



ONE DOES NOT SIMPLY

WALK INTO A BUILDING

(OR DO THEY?)

imgflip.com

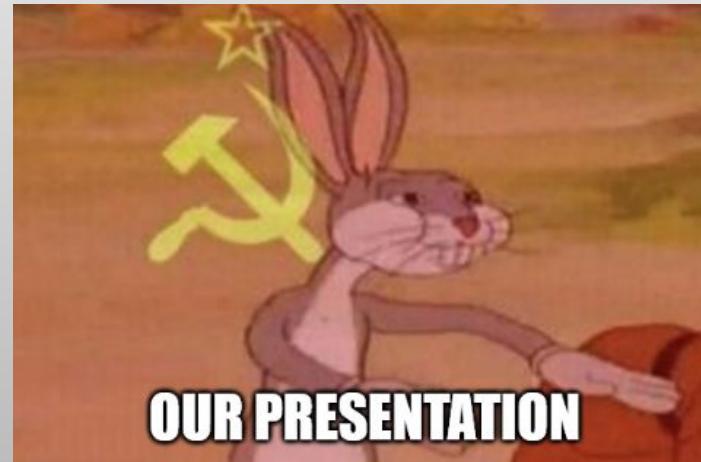
Slides !



[https://blog.volker-carstein.com/secsea_2024 one does not simply walk into a building.pdf](https://blog.volker-carstein.com/secsea_2024_one_does_not_simply_walk_into_a_building.pdf)

Briefing

- I. Contexte et objectifs de la mission
- II. Intrusion initiale
- III. Maintien d'accès
- IV. Collecte des objectifs
- V. Conclusion



Who am I ?

Volker Carstein (@volker_carstein)



- Pentester le jour, jack of all trades la nuit
- Work @ Bsecure, freelance @ Parabellum Services
- Ingénierie sociale, OSINT et sécurité offensive (préférence pour l'Active Directory)
- Speaker @ LeHack, Barbhack, Insomni'hack, SecSea, etc

I - Contexte et objectifs de la mission

- Mission de “pentest” physique chez Bsecure
- Une semaine, deux auditeurs
- **Objectifs :**
 - Entrer dans le bâtiment (duh)
 - Voler des informations confidentielles
 - Voler du matériel
 - Voler un vélo (???)
 - Si possible attaquer la partie IT, mais pas la priorité



II - Intrusion initiale

- Idéalement, pour préparer une intrusion, combien de temps de préparation et recherche faut-il ?
 1. Aucun 😎
 2. Un jour
 3. Environ une semaine
 4. Plus d'une semaine



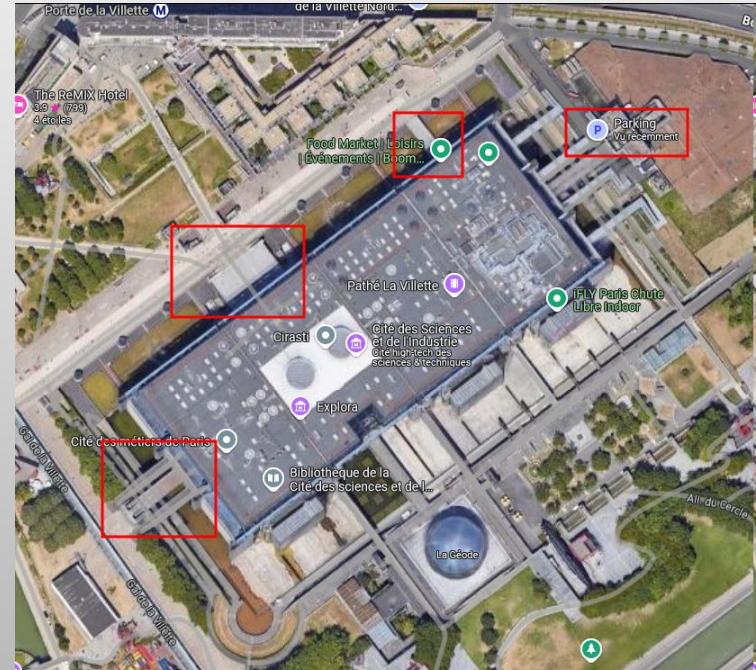
II - Intrusion initiale

- Idéalement, pour préparer une intrusion, combien de temps de préparation et recherche faut-il ?
 1. Aucun 😎
 2. Un jour
 3. **Environ une semaine**
 4. Plus d'une semaine



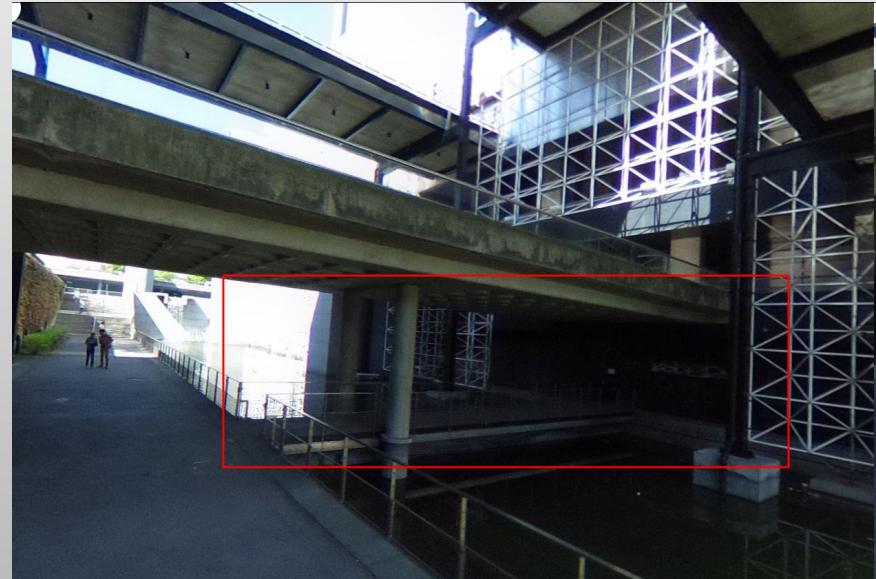
II - Intrusion initiale : recherche

- Photos satellite (Maps, Earth, Yandex, etc.)



II - Intrusion initiale : recherche

- Photos satellite (Maps, Earth, Yandex, etc.)
- Photos street view



II - Intrusion initiale : recherche

- Photos satellite (Maps, Earth, Yandex, etc.)
- Photos street view
- Plans (pour touriste, évacuation/sécurité incendie, etc.)
- Photos à l'intérieur des locaux
- Photos de badges (pour potentielle copie)
- OSINT sur les employés/prestataires (qui est à quel poste, dress code, etc.)
 - Particulièrement utile pour l'ingénierie sociale

II - Intrusion initiale : recherche



+ Sortie de secours

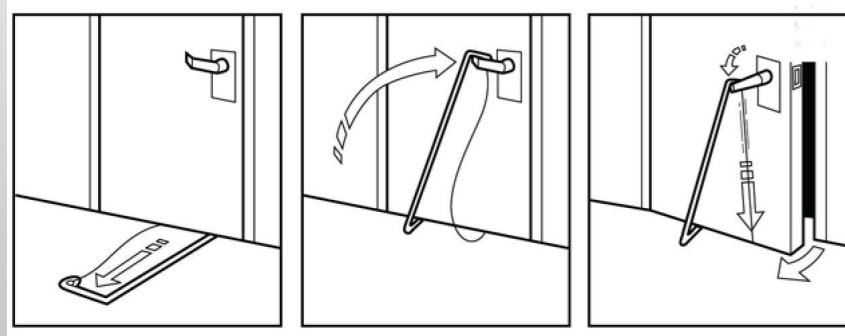


II - Intrusion initiale : matériel



II - Intrusion initiale : matériel

- Dress code adapté (en accord avec les recherches et le prétexte)
- Matériel de crocheting
 - bypass de porte
 - crochets
 - bump keys
 - pickgun
 - under-the-door tool
- Matériel pour copie de badge (Flipper Zero par exemple)
- Tout ce qui peut être utile (câbles, chargeurs, adaptateur, multitool)



STEP 1:

Insert tool under the door

STEP 2:

Work tool over the latch

STEP 3:

Pull down on cable to open the door

II - Intrusion initiale : matériel

Lettre d'autorisation/"de sortie de prison"

- Autorise l'intrusion dans le cadre d'un test de sécurité mandaté par l'organisation cliente
- Contient l'identité des auditeurs, de leur l'entreprise, la mission, l'organisation cliente, la personne de référence à contacter (souvent le commanditaire)
- Évite les problèmes si les auditeurs sont repérés et/ou arrêtés en prouvant que l'intrusion est légale. L'utilité est de se protéger aussi bien légalement que physiquement
- Pas d'intrusion sans cette lettre, **c'est essentiel** ! Un exemplaire par auditeur minimum

II - Intrusion initiale

- Par où passer ?
 1. La porte de livraison
 2. Le garage
 3. Les fenêtres sur rue
 4. La sortie de secours



II - Intrusion initiale : Porte de livraison

- Tous les matins, livraison de nourriture pour la cantine de l'entreprise
- La porte est bloquée ouverte pour transporter les palettes
- On passe comme si de rien n'était, personne ne dit rien
- **Intrusion initiale OK** : on est au rez-de-chaussée
- Ascenseur et portes à badge pour monter dans les étages :(

II - Intrusion initiale : Garage

- Lorsqu'une voiture rentre, on la suit à pied
- Ni la caméra ni le poste de sécurité ne réagissent
- **Intrusion initiale OK** : on est au garage (-1), présence du garage à velo
- Ascenseur et portes à badge pour monter dans les étages :(



II - Intrusion initiale : Fenêtres sur rue

- De nuit, on remarque qu'on peut dévisser les fenêtres
- En grattant le mastic et avec un lève-vitre, on peut s'ouvrir l'accès
- Peu discret et trop complexe, **méthode abandonnée**
- On apprendra plus tard que les fenêtres donnent sur le sous-sol, d'où il est difficile de remonter

II - Intrusion initiale : Sortie de secours

- Porte crochetable de nuit avec un under-the-door tool
- Caméra pointée sur la porte, aucune détection
- **Intrusion initiale OK** : on est au rez-de-chaussée, de nuit uniquement :(
- Ascenseur et portes à badge pour monter dans les étages :(



III - Maintien d'accès

- Comment revenir sans crochetage/tailgate/bon timing ?
- Comment circuler librement ? Ascenseurs, portes pour les escaliers, etc.



III - Maintien d'accès

- Portes à badge pour accéder aux escaliers : **crochetables** !
- Accès à tous les étages, mais risque de se faire repérer à chaque changement



**UTILISER
UN TOOL DE
BYPASS DE PORTE**



**UTILISER UN
COUTEAU SUISSE**

III - Maintien d'accès

- Une fois dans les étages (tailgate dans l'ascenseur, crochetage pour l'accès aux escaliers), se balader pour repérer des badges laissés sans surveillance
- Deux minimum pour pérenniser nos accès
- En prévoir plus au cas où les badges volés puissent être révoqués
- **Maintien d'accès OK**



III - Maintien d'accès : bonus !

- Dans une des salles de réunion au rez-de-chaussée, certaines fenêtres donnent sur la rue
- Rentrer dans la salle, ouvrir certaines fenêtres (sans contacteur d'alarme)
- Les bloquer pour qu'elles restent collées au montant (un peu de discrétion quand même)
- Revenir plus tard (de nuit, le lendemain), pousser la fenêtre depuis l'extérieur pour entrer
- **Maintien d'accès OK**

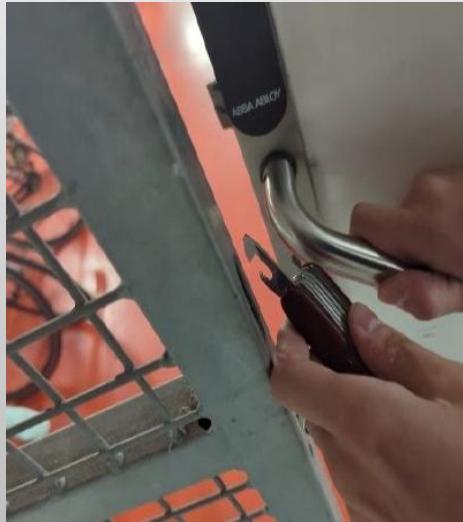
IV - Collecte des objectifs

- Entrer dans le bâtiment ✓
- Voler des informations confidentielles
- Voler du matériel
- Voler un vélo
- Si possible attaquer la partie IT, mais pas la priorité



IV - Collecte des objectifs : vélo

- Comme pour les portes donnant accès aux escaliers, bypass au couteau suisse



IV - Collecte des objectifs

- Entrer dans le bâtiment ✓
- Voler des informations confidentielles
- Voler du matériel
- Voler un vélo ✓
- Si possible attaquer la partie IT, mais pas la priorité



IV - Collecte des objectifs : matériel

- Arrivée tôt le matin (7h30), avant tous les employés
- Local de stockage de matériel de l'IT Corner : fermé à clé
- Crochetage via bump key
- Beaucoup de matériel accessible !



IV - Collecte des objectifs : matériel

- Vol de plusieurs PC, téléphones, câbles, etc.
- Vol de vêtements brandés au nom du client
 - T-shirts
 - Hoodies
 - Les porter rend notre présence encore plus crédible



IV - Collecte des objectifs : matériel

- Porte du PC sécurité ouverte toute la journée, une personne dedans
- Appel au PC sécurité, prétendant un malaise au dernier étage
- Pendant que le garde s'absente, vol de matériel, entre autres
 - Talkie-walkie
 - **Enregistrement des caméras de surveillance**



IV - Collecte des objectifs : matériel

- Arrivée tôt le matin (7h30), avant tous les employés
- Dans une salle du premier étage, une boîte à clé avec le code dessus, laissée ainsi par le personnel de ménage
- Vol du passe général du bâtiment
- Copie de la clé auprès d'un serrurier du coin avec un peu d'ingénierie sociale



IV - Collecte des objectifs

- Entrer dans le bâtiment ✓
- Voler des informations confidentielles
- Voler du matériel ✓
- Voler un vélo ✓
- Si possible attaquer la partie IT, mais pas la priorité



IV - Collecte des objectifs : informations

- Deux salles de réunions très importantes (réunions investisseurs, de direction, etc.)
- PCs fonctionnant sous Windows hébergeant Zoom (Chrome OS dans les autres salles)
- Dump du disque dur pour récupérer le mot de passe de l'admin local
- But : poser une backdoor pour espionner les réunions



IV - Collecte des objectifs : informations

- Désactiver Defender et Firewall (le PC n'est pas monitoré donc aucun souci)
- Faire connecter le PC de réunion à un réseau VPN sous notre contrôle
- Activer l'option pour faire du **RDP Shadow**
- Se connecter en RDP pendant une réunion et l'enregistrer
- **Profit !**



IV - Collecte des objectifs : informations

- Localiser les bureaux des CEO, CFO, employé.e gérant les virements, etc.
- “Don’t ask to ask, just ask!”
- Aucun bureau fermé, on fouille tout
 - Quelques documents
 - Poubelle confidentielle
 - Clés d’une voiture/moto (?)



IV - Collecte des objectifs : informations

- Dans une salle de réunion vide de bon matin, crochetage et déballage de tous les documents de la poubelle
- **Codes bancaires valides, CBs, chéquiers signés “en blanc” etc.**
- + documents très personnels d'employé.e.s



IV - Collecte des objectifs

- Entrer dans le bâtiment ✓
- Voler des informations confidentielles ✓
- Voler du matériel ✓
- Voler un vélo ✓
- Si possible attaquer la partie IT, mais pas la priorité



IV - Collecte des objectifs : IT

- Accès à la salle serveur trivial avec le passe général
- Un PC de la salle est déverrouillé et l'user connecté à des droits intéressants
- Backdoor pour donner l'accès distant à deux collègues
- Compromission de la CI/CD de l'entreprise



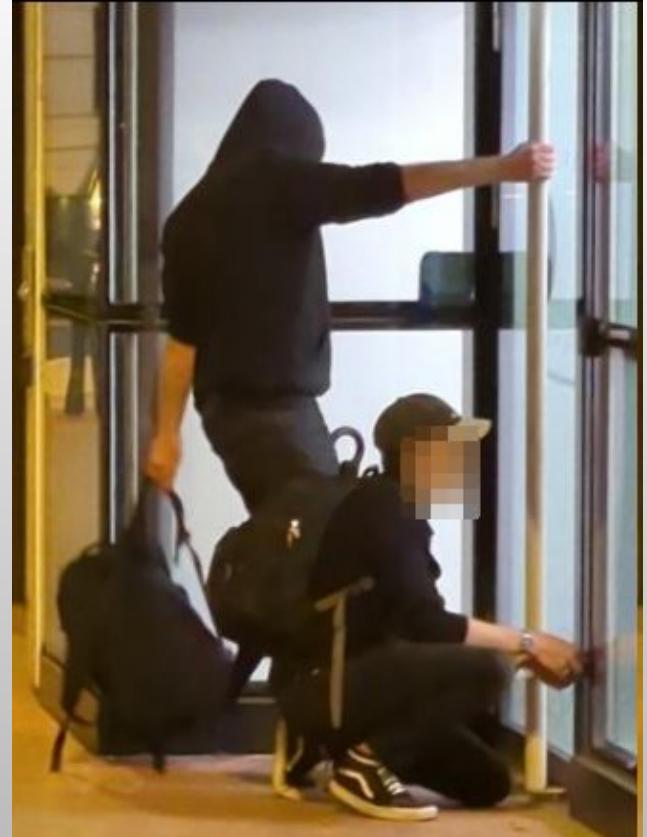
IV - Collecte des objectifs

- Entrer dans le bâtiment ✓
- Voler des informations confidentielles ✓
- Voler du matériel ✓
- Voler un vélo ✓
- Si possible attaquer la partie IT, mais pas la priorité ✓



IV - Conclusion : anecdotes

- Soirée pizza pendant la backdoor 🍕



IV - Conclusion : anecdotes

- Soirée pizza pendant la backdoor 🍕
- Spotted 🎥



IV - Conclusion : anecdotes

- Soirée pizza pendant la backdoor 🍕
- Spotted 📹
- L'agent de sécurité aveugle 🚔



IV - Conclusion : anecdotes

- Soirée pizza pendant la backdoor 🍕
- Spotted 📹
- L'agent de sécurité aveugle 👮
- Groot le pommier 🌱

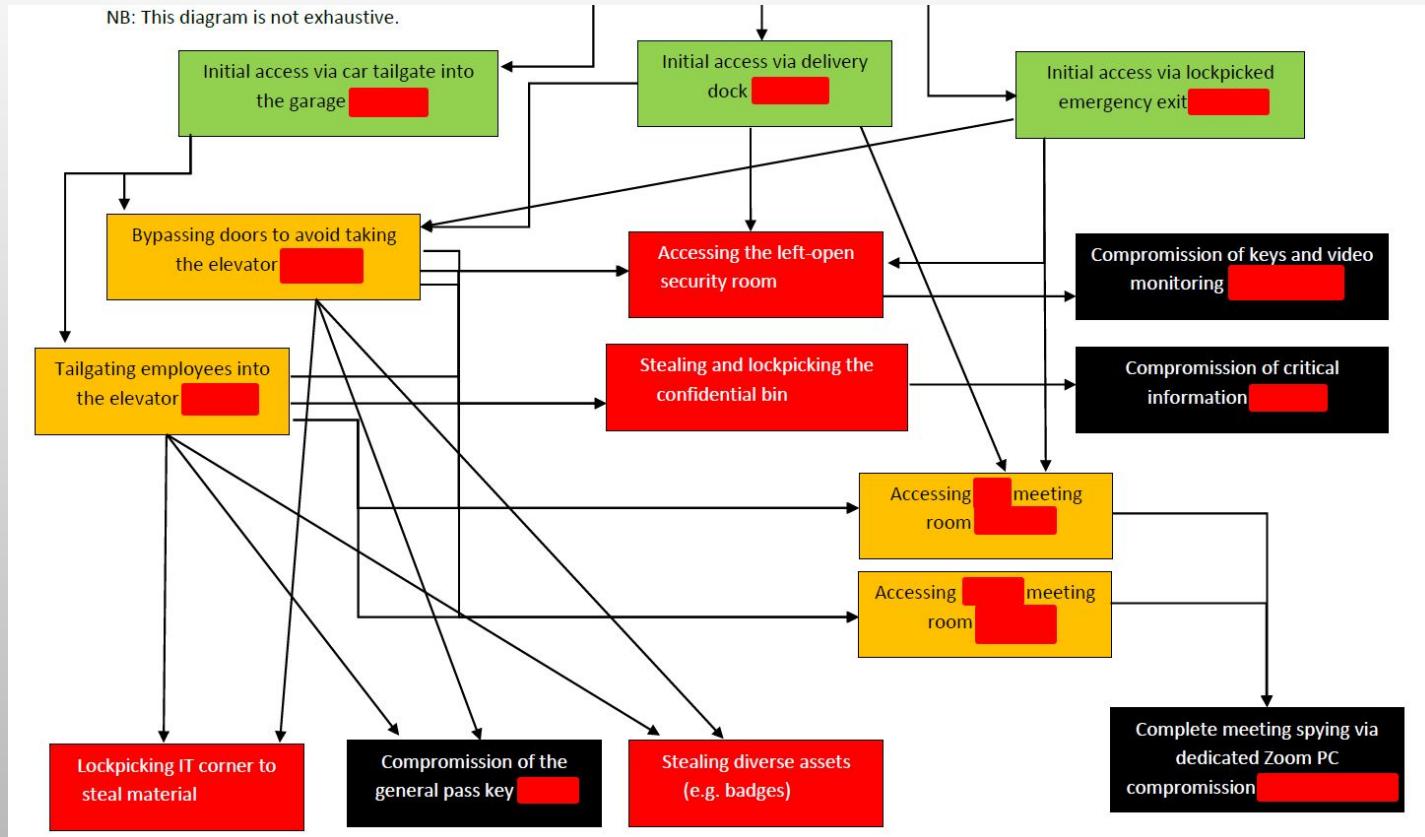


IV - Conclusion : anecdotes

- Soirée pizza pendant la backdoor 🍕
- Spotted 📹
- L'agent de sécurité aveugle 🚂
- Groot le pommier 🌱
- Le scooter du CEO 🛵



V - Conclusion



V - Conclusion

Côté RED

- Bien faire ses recherches, tous les détails peuvent être importants
- Avoir du bon matériel pour avoir un éventail large de possibilités (aussi, 2 = 1 et 1 = 0)
- Prendre le temps pour les photos en mode white team et debrief avec le client
- Toujours avoir sa lettre de sortie de prison
- Ingénierie sociale
 - Pretexting (pas forcément complexe)
 - “Avoir l’air d’être là où on doit être”
- Parfois il faut aussi de la chance 



V - Conclusion

Côté BLUE

- La sécurité globale c'est la sécurité du maillon le plus faible
- La culture d'entreprise peut faire beaucoup de choses (port du badge par ex)
- Penser à ne pas sécuriser que ses entrées
- Attentions aux prestataires !
 - Agent de sécurité, Restauration
 - Gestion des déchets, Ménage
- Toujours plus d'un seul backup de caméra



V - Conclusion

- Recommandations sur la sécurisation des systèmes de contrôle d'accès physique et de vidéoprotection - ANSSI
- Documents issus de la conférence thématique “Sécurité de l'Information et Sécurité Physique” du CLUSIF le 15 décembre 2015
- 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

