
ONE DOES NOT SIMPLY
WALK INTO A BUILDING
(OR DO THEY ?)
imgflip.com

Briefing

I. Context and goals of the mission
II. Initial intrusion
III. Access persistence
IV. Goal collection
V. Conclusion

Who am I?

Volker Carstein (@volker_carstein)

- Pentester by day, jack of all trades by night
- Work @ BSECURE (pentest, physical intrusion, RTO)
- Social engineering, OSINT and offensive security (a preference for Active Directory)
- Speaker @ LeHack, Barbhack, Insomni'hack, SecSea, etc

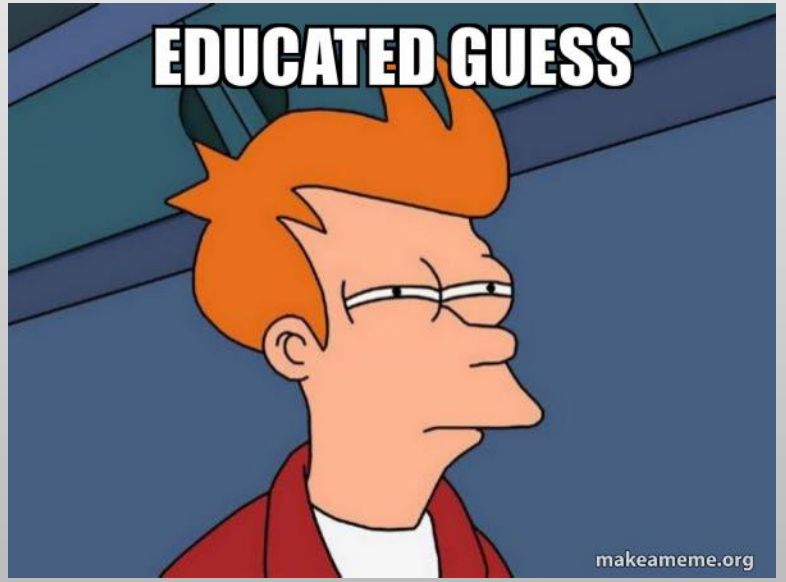
I - Context and goals of the mission

- Physical “pentest” mission at Bsecure
- One week, 2 auditors
- **Goals:**
  - Enter the building (duh)
  - Steal confidential information
  - Steal equipment
  - Steal a bicycle (???)
  - If possible attack the IT part, but not a priority

II - Initial intrusion

- Ideally, to prepare an intrusion, how much preparation and research is needed?

1. None 😎
2. One day
3. About a week
4. More than a week



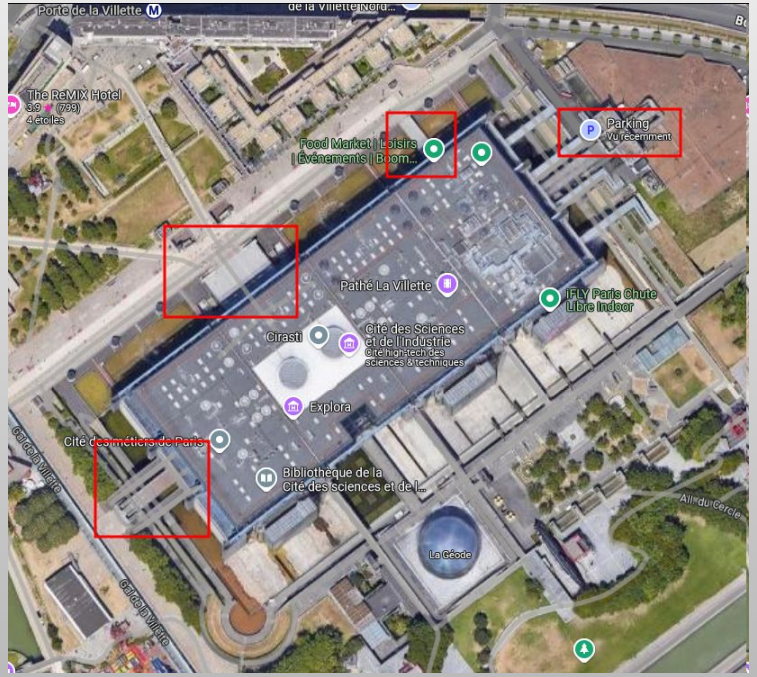
II - Initial intrusion

- Ideally, to prepare an intrusion, how much preparation and research is needed?

1. None 😎
2. **One day**
3. **About a week**
4. More than a week

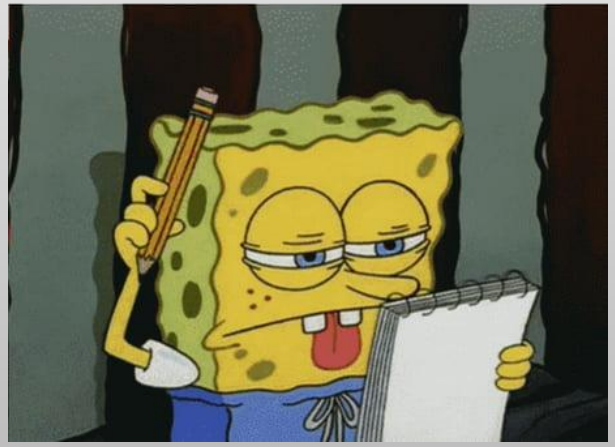
II - Initial intrusion: research

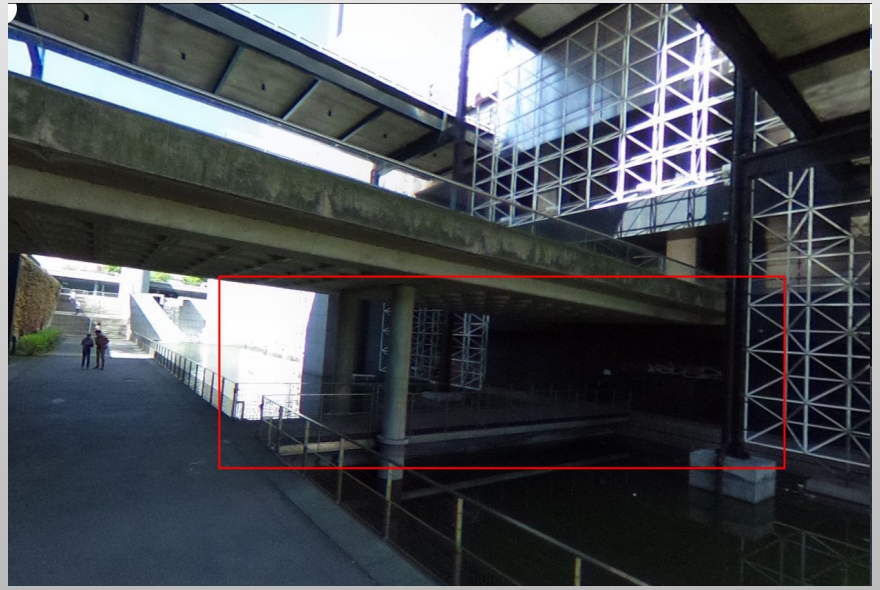
- Satellite pictures (Maps, Earth, Yandex, etc.)



II - Initial intrusion: research

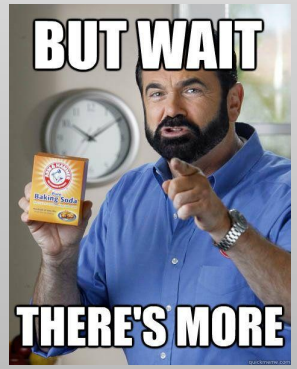
- Satellite pictures (Maps, Earth, Yandex, etc.)
- Street view pictures





II - Initial intrusion: research

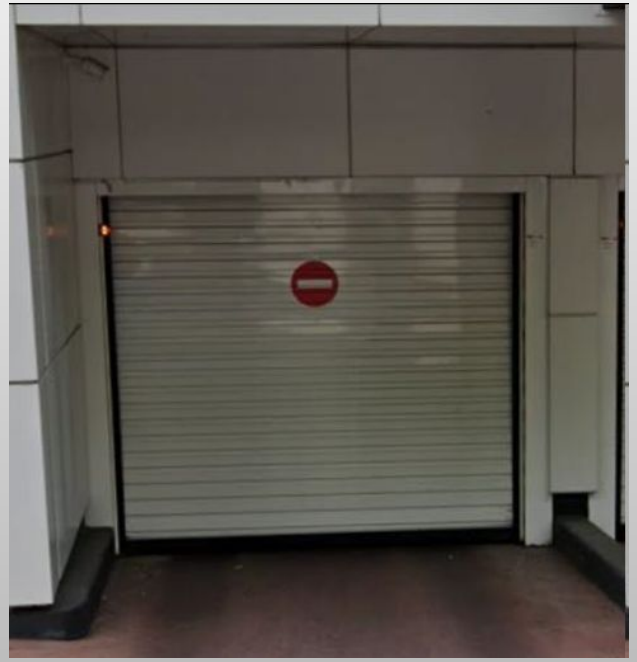
- Satellite pictures (Maps, Earth, Yandex, etc.)
- Street view pictures
- Plans (for tourists, evacuation/fire safety, etc.)
- Pictures inside the buildings



II - Initial intrusion: research

- Pictures of the badges (for potential copies)
- OSINT on employees/providers (their position, dress code, etc.)
    - Particularly useful for social engineering

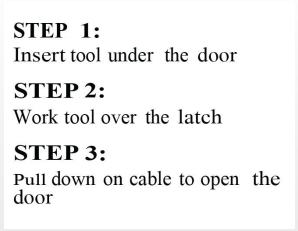
II - Initial intrusion: research



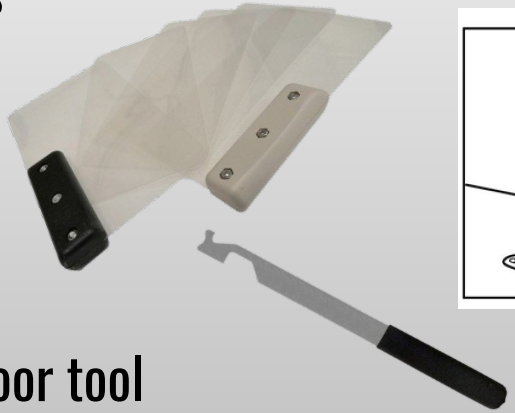
\+ Emergency exit

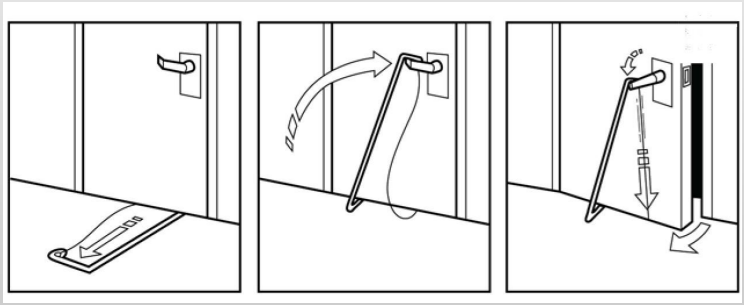
II - Initial intrusion: tools

II - Initial intrusion: tools



- Adequate dress code (in accordance with the research and the pretext)
- Lockpicking tools
  - door bypass
  - lockpicks
  - bump keys
  - pickgun
  - under-the-door tool





- Tools for badge copy (Proxmark, Flipper Zero, etc.)
- Anything that can be useful (cables, chargers, adapters, multitool)

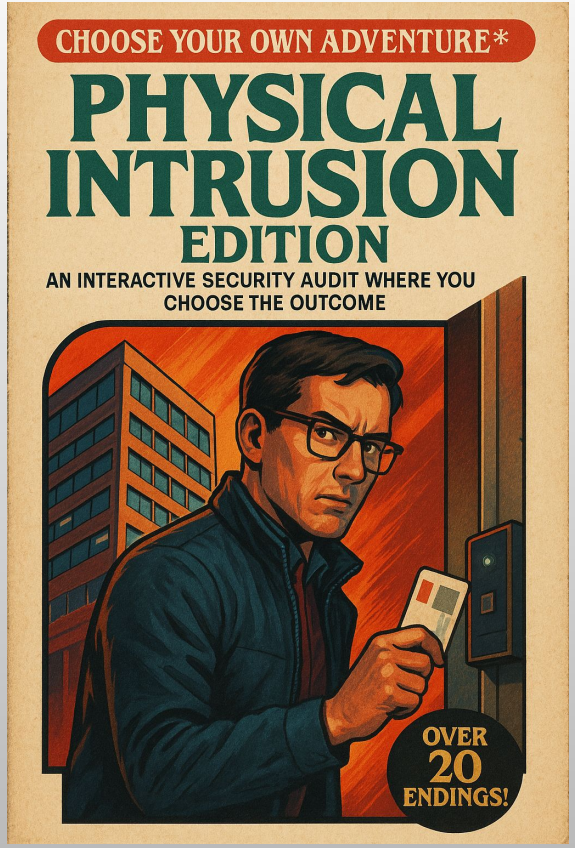
II - Initial intrusion: tools

Authorization letter/”get out of jail” card

- Allows the intrusion in the context of a security test mandated by the client organization
- Contains the identity of the auditors, their company, the mission, the client organization, the referent person to be contacted (often the person in charge of the engagement)
- Avoids issues if the auditors are detected and/or arrested by proving the intrusion is legal
- No intrusion without this letter, **it is crucial!** Minimum one copy per auditor

II - Initial intrusion

- How to get in?
    1. The delivery door
    2. The garage
    3. Windows accessible from the street
    4. The emergency exit



II - Initial intrusion: windows by the street

- By night, we notice that we can unscrew the panes
- By scratching the seal and with a window suction cup, we can gain access
- Not discreet and too complex, abandoned method
- We later learn than the windows lead to the basement, from where it is complicated to access the upper floors

II - Initial intrusion: emergency exit

- Door can be lockpicked by night with an under-the-door tool
- Camera pointed at the door, no detection
- **Initial intrusion OK**: we're at the ground floor, by night only:(
- Elevator and badge doors to access the upper floors:(

II - Initial intrusion: the delivery door

- Every morning, food delivery for the company cafeteria
- Door is left wide open because employees need to move pallets into the building
- We enter nonchalantly, no one says a thing
- **Initial intrusion OK**: we are at the ground floor
- Elevator and badge doors to access the upper floors:(

II - Initial intrusion: garage

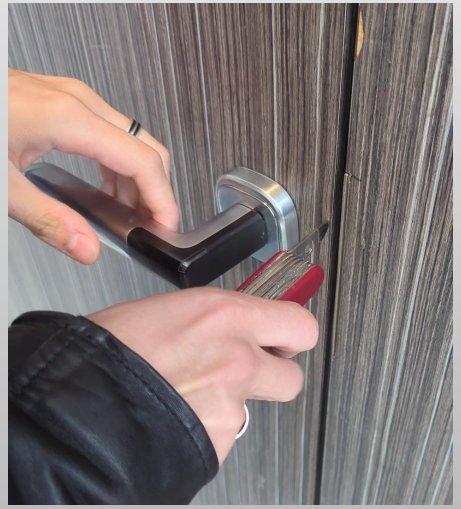
- When a car enters, we follow it on foot
- Neither the camera nor the security control center react
- **Initial intrusion OK:** we're at the garage (-1), **bicycle garage there**
- Elevator and badge doors to access the upper floors:(

III - Access persistence

- How to come back without lockpicking/tailgating/good timing?
- How to move around freely? Elevators, doors for the stairs, etc.

III - Access persistence

- Badge doors to access the stairs: **can be lockpicked!**
- Access to all floors, but risk of being detected at each floor change



III - Access persistence

- Once we've reached all floors (tailgating in the elevator, lockpicking for stair access), we walk around to find badges that were left without surveillance

- Two minimum to sustain our access
- Get more in case stolen badges are revoked
- **Access persistence OK**

III - Access persistence: bonus!

- Among one of the ground floor meeting rooms, some windows give access to the street
- We get inside the room, open certain windows (with no alarm trigger/sensor)
- Block them so they remain stuck against the frame (with some discretion)
- Come back later (by night, the day after), push the window from the exterior to enter
- **Access persistence OK**

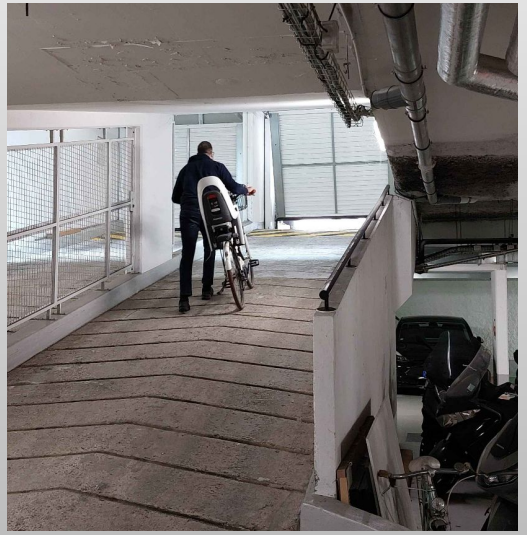
@volker_carstein

IV - Goal collection

- Enter the building ✅
- Steal confidential information
- Steal equipment
- **Steal a bicycle**
- If possible attack the IT part, but not a priority

IV - Goal collection: bicycle

- The same way we did with the doors that gave access to the stairs, SAK bypassing



IV - Goal collection

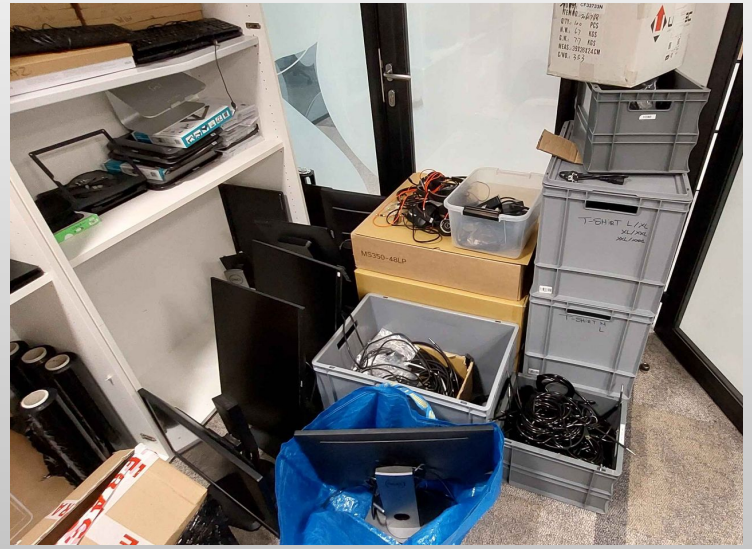
- Enter the building ✅
- Steal confidential information
- **Steal equipment**
- Steal a bicycle ✅
- If possible attack the IT part, but not a priority

IV - Goal collection: equipment

- We arrive early in the day (7:30 am), before all the employees
- IT Corner equipment storage facility: locked (key lock)
- Lockpicking via bump key
- A lot of available equipment!

IV - Goal collection: equipment

- **Theft of multiple PCs, phones, cables, etc.**
- Theft of clothes branded with the client's name
  - T-shirts
  - Hoodies
  - **Wearing them makes our presence more credible**



IV - Goal collection: equipement

- Door of the security control station opened all day, one person inside
- Call to the security call station, pretexting that someone fainted at the top floor
- During the guard's absence, equipment theft among which:
  - Walkie-talkie
  - **Surveillance camera recordings**

IV - Goal collection: equipment

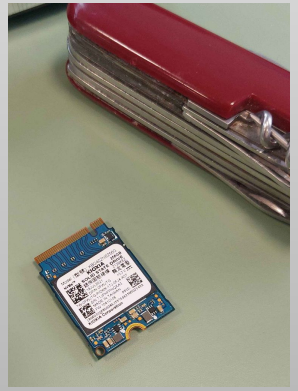
- We arrive early in the day (7:30 am), before all the employees
- In a room on the first floor, a key box with the code on it, left there by the cleaning staff
- **Theft of the building's all-purpose/master key**
- Copy of the key thanks to a locksmith with a bit of social engineering

IV - Goal collection: equipment

- Enter the building ✅
- **Steal confidential information**
- Steal equipment ✅
- Steal a bicycle ✅
- If possible attack the IT part, but not a priority

IV - Goal collection: information

- Two very important meeting rooms (investor meetings, direction, etc.)
- PCs running on Windows with Zoom (Chrome OS in other rooms)
- Hard drive dump to retrieve the local admin password
- Goal: plant a backdoor to spy on meetings



IV - Goal collection: information

- Deactivate Defender and Firewall (the PC isn't monitored so no problem here)
- Connect the meeting PC to a VPN network under our control
- Activate the option to do **RDP Shadow**
- Connect in RDP during a meeting and record it
- **Profit!**

IV - Goal collection: information

- Locate the offices of the CEO, CFO, employee who manages bank transfers, etc.
- “Don’t ask to ask, just ask!”
- No locked office, we search everything
  - A few documents
  - Confidential bin
  - Car/bike keys (?)

IV - Goal collection: information

- In an empty meeting room early in the morning, we lockpick and take out all the documents from inside the bin
- **Valid bank codes, credit cards, “blank” signed bank checks, etc.**
  + **very personal employee documents**

IV - Goal collection

- Enter the building ✅
- Steal confidential information ✅
- Steal equipment ✅
- Steal a bicycle ✅
- **If possible, attack the IT part, but not a priority**

IV - Goal collection: IT

- Easy access to the server room with the master key
- One PC in the room is unlocked and the logged-on user has interesting security rights
- Backdoor to give remote access to two colleagues
- **Compromission of the company's CI/CD**

IV - Goal collection

- Enter the building ✅
- Steal confidential information ✅
- Steal equipment ✅
- Steal a bicycle ✅
- If possible attack the IT part, but not a priority ✅

V - Conclusion: stories

- Pizza during the backdoor 🍕

V - Conclusion: stories

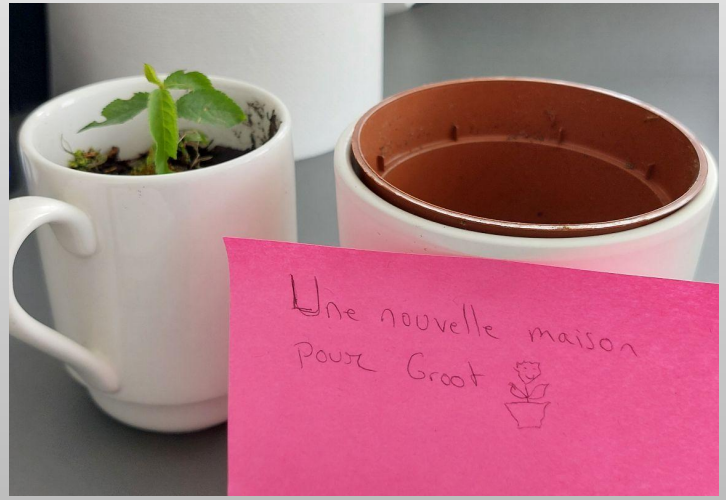
- Pizza during the backdoor 🍕
- Spotted 📹

V - Conclusion: stories

- Pizza during the backdoor 🍕
- Spotted 📹
- The blind security agent 👮

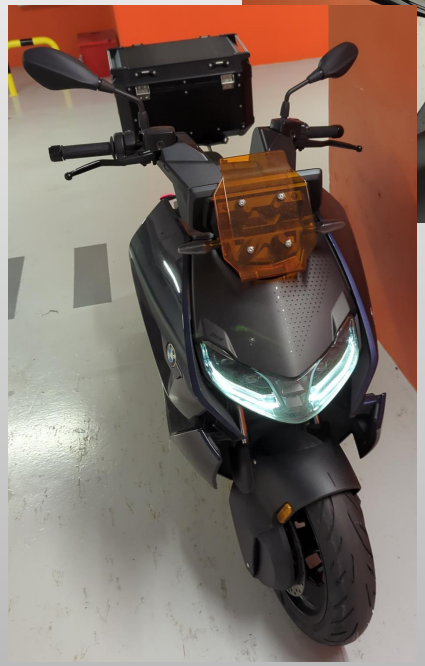
V - Conclusion: stories

- Pizza during the backdoor 🍕
- Spotted 📹
- The blind security agent 👮
- Groot the apple tree 🌱



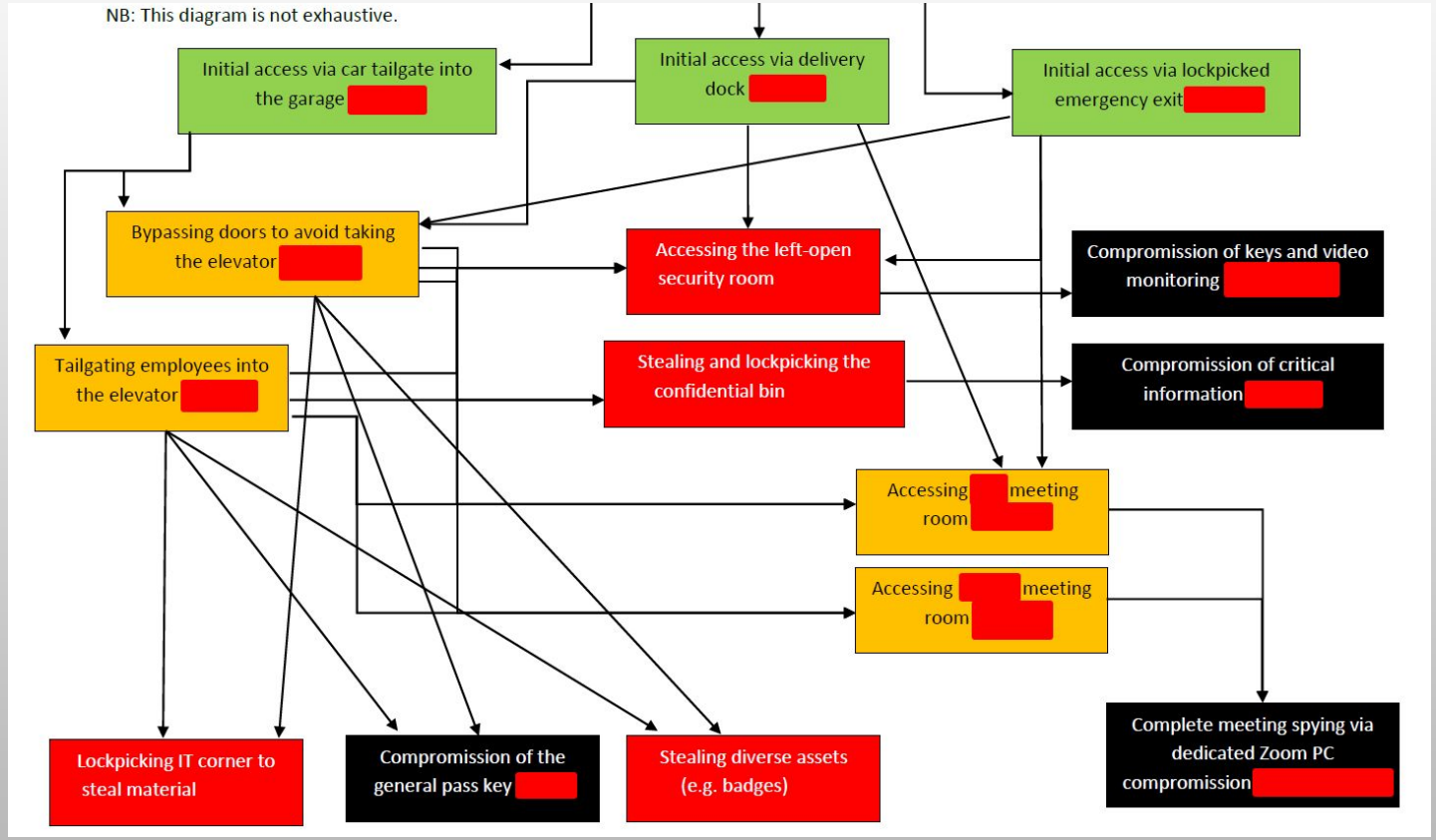
V - Conclusion: stories

- Pizza during the backdoor 🍕
- Spotted 📹
- The blind security agent 👮
- Groot the apple tree 🌱
- The CEO's motorbike 🛵



@volker_carstein

V - Conclusion



V - Conclusion

Three pillars to construct your (physical) security on

- **People**
  - training, awareness, company culture
- Process
  - visitor procedures, onboarding, offboarding
  - external service providers management
- Technology
  - badges, cameras, door controls, physical barriers

V - Conclusion

For the WHITE TEAM / Before the engagement

- Scope
  - What must be tested
  - What must be excluded
- Rules of Engagement (RoE)
- Legal and Ethical considerations

V - Conclusion

For the WHITE TEAM / Before the engagement

- Scope
- Rules of Engagement (RoE)
  - What's ok to use/do, what's not
  - Tailgating? Employees personal belongings? SE techniques?
  - Breaking stuff? Disruption of production operations?
  - Safety considerations (for auditors as well as the audited company employees)
- Legal and Ethical considerations

V - Conclusion

For the WHITE TEAM / Before the engagement

- Scope
- Rules of Engagement (RoE)
- Legal and Ethical considerations
  - Proper authorization letter
  - Defined points of contact (24/7 reachable)
  - Pre-agreed communication plan for updates, alerts, or pauses
  - Some SE attacks might not feel nice to use, but YMMV

V - Conclusion

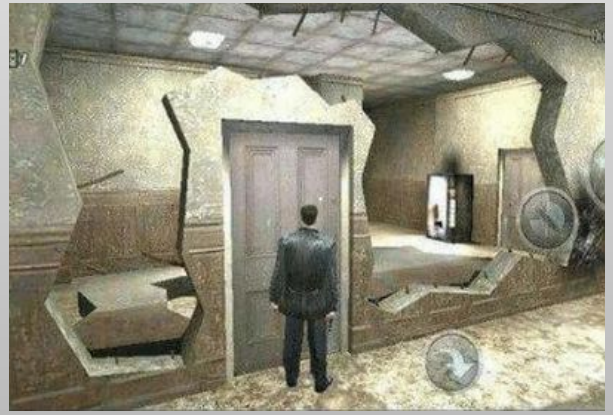
For the RED TEAM

- Do your research well, every detail can be important
- Have good equipment for a large panel of possibilities (also, 2 = 1 and 1 = 0)
- Take the time for pictures in white team mode and the debrief with the client
- Always carry your “get out of jail” card
- Social engineering
  - Pretexting (not necessarily complex)
  - “Appear to be where you’re supposed to be”
- Sometimes you also need luck 🤷

V - Conclusion

On the BLUE side

- The global security level is the same as the level of its weakest element
- The corporate culture can do a lot (badge wearing, for instance)
- Thinking of not only securing the entrances
- Beware of the service providers!
    - Security agents, catering, waste management, cleaning
- Always more than a single camera backup



V - Conclusion

- Recommandations sur la sécurisation des systèmes de contrôle d'accès physique et de vidéoprotection - ANSSI
- Documents from "Sécurité de l'Information et Sécurité Physique" - CLUSIF 12/15/15
- Mechanisms of influence, a short guide to social engineering - Volker @ SecSea 2021
- Physical intrusion: Defeating On Site Security - Joker2a & El0_ @ leHack 2024
- I'll Let Myself In: Tactics of Physical Pen Testers - Deviant Ollam
- You're Probably Not Red Teaming... And Usually I'm Not, Either - Deviant Ollam

V - Conclusion

https://blog.volkercarstein.com/grehack_2025_one_does_not_simply_walk_into_a_building.pdf

@volker_carstein