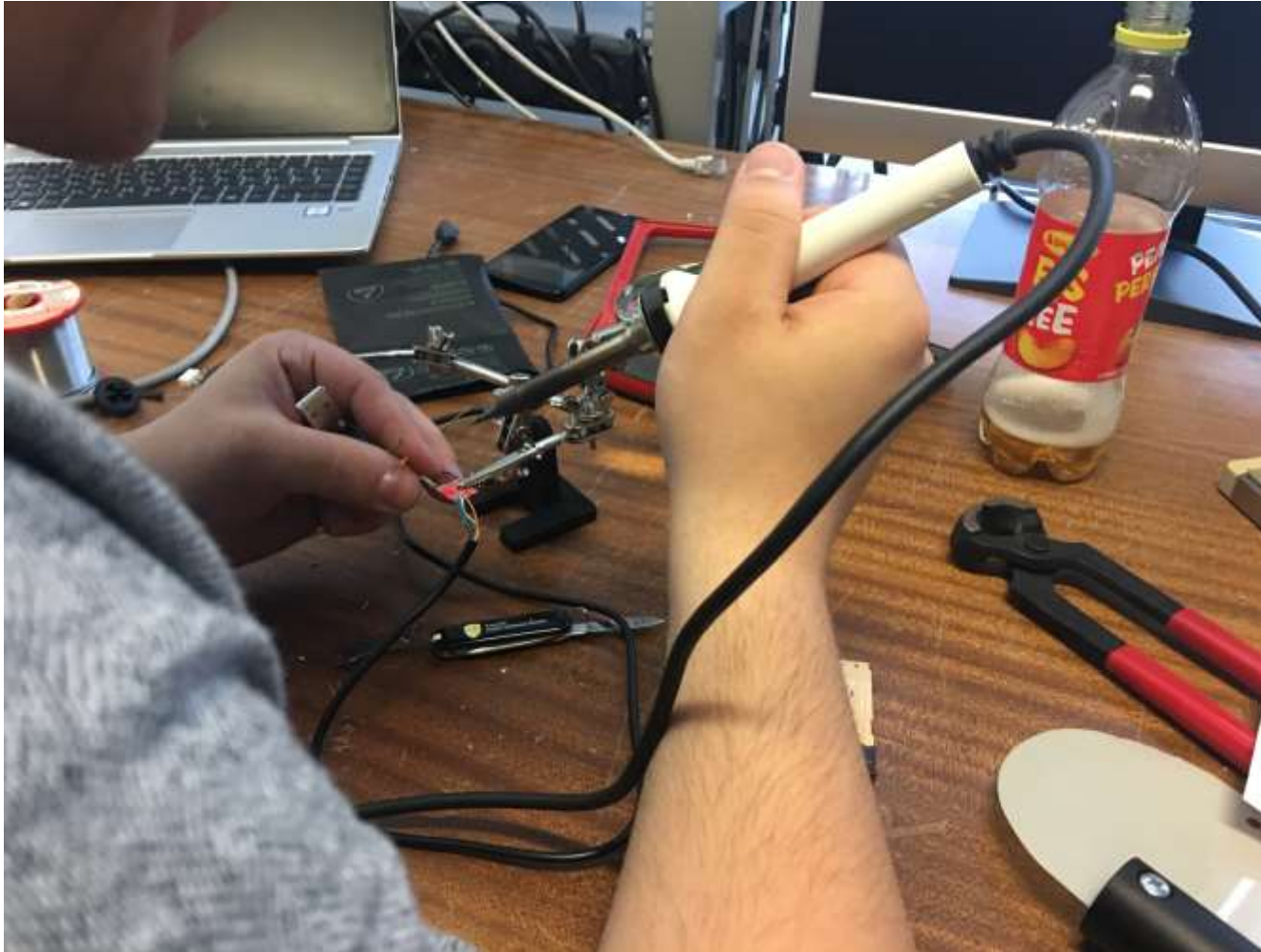


## > Steal RFID cards

- Proxmark
- RFID Thief



## Scenario 4: Physical Entrance



## Scenario 4: Physical Entrance



# Scenario 4: Physical Entrance

> Place keyloggers / BadUSB or RubberDucky



> PwnBox / Raspberry Pi

- with NAC bypass and 4G backchannel



# *Thank you for your attention!*

***Looking for a job?***

<https://glhf.at>

***René Freingruber***

*Information Security Auditor*

***Kapsch BusinessCom***

Wienerbergstraße 53 | A-1120 Vienna | Austria

Mobile +43 (0)664 628 5760

email: rene.freingruber@kapsch.net



**Please note:**

The contents of this presentation are the intellectual property of Kapsch AG. All rights reserved regarding the copying, duplication, modification, usage, publication, or passing on of the contents to third parties. The aforementioned actions are expressly forbidden without the prior written approval of Kapsch AG. Product and company names may be the registered brand names or proprietary trademarks of third parties. These are used in this presentation solely for illustration purposes and to the advantage of the lawful owner, with no intent to infringe their property rights.