COLLOQUE

JEUDI 1ER DÉCEMBRE 2016

AMPHITHÉÂTRE ROPARTZ, PALAIS DES ARTS, PLACE ANNE DE BRETAGNE, VANNES

LA TRANSFORMATION NUMÉRIQUE POUR LES COLLECTIVITÉS TERRITORIALES : QUELS ENJEUX DE SÉCURITÉ ET QUELS ACCOMPAGNEMENTS ?

Hervé TROALIC

FROM NULL TO ADMIN

Retour sur des cas pratiques de prises de contrôle des systèmes à distance

FROM NULL TO ADMIN

- Quel que soit l'attaquant,
- Quel que soit sa position sur les réseaux,
- Quelles que soient ses motivations.

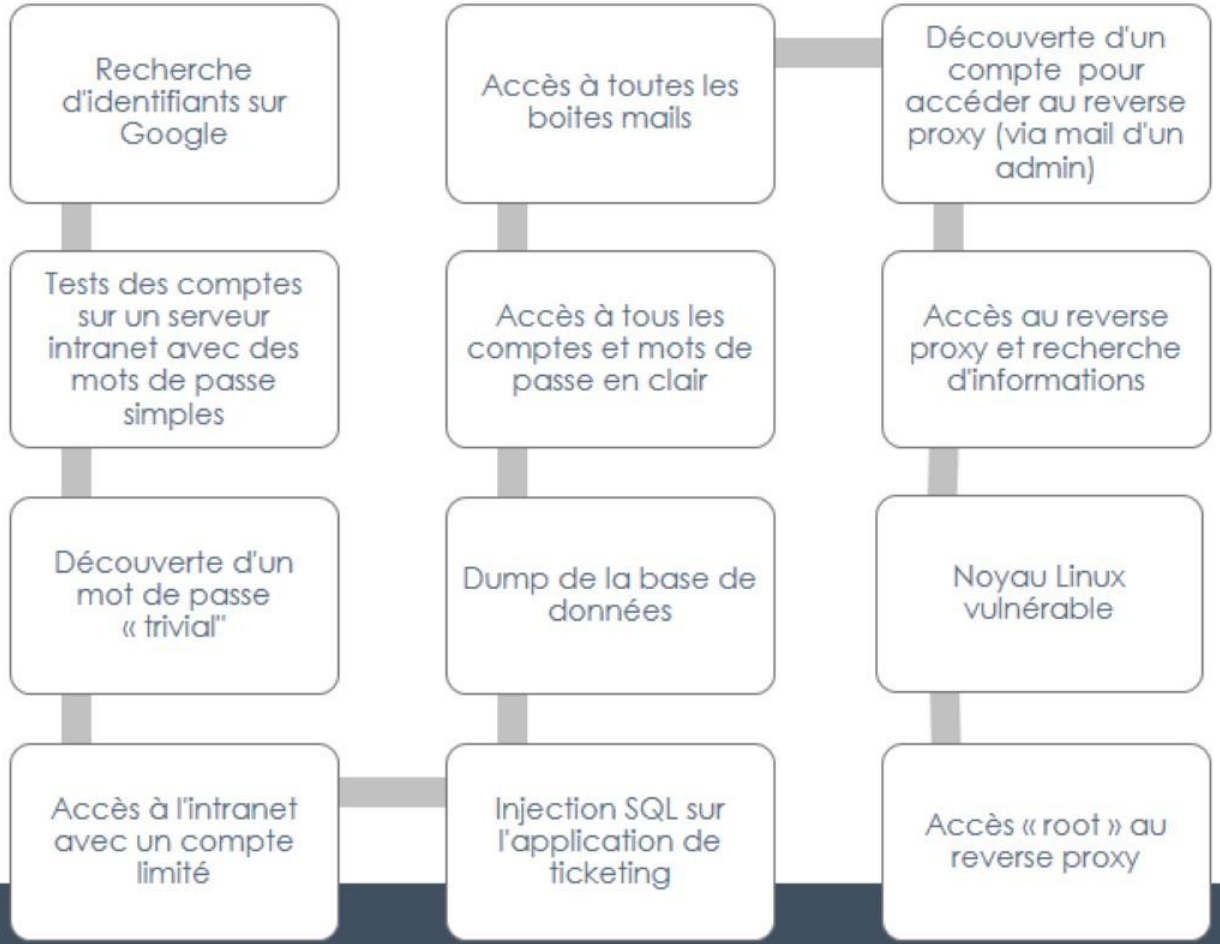
- Le « saint graal » sera toujours de devenir « Administrateur » de votre Système d'Information (SI) !

Cela n'arrive que dans les films !
Je ne me sens pas concerné, nous ne sommes pas une banque…

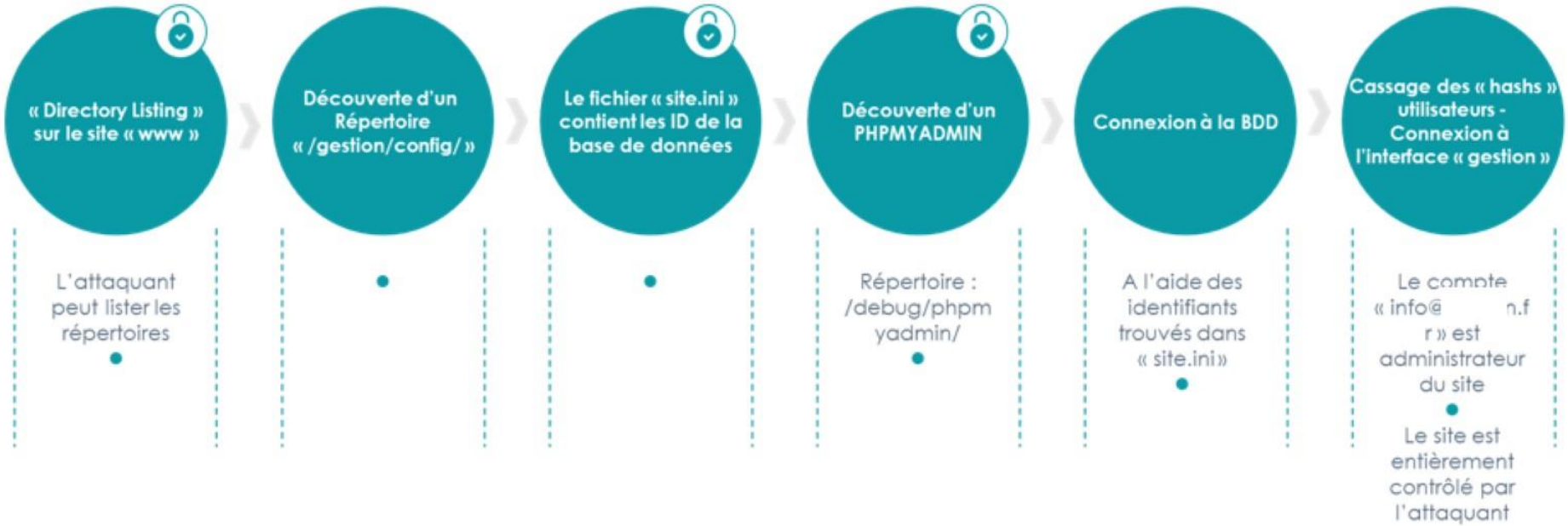
Illustre inconnu

Les exemples suivants sont tous tirés d'expériences réelles.

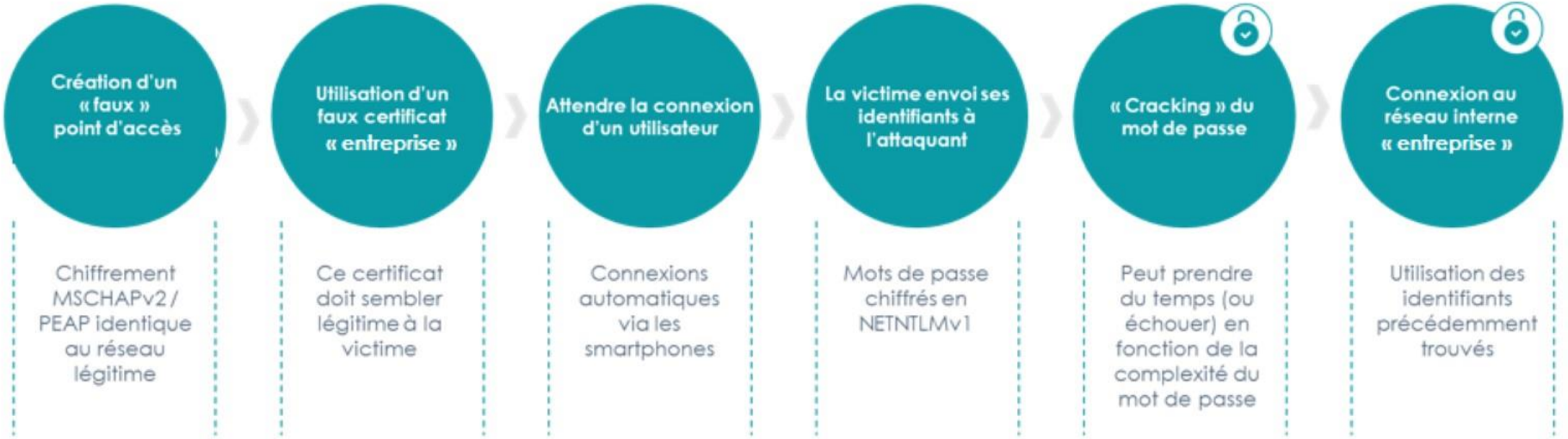
1IER CAS : ACCÈS ADMINISTRATEUR SUR UN « REVERSE PROXY »



2ND CAS: CONTRÔLE D'UN SITE INTERNET



3IÈME CAS : WIFI BUREAUTIQUE / CONNEXION ILLÉGITIME AU RÉSEAU



4IÈME CAS : ACCÈS AU RÉSEAU INTERNE DEPUIS L'INTERFACE DE CRÉATION DE COMPTES

Tentative de création de compte

Découverte d'une requête "GetUsers"

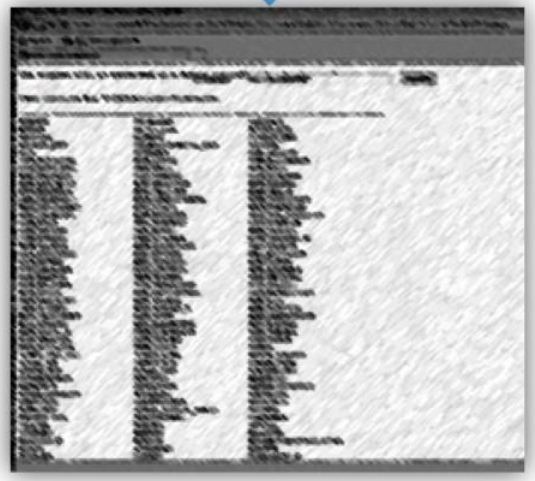
Lancement de la requête sans paramètre

Récupération des login/mots de passe en MD5

"Crack" des MD5 et récupération du mot de passe "super-admin"

Ajout d'une "backdoor" ASP sur un profil utilisateur

Execution de commandes sur le réseau interne



ON FAIT QUOI MAINTENANT ?

- Etes-vous sûr d'avoir identifié tous vos risques ?
- L'audit restera toujours un bon moyen d'éviter le pire
- Comment gérez-vous vos mots de passe ? Avez-vous pensé à l'authentification forte pour les utilisateurs à privilèges ?
- Avez-vous prévu de formaliser une politique des accès et des habilitation ?
- Avez-vous une réflexion sur la sécurité des configurations des serveurs ?
- Est-ce que vous faites des tests avant de mettre en production ?

MERCI