HACKING ETHIQUE : ACCOMPAGNER LES ÉQUIPES EN CHARGE DES ÉVOLUTIONS DU SI

NICOLAS BONNEFOUS
COO/CTO @VAADATA
Ethical Hacking – 5 Juillet 2019

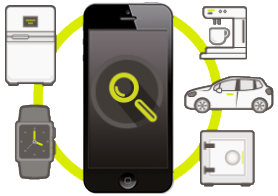
vaadata

VAADATA

SÉCURITÉ WEB, MOBILE ET IOT

Spécialiste en tests d'intrusion (pentests).

Clients en national et en international



Audits de sécurité (pentests)

- Sites web, logiciels SaaS, apps mobiles
- IoT
- SI exposé sur le web
- Facteur humain (social engineering)

Consulting sécurité, Formations

CONTEXTE BANQUES / FINTECH

ECOSYSTEME EN PLEINE MUTATION

Interopérabilité monétique

Digitalisation intégrale

Multiplication à outrance des acteurs du paiement

Instant Payment

APIs bancaires

Fusion-Acquisition, regroupements MASSIFS

NFC, QR Code

[concept]
HACKING ÉTHIQU

[concept] HACKING ÉTHIQUE

HACKING

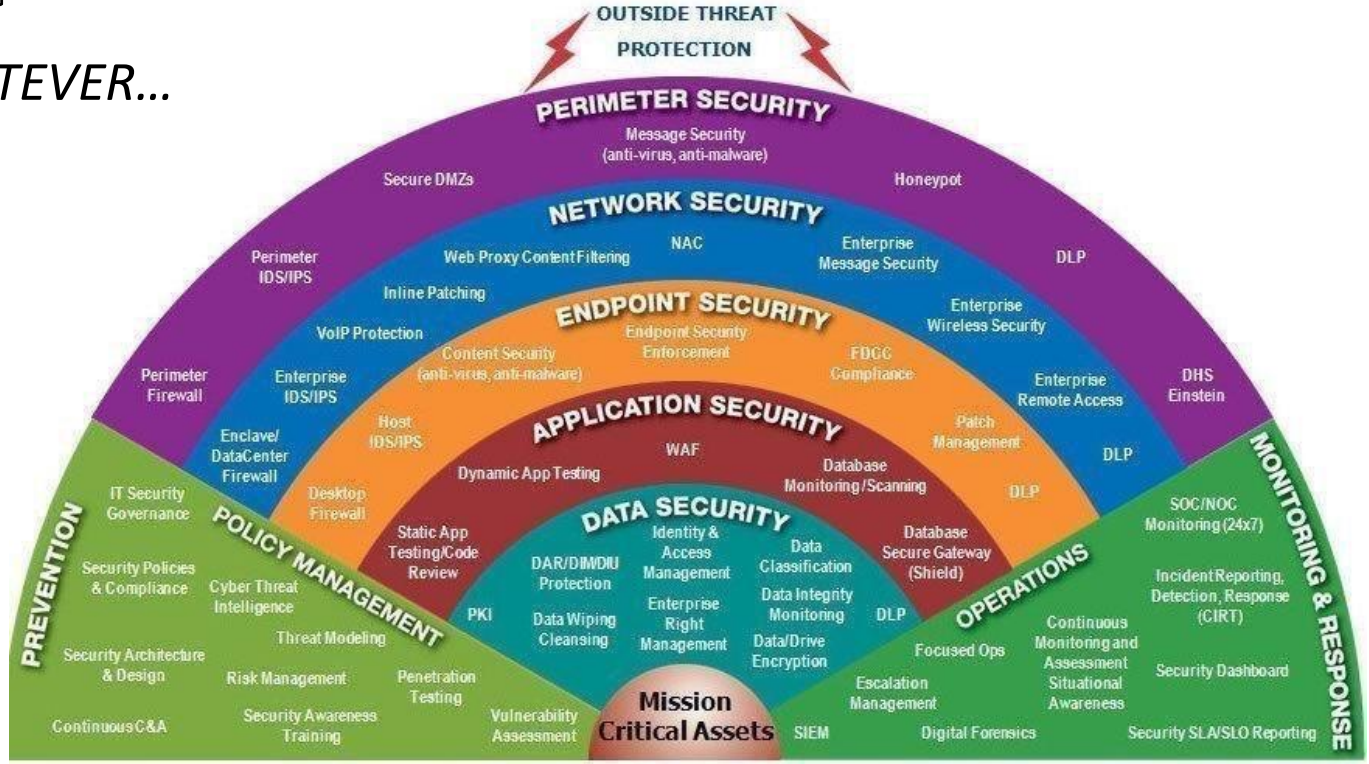
Le hacking peut se définir […] comme un ensemble de techniques permettant d'exploiter les failles et vulnérabilités d'un élément ou d'un groupe d'éléments matériels ou humains.

Source : Wikipedia

[concept] HACKING ÉTHIQUE

HACKING

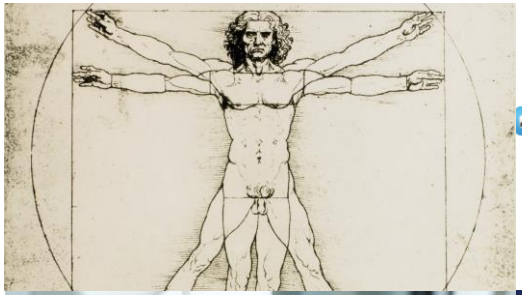
WHATEVER…



[concept] HACKING ÉTHIQUE

HACKING

Que peut-on « hacker » ?






BLACK / GREY / WHITE BOX
SECURITY TESTING

ACCOMPAGNER LES ÉVOLUTIONS DU SI

SÉCURITÉ EN CONTINU ?

Quel sens donner à cette « continuité » dont tout le monde parle ?

☞ Tests automatisés ? Tests manuels ?

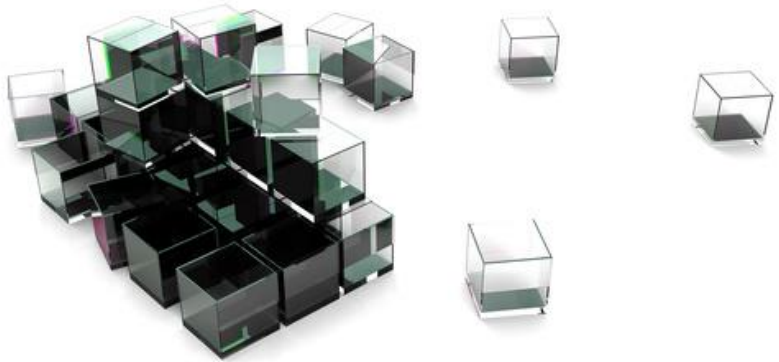
Que peut-on réellement tester en continu ?

☞ Quelle surface ? Quel rythme d'évolutions ?

QUELS TYPES DE TESTS

OBJECTIFS / POSITION

Boite noire, grise, ou blanche ?



QUEL PÉRIMÈTRE

PÉRIMÈTRE DES TESTS D'INTRUSION

Quel périmètre ?

Type de « surface d'attaque » ?

Défini par qui ?

Risques en dehors du périmètre ?

Attaque globale ?


SECURITY BY DESIGN
KEEP IT SIMPLE
vaadata

COMPLEXITÉ vs. SÉCURITÉ

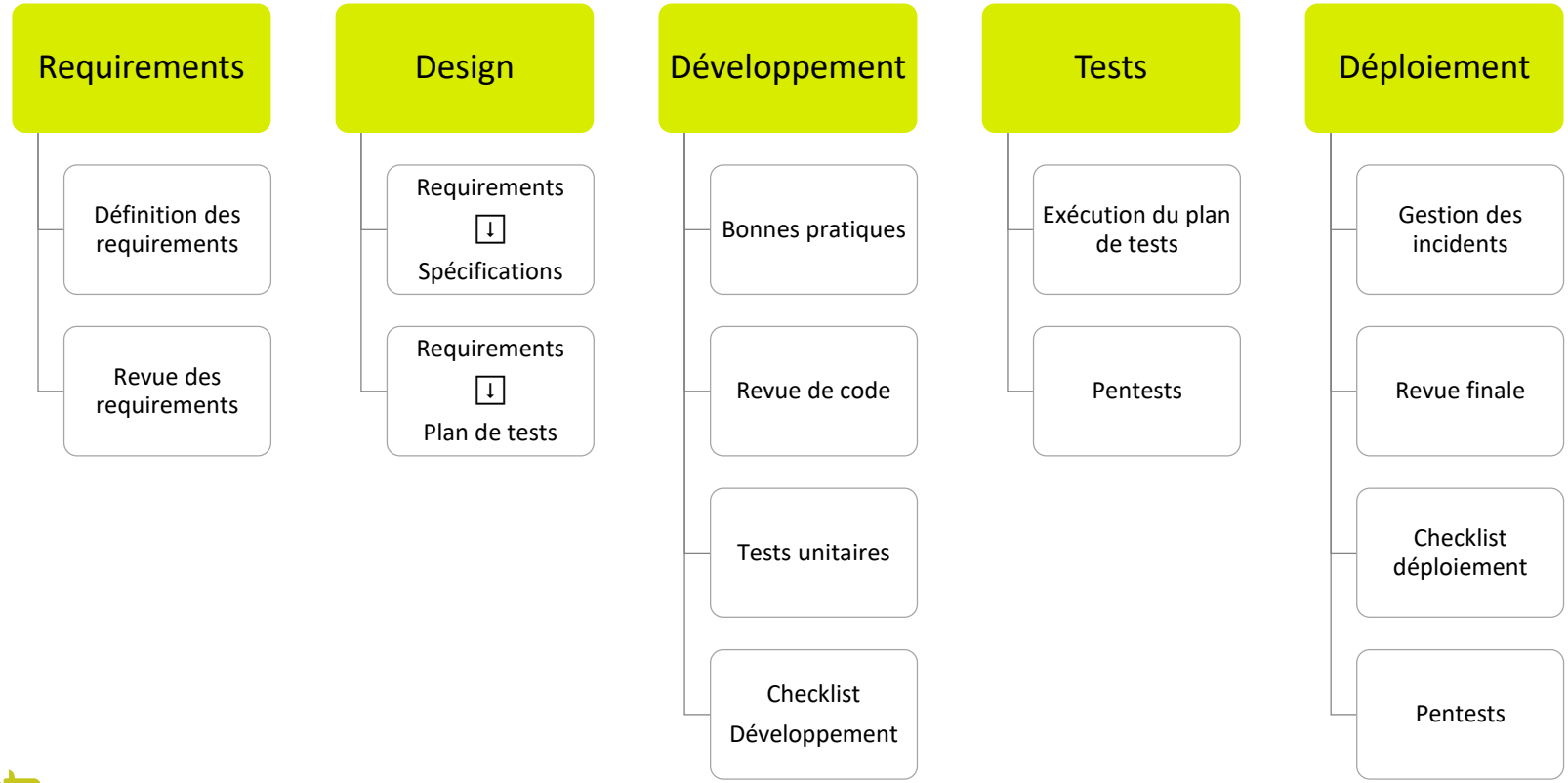
LA COMPLEXITÉ EST LE PIRE ENNEMI DE LA SÉCURITÉ

COMPLEXITY IS THE WORST ENEMY OF SECURITY

Bruce Schneier, Mikko Hyppönnen…

SECURITY BY DESIGN

CYCLE DE DÉVELOPPEMENT



TESTS DE SÉCURITÉ RÉGULIERS

QUELLE FRÉQUENCE ?

FAIRE DES TESTS ☛ APPLIQUER DES CORRECTIFS

A QUEL RYTHME ? Mensuel ? Trimestriel ?

Contraintes :

- Time To Market
- Réactivité des équipes (développement, devops)
- Budget
- Volonté

VARIER LES REGARDS

2 CAS D’ATTAQUES
TECHNIQUE / INGÉNIERIE SOCIALE

CAS #1 - WEB

2 CAS D'ATTAQUES DÉTAILLÉS

CAS #1 – WEB – PUZZLE ATTACK

Faille Technique VS Faille Logique

Failles techniques = injections, mauvaises gestion de session, CSRF, composants vulnérables…

Beaucoup de failles techniques sont détectables via l'utilisation d'outils.

Les failles logiques ne sont pas détectables via des outils, du moins pas de manière générique.

Il est nécessaire de connaître la logique métier de l'application étudiée afin de pouvoir déterminer qu'un certain comportement est une faille logique.

Faille logique = liée au métier de l'application.

Exemples ? McDonalds & iPhone

2 CAS D'ATTAQUES DÉTAILLÉS

CAS #1 – WEB – PUZZLE ATTACK

Exemple rencontré lors d'un audit.

Une plateforme de partage de données permet, en dehors de ses fonctionnalités de base, les actions suivantes :

- Création d'un espace public
- Personnalisation des CSS
- Création de contenu personnalisé (HTML)
- Choix d'une page par défaut sur l'espace
- Invitation d'utilisateurs à rejoindre l'espace (email automatique)

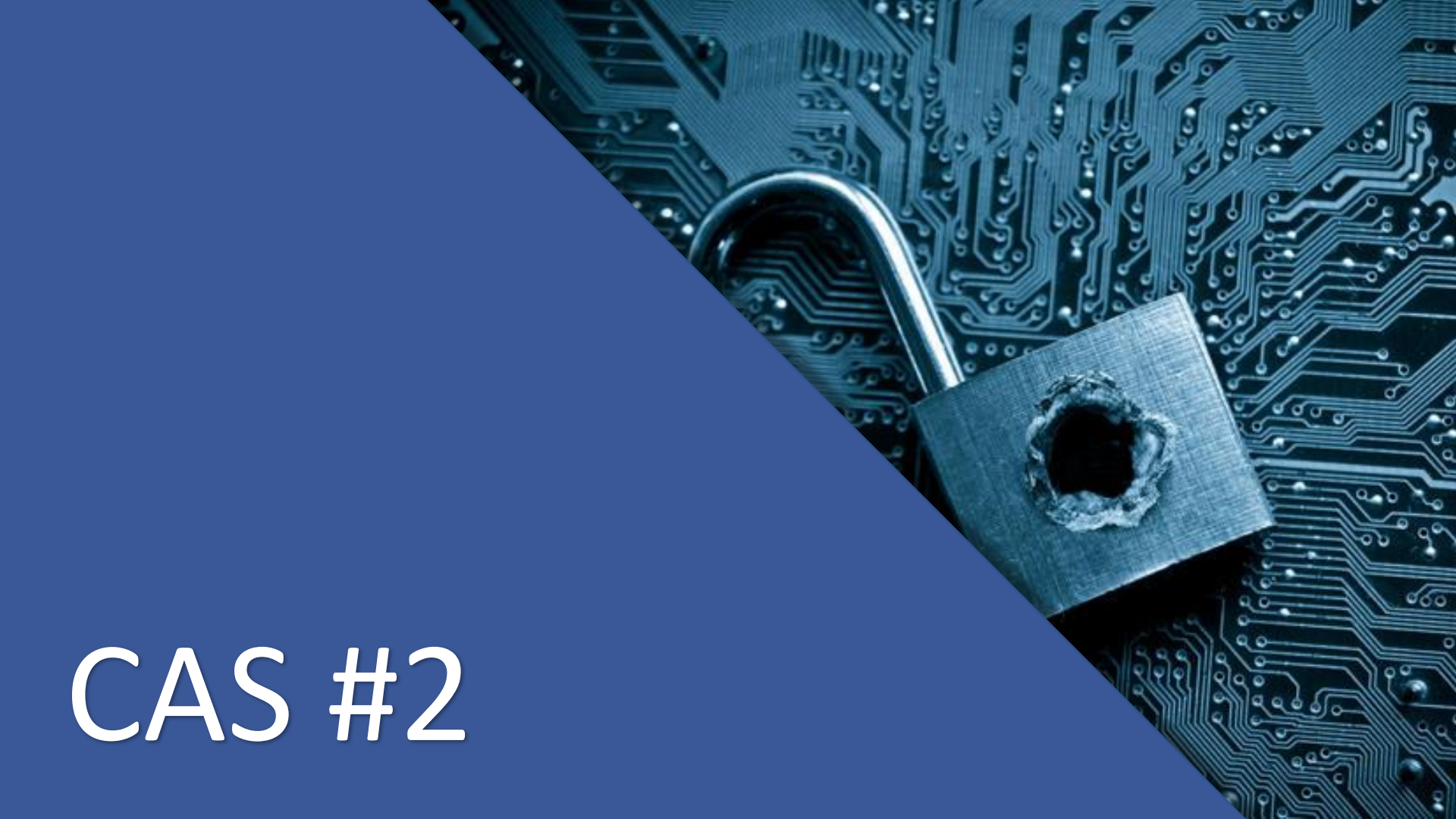
➤ Résultat ?

2 CAS D'ATTAQUES DÉTAILLÉS

CAS #1 – WEB – PUZZLE ATTACK

Attaque :

- Création d'un espace public (avec une adresse web qui donne confiance)
- Création de contenu personnalisé (création d'un faux formulaire de login envoyant les identifiants sur un serveur « pirate »)
- Personnalisation des CSS (pour copier l'apparence de la page officielle d'authentification)
- Choix d'une page par défaut sur l'espace (☛ la fausse page de login)
- Invitation d'utilisateurs à rejoindre l'espace (email automatique ☛ On invite tout le monde)



CAS #2

2 CAS D'ATTAQUES DÉTAILLÉS

#2 – Startup Allemande – Finance – 200 personnes (1/5)

Contexte :

- Premier audit d'ingénierie sociale
- Pas de réels efforts de sensibilisation en interne

Objectifs de l'audit :

- Evaluer la sécurité de la société au global, sans objectif particulier

2 CAS D'ATTAQUES DÉTAILLÉS

#2 – Startup Allemande – Finance – 200 personnes (2/5)

Collecte d'informations :

L'audit est réalisé en boite noire, les attaques techniques et humaines sont autorisées.

Les applications sensibles sont plutôt robustes, les vulnérables peu intéressantes.

Peu d'informations sont obtenues quant aux rôles des personnes dans la société et quant aux fonctionnalités mises à disposition dans les applications et accès identifiés.

2 CAS D'ATTAQUES DÉTAILLÉS

#2 – Startup Allemande – Finance – 200 personnes (3/5)

Scénario :

Nous partons sur un scénario « à l'aveugle », visant une grande partie des collaborateurs (sauf l'équipe IT interne).

Nous prétextons une fuite de mots de passe, en usurpant l'identité d'une personne de l'équipe IT interne.

Une soixantaine de personnes seront visées.

2 CAS D'ATTAQUES DÉTAILLÉS

#2 – Startup Allemande – Finance – 200 personnes (4/5)

Exécution :

Dear all,
Recently, we have discovered a leak of a large number of credentials linked to XXXXX' accounts.
It is an important security breach.

Therefore, we have created an internal tool to check if your passwords have been compromised or not.
Please use it as soon as possible and change immediately your passwords if they appear as compromised.
security.XXXXX.de

You also have an active role to play in ensuring the security of your information.

Thanks for the collaboration!

2 CAS D'ATTAQUES DÉTAILLÉS

#2 – Startup Allemande – Finance – 200 personnes (5/5)

Résultat :

6 mots de passe obtenus, nous permettant l'accès à de nombreux services en ligne utilisés par les collaborateurs :

- Plateforme de partage de fichiers sensibles
- Console de management
- Dépôts de code
- Gestion des tickets de support


MERCI !