



# Formation OpenClassrooms Administrateur Systèmes, Réseaux Et Sécurité

## Soutenance Projet-12

Stéphane Perfetti

29/01/2025

# Projet 12

-  
Évaluez et  
améliorez le  
niveau de  
sécurité d'un  
domaine

Windows et de  
l'Active Directory  
associé

- Scénario :
  - Dans un contexte de forte augmentation des menaces informatiques contre les établissements de santé, la direction de la clinique de Frontignan souhaite faire auditer son SI.
  - Nous sommes missionnés pour auditer le niveau de sécurité du SI.
- Sommaire :
  - Détails de la mission
  - Logigramme du déroulé du pentest
  - Détails des vulnérabilités découvertes et de leurs recommandations court et long terme associées
  - Présentation des livrables: Rapport de pentest et Plan d'actions

# Détails de la mission:

- L'audit évaluera le niveau de sécurité du domaine Windows et de son Active Directory.
- Le pentest (de type Grey Box) s'effectuera avec un accès au réseau mais sans identifiant de connexion au domaine.
- Un rapport de pentest devra présenter:
  - les informations collectées lors des différentes étapes,
  - la méthodologie suivie, étape par étape,
  - les vulnérabilités découvertes.
- Un plan d'action a court et long terme devra proposer des recommandations afin de remédier aux vulnérabilités mise en évidences lors du pentest.

# Identification des hôtes réseaux et du domaine

- Hôtes présent sur le réseau:

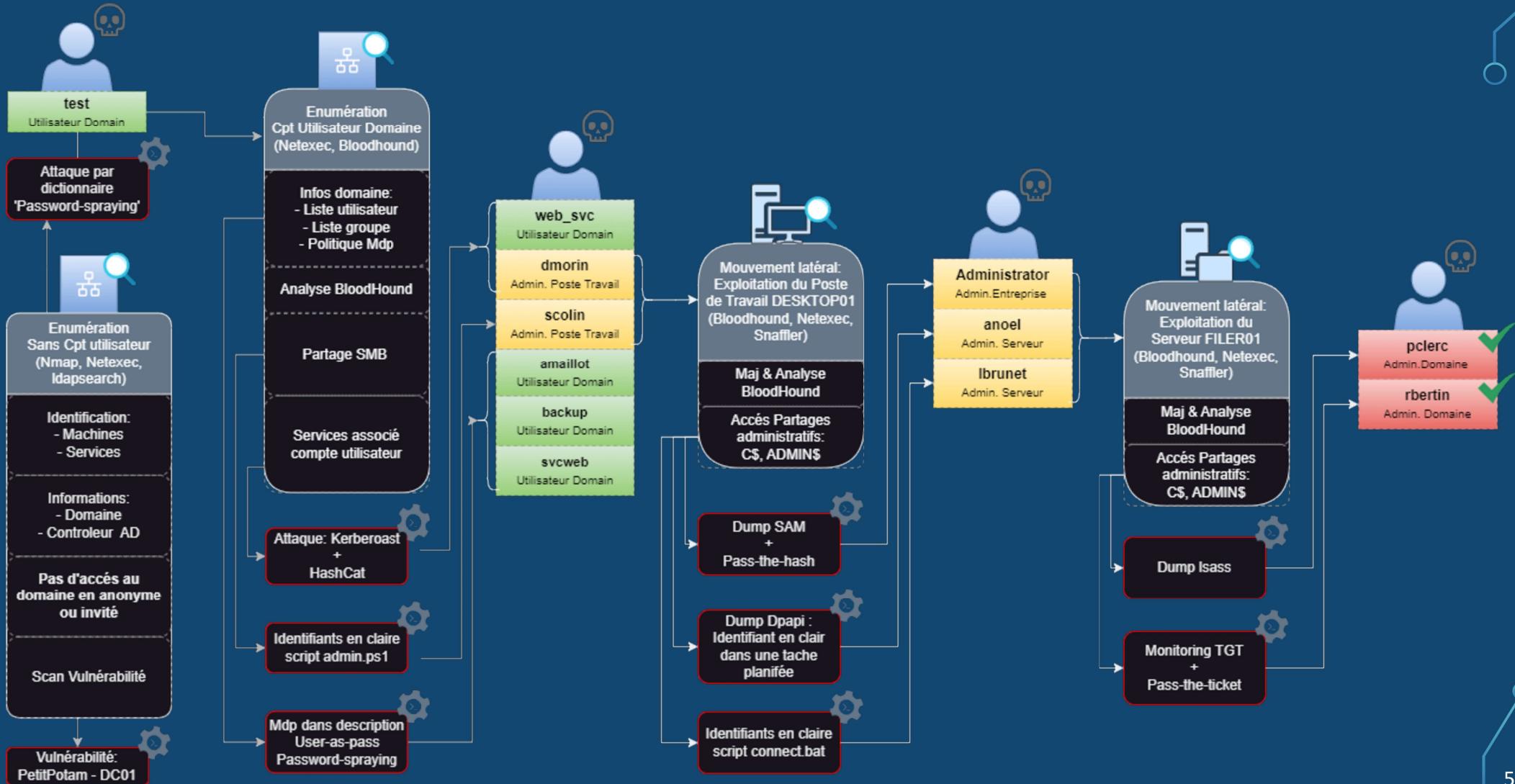
- |             |                |  |
|-------------|----------------|--|
| ➤ DC01      | (10.10.10.101) | - Serveur AD, Windows Serveur 2019         |
| ➤ FILER01   | (10.10.10.112) | - Serveur de fichier, Windows Serveur 2019 |
| ➤ DESKTOP01 | (10.10.10.117) | - Poste de travail, Windows 10             |

Rq: Le détails des services proposés pour chaque hôtes est disponible dans le rapport de pentest.

- Domaine: travers.ic

Rq: La configuration et les fonctionnalités du contrôleur de domaine sont disponibles dans le rapport de pentest.

# Logigramme du pentest



# Vulnérabilités découvertes & Recommandations court terme associées

## Définition:

- Notion de niveau de criticité: sous-ensembles logiques du SI dont les besoins de sécurité, le niveau d'exposition ou de sensibilité, sont homogènes et dont le niveau de confiance est équivalent.

# Politique de mot de passe

## Vulnérabilités:

- V02: Mot de passe faible, génériques, ou facilement devinable.
- V05: Mot de passe identique pour plusieurs comptes utilisateurs et/ou administrateurs.

## Recommandation:

R01 - Mettez en place une politique de mot de passe forte (Priorité: 1/10)

- Action à réaliser:
  - Créer ou modifier la politique de mot de passe générale avec à minima :
    - Mots de passe d'au moins 12 caractères, sans longueur maximale ;
    - Mots de passes complexes (lettres, chiffres, caractères spéciaux) ;
  - Les comptes administrateurs doivent se voir appliquer une stratégie de mot de passe affinée (Password Settings Object), leur imposant un mot de passe complexe adapté au niveau de criticité du compte afférant, et un renouvellement lors de l'attribution du compte.
- Ressources:
  - aussi guide authentification multifacteur et mots de passe
  - <https://www.cnil.fr/fr/mots-de-passe-une-nouvelle-recommandation-pour-maitriser-sa-securite>

# Robustesse des mots de passes

## Vulnérabilités:

- V03: Mot de passe présent dans la description de compte utilisateur
- V04: Mot de passe identique au nom d'utilisateur

## Recommandation:

### RC02 - Mécanisme de contrôle de la robustesse des mots de passes (Priorité: 2/10)

- Action à réaliser:
  - Mettre en place un mécanisme de contrôle de la robustesse des mots de passes:
    - Respect des règles définies dans la politique de sécurité de mots de passe;
    - Comparer les mots de passe lors de la création à une base de données répertoriant les mots de passe les plus utilisés ou bien ceux qui ont été compromis;
    - Repérer les mots de passe contenant des motifs (ou des répétitions de motifs) spécifiques (comme une suite de chiffre telle que « 12345 », la suite des premières lettres des claviers comme « azerty », etc);
    - Repérer les mots de passe contenant des informations personnelles saisies lors de la création du compte, comme les noms et prénoms ou encore les dates de naissance ;
    - Lors d'un renouvellement du mot de passe, interdire la réutilisation d'un mot de passe parmi les X derniers mots de passe déjà utilisés
- Ressources:
  - aussi guide authentification multifacteur et mots de passe
  - <https://www.cnil.fr/fr/mots-de-passe-une-nouvelle-recommandation-pour-maitriser-sa-securite>

# Dissémination de secret d'authentification

## Vulnérabilités:

- V10: Identifiants admin serveur en clair dans un script en partage administratif sur DESKTOP01.
- V11: Compte Admin Domain connecté sur une machine autre qu'un contrôleur de domaine.

## Recommandation:

RC03 - Maîtriser la dissémination de toute forme de secret d'authentification réutilisable  
(Priorité: 3/10)

- Action à réaliser:
  - Proscrire la connexion à des ressources de niveau de criticité donné avec un compte d'administration de niveau de criticité supérieure.
  - Dédier des comptes d'administration adaptés au niveau de criticité de la ressource administrée.
  - Ne pas permettre le stockage de secrets d'authentification d'un niveau de criticité donné sur des ressources de niveau de criticité inférieure.
- Ressources:
  - ANSSI Recommandations pour l'administration sécurisée des SI reposant sur AD – R29 - R64

# Secrets d'authentifications dans des tâches planifiées

## *Vulnérabilités:*

- V09: Identifiant présent dans des tâches planifiées

## *Recommandation:*

RC04 - Traiter les risques liés aux secrets d'authentifications des tâches planifiées  
(Priorité: 4/10)

- Action à réaliser:
  - Prohiber l'utilisation de secret d'authentification d'un niveau de criticité donné dans des tâches planifiées a destination de ressource d'un niveau criticité moindre.
  - Privilégier l'utilisation de comptes système locaux pour l'exécution de tâche planifiées.
- Ressources:
  - ANSSI Recommandations pour l'administration sécurisée des SI reposant sur AD - R33

# Secrets d'authentifications figurant dans des scripts

## Vulnérabilités:

- V06: Identifiant d'un compte administrateur poste de travail en clair dans un script en accès partagé sur FILER01

## Recommandation:

RC05 - Traiter les risques liés aux secrets d'authentifications figurant dans des scripts  
(Priorité: 5/10)

- Action à réaliser:
  - Prohiber l'utilisation de secret d'authentification dans des scripts accessibles en lecture par des comptes de moindre privilège.
  - Mettre en place un processus de contrôle des scripts.
- Ressources:
  - ANSSI Recommandations pour l'administration sécurisée des SI reposant sur AD - R31

# Comptes d'administration locaux

## *Vulnérabilités:*

- V08: Compte administrateur local identique sur plusieurs machines

## *Recommandation:*

### RC06 – Traitement des comptes d'administration locaux (Priorité: 6/10)

- Action à réaliser:
  - Pour chaque ressource du domaine, modifier les mots de passe administrateurs locaux en les rendant uniques et non prédictibles.
  - Enregistrer les mots de passe administrateurs dans un gestionnaire de mots de passe sécurisés et stockés sur une ressource de niveau de criticité égale ou supérieure.
- Ressources:
  - ANSSI Recommandations pour l'administration sécurisée des SI reposant sur AD - R30

# Attaques Kerberoasting

## Vulnérabilités:

- V07: Kerberoasting, service dont le SPN est porté par un compte utilisateur

## Recommandation:

RC07 - Traiter les risques des attaques par Kerberoasting (Priorité: 7/10)

- Action à réaliser:

- Les comptes utilisateurs ayant un Service Principal Name (SPN) déclaré dans l'AD ne doivent pas appartenir au groupe administrateur du domaine ou pouvoir accéder à des ressources de haut niveau de criticité.
- Les comptes utilisateurs ayant un Service Principal Name (SPN) déclaré dans l'AD doivent se voir appliquer une stratégie de mot de passe affinée (Password Settings Object), leur imposant un mot de passe complexe, avec une longueur supérieure à 32 caractères.

- Ressources:

- ANSSI Recommandations pour l'administration sécurisée des SI reposant sur AD – R69 - R70

# Délégations Kerberos

## *Vulnérabilités:*

- V12: Service en délégation non contrainte

## *Recommandation:*

RC08 - Traiter les risques inhérents aux délégations Kerberos (Priorité: 8/10)

- Action à réaliser:
  - Resserve les délégations non contraintes exclusivement à des ressources de niveau de criticité haute (et idéalement, à des contrôleurs de domaine uniquement).
  - Interdire la délégation Kerberos des comptes d'administration (a minima des comptes d'administration du domaine) en leur donnant l'appartenance au groupe de sécurité des utilisateurs protégés, soit en activant l'attribut « NOT\_DELEGATED ».
- Ressources:
  - ANSSI Recommandations pour l'administration sécurisée des SI reposant sur AD – R65

# Attaques sur NTLM

*Vulnérabilités:*

- V01: PetitPotam

*Recommandation:*

RC09 - Traiter les des attaques sur NTLM (Priorité: 9/10)

- Action à réaliser:

- Interdire l'authentification NTLM pour les comptes appartenant aux groupes de sécurité de plus haut niveau de criticité, en leur donnant l'appartenance au groupe de sécurité des utilisateurs protégés.
- Étendre si possible cette recommandation à tous les comptes d'administration de plus faible niveau de criticité.

- Ressources:

- ANSSI Recommandations pour l'administration sécurisée des SI reposant sur AD – R71
- Microsoft - KB5005413 - Usage de PetitPotam pour la vulnérabilité AD CS

# Recommandations long terme

# Recommandation long terme:

- RL01 - Cloisonnement de l'annuaire AD et du SI
  - Mettre en œuvre un modèle de gestion des accès privilégiés, en définissant des zones de confiances reposants sur leurs niveaux d'exposition ou de criticité, afin d'y d'appliquer une gestion des privilèges adaptée.
  - ANSSI Recommandations pour l'administration sécurisée des SI reposant sur AD - §2
- RL02 - Renouveler automatiquement les mots de passe des comptes d'administration locaux
  - Mettre en œuvre la solution LAPS 22 intégrée à l'AD, afin de gérer de manière sécurisée la diversification et le renouvellement automatique des mots de passe des comptes administrateurs locaux de toutes les ressources intégrées à l'AD.
  - ANSSI Recommandations pour l'administration sécurisée des SI reposant sur AD - R30

# Recommandation long terme:

- RL03 – Sécuriser les connexions à des ressources de moindre confiance
  - Mettre en œuvre une solution technique et imposer l'utilisation de l'option 'restricted admin' pour toutes les connexions RDP vers des ressources de même ou moindre niveau de confiance depuis des postes d'administration.
  - Mettre en œuvre et configurer les paramètres de sécurité Windows permettant de restreindre les ouvertures de session des comptes d'administration sur des ressources de moindre niveau de confiance.
  - ANSSI Recommandations pour l'administration sécurisée des SI reposant sur AD - R64
- RL04 – Authentification multifacteur
  - Mettre en œuvre une solution d'authentification multifacteur pour les comptes d'administration.
  - ANSSI Guide authentification multifacteur et mots de passe

# Livrables:

- Rapport de pentest:

**RAPPORT DE PENTEST**

 Clinique  
de Frontignan

Client: Clinique de Frontignan  
Auditeur : S.Perfetti

**Table Des Matières**

1 Contexte Et Périmètre.....	3
2 Méthodologie.....	3
3 Résumé des vulnérabilités.....	3
4 Logigramme du pentest.....	4
5 Déroulé Du Pentest.....	5

- Plan d'action:

**PLAN D'ACTION**

 Clinique  
de Frontignan

Client: Clinique de Frontignan  
Auditeur : S.Perfetti

**Table Des Matières**

1 Contexte.....	3
2 Définitions.....	3
3 Plan d'action à court terme.....	4
3.1 RCQ1 - Mettez en place une politique de mot de passe forte.....	4
3.2 RCQ2 - Mécanisme de contrôle de la robustesse des mots de passes.....	5
3.3 RCQ3 - Maîtriser la dissémination de toute forme de secret d'authentification réutilisable.....	5

# Questions / Réponses

# Voies d'améliorations :